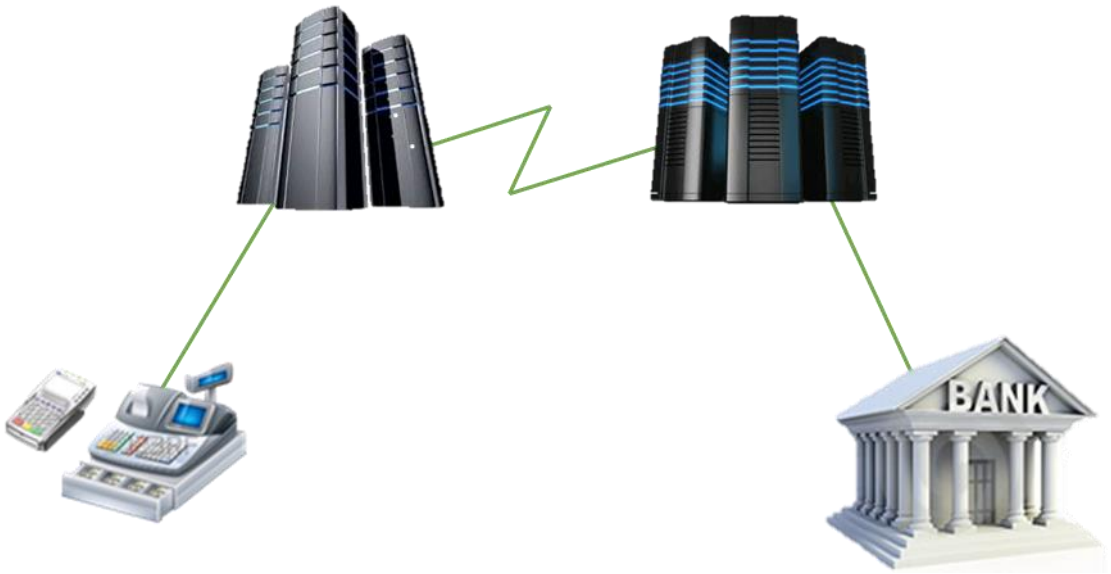
Manual de Especificaciones
Host to Host
Transbank <-> Comercio

Versión 2.2
(Enero 2021)



Control de versiones

NÚMERO DE VERSIÓN	FECHA	AUTOR	DESCRIPCIÓN DE CAMBIOS
1.0	18/06/2012	Rodrigo León	Versión inicial
1.1	22/11/2012	Rodrigo León	Elimina referencias a reversas FC Inclusión de la posibilidad de reversar una transacción por problemas en el punto de venta. Modificación de flujos por traslado del ingreso de los 4 últimos dígitos desde el pinpad hacia la caja Modificación de flujos detallando por separado la lectura de la tarjeta y la solicitud de transacción (aplica en venta y anulación) Ajuste del *timeout* en el punto de venta a 20 segundos en caso de no respuesta de la transacción Aclaración de descripción parámetro del submódulo de caja (POS) para el parámetro multicódigo Eliminación de parámetros de caja que ahora son controlados por el PINPAD (Montos mínimos de compra, flag de validación 4 últimos dígitos) Eliminación de parámetros que no aplican en la nueva arquitectura de PINPAD (Marcas aceptadas, encabezado del comprobante, pie de página)
1.2	03/12/2012	Rodrigo León	Inclusión de la glosa de ahorro en el pie de página de la copia de cliente del voucher.
1.3	14/12/2012	Rodrigo León	Modificación de la glosa fija de transacción con ahorro por una glosa variable de la respuesta del requerimiento de venta.
1.4	04/01/2013	Rodrigo León	Corrección orden glosas del voucher "EMPLEADO" y "NUMERO DE BOLETA" y normalización de glosa "NUMERO DE TARJETA" en lugar de "TARJETA CRÉDITO" y "TARJETA DEBITO" y fusión de las líneas vuelto, donación y propina para el caso de voucher débito. Corrección de glosa de despliegue en el PINPAD y punto de venta en la lectura de la tarjeta
1.5	21/06/2013	Rodrigo León	Ajustes de glosas, numeración y títulos Corrección de voucher de anulación Actualización alternativa de conexión *Host to Host*
1.6	27/08/2013	Rodrigo León	Corrección diagrama de flujo de anulación
1.7	14/08/2014	Elias Brehme	Se corrige formato en general de los voucher. En particular se explicita las validaciones y modo de impresión de monto de cuota y glosa tipo de cuota. Se incorpora voucher de dólar
1.8	03/02/2016	Elias Brehme	Se elimina de los encabezados venta "con pin" Se reducen las glosas de pie de pagina
1.9	01/01/2017	Elias Brehme	Se elimina textos desactualizados o contenidos en otros manuales.
1.9	18/06/2018	Christian Cobo	El presente documento es una versión beta; está en revisión.
1.91	28/09/2018	Christian Cobo	1.8.4.2 Transacciones de administración de red Echo Test (Handshake). (**Página 48)** Se incorpora recomendaciones para el uso del comando de "Echo Test"
1.92	25/10/2018	Christian Cobo	Se incorpora recomendaciones para el aplicativo de Caja del Comercio
2.0	28/10/2019	Christian Cobo	Se actualiza documento con instrucciones para usar Multicódigo. (**Páginas 15-16-17)**
2.1	28/07/2020	Christian Cobo	Se actualiza documento con el comando de Handshake y ejemplo. **(Página 53)**
2.2	29/01/2021	Rodrigo León	Ajuste del *timeout* en el punto de venta nuevamente a 30 segundos en caso de no respuesta de la transacción (modificación a versión 1.1). Corrección tipo dato del *timeout* interacción con el pinpad – 9(03)

Control de versiones 2
1 DESCRIPCIÓN DEL SISTEMA HOST TO HOST 7
1.1 INTRODUCCIÓN 7
1.2 OTROS MANUALES 7
1.3 DIAGRAMA DE CONFIGURACIÓN HOST TO HOST PARA VENTAS PRESENCIALES 8
1.4 DIAGRAMA GENERAL DE CONFIGURACIÓN HOST TO HOST A NIVEL APLICATIVO 10
1.5 CONSIDERACIONES GENERALES 11
1.5.1 Consideraciones a la utilización de cajas host autoservicio 11
1.6 SOFTWARE DE CONECTIVIDAD TRANSBANK 13
1.6.1 Descripción general 13
1.6.2 Definiciones generales 13
1.6.3 Seguridad de la información 14
1.6.3.1 Confidencialidad de la información. 14
1.6.3.2 Seguridad en la red. 14
1.6.3.3 Seguridad para tarjeta de Débito/Crédito 14
1.6.3.4 Manejo del número secreto (PIN) 14
1.6.3.4.1 Interacción con Dispositivo de Seguridad (PINPAD) 15
1.6.3.4.2 Manejo de llaves de encriptación 15
1.6.3.5 Encriptación de Mensajes. 15
1.6.3.6 Integridad de la información 15
1.6.4 Validaciones generales 16
1.6.4.1 Lectura y Validación de las Tarjetas. 16
1.6.4.2 Ingreso manual del número de tarjeta. 16
1.6.4.3 Validación del número de tarjeta (Transacción sin PIN) 16
1.6.5 Multicódigo (Código de comercio prestador) 16
1.6.6 Ventas en Moneda Dólar (Bimoneda) 17
1.6.7 Tipos de tarjetas soportadas 18
1.6.8 Tipos de Transacciones Soportadas. 18
1.7 SUBMÓDULO DE CAJA (POS) 20
1.7.1 Consideraciones generales 20
1.7.1.1 Interfaz con Aplicación del punto de venta. 20
1.7.1.2 *Time Out* de la aplicación del punto de venta. 20
1.7.2 Número Único de Transacción. 20
1.7.3 Transacciones de Venta y Anulación. 21
1.7.3.1 Venta en Cuotas 21
1.7.3.2 Anulación de Ventas. 21
1.7.3.3 Número y Tipo de Cuotas. 23
1.7.4 Promociones en Línea 23
1.7.5 Parámetros del Submódulo de caja (POS). 24
1.7.5.1 Tabla de tarjetas 27
1.7.5.1.1 Tarjetas Bancarias 27
1.7.5.1.2 Tarjetas No Bancarias 27
1.7.6 Funcionalidades Soportadas 27
1.7.6.1 Transacciones Financieras 27
1.7.6.2 Transacciones Administrativas 28
1.7.7 Funcionalidades del punto de venta bajo modalidad CON CONSULTA DE cuotas 29
1.7.7.1 Menú único 31
1.7.7.1.1 Inteligencia definida 31
1.7.7.2 Valor Cuota en el punto de venta 31
1.7.7.3 Productos sin interés en los puntos de venta 31
1.7.7.4 Transacción de consulta en las transacciones financieras 32
1.7.8 Transacciones financieras con Tarjetas de Crédito 33
1.7.8.1 Venta Normal. 33
1.7.8.1.1 Venta normal bajo modalidad nuevas cuotas 33
1.7.8.2 Venta en cuotas normales. 34
1.7.8.2.1 Venta en cuotas normales bajo modalidad nuevas cuotas 34
1.7.8.3 Venta en 2 Cuotas sin Interés (2CSI) 35
1.7.8.3.1 En el Voucher de Venta y Anulación 35
1.7.8.3.2 Valor Cuota Sin Intereses. 35
1.7.8.4 Venta en 3 Cuotas sin Interés (3CSI) 36
1.7.8.4.1 En el Voucher de Venta y Anulación 36
1.7.8.4.2 Valor Cuota Sin Intereses. 36
1.7.8.5 Venta en N-Cuotas (Cuotas Comercio con abono mensual) 36
1.7.8.5.1 Venta en cuotas bajo modalidad SPDH 3.1 36
1.7.8.5.2 Venta en N-Cuotas bajo modalidad Nuevas Cuotas 37
1.7.8.6 Venta en Cuotas Iguales y Conocidas con Interés (CIC Reload) 38
1.7.8.7 Promociones bajo modalidad Nuevas Cuotas 38
1.7.8.7.1 Promociones emisoras administradas por Transbank 39
1.7.8.7.2 Promociones comercio 39
1.7.8.8 PIN en Crédito 39

1.7.9 Transacciones financieras con tarjeta de débito ... 39
1.7.9.1 Transacciones con Tarjeta de Débito - Venta Débito. ... 40
1.7.9.2 Transacciones con Tarjeta de Débito - Venta Débito con Vuelto. ... 40
1.7.9.2.1 Operación en el Punto de Venta. ... 40
1.7.9.2.2 Transacciones de anulación ... 40
1.7.10 Transacciones administrativas ... 41
1.7.10.1 Carga de Llaves ... 41
1.7.10.2 Cierre Batch ... 41
1.8 SUBMÓDULO DE HOST DE COMERCIO ... 42
1.8.1 Objetivo ... 42
1.8.2 Consideraciones Generales. ... 42
1.8.2.1 Habilitación de Conexiones a Transbank. ... 42
1.8.2.1.1 Especificaciones Técnicas de la Conexión. ... 42
1.8.2.1.2 Proveedores de enlace validados por Transbank - Servicio Host. ... 42
1.8.2.2 Alternativa de Conexión *Host to Host* ... 43
1.8.2.3 Servicio FTP ... 43
1.8.2.4 Monitoreo Enlace ... 44
1.8.2.5 Protocolos de Comunicación. ... 44
1.8.2.6 Características de la Conexión TCP/IP. ... 44
1.8.3 Consideraciones Generales. ... 45
1.8.3.1 Características Exigidas a la Red de Comunicaciones del Comercio ... 45
1.8.3.1.1 Control de Acceso del Software de Caja ... 45
1.8.3.1.2 Seguridad TLS 1.2 ... 46
1.8.3.1.3 Seguridad en la Red WI-FI del Comercio ... 46
1.8.3.2 Formato de Mensajes ... 47
1.8.3.3 TPDU ... 47
1.8.3.4 *Header* ... 47
1.8.3.5 Campos Adicionales ... 48
1.8.4 Funcionalidades Soportadas ... 48
1.8.4.1 Transacciones de reversa ... 48
1.8.4.2 Transacciones de administración de red ... 49
1.8.4.3 Flujo de los Mensajes. ... 49
1.8.4.3.1 Transacción Normal. ... 50
1.8.4.3.2 Transacción con Reversa por timeout de la Caja. ... 51
1.8.4.3.3 Transacción con Data Incorrecta. ... 52
1.8.4.3.4 Transacción con Formato Erróneo. ... 52
1.8.4.3.5 Transacción Administración de red - Echo Test – Handshake ... 53
1.8.4.4 Tratamiento de Mensajes en el Host del Comercio. ... 54
1.8.4.4.1 Respuesta de Transacciones de Administración de Red ... 54
1.8.4.4.2 Mensaje de Reversa ... 54
1.8.4.4.3 Parámetros de Comunicación ... 54
2 CRITERIOS PARA LA GENERACIÓN DE REVERSAS ... 55
3 INTERACCIÓN CON EL PINPAD ... 55
3.1 Mensajes/acciones entre caja/PINPAD ... 55
3.1.1 Transacción con tarjeta de Débito ... 55
3.1.2 Transacción con tarjeta de Crédito nacional/internacional sin PIN ... 56
3.1.3 Transacción con tarjeta de Crédito nacional con PIN ... 57
3.1.4 Transacción con tarjeta de Crédito nacional con PIN venta bajo modalidad Nuevas Cuotas 58
4 FLUJO DE TRANSACCIONES ... 59
4.1 Transacción de venta con tarjeta de crédito sin Interés (NCuotas – 3CSI, 2CSI) ... 59
4.2 Transacción de venta con Interés (aplicable para CIC, CICR, Venta Normal) ... 60
4.3 Consulta de valor cuota ... 60
4.4 Anulación de transacciones ... 61
4.5 Transacción de débito ... 61
4.6 Impresión de voucher ... 62
4.7 Reversa FT ... 62
5 CONSIDERACIONES PARA EVALUACIÓN DE SOLUCIONES ... 63
5.1 Impresión de Comprobantes ... 63
5.2 Aplicación de Caja ... 63
5.3 Mensaje de Requerimiento. ... 63
5.4 Administración de las comunicaciones ... 63
5.5 Pruebas PINPAD ... 64
6 PA-DSS (NORMAS DE SEGURIDAD DE DATOS PARA LAS APLICACIONES DE PAGO) ... 65
6.1 Control de versiones ... 66
6.2 Introducción ... 67
6.2.1 Finalidad de este documento ... 67
6.2.2 Relación entre PCI DSS y PA-DSS ... 67
6.2.3 Alcance de las PA-DSS ... 67

6.3 Aplicabilidad de las PA-DSS a las terminales de hardware 69
6.4 Funciones y responsabilidades 70
6.4.1 Marcas de pago 70
6.4.2 Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC) 70
6.4.3 Proveedores de software 71
6.4.4 PA-QSA 71
6.4.5 Revendedores e integradores 71
6.4.6 Clientes 72
7 Guía de Implementación de las PA-DSS 73
7.1 Requisitos del Asesor de Seguridad Certificado para las Aplicaciones de Pago (PA-QSA) 73
7.2 Laboratorio de pruebas 73
7.3 Información sobre la aplicabilidad de las DSS de la PCI 73
7.4 Instrucciones y contenido para el informe de validación 75
7.5 Pasos de conclusión de las PA-DSS 76
7.6 Guía del programa PA-DSS 78
7.7 Requisitos y Procedimientos de Evaluación de Seguridad de de las PCI DSS 78
7.8 Anexo A: Resumen de contenidos para la Guía de implementación de las PA-DSS 90

CONFIDENCIALIDAD

La información contenida en este documento es propiedad de Transbank y sólo puede ser utilizado por quienes Transbank autorice expresamente y para los fines que son descritos en éste.

1 DESCRIPCIÓN DEL SISTEMA HOST TO HOST

1.1 INTRODUCCIÓN

Mediante una conexión del tipo *Host to Host*, un establecimiento comercial que posee su propia red de concentradores con terminales de puntos de venta como cajas registradoras puede conectar su sistema a través de un *Host* (*Host* comercio) que reciba desde los diferentes puntos de ventas las transacciones y sean enviadas al sistema de Transbank (*Host* Transbank), con el objeto de autorizar y capturar en línea las transacciones con tarjeta de crédito y tarjeta de débito.

1.2 OTROS MANUALES

Este manual se construyó en base o en conjunto con los siguientes manuales:

Para todos los comercios:

1. Manual De Comandos Pinpad Host
2. Manual De Especificaciones Host
3. Manual De Voucher Host
4. Manual De Operaciones Host
5. Manual De Archivos De Cuadraturas

Internos de TBK:

6. Manual De Mensajería SPDH Host
7. Manual De Diseño Construcción De Pinpad Host

Comercios Onus:

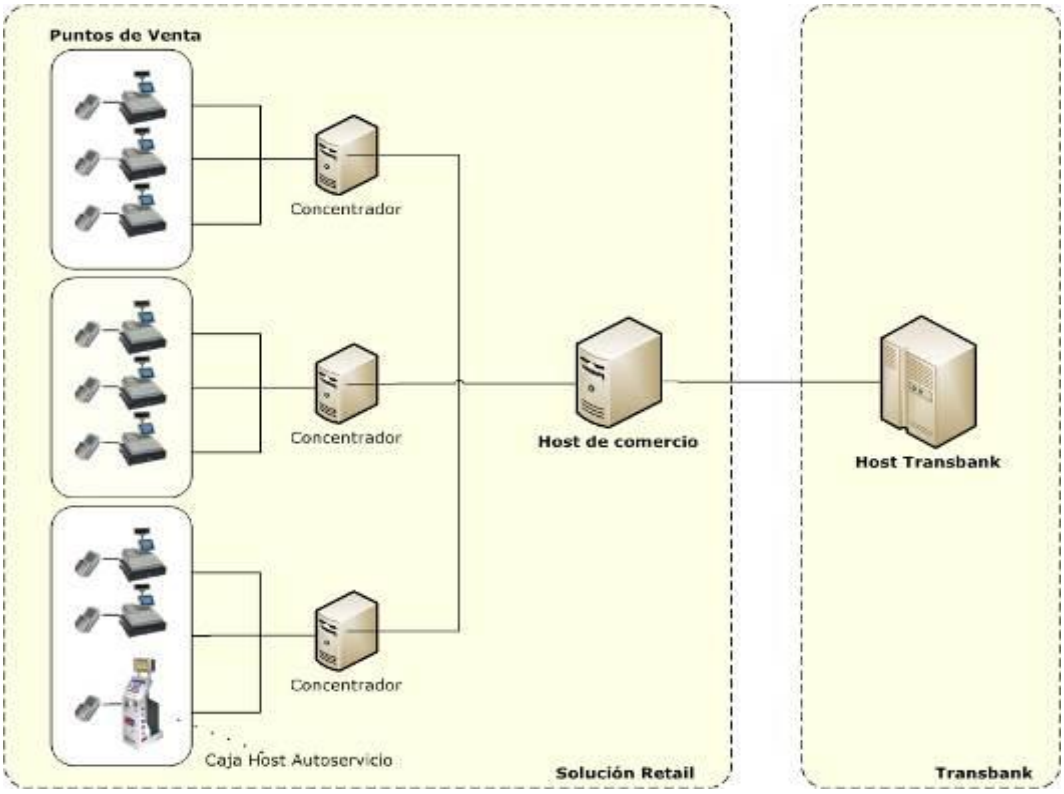
8. Manual de comandos ONUS pinpad HOST
9. Manual de Especificaciones ONUS HOST

Comercios Autoservicio:

10. Manual de Especificaciones HOST autoservicio ux300

1.3 DIAGRAMA DE CONFIGURACIÓN HOST TO HOST PARA VENTAS PRESENCIALES.

El diagrama siguiente muestra un esquema general de este tipo de conexión:



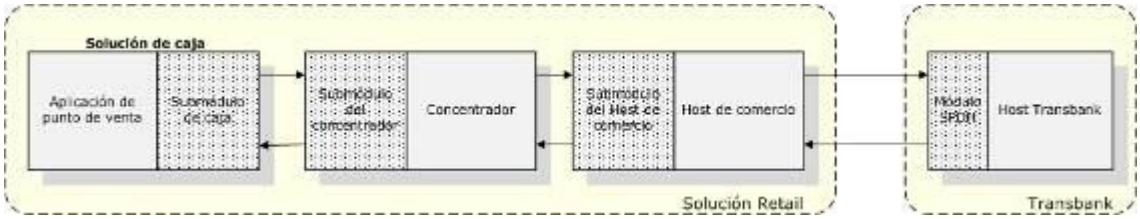
La descripción de cada uno de los elementos se indica a continuación:

ELEMENTO	DESCRIPCIÓN
Host de Transbank	Corresponde al servidor de Transbank donde reside la aplicación que permite autorizar y capturar transacciones con tarjetas de crédito y débito (módulo SPDH)
Host de Comercio	Corresponde al servidor del comercio donde reside la aplicación que permite conectarse con el *Host* de Transbank para autorizar y capturar transacciones con tarjetas de crédito y débito. Es el encargado de administrar la red de concentradores y puntos de ventas (POS) del comercio.
Concentrador	Dispositivo que permite administrar un grupo de terminales, formatea y envía las transacciones de estos hacia y desde el *Host* del comercio. En algunas configuraciones es posible que la figura del concentrador no aparezca y sólo se vea una red de POS conectados directamente al *Host* central del comercio.

Punto de venta (POS)	Dispositivo donde reside una aplicación, conocida como aplicación de caja, ejecutándose y que permite realizar las transacciones en el comercio. Puede ser una caja registradora o un PC. Desde el punto de vista del software de conectividad con Transbank, el POS debe tener una identificación única dentro de la red del comercio, para ello se le debe asignar un *Terminal ID* proporcionado por Transbank. En el diagrama anterior se presenta un POS definido como "caja *host* autoservicio". Este punto de venta corresponde a una caja *host* con las mismas características de los puntos de venta atendidos por operadores del comercio, con las excepciones propias de una caja auto atendida, donde es el mismo tarjeta habiente quien realiza la operatoria del punto de venta. Cada una de estas excepciones son consideradas y detalladas en capítulos posteriores de este documento
Dispositivo de seguridad (PINPAD)	Corresponde a un dispositivo proporcionado por Transbank, que se conecta al POS del comercio, el cual es utilizado para ingresar los datos del medio de pago utilizado por el cliente. Este dispositivo tiene las siguientes características: ▪ Está protegido contra intervenciones externas. ▪ Destrucción de la información ante la apertura. ▪ No modificable su operación mediante programación o por otros medios. ▪ No permite memory dumps. ▪ No es posible obtener PIN's, llaves u otros datos secretos contenidos en él. ▪ Tiene lector de banda magnética (*Track* I y II). ▪ Tiene lector de chip EMV compatible, con y sin contacto (de acuerdo al modelo). ▪ Tiene antena para lectura *Contactless* (de acuerdo al modelo) ▪ Resuelve las transacciones de venta (incluyendo las reversas correspondientes) de forma autónoma, entregando la mensajería a la caja para el envío a Transbank. ▪ Valida la respuesta de los requerimientos aplicando las actualizaciones de parámetros que correspondan.

1.4 DIAGRAMA GENERAL DE CONFIGURACIÓN HOST TO HOST A NIVEL APLICATIVO

El diagrama siguiente muestra un esquema general desde el punto de vista aplicativo.



Desde el punto de vista de aplicaciones es posible distinguir los siguientes componentes:

ELEMENTO	DESCRIPCIÓN
Aplicación de punto de venta	Corresponde a la aplicación utilizada por el comercio para realizar la función propia de la caja; es decir, la gestión de venta de productos. Es aquí en donde se inicia toda transacción. Usualmente el cuerpo principal de esta aplicación reside en la caja misma, pudiendo existir elementos funcionales residentes además en el concentrador de local o también en algún *host* central. En caso de que la aplicación del comercio requiera realizar una transacción con tarjetas de crédito o débito administradas por Transbank, la aplicación del comercio debe interactuar con el componente denominado "Software de Conectividad Transbank", descrito en este documento.
Software de conectividad Transbank	Corresponde a un conjunto de módulos que en su conjunto permiten a una aplicación de comercio realizar transacciones de pago con tarjetas de crédito o débito. El Software de Conectividad Transbank usualmente se estructura en los siguientes Submódulos: ▪ Submódulo de caja (POS). ▪ Submódulo del concentrador. ▪ Submódulo del *Host* de Comercio.

1.5 CONSIDERACIONES GENERALES

ES FULL ON-LINE:
No se contempla operar con transacciones que no sea atendidas/resueltas por el *Host* de Transbank. Por lo tanto el *Host* Comercio **NO** tiene la facultad de atender/resolver transacciones en forma autónoma.

REQUIERE PRESENCIA DE TARJETA:
El ingreso del número de tarjeta es solo vía presencia de la tarjeta (vía lecturas de banda magnética o chip, con y sin contacto).

Para efectos del ingreso de datos por parte del cliente (captura de información de la tarjeta, confirmación del monto, selección de cuotas, ingreso de PIN) la solución contempla conectar al POS, un dispositivo seguro (PINPAD) proporcionado por Transbank el cual tiene las siguientes características:

1. Lector de banda magnética
2. Lector de tarjetas Chip EMV compatible, con y sin contacto
3. Algoritmo de encriptación DES y 3DES
4. Acepta ingreso y encriptación de PIN
5. Administración de llaves dinámicas vía el método **DUKPT**.

Si el servicio y/o conexión entre el *host* del comercio y el *host* de Transbank no se encontrase disponible, el comercio debe almacenar las transacciones no resueltas y/o en curso como reversas pendientes (máximo una por cada punto de venta) para enviar a Transbank. Una vez re-establecido y normalizado el servicio deberá proceder al envío de estas transacciones al *host* de Transbank.

En caso de no haber comunicación con el Host de Transbank, no se podrá operar con el producto tarjeta de Crédito y Débito[1], pero el punto de venta debe poder seguir cursando transacciones con un medio de pago distinto.

1.5.1 Consideraciones a la utilización de cajas host autoservicio

La caja *host* autoservicio considera la implementación de un *host retail* estándar donde existan cajas atendidas por operadores/cajeros y cajas en las que sea el mismo cliente quien realiza la operación, tal como lo hace actualmente un operador/cajero. La implementación de una caja *host* autoservicio considera lo siguiente:

TÓPICO	CONSIDERACIÓN
Validación del número de tarjeta (Transacción sin PIN)	Las cajas *host* de autoservicio **NO operan con tarjetas sin PIN**, lo anterior implica que la aplicación de caja **debe rechazar** el intento de operación con estas tarjetas.
Anulación de ventas	Las cajas *host* de autoservicio **NO** consideran la transacción de anulación como una operación en el punto de venta, sino que como un proceso administrativo a realizar por el comercio, por lo que **NO** debe implementarse en el punto de venta.

[1] Se espera que la solución de comunicaciones del comercio provea un *uptime* superior a 99,8 %. Esto se logra con redundancia de los enlaces de comunicaciones.

Impresión y reimpresión (duplicado) de comprobantes	La impresión de voucher en cajas *host* autoservicio **NO** debe considerar la reimpresión de estos en el punto de venta, así como la impresión de la copia para el comercio. Es responsabilidad de este último la consideración de respaldo del voucher de comercio, así como de la entrega de una reimpresión en caso de solicitud por parte del tarjeta habiente. De esta forma, la caja *host* autoservicio debe imprimir **SÓLO** la copia cliente del voucher, así como sus vouchers de premio si corresponde.
Control de impresión	La caja *host* autoservicio **debe mantener el control de la disponibilidad** de papel e imposibilitar al tarjeta habiente de realizar una transacción de venta si el remanente de papel no es suficiente para imprimir el (los) vouchers de la transacción en forma completa o si existe indisponibilidad del mismo.
Transacciones administrativas	El gatillado de transacciones administrativas propias del punto de venta (carga de llaves, cierre batch) deben realizarse en forma automática bajo esta modalidad, o a través de un proceso definido y validado por Transbank.
Voucher PEL	Se deben imprimir los voucher de PEL según normas de PEL Como en pel y en autorservicio no se permite imprimir duplicado de voucher pel
Mensajes en pantalla de caja	Caja debe considerar mensajes informativos al cliente Acontinuacion se detallan

Mensajes a mostrar en pantalla de caja autoservicio:

1)
Caja inicia transacción y pinpad le informa que la transacción es sin pin y debe ingresar 4ud de la tarjeta.
Como caja es autoservicio, la caja es quien aborta transacción y muestra en pantalla:

ESTA UTILIZANDO UNA TARJETA QUE NO TIENE HABILITADA SU CLAVE

POR FAVOR REINTENTE CON OTRA TARJETA

2)
Al recibir la caja una transacción terminal aprobada, que indica que debe imprimir voucher con firma:
Caja debe cursar reversa de esta transacción (no permitir venta mientras esta reversa no se concrete) y además mostrar en pantalla:

NO SE PUDO VALIDAR LA CLAVE, SU TRANSACCIÓN SERÁ ANULADA

POR FAVOR REINTENTE NUEVAMENTE O UTILIZE OTRA TARJETA

1.6 SOFTWARE DE CONECTIVIDAD TRANSBANK

1.6.1 Descripción general

El Software de Conectividad Transbank (SCT) hace referencia al conjunto de módulos que en conjunto permiten a una aplicación de comercio (POS) realizar transacciones de pago con tarjetas de crédito o débito. Dentro del SCT, en forma usual es posible encontrar los siguientes Submódulos:

- **Submódulo de caja (POS)**: Residente en la caja misma y sus funciones principales son:
  - Administración y mantención de la interacción con la aplicación del comercio.
  - Administración y mantención de la interacción con el cajero y con el tarjeta-habiente a efectos de concretar el pago.
  - Utilización y administración del dispositivo de seguridad con el fin de solicitar las operaciones de venta y anulación, validación de respuestas de requerimientos y actualización de parámetros locales (Referencia: `Manual de comandos pinpad Host to Host TRANSBANK - Comercio bajo protocolo SPDH 4.0`).
  - Administración y mantención de la comunicación con Transbank a través de los Submódulos de concentrador y *host* de comercio.

- **Submódulo del concentrador**: Residente en el concentrador de sucursal. Su función es concentrar la comunicación entre el *host* de comercio y las cajas.

- **Submódulo del host de comercio**: Residente en el *host* central del comercio. Su función es comunicarse con los concentradores (o las cajas en caso de existir Submódulo de concentrador) y al mismo tiempo con el host central de Transbank. Dado esto, sólo este módulo requiere implementar el protocolo de mensajería SPDH propio de Transbank para el envío y recepción de transacciones. Hacia el lado del comercio, la solución de conectividad puede utilizar cualquier protocolo que cumpla los requerimientos planteados en este documento.

1.6.2 Definiciones generales

- ***Terminal ID*** **(Dirección lógica)**:

  Corresponde al identificador lógico único asignado por Transbank para cada punto de venta de la red del comercio. Dentro de sus características es posible mencionar:

  - Este identificador debe viajar en todo mensaje que es enviado al *host* de Transbank (y devuelto en el mensaje de respuesta).
  - De estar asignado a un punto de venta no debe repetirse en otro.
  - No debe contener valores nulos.
  - Es generado por Transbank y es un parámetro del punto de venta.
  - El comercio debe mantener en el servidor un mapeo de la asignación de *Terminal ID* por local y su punto de venta correspondiente.
  - El comercio no puede crear nuevos *Terminal ID*, en caso de requerir adicionales para habilitar nuevos puntos de ventas deben ser solicitados al área de operaciones de Transbank, específicamente al ejecutivo de servicios asignado.

- Si el *host* de Transbank recibe un requerimiento con un *Terminal ID* desconocido, replicará el requerimiento recibido indicando que el *Terminal ID* no es válido a través del código de respuesta.
- También se asigna un *Terminal Id* para el *host* del comercio para que envíe mensajes de Echo Test[2] al *host* de Transbank.

- **Código de comercio (*Retailer ID*)**:

  Al igual que en el *Terminal ID*, el software autorizador en el *host* de Transbank requiere que a cada punto de venta dentro de la red de ese comercio le sea asignado un identificador de comercio el cual se llamará ID de comercio y generalmente es uno por local. Esto quiere decir que cada uno de los puntos de venta de ese local les será asignado el mismo código de comercio.

1.6.3 Seguridad de la información

1.6.3.1 Confidencialidad de la información.

De acuerdo a las normativas vigentes, las transacciones con Tarjeta de Crédito y Débito requieren la incorporación de los siguientes elementos de seguridad en el sistema del cliente:

- La información de la tarjeta leída en el punto de venta **NO** debe ser almacenada en ningún sistema computacional. Para efectos de cuadratura e identificación de transacciones, se debe utilizar el número único de transacción, descrito posteriormente en el Submódulo de caja.

- Adicionalmente a los requisitos de encriptación de mensajes, bajo la normativa vigente para operaciones con tarjetas de Débito, exige que la información de los *tracks* (I y II) y PIN *block* (encriptado) que viaja por los sistemas del comercio en este tipo de transacciones **NO** sea almacenado en ninguno de sus componentes (caja, concentrador, *host* de comercio).

1.6.3.2 Seguridad en la red.

La información grabada en la tarjeta (*track* I, *track* II y otras) será leída **sólo** por los dispositivos de seguridad (PINPAD) conectados a las cajas registradoras o puntos de venta. Estos dispositivos procederán a encriptar estos elementos para que esta información no se encuentre disponible.

1.6.3.3 Seguridad para tarjeta de Débito/Crédito

Para garantizar la seguridad y confidencialidad de los datos, exigido por las normativas vigentes para las transacciones con tarjeta de débito, es necesario introducir en la conexión *Host to Host* con Transbank el manejo del número secreto del cliente (PIN) para tarjetas de débito así como para tarjetas de crédito (nacionales).

1.6.3.4 Manejo del número secreto (PIN)

El PIN del cliente debe ser encriptado por hardware desde el inicio de la transacción.

[2] Echo Test: transacción que permite al *host* del comercio comprobar el estado actual de la comunicación con el servidor Transbank (a nivel de aplicación).

Para ello se utiliza el dispositivo de seguridad (PINPAD) conectado al punto de venta, el cual usará el algoritmo Triple DES (3Des) según la norma ANSI X3.92 estándar.

1.6.3.4.1 Interacción con Dispositivo de Seguridad (PINPAD)

En el capítulo "Interacción con el PINPAD" se incluye la forma de interactuar que tendrá el punto de venta con el dispositivo de seguridad (PINPAD), como la lectura y encriptación de la tarjeta, la captura del PIN, devolución de cuatro últimos dígitos.

Para poder interactuar con el PINPAD, existe un manual técnico adicional (Referencia: `Manual de comandos pinpad Host to Host TRANSBANK - Comercio bajo protocolo SPDH 4.0`).

1.6.3.4.2 Manejo de llaves de encriptación

Dado que la solución incorpora la encriptación de PIN (número secreto para tarjetas de débito y crédito) y generación de MAC (Autenticación de mensajes) los cuales utilizan algoritmos de encriptación DES, se hace necesario tener un manejo de llaves. Transbank utiliza el modelo de "Llave única derivada por transacción" o DUKPT por sus iniciales en inglés para el PIN y *master key/working key* para MAC, lo cual significa que tanto en el PINPAD como en el *host* de Transbank se inyectan inicialmente *master keys* (para calcular MAC) y con ellas se hace intercambio de *working keys*, que son las llaves a utilizar para calcular MAC.

Para efectos del intercambio de *working key*, se dispone de tres tipos de transacciones, el Cierre *batch*, la Carga de llaves y las ventas con tarjeta de crédito y débito. Mediante estas transacciones el *host* de Transbank genera nuevas *working key* (MAC) y las envía en el mensaje de respuesta.

1.6.3.5 Encriptación de Mensajes.

Para asegurar la confidencialidad de la información, los mensajes de las transacciones o al menos los datos sensibles deben viajar encriptados en los distintos tramos de la conexión, tanto en el requerimiento como en la respuesta. Como datos sensibles se consideran:

- PIN de la tarjeta
- El número de tarjeta.
- La fecha expiración.
- El número de cuenta del tarjeta habiente.
- El monto de la transacción (dato validado en Autenticación de Mensajes o MAC).

Dentro de los tramos de la conexión se consideran:

- Tramo punto de venta-concentrador-*host* del comercio: En este tramo la información sensible está protegida y encriptada desde el PINPAD.

- Tramo *host* de Comercio – *host* Transbank: En este tramos se utilizan encriptores de línea.

1.6.3.6 Integridad de la información

Para efectos de asegurar la integridad de los mensajes que viajan desde el *host* de Comercio y el *host* Transbank (y viceversa) se introduce el concepto de Autenticación de Mensajes o MAC.

El MAC es un dato que viaja dentro del mensaje (del requerimiento y de la respuesta) y que es validado por el PINPAD. Si la validación falla, significa que algún dato del mensaje fue modificado en el trayecto, por tanto ese mensaje será rechazado generándose una reversa automática desde el PINPAD.

1.6.4 Validaciones generales

1.6.4.1 Lectura y Validación de las Tarjetas.

Toda transacción que requiere lectura de tarjeta debe ser leída a través del PINPAD. De esta forma el PINPAD procederá a la encriptación de la información de la tarjeta para su envío seguro a Transbank.

1.6.4.2 Ingreso manual del número de tarjeta.

La conexión *Host to Host* bajo protocolo SPDH para ventas presenciales, **NO** permite ingreso manual del número de tarjeta, por lo cual **sólo se puede operar con lectura de banda magnética o lectura de chip EMV (con y sin contacto)**.

1.6.4.3 Validación del número de tarjeta (Transacción sin PIN)

Los comercios deben considerar que para cursar transacciones con tarjetas de crédito que no solicitan PIN, el operador del punto de venta deberá ingresar los cuatro últimos dígitos de la tarjeta en la caja. Lo anterior permite la comparación del dato ingresado con los cuatro últimos dígitos entregados por la lectura de la tarjeta. Si la comparación indica que son diferentes, se rechazará por tarjeta inválida.

Se excluyen de esta norma las tarjetas de débito Redcompra, Maestro, Electrón y otras que Transbank defina a futuro.

1.6.5 Multicódigo (Código de comercio prestador)

El concepto Multicódigo es utilizado en la prestación de servicios de pago a terceros, desde un comercio establecido.

Se define como Comercio Responsable al comercio encargado de la generación de la transacción entre un tarjeta habiente y un comercio hacia Transbank, este facilita su aplicación de caja para poder realizar dicha transacción.

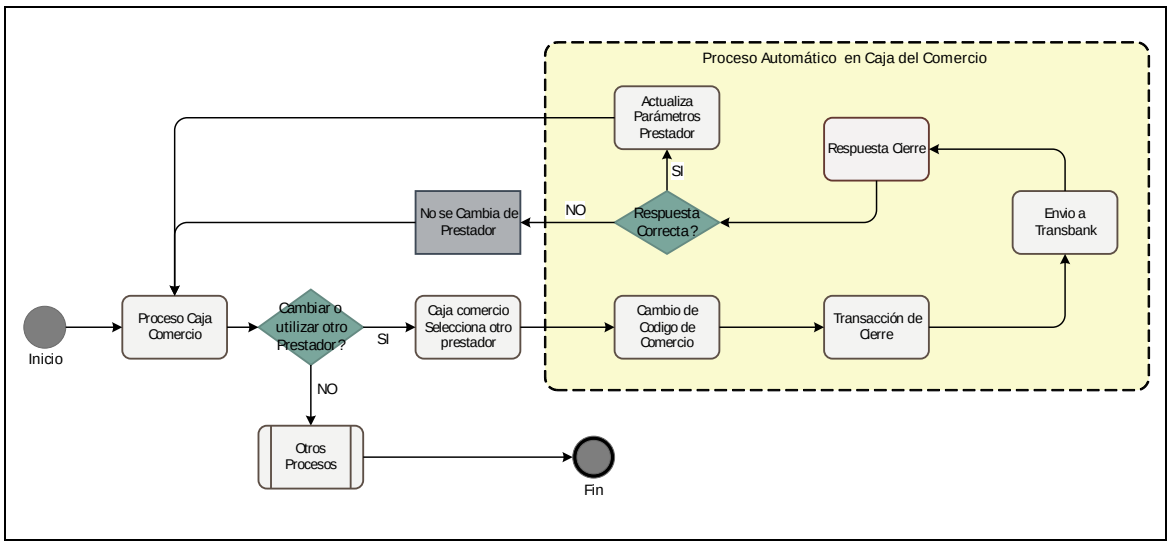
Se define como Comercio Prestador al comercio que, haciendo uso de las funcionalidades que ofrece el comercio responsable, puede ofrecer sus servicios a través de éste y por ende, puede recibir los pagos correspondientes al servicio prestado.

La cantidad de Comercios Prestadores que deberá manejar la aplicación de caja corresponde al número total de comercios para los cuales, el Comercio Responsable, permite el pago de sus servicios. Asimismo, los productos asociados a cada código de comercio deben mantener su correspondencia con el acuerdo comercial correspondiente y la aplicación debe hacerse responsable de mantener esta integridad.

Para el caso de la anulación de una transacción de venta Multicódigo, el *Retailer ID* debe corresponder al Comercio Prestador (a quién se le abonó la transacción) y no del Comercio Responsable.

Es necesario realizar una "transacción de cierre" cada vez que se cambie de "Prestador, con este cierre se actualizarán los productos asociados al prestador.

Para cambiar de "prestador" (Multicódigo) y para "Venta en moneda Extranjera"(Bimoneda) el flujo seria el siguiente:



1.6.6 Ventas en Moneda Dólar (Bimoneda).

Si un Comercio *Host* requiere vender en moneda dólar americano, esté deberá tener un contrato con Transbank que autoriza la venta en Dólares. Transbank asignará un *Terminal ID* para los puntos de venta, así como un código de comercio exclusivo para la venta en esta moneda, los cuales deberán ser utilizados exclusivamente para transacciones en dicha moneda. Para este tipo de transacciones se debe indicar en el mensaje de requerimiento el *Terminal ID* y código de comercio asociado y específico de la moneda.

Al trabajar con dólar la caja por definición es Multicódigo o Multicomercio.
Ver sección 1.6.5 Multicódigo.

La caja debe disponer de un sistema automático para cambio de terminal y comercio, los cuales deben estar pre configurados y realizar un cierre Bach automático al intercambiarlos tal como se explica en la sección Multicódigo.

Podría tener por ejemplo 4 terminales y 4 comercios configurados:

1. Prestador 1 comercio 1 peso
2. Prestador 2 comercio 2 peso
3. Prestador 3 comercio 3 dólar
4. Prestador 4 comercio 4 dólar

A modo de ejemplo:
Al iniciar una venta se debe seleccionar con cuál de estas 4 configuraciones se hará.

Si la venta anterior fue hecha con la misma configuración, no se requiere el cierre, si se realiza una venta con una nueva configuración se debe realizar cierre.

1.6.7 Tipos de tarjetas soportadas

El sistema de Transbank soporta la autorización y captura de transacciones con tarjeta de crédito y tarjeta de débito de las siguientes marcas:

- Tarjetas de crédito bancarias:
  - Visa
  - Mastercard
  - Magna
  - Diners Club
  - American Express

- Tarjetas de crédito NO bancarias
  - **Referencia**: ANEXO NO BANCARIAS MANUAL DE ESPECIFICACIONES TÉCNICAS CONEXIÓN HOST TO HOST

- Tarjetas de débito
  - Débito nacional (Redcompra)
  - Maestro
  - Electrón

La aplicación del punto de venta debe determinar el tipo de tarjeta utilizada en la transacción, de forma tal de decidir cual será el flujo por el cual será procesada (flujo de crédito ó débito).

Las transacciones de crédito podrían requerir el uso de PIN si es que la lectura de la tarjeta así lo indica. Estas transacciones son las denominadas Venta con tarjeta de crédito con pin.

1.6.8 Tipos de Transacciones Soportadas.

Las transacciones soportadas por el sistema de Transbank pueden agruparse en financieras, administrativas y de administración de red. Cada una de las transacciones soportadas son atómicas, esto implica que no pueden enviarse dos transacciones combinadas.

Las transacciones soportadas se dividen en cuatro tipos:

TRANSACCIONES FINANCIERAS	
TRANSACCIÓN	**DESCRIPCIÓN**
Venta con tarjeta de crédito	Esta transacción permite ventas con tarjetas de crédito financieras y no financieras, con y sin cuotas, con y sin propina.
Venta con tarjeta de crédito con PIN	Esta transacción permite ventas de Crédito ingresando pin, con y sin cuotas, con y sin propina.
Venta con tarjeta de débito	Esta transacción permite ventas de Débito ingresando pin, sin cuotas.
Venta con vuelto con tarjeta de débito (CashBack)	Esta transacción permite ventas de Débito con vuelto (Cashback) ingresando PIN, sin cuotas.
Anulación con tarjeta de crédito	Esta transacción permite anulaciones de ventas realizadas sólo con Tarjetas de Crédito.
Anulación con tarjeta de débito	No aplica.

Consulta Valor Cuota	Esta transacción permite obtener el producto que el punto de venta debe aplicar de acuerdo a las condiciones comerciales de la venta así como de las características de la tarjeta deslizada.
Venta con tarjeta de crédito en modalidad no presencial (sin pin)	Esta transacción permite ventas con tarjetas de crédito financieras y no financieras, con y sin cuotas, con y sin propina, en modalidad no presencial, sin presencia del tarjeta habiente y sin el ingreso de PIN ni deslizamiento de tarjeta
Anulación con tarjeta de crédito en modalidad no presencial (sin pin)	Esta transacción permite anulaciones de ventas realizadas sólo con Tarjetas de Crédito, sin presencia del tarjeta habiente.

TRANSACCIONES ADMINISTRATIVAS	
TRANSACCIÓN	**DESCRIPCIÓN**
Carga de llaves	Esta transacción permite al *Host* del comercio requerir y cargar nuevas *working key* desde Transbank.
Cierre Batch	Esta transacción permite al punto de venta intercambiar totales con el *Host* de Transbank. Junto con esto, en esta transacción el *Host* envía en la respuesta un nuevo juego de *working keys* y la información de los códigos de servicio actualizados.

TRANSACCIONES DE REVERSA	
TRANSACCIÓN	**DESCRIPCIÓN**
Reversa por *timeout* de una transacción financiera	Esta transacción permite reversar cualquier tipo de transacción financiera que presente problemas en la respuesta entregada por Transbank frente a un requerimiento.
Reversa por problemas en el punto de venta	Esta transacción permite, como última instancia, reversar una transacción que por problemas del punto de venta no puede ser finalizada, por ejemplo, imposibilidad de imprimir los comprobantes.
Reversa por autenticación de mensajes (MAC) en mensaje de respuesta Transbank	Esta transacción permite reversar cualquier tipo de respuesta enviada por Transbank que presente problemas en la validación de este mensaje.

TRANSACCIONES DE ADMINISTRACIÓN DE RED	
TRANSACCIÓN	**DESCRIPCIÓN**
EchoTest (*Handshake*)	Esta transacción permite al *Host* del comercio comprobar el estado actual de la comunicación con el servidor Transbank (a nivel de aplicación). Debe ser utilizada cuando el comercio desea verificar si el servidor de Transbank está atendiendo sus requerimientos.

1.7 SUBMÓDULO DE CAJA (POS)

El objetivo de éste es interactuar en la captura y validación de la información necesaria para generar las transacciones respectivas hacia el Host de Transbank.

1.7.1 Consideraciones generales

1.7.1.1 Interfaz con Aplicación del punto de venta.

Al momento de realizar una transacción financiera, el comercio debe operar de manera normal dentro de su aplicación de caja hasta el punto en que le solicite al cliente con qué medio de pago se realiza la transacción. Si éste es con tarjeta bancaria, la aplicación de caja del comercio debe indicar claramente la opción de transacción con Transbank, y debe entregar el control al Submódulo de caja, mediante la acción de presionar una tecla, un botón o una opción del menú. Para el caso de transacciones con tarjetas no bancarias, debe diferenciarse en el punto de venta.

Se exige que la interacción entre la aplicación del punto de venta y el Submódulo de caja sea simple, mediante llamados a rutinas que como parámetros intercambian sus datos para realizar la transacción.

1.7.1.2 *Time Out* de la aplicación del punto de venta.

Para las transacciones financieras es necesario que el punto de venta incorpore un *timeout* parametrizable posterior a la entrega del control al PINPAD para la captura de datos de la tarjeta y tarjetahabiente, de forma tal que al finalizar este *timeout*, el aplicativo de caja debe volver al menú de selección de medios de pago. Otra forma de proveer esta funcionalidad es proporcionando una tecla de escape, para poder dar la opción de salir en cualquier instancia de la transacción previo al envío al *Host* de Transbank para su autorización.

1.7.2 Número Único de Transacción.

Para efectos de identificar cada transacción de tipo financiera, se debe generar un identificador único para cada uno de los mensajes que sean enviados al Host de Transbank.

Este identificador tiene las siguientes características:

- Debe ser único para toda la red de este comercio y no debe repetirse por lo menos durante un mes.
- Debe ser informado en los mensajes que viajan al *Host*.
- El comercio debe utilizar este número para realizar la cuadratura de transacciones.
- Cuando se deba anular una transacción de crédito, se debe informar el número único de la transacción de origen en el mensaje que es enviado al Host de Transbank.
- No debe contener valores nulos.

Transbank sugiere la siguiente estructura:
AAAAMMDDHHMMSSLLLCCCXXXXXX
Donde se considera la fecha y hora
LLL es un número del local
CCC es el número de la caja o punto de venta
XXXXXX es un contador

1.7.3 Transacciones de Venta y Anulación.

1.7.3.1 Venta en Cuotas

Las tarjetas de crédito bancarias emitidas en Chile, son las únicas que pueden operar transacciones de ventas con cuotas para la venta con tarjeta de crédito. Las tarjetas de crédito no emitidas en Chile no pueden operar en cuotas.

Cuando se procesa una venta con alguna de las tarjetas de las marcas señaladas anteriormente en terminales que pueden efectuar ventas en cuotas, se debe solicitar el ingreso de la cantidad de cuotas. Una tarjeta de crédito emitida en Chile se determina mediante una verificación visual del nombre del Banco emisor impreso en la parte inferior de la tarjeta.

Por tanto, pueden operar en venta con cuotas, sólo las tarjetas de crédito emitidas en Chile que correspondan a:

- Tarjetas Bancarias
  - Visa
  - Mastercard
  - Magna
  - Diners
  - Amex (American Express)

- Tarjetas No Bancarias (Referencia: Anexo Manual de especificaciones técnicas para tarjetas no bancarias)
  - Presto
  - Cencosud
  - Ripley/Extra
  - CMR

LOS SIGUIENTES PRODUCTOS OPERAN EN CUOTAS Y DEPENDERÁN DE SI EL COMERCIO OPERARÁ O CON LA MODALIDAD NUEVAS CUOTAS, A SABER:

PRODUCTOS QUE OPERAN EN CUOTAS	
COMERCIO BAJO MODALIDAD NUEVAS CUOTAS	**COMERCIO SIN MODALIDAD NUEVAS CUOTAS**
CUOTAS NORMALES	CUOTAS NORMALES
CUOTAS SIN INTERÉS (2CSI, 3CSI, N-CUOTAS)	CUOTAS SIN INTERÉS (3CSI, NCUOTAS)
CUOTAS IGUALES Y CONOCIDAS (CIC, CIC RELOAD)	CUOTAS COMERCIO

PARA EL CASO DE FUNCIONAMIENTO BAJO MODALIDAD NUEVAS CUOTAS EXISTEN CONSIDERACIONES RESPECTO AL MODO EN COMO SE REALIZA LA INTERACCIÓN ENTRE EL TARJETA HABIENTE Y LA SOLUCIÓN DE PUNTO DE VENTA, LAS CUALES SON DETALLADAS EN PUNTOS POSTERIORES DE ESTE DOCUMENTO.

Las tarjetas de Débito, indistintamente de donde fueron emitidas no pueden operar en cuotas.

1.7.3.2 Anulación de Ventas.

Para poder controlar las anulaciones de ventas, se debe implementar un sistema que valide, al momento de efectuar una anulación, que la transacción original fue realizada exitosamente. Para lograr controlar las anulaciones, debe realizarse una consulta a una base de datos o archivo que contenga las transacciones de venta.

Lo anterior, permite confirmar la existencia de una transacción que debe ser anulada, mediante la recuperación de sus datos, por lo cual las anulaciones corresponderán siempre a transacciones realizadas y no existirá inconsistencia, entre la transacción y su anulación. Asimismo, las anulaciones de ventas deberán incluir el "**número único de la transacción**" de la **venta original**.

Para el caso de multicódigo, el código de comercio que debe ser utilizado para realizar éstas debe ser el código de comercio Prestador (el que realizó la venta) y no el del comercio Responsable.

Previo al proceso de anulación deben realizarse las siguientes verificaciones:

- Debe identificarse que la transacción a anular corresponda a la venta.
- No debe permitirse la anulación de una venta que fue reversada; o que no fue exitosa (autorizada por Transbank y finalizada OK)
- No permitir anular más de una vez una transacción.
- En el caso de anulaciones parciales la suma de los montos de éstas no debe exceder el monto total de la venta original a anular.
- Si el comercio utilizará la anulación parcial, puede anular una venta parcialmente en más de una ocasión, pero debe controlar en cada una el saldo pendiente de anulación, no permitiendo en ningún momento que la acumulación de anulaciones sea mayor al monto total de la compra original, para esto debe considerar también las propinas o donaciones, campos que se deben anular consistentemente con la venta original.
- Si el comercio lo deseé puede permitir solo una anulación parcial al igual que ocurre en las anulaciones totales, para este caso debe disponer de otro medio de devolución si se el cliente lo solicitare.
- Aplicación debe controlar que la anulación se permite solo hasta 10 días después de la venta, al día 11 no debe permitir iniciar anulación desde el punto de venta, pudiendo anular a través de un procedimiento alternativo con Transbank (Portal por ejemplo).
- Para todas las anulaciones se debe mantener los campos de donación o propina con sus valores originales.
- Las **anulaciones parciales** sólo pueden efectuarse para las transacciones del tipo:
    - Venta Normal (sin cuotas).
    - Venta en Cuotas Normales

Al momento de anular una transacción se deben solicitar datos que permitan buscar la transacción original, entre las cuales se debe incluir:

- El deslizamiento de la tarjeta de supervisor o un control de acceso a través de la aplicación, para el inicio del proceso de anulación.
- El deslizamiento de la tarjeta con la cual se realizó la transacción original.
- El ingreso del Nº único de transacción o algún mecanismo que permita buscar la transacción original e identificarla como única.
- Validación de que la tarjeta que está realizando la anulación sea la misma que realizó la compra. No es posible anular una transacción con una tarjeta que no haya realizado la venta.
  Para este caso, la caja debe rescatar de sus registros los 4 últimos dígitos de la tarjeta que realizo la venta e informarlos al pinpad, el cual compara con los 4 últimos dígitos de la tarjeta que quiere anular y entrega la aprobación o rechazo a la caja.

Por último, en cualquier caso que escape a esta definición, debe ser informada previamente a Transbank.

1.7.3.3 Número y Tipo de Cuotas.

En la siguiente tabla se muestran los parámetros de cuotas y tipo de cuotas que pueden ser ingresados, según la marca de la tarjeta:

Estos valores deben ser manejados en la aplicación de forma tal que frente a las respuestas de Transbank permitan su habilitación o deshabilitación.

MARCA DE TARJETA (EMITIDA EN CHILE)	TIPO DE CUOTAS SOPORTADAS	RANGO DE CUOTAS
Visa	Cuotas Normales Cuotas Sin Intereses Cuotas Comercio N-Cuotas	<Parámetro desde> 2 a 99 <Parámetro> 2 ó 3 <Parámetro desde> 4 a 36 <Parámetro desde> 4 a 12
Mastercard	Cuotas Normales Cuotas Sin Intereses Cuotas Comercio N-Cuotas	<Parámetro desde> 2 a 99 <Parámetro > 2 ó 3 <Parámetro desde> 4 a 36 <Parámetro desde> 4 a 12
Magna	Cuotas Normales Cuotas Sin Intereses Cuotas Comercio N-Cuotas	<Parámetro desde> 2 a 99 <Parámetro > 2 ó 3 <Parámetro desde> 4 a 36 <Parámetro desde> 4 a 12
American Express	Cuotas Normales Cuotas Sin Intereses Cuotas Comercio N-Cuotas	<Parámetro desde> 2 a 99 <Parámetro > 2 ó 3 <Parámetro desde> 4 a 36 <Parámetro desde> 4 a 12
Diners	Cuotas Normales Cuotas Sin Intereses Cuotas Comercio N-Cuotas	<Parámetro desde> 2 a 99 <Parámetro > 2 ó 3 <Parámetro desde> 4 a 36 <Parámetro desde> 4 a 12
Tarjetas No Bancarias	**Referencia**: Anexo Manual de especificaciones técnicas conexión Host to Host para tarjetas no bancarias	**Referencia**: Anexo Manual de especificaciones técnicas conexión Host to Host para tarjetas no bancarias

Nota*:* Los valores y rangos de cuotas pueden variar de acuerdo a las definiciones comerciales y productos de Transbank y sus emisores. Los cuales deben ser revisados en la definición de cada uno de estos.

En el caso de las **cuotas normales** Transbank valida el número máximo aceptable según el Banco emisor.

EL MANEJO DETALLADO DE LOS TIPOS DE CUOTAS "2 Y 3 CUOTAS SIN INTERÉS" ASÍ COMO PARA "CUOTAS IGUALES Y CONOCIDAS (CIC, CIC-RELOAD)", PERTENECIENTES A LA MODALIDAD DE NUEVAS CUOTAS SE DETALLAN EN CAPÍTULOS POSTERIORES.

1.7.4 Promociones en Línea

La funcionalidad de Promociones en Línea está disponible tanto para las transacciones de Crédito como de Débito. El PINPAD es el encargado de entregar los códigos y glosas correspondientes a la promoción en línea de acuerdo a la validación de la respuesta del requerimiento.

Esta funcionalidad consiste en premiar a clientes, comercios y dependientes a través de un sorteo efectuado en forma instantánea (en línea) mientras se desarrolla una transacción de venta con Tarjeta de Crédito y/o Débito en el punto de venta; en este caso, la aplicación del punto de venta debe "reaccionar" frente a una transacción de respuesta de venta que viene "marcada" como Transacción Premiada y cuyo beneficiario es el usuario de la tarjeta.

Este proceso es manejado a nivel de Transbank y sin impacto al comercio, que implique un desarrollo tecnológico.

Las acciones que debe tomar el punto de venta cuando una transacción sea premiada deben ser:

- Imprimir un vale de premio, adicional a los vales estándares, en el cual se detalle el premio que ganó la transacción, así como la forma y responsable de la entrega del premio antes de imprimir el voucher de la venta

- Para la transacción ganadora, el punto de venta debe desplegar el mensaje "TRANSACCIÓN PREMIADA" en el visor.

- Se debe imprimir a continuación el vale de venta según el estándar normal, pero agregando el código de verificación del premio y una glosa que indique TRANSACCIÓN PREMIADA. En la reimpresión de voucher, no debe imprimirse ni código de verificación del premio ni la glosa del premio.

- No será posible re-imprimir un vale de premio; ni emitir vales de Premio en papeles autocopiativos.

  Existen **tres** tipos de promociones **distintas**, *cada una con un voucher de aviso de premio distinto*:

- **Promociones de Entrega Simultánea:** en este caso el premio es entregado en el lugar donde fue realizada la transacción. En general, el premio será responsabilidad de la entidad que genera la promoción, sin acción del comercio, a no ser que su participación sea por acuerdo bilateral y con la capacitación correspondiente

- **Promociones de Entrega Diferida**: en este caso, el tarjetahabiente debe contactarse con el teléfono que aparece en el voucher de aviso de premio.

- **Descuentos al Tarjetahabiente**: en este caso, en el próximo estado de cuenta del tarjetahabiente, se generará un descuento asociado a la promoción.

1.7.5 Parámetros del Submódulo de caja (POS).

El Submódulo de caja debe manejar un conjunto de parámetros del POS, los cuales podrán ser actualizados por el personal autorizado del comercio, para lo cual se exige que para ello se implemente un esquema de seguridad al acceso a dichos parámetros. En la siguiente tabla se especifican estos parámetros:

PARÁMETRO	TIPO DE DATO	DESCRIPCIÓN
Nombre Comercio	X(38)	Nombre del comercio a imprimir en los voucher
Dirección Comercio	X(38)	Dirección del comercio a imprimir en los voucher
Comuna o ciudad	X(38)	Comuna o Ciudad del comercio a imprimir en los voucher
Terminal_ID	X(16)	Identificación del punto de venta asignada por Transbank. Parámetro de Suma importancia, ya que es el que indica quién está realizando la transacción. Configurar mal este parámetro podría retornar un rechazo 820

ID_Comercio	X(12)	Número de comercio asignado por Transbank al punto de venta. Parámetro de suma importancia, ya que es el que indica a quién se le abonará la transacción. Para el caso de multicódigo, la aplicación debe administrar una lista de N códigos de comercio, uno correspondiente al comercio responsable y N-1 a los comercios prestadores ambos códigos de comercio, el del prestador así como el del comercio responsable. Este código es de largo 8 con un prefijo fijo "5970" que va al principio ej: 597012345678 Configurar mal este parámetro podría retornar un rechazo 150
CREDITO	X(01)	Habilita/deshabilita la transacción de Venta con tarjeta de credito. Valores Posibles: **(Y/N)** Nota: Por defecto este campo debe tener el valor "**Y**".
Débito	X(01)	Habilita/deshabilita la transacción de Venta con tarjeta de Débito. Valores Posibles: **(Y/N)** Nota: Por defecto este campo debe tener el valor "**Y**".
Flag_Propina	X(01)	Habilita / deshabilita el ingreso de una propina por transacción Valores Posibles: Valores Posibles: **(Y/N)** Nota: Por defecto este campo debe tener el valor "**N**".
Cash_Back	X(01)	Habilita / deshabilita opción *Cashback* (Venta con vuelto) para las transacciones de Débito. Valores Posibles: **Y** = Habilita la opción de CASH-BACK (venta con vuelto) para las transacciones de Débito. **N** = No permite realizar ventas con vuelto en transacciones débito. Nota: Por defecto este campo debe tener el valor "**N**"
Monto_Vuelto1	9(6)	Permite definir el monto asociado a la opción de vuelto al tarjeta habiente. Valor por defecto: $5.000
Monto_Vuelto2	9(6)	Permite definir el monto asociado a la opción de vuelto al tarjeta habiente. Valor por defecto: $10.000
Monto_Vuelto3	9(6)	Permite definir el monto asociado a la opción de vuelto al tarjeta habiente. Valor por defecto: $20.000
Monto_Vuelto4	9(6)	Permite definir el monto asociado a la opción de vuelto al tarjeta habiente. Valor por defecto: $50.000
Flag_Empleado	X(01)	Habilita/deshabilita la solicitud de número de empleado. Valores Posibles: **Y** = Habilita la opción de solicitar el código de empleado. **N** = No permite ingresar el código de empleado. Nota: Por defecto, debe tener valor "**Y**".
Flag_Boleta	X(01)	Habilita / deshabilita la solicitud de número de boleta. Valores Posibles: **Y** = Habilita la opción de solicitar el número de boleta **N** = No permite ingresar el número de boleta. Nota: Por default este campo debe tener el valor "**Y**".
Flag PEL	X(01)	Flag que indica que comercio participa de las promosiones en línea de TBK e imprime los voucher de PEL y la glosa de PEL en los voucher del cliente y comercio (Y/N) Por default: Y

Flag voucher Cliente	X(01)	Flag que indica que se debe imprimir voucher cliente (Y/N) Por default: Y
Flag voucher comercio	X(01)	Flag que indica que se debe imprimir voucher comercio (Y/N) Por default: Y
Timeout Respuesta	9(02)	Tiempo máximo que espera el POS por la respuesta a un mensaje enviado a Transbank. Este tiempo viene dado en segundos y por default debe tener el valor 30 (treinta segundos).
Timeout interacción con el pinpad	9(03)	Tiempo máximo que espera el punto de venta luego de enviar un comando al pinpad. Hay que considerar los tiempos que requiere el pinpad para interactuar con el TH Valor por defecto 120 segundos Podrían definirse distintos timeout por cada tipo de interacción ver manual de comandos
Venta	X(01)	Permite habilitar o deshabilitar la transacción de Venta. Por defecto esta transacción debe estar habilitada. Valores: **Y** = VENTA habilitado **N** = No permite Venta Esto puede ser utilizado por un mesón de atención donde solo se realizan anulaciones
Anulación	X(01)	Permite habilitar o deshabilitar la transacción de Anulación. Por defecto esta transacción debe estar habilitada. Valores: **Y** = Anulación habilitado. **N** = No permite Anulación. Pensando en cajas donde solamente se realizan ventas y las anulaciones se realizan en mesón de atención
Permite Cuotas	X(01)	Caja podría trabajar solamente sin cuotas Valores: **(Y/N)**
Valor Velocidad PINPAD	9(05)	Permite definir los parámetros de velocidad en que se debe comunicar con el PinPad.
Tipo conexión de pinpad	9(05)	Usb - serial
Versión de pinpad	9(05)	15.01
Cuota Maxima NCuotas	9(02)	Cuota máxima para el producto NCuotas, configurable en el punto de venta de acuerdo a lo establecido con Transbank en su utilización. Este campo se enmarca dentro de la nueva definición de funcionalidades de pago.
Encabezado Crédito	X(38)	VENTA CREDITO
Encabezado debito	X(38)	VENTA DEBITO
Encabezado prepago	X(38)	VENTA PREPAGO
Encabezado no Bancaria	X(38)	VENTA NO BANCARIA
Encabezado Anulación no Bancaria	X(38)	ANULACION NO BANCARIA
Encabezado Anulación	X(38)	ANULACION CREDITO
Glosa Duplicado	X(38)	*** DUPLICADO ***
Pie de voucher 1	X(38)	ACEPTO PAGAR SEGÚN CONTRATO CON EMISOR
Pie de voucher 2	X(38)	ACEPTO EL DETALLE DE CUOTAS INDICADO

Para definir las marcas o tipos de tarjetas que el punto de venta deberá aceptar, en el punto de venta debe definirse una tabla que maneje los siguientes parámetros:

1.7.5.1 Tabla de tarjetas

1.7.5.1.1 Tarjetas Bancarias

TARJETA	GLOSA	MARCA
VISA	VISA	VI
MASTERCARD	MASTERCARD	MC
DINERS	DINERS	DC
AMERICAN EXPRESS	AMEX	AX
MAGNA	MAGNA	MG
DISCOVER	DISCOVER	DS
DEBITO	DEBITO	DB

Los valores "glosa" y "marca" son devueltos por el PINPAD y deben aparecer en todas las pantallas en donde haya que mostrar el tipo de tarjeta. La marca es un identificador del tipo de tarjeta que se usa en la impresión de comprobantes.

1.7.5.1.2 Tarjetas No Bancarias

Para el caso de las tarjetas no bancarias soportadas, remitirse al *Anexo No Bancarias Manual de Especificaciones*.

NOMBRE MARCA DE TARJETA	ABREVIACIÓN DE TARJETA
RIPLEY	TR
PRESTO	TP
MAS	TM
CMR	TC

1.7.6 Funcionalidades Soportadas

1.7.6.1 Transacciones Financieras

Venta con tarjeta de crédito. Presencial/No Presencial. Esta transacción permite ventas con tarjetas de Crédito, con y sin cuotas, con y sin propina. Para el caso de transacciones en modalidad no presencial, no requiere el deslizamiento de tarjeta, la presencia del tarjeta habiente ni el ingreso de PIN por parte de este último (**Referencia**: `Anexo No Bancarias Manual de Especificaciones Técnicas Conexión Host to Host`).

Venta con tarjeta de crédito con pin. Esta transacción permite ventas de Crédito ingresando PIN, con y sin cuotas, con y sin propina.

Venta con tarjeta de débito. Esta transacción permite ventas de Débito ingresando PIN, sin cuotas.

Venta con vuelto con tarjeta de débito. Esta transacción permite ventas de Débito con vuelto (*Cashback*) ingresando PIN, sin cuotas.

Anulación de venta con tarjeta de crédito. Esta transacción permite anulaciones de ventas realizadas **sólo** con Tarjetas de Crédito. Para el caso de transacciones en modalidad no presencial, no requiere el deslizamiento de tarjeta ni la presencia del tarjeta habiente (**Referencia**: `Anexo manual de especificaciones técnicas conexión Host to Host para ventas con tarjetas de crédito en modalidad no presencial`).

Referencia de flujos de transacciones: Flujos de Transacciones

1.7.6.2 Transacciones Administrativas

Carga de llave. Esta transacción permite al *host* del comercio requerir y cargar nuevas working keys desde Transbank.

Cierre Batch. Esta transacción permite al punto de venta intercambiar totales con el *Host* de Transbank. Junto con esto, en esta transacción el *host* envía en la respuesta un nuevo juego de *working keys* y los códigos de servicio actualizados. Esta transacción, al igual que las transacciones financieras, se solicita la mensajería y posteriormente la validación de la respuesta al PINPAD.

TIPOS DE TRANSACCIONES SOPORTADAS BAJO MODALIDAD CON CONSULTA DE CUOTAS			
TIPOS DE TRANSACCIONES	**TRANSACCIONES**	**FUNCIONALIDADES SOPORTADAS**	
TRANSACCIONES FINANCIERAS	TRANSACCIONES CON TARJETA DE CRÉDITO	VENTA NORMAL	
			VENTA NORMAL CON MES DE GRACIA
		VENTA EN CUOTAS NORMALES	
			CONSULTA VALOR CUOTA
			VENTA EN CUOTAS CON PAGO DIFERIDO
		2 CUOTAS SIN INTERÉS (2CSI)	
		3 CUOTAS SIN INTERÉS (3CSI)	
		CUOTAS IGUALES Y CONOCIDAS	
			CONSULTA VALOR CUOTA
			CIC O CUOTAS COMERCIO RELOAD.
			CIC O CUOTAS COMERCIO SIN INTERÉS
		N – CUOTAS	
		PROMOCIONES EN LÍNEA	
		VENTA CON PROPINA	
		VENTA SIN PROPINA	
		PIN CRÉDITO	
			VENTA NORMAL
			VENTA CUOTAS NORMALES
			2CSI
			3CSI
			CUOTAS IGUALES Y CONOCIDAS
			N – CUOTAS
			PROMOCIONES EN LÍNEA
			CONSULTA VALOR CUOTA
		ANULACIONES	
			MONTO TOTAL
			MONTOS PARCIALES ▪ ANULACIÓN VENTA NORMAL. ▪ ANULACIÓN CUOTAS NORMALES.
	TRANSACCIONES CON TARJETA DE DÉBITO	DÉBITO NORMAL	
		DÉBITO CON VUELTO	
		PROMOCIONES EN LÍNEA	
TRANSACCIONES ADMINISTRATIVAS	CARGA DE LLAVES		
	CIERRE BATCH		
	HANDSHAKE		

1.7.7 Funcionalidades del punto de venta bajo modalidad CON CONSULTA DE cuotas

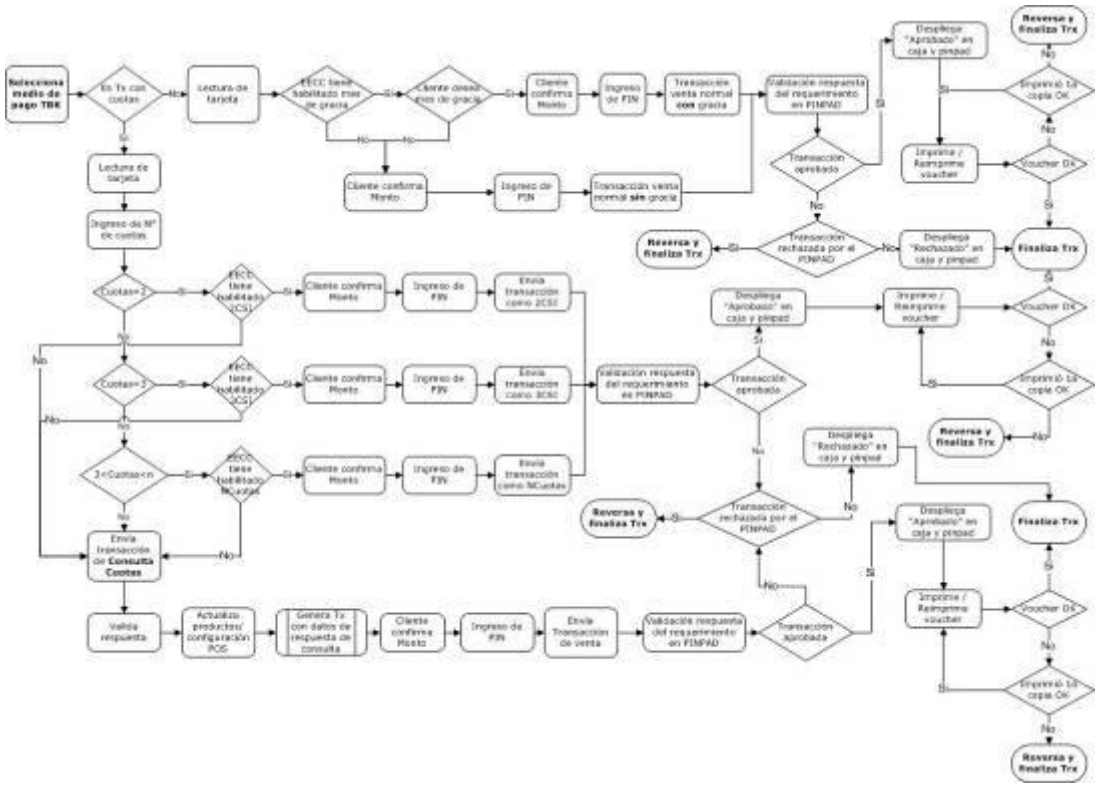
En modalidad nuevas cuotas, se produce un cambio importante en la forma de operar del punto de venta, el cual se detalla a continuación.

<u>IMPORTANTE</u>: Estas consideraciones (capítulos 1.6.8.XX) no aplican si la modalidad a aplicar es la de retail estándar SPDH 3.1

Esta versión incorpora una variante en la forma en cómo se realiza el proceso transaccional de la venta, incorporando elementos nuevos que afectan directamente al aplicativo de caja además de cada uno de los submódulos descritos previamente.

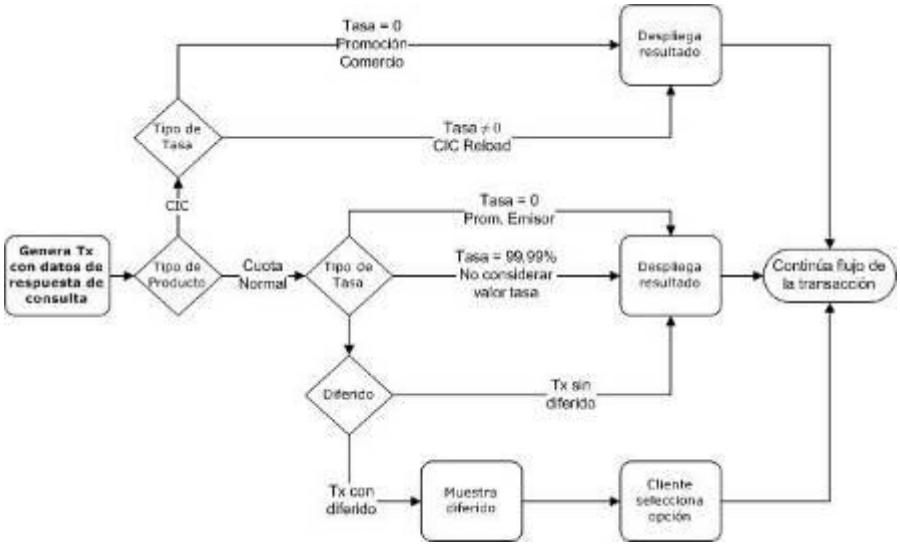
Su objetivo es simplificar la operatoria actual del comercio para cursar una transacción de venta para **tarjetas bancarias emitidas en Chile**. Está asociado directamente al algoritmo de inteligencia definido como regla de negocio para las transacciones en cuotas. Asimismo, este cambio en la operación va de la mano con una modificación en el aplicativo del punto de venta, dado que en forma paralela a la variación en la operación de la venta en cuotas, se establecen condiciones adicionales descritas en capítulos posteriores (ej. menú único).

Para esta versión de SPDH 4.0, se incorporan nuevas funcionalidades al modelo actual existente, a modo de facilitar la operatoria en el punto de venta, así como de disminuir la inteligencia actual del mismo, y entregar gran parte de las decisiones a los sistemas internos de Transbank. Para lo anterior expuesto, se define el siguiente flujo de pago de transacciones, el cual debe ser incorporado en cada uno de los desarrollos realizados bajo las definiciones de este documento:



El flujo anterior define las condiciones con las cuales es necesario evaluar una transacción al momento de realizarla, en primera instancia dando prioridad a los

productos sin intereses habilitados en el comercio, bajo los cuales es posible realizar la transacción hacia Transbank en forma directa (tal cual como ocurre en las versiones previas de SPDH). En el caso de transacciones que pudiesen tener intereses, y de acuerdo a la configuración del punto de venta, realizar una consulta previa a Transbank que defina la transacción a realizar (la mejor alternativa al tarjeta habiente). La especificación de la generación de la transacción a partir del resultado de la consulta de valor cuota es especificada en el siguiente diagrama de flujo:



De esta forma es posible definir la siguiente secuencia en el flujo de la transacción, determinada por un **menú único** definido por Transbank y detallado en el siguiente capítulo:

1. Cliente solicita medio de pago Transbank (tarjeta de crédito bancaria emitida en Chile).
2. Operador ingresa monto y consulta número de cuotas al tarjeta habiente.
3. Operador solicita lectura de tarjeta.
4. Aplicación valida configuración del punto de venta de acuerdo al orden de prioridad indicado en siguiente punto.
5. Aplicación opera bajo el siguiente orden de prioridad de productos:
    a. Productos sin intereses habilitados en el punto de venta, los cuales son validados (si se encuentran activos o inactivos) y gatillados por el punto de venta. Si transacción es sin interés, el punto de venta solicita al PINPAD la transacción financiera y la gatilla a Transbank de acuerdo a la configuración del punto de venta.
    b. Productos con intereses se solicita al PINPAD la transacción de consulta de valor cuota y se envía a Transbank.
6. Con respuesta de consulta de cuotas y selección de condiciones por parte del tarjeta habiente, se solicita al PINPAD la transacción financiera y se envía hacia Transbank.
7. El PINPAD valida respuesta de Transbank a transacción financiera.
8. Si transacción es aprobada, imprime voucher de acuerdo al producto recogido de la consulta y finaliza transacción.

Para las **tarjetas de crédito emitidas en el extranjero** no aplica la venta en cuotas, por tanto la consulta descrita entregará un rechazo con glosa indicando el error (por ejemplo, Servicio inhabilitado).

Para las **tarjetas de débito** no aplica la venta en cuotas, por tanto la consulta descrita entregará un rechazo con glosa indicando el error (por ejemplo, Menú inválido).

1.7.7.1 Menú único

Incorporado en el punto de venta en su totalidad, su objetivo es simplificar la operatoria actual del comercio para cursar una transacción de venta para tarjetas bancarias. Está asociado directamente al algoritmo de inteligencia definido como regla de negocio para las transacciones en cuotas.

Para tarjetas emitidas en el extranjero se debe mantener la lógica actual (venta normal sin PIN).

1.7.7.1.1 Inteligencia definida

Busca para la transacción de cuota (número de cuotas informado), la única alternativa de tipo de producto que existe en la nueva solución, según el algoritmo que mantiene la lógica de Transbank.

- Cuotas sin interés.
  - Producto contratado (2CSI, C3C, N-cuotas).
  - Promoción emisor.
  - Promoción comercio.
- Cuotas con interés (posterior a la respuesta de consulta de valor cuota)
  - CIC Reload.
  - Cuotas Normales.
  - CIC.

1.7.7.2 Valor Cuota en el punto de venta

Para toda transacción en cuota, el valor cuota debe ser mostrado al operador en la solución de punto de venta así como al tarjeta habiente antes de confirmar la transacción. Asimismo, debe ser informado en el comprobante de venta.

Para las transacciones CIC Reload (CIC con interés, descritas en capítulos posteriores), el valor cuota será calculado por Transbank y entregado en la consulta de valor cuota, de acuerdo a la lógica definida en este documento. No existe la opción al comercio de modificar el valor cuota o su tasa de interés asociada.

Para las transacciones venta en cuotas normales, el valor cuota será proporcionado por Transbank previo a la concreción de la venta. En caso de encontrarse Transbank fuera de línea, la operación de estas transacciones se realizará sin entregar el valor cuota, generándose el ciclo actual de venta para venta en cuotas normales.

1.7.7.3 Productos sin interés en los puntos de venta

Para el caso de los productos sin interés, está definido que es el punto de venta quien mantiene la lógica de configuración y administración de estos, su administración está limitada para la habilitación/deshabilitación de estos productos, quedando en manos de la administración de Transbank el activar o desactivar cada uno de estos. Bajo esta premisa, se define lo siguiente:

1. Los puntos de venta deberán conocer los productos sin intereses que tiene contratado el comercio (2CSI, 3CSI, N-CUOTAS) lo cual deberá ser implementado de la siguiente manera:
    a. Si el tarjeta habiente ingresa Nº cuotas = 2 y parámetro 2CSI se encuentra encendido en el PINPAD, entonces debe generar venta en 2 cuotas sin interés.

    b. Si el tarjeta habiente ingresa Nº cuotas = 3 y parámetro 3CSI se encuentra encendido en el PINPAD, entonces debe generar venta 3CSI.

    c. Si el tarjeta habiente ingresa un Nº de cuotas entre 4 y el máximo permitido al comercio (parámetro N-Cuotas, valor tope 12), entonces debe generar una venta N-Cuotas.

    d. Si no cumple ninguna de las anteriores condiciones, entonces deben generar TX de consulta hacia Transbank.

1.7.7.4 Transacción de consulta en las transacciones financieras

La finalidad de esta transacción es que Transbank aplique la lógica de deducción de producto, y retorne el tipo de producto que el punto de venta debe asignar en la transacción financiera asociada a la elección del tarjeta habiente. El flujo de esta transacción es el siguiente:

1. Punto de venta genera transacción de consulta hacia Transbank, en la cual debe informarse entre otros datos, el monto de la venta, el nº de cuotas escogido por el tarjeta habiente y la configuración actual del punto de venta.

2. Transbank aplica lógica de deducción de producto:
    a. Promoción Emisor: tipo producto depende de promoción, tasa = 0%
    b. Promoción Transbank: tipo producto = CIC, tasa = 0%
    c. CIC Reloaded: tipo producto = CIC, tasa = tasa máxima producto
    d. Cuotas Normales: tipo producto = cuotas normales, tasa variable

3. Cuando la lógica determina que corresponde Cuota Normal, entonces Transbank genera la obtención del valor de de la cuota, la tasa aplicada, así como los valores para diferido a 1, 2 y 3 meses.

4. Transbank responde la transacción de consulta al punto de venta, informando, entre otros parámetros:

    a. Tipo de cuota
    b. Valor de cuota
    c. Tasa Interés
    d. Glosa tipo de cuota
    e. Tipo de promoción
    f. Glosa promoción
    g. Valor diferido 1 mes
    h. Valor diferido 2 mes
    i. Valor diferido 3 mes

5. Cuando en la respuesta de la transacción de consulta, se informa que el tipo de cuota corresponde a Cuotas Normales y existen valores para diferido, entonces el punto de venta debe presentar los valores para diferido al operador (a través de la aplicación) así como al tarjeta habiente, informando la selección del tarjeta habiente en la transacción financiera. Por ejemplo:

MONTO CUOTA	$11.500
DIFERIDO 1 MES	$12.950
DIFERIDO 2 MESES	$14.875
DIFERIDO 3 MESES	$16.930

6. La aplicación gatilla el envío de la transacción de acuerdo a la selección del tarjeta habiente hacia Transbank.

7. Transbank responde al *host* de comercio con el resultado de la operación (aprobación o rechazo)

8. El PINPAD valida la respuesta de Transbank y de encontrarse aprobada comienza la impresión del voucher. En caso de ser rechazada la transacción, el rechazo debe plasmarse en la aplicación informando al operador, como en el PINPAD, informando al tarjeta habiente.

9. La operación finaliza con la impresión correcta del voucher (original y copia).

1.7.8 Transacciones financieras con Tarjetas de Crédito

La operatoria de las transacciones de crédito soportadas debe consultarse en el Manual de Operaciones de Transbank.

1.7.8.1 Venta Normal.

Funcionalidad que permite al comercio obtener autorización para ventas con tarjeta de crédito sin cuotas.

1.7.8.1.1 Venta normal bajo modalidad nuevas cuotas

Adicionalmente permite al comercio, si esta funcionalidad se encuentra habilitada, ofrecer o no al tarjeta habiente un **mes de gracia** en el cargo de la primera cuota, reflejado en el voucher impreso. A continuación se presenta el flujo de las transacciones para la venta normal considerando ambas opciones (con o sin mes de gracia).

1.7.8.2 Venta en cuotas normales.

Alternativa que permite al comercio obtener autorización por ventas en cuotas normales en un rango de 2 a 24 (o 36 según la aceptación de cada emisor de Tarjetas de Crédito). Para efectos de pago, al comercio se le abona el total de la venta de una vez, pero al cliente su banco emisor le carga en cuotas aplicándole el interés determinado por el Banco.

1.7.8.2.1 Venta en cuotas normales bajo modalidad nuevas cuotas

Toda transacción en cuotas normales (determinada por la inteligencia) generará una solicitud de cálculo de valor cuota a Transbank, quien tiene toda la información necesaria para determinar este dato; la cual depende de diversos factores y son distintos para cada tarjeta habiente.

En caso que el emisor esté adherido al diferimiento de la transacción; la respuesta a la solicitud de TBK serán los valores cuota normal y por cada diferimiento (hasta tres)

La selección del valor cuota a pagar efectuada por el tarjeta habiente dará origen finalmente a la solicitud de autorización de la venta.

Cabe señalar que al procesador emisor se le solicitará no volver a efectuar nuevos cálculos, pues el modelo debe considerar el honrar lo informado en el comprobante de venta.

De acuerdo a lo anterior, los datos que entrega Transbank como respuesta a la solicitud son:

- Código de autorización
- Valor cuota sin diferimiento
- Tasa de interés sin diferimientos
- Valor cuota con diferimiento 1 mes (si aplica)
- Tasa de interés con diferimiento 1 mes (si aplica)
- Valor cuota con diferimiento 2 meses (si aplica)
- Tasa de interés con diferimiento 2 mes (si aplica)
- Valor cuota con diferimiento 3 meses (si aplica)
- Vasa de interés con diferimiento 3 meses (si aplica)

Dado que la nueva modalidad de cuota normal debe ser implementada exclusivamente bajo el menú único y la inteligencia entregada por Transbank, el punto de venta deberá reconocer si la transacción enviada por Transbank presenta la opción de diferimiento del valor cuota al tarjeta habiente, la cual debe quedar reflejada en tanto en el punto de venta como en el voucher posteriormente impreso. El flujo de una transacción de venta en cuotas normales se presenta a continuación:

1.7.8.3 Venta en 2 Cuotas sin Interés (2CSI)

Alternativa que permite al comercio, ***solo si está habilitado para este producto y si se encuentra bajo la modalidad de nuevas cuotas***, obtener autorización para ventas **en 2 cuotas contado sin interés**. Tanto el pago al comercio como el cargo al cliente es en dos cuotas.

Es importante señalar que si el comercio se encuentra habilitado para operar con el producto Venta 2 cuotas contado sin interés (2CSI), automáticamente cambia el rango de cuotas normales para las ventas, este será de 4 a 24 (o 36 según la aceptación de cada Emisor de Tarjetas de Crédito).

1.7.8.3.1 En el Voucher de Venta y Anulación

Para la impresión del voucher es necesario destacar en el comprobante

- Se debe informar en el comprobante el monto de cada cuota.
- Tipo de cuotas Sin Intereses.
- Número de cuotas 2.

Detalle de Voucher (**Referencia**: Diseño de comprobantes)

1.7.8.3.2 Valor Cuota Sin Intereses.

El valor de las CUOTAS SIN INTERESES, que se utiliza sólo para la impresión de los comprobantes, depende del monto total de la venta y el número de cuotas. En caso que el monto total de la venta no sea divisible por el número de cuotas, la última cuota se redondea al valor divisible inmediatamente superior y el resto de las cuotas quedan con el valor divisible inmediatamente inferior.

EJEMPLO: MONTO NO DIVISIBLE POR 2		**EJEMPLO 2: MONTO DIVISIBLE POR 2**	
Monto	$ 9.999	Monto	$ 10.000
Valor Cuota 1	$ 4.999	Valor Cuota 1	$ 5.000
Valor Cuota 2	$ 5.000	Valor Cuota 2	$ 5.000

1.7.8.4 Venta en 3 Cuotas sin Interés (3CSI)

Alternativa que permite al comercio, ***solo si está habilitado para este producto,*** obtener autorización para ventas **en 3 cuotas contado sin interés**. Tanto el pago al comercio como el cargo al cliente es en tres cuotas.

Es importante señalar que si el comercio se encuentra habilitado para operar con el producto Venta 3 cuotas contado sin interés (3CSI), automáticamente cambia el rango de cuotas normales para las ventas, este será de 4 a 24 (o 36 según la aceptación de cada Emisor de Tarjetas de Crédito).

1.7.8.4.1 En el Voucher de Venta y Anulación

Para la impresión del voucher es necesario destacar en el comprobante

- Se debe informar en el comprobante el monto de cada cuota.
- Tipo de cuotas Sin Intereses.
- Número de cuotas 3.

Detalle de Voucher (Referencia: Diseño de comprobantes)

1.7.8.4.2 Valor Cuota Sin Intereses.

El valor de las CUOTAS SIN INTERESES, que se utiliza sólo para la impresión de los comprobantes, depende del monto total de la venta y el número de cuotas. En caso que el monto total de la venta no sea divisible por el número de cuotas, la última cuota se redondea al valor divisible inmediatamente superior y el resto de las cuotas quedan con el valor divisible inmediatamente inferior.

EJEMPLO: MONTO NO DIVISIBLE POR 3		**EJEMPLO 2: MONTO DIVISIBLE POR 3**	
Monto	$10.000	Monto	$ 30.000
Valor Cuota 1	$ 3.333	Valor Cuota 1	$ 10.000
Valor Cuota 2	$ 3.333	Valor Cuota 2	$ 10.000
Valor Cuota 3	$ 3.334	Valor Cuota 3	$ 10.000

1.7.8.5 Venta en N-Cuotas (Cuotas Comercio con abono mensual)

Alternativa que permite al comercio, solo si está habilitado para este producto, obtener autorización para ventas en cuotas comercio con abono mensual, que van de 4 a un máximo de 12, las cuales son iguales y conocidas, no afectas a intereses, ni impuesto al crédito. Tanto el pago al comercio como el cargo al cliente se le abonan según el número de cuotas de la transacción.

1.7.8.5.1 Venta en cuotas bajo modalidad SPDH 3.1

N-cuotas es un producto similar a Cuotas Comercio tasa 0, la diferencia de implementación radica en el punto de venta para reconocer la habilitación de este producto y generar la transacción correspondiente de encontrarse dentro del número de cuotas solicitadas por el tarjeta habiente:

1. El Producto N-Cuotas es excluyente del producto Cuotas Comercio. Asimismo, el comercio sólo puede tener habilitada una sola de ellas.

2. El producto N-Cuotas permite desde un número de 4 a 12 cuotas.

Las restricciones antes mencionadas deben ser **paramétricas** en el aplicativo de caja.

Para el cálculo de la cuota para esta transacción se debe realizar el siguiente algoritmo:
Cuota = Monto de Venta / Número de Cuota.

Para cada transacción con tarjeta de crédito en N-Cuotas, el aplicativo de caja debe generar un comprobante de venta con dos copias. La copia original la debe guardar el comercio y la segunda copia se debe entregar al cliente.

Se utilizará comprobante definido para N-Cuotas en el anexo "Diseño de Comprobantes".

Ejemplo:

Monto de Venta	=	100.000
Número de Cuota con Tasa Cero	=	9
Cuota Igual	=	11.111,111111111111111111
Valor Techo	=	11.112

Nota Ejemplo:

- Para el valor de esta cuota se considera el valor techo de este resultado.
- El valor techo es el entero inmediatamente superior al valor decimal obtenido.
- Las anulaciones de transacciones de este tipo se realizan de la misma forma que una anulación de ventas cuotas comercio.

1.7.8.5.2 Venta en N-Cuotas bajo modalidad Nuevas Cuotas

N-cuotas es un producto similar a Cuotas Iguales y Conocidas con promoción emisor tasa = 0, la diferencia de implementación radica en el punto de venta para reconocer la habilitación de este producto y generar la transacción correspondiente de encontrarse dentro del número de cuotas solicitadas por el tarjeta habiente:

3. El Producto N-Cuotas es excluyente del producto CIC Reload descrito a continuación. Asimismo, el comercio sólo puede tener habilitada una sola de ellas.
4. El producto N-Cuotas permite desde un número de 4 a un máximo paramétrico de 12 cuotas a elección del comercio (esto implica que el comercio puede optar hasta un máximo de 12 cuotas). De elegir el comercio un valor menor de N-CUOTAS, implica que el valor máximo para las cuotas está condicionado por el contrato establecido con Transbank.

Las restricciones antes mencionadas deben ser **paramétricas** en el aplicativo de caja y PINPAD, y actualizadas en cada transacción de respuesta de Transbank, así como en las de rechazo en la cual se indique (código de rechazo 218).

Para el cálculo de la cuota para esta transacción se debe realizar el siguiente algoritmo:
Cuota = Monto de Venta / Número de Cuota.

Para cada transacción con tarjeta de crédito en N-Cuotas, el aplicativo de caja debe generar un comprobante de venta con dos copias. La copia original la debe guardar el comercio y la segunda copia se debe entregar al cliente.

Se utilizará comprobante definido para N-Cuotas en el anexo "Diseño de Comprobantes".

Ejemplo:

Monto de Venta	=	100.000
Número de Cuota con Tasa Cero	=	9
Cuota Igual	=	11.111,1111111111111111111
Valor Techo	=	11.112

Nota Ejemplo:

- Para el valor de esta cuota se considera el valor techo de este resultado.
- El valor techo es el entero inmediatamente superior al valor decimal obtenido.
- Las anulaciones de transacciones de este tipo se realizan de la misma forma que una anulación de ventas cuotas comercio.

1.7.8.6 Venta en Cuotas Iguales y Conocidas con Interés (CIC Reload)

El producto CIC Reload corresponde al producto CIC con intereses y **SOLAMENTE se aplica bajo modalidad Nuevas Cuotas**. **El comercio no tendrá la opción de definir el valor cuota**, y por lo tanto **no define la tasa de interés**.

Siempre se aplicará la tasa de interés definida para el producto en el contrato. Para los casos en que el comercio haya tenido contratado el producto CIC; éste es reemplazado por CIC Reload.

Este cambio implica necesariamente que al comercio le sea habilitado el menú único y, por lo tanto, las transacciones que realice de este producto serán determinadas por la inteligencia desarrollada por Transbank. Este nuevo producto no cambia la forma de operar de las Cuotas Comercio, sino que regula su otorgamiento. Su finalidad es prohibir que el comercio modifique la tasa para este producto, operando siempre con la tasa máxima del producto (definida por TBK) o con tasa 0%, cuando comercio se encuentre en promoción.

El punto de venta debe continuar controlando la validación respecto al producto N-Cuotas; vale decir, **CIC Reload y N-cuotas son productos excluyentes**.

En la práctica, cuando un comercio contrata este producto, al realizarse una transacción de consulta al Base24, la lógica de deducción de producto informará que corresponde una venta de tipo CIC, con tasa máxima definida para el producto. Si un comercio no contrata este producto y realiza transacciones con cualquier aplicación actualizada con CUOTAS, no podrá realizar ventas de tipo CIC con interés, solo de CIC sin interés cuando contrate una promoción Transbank.

1.7.8.7 Promociones bajo modalidad Nuevas Cuotas

Las promociones que deben ser reconocidas e informadas al momento de efectuarse la venta son:

- Promociones emisoras del tipo transformación de transacciones en cuotas normales a cuotas sin interés que son administradas por Transbank.
- Promociones ofrecidas por el comercio a sus tarjeta habientes del tipo transformación a cuotas sin interés (asociadas al producto CIC).

- Promociones emisoras del tipo transformación transacciones en cuotas normales a cuotas sin interés informadas por los emisores.

Al determinar la promoción a aplicar, se informará al tarjeta habiente en el comprobante de venta que dicha transacción está afecta a una promoción, y se entregará el valor cuota, como el valor de la venta dividido por el número de cuotas, redondeando el valor cuota en la última cuota, si es necesario.

1.7.8.7.1 Promociones emisoras administradas por Transbank

En caso de existir una promoción del tipo emisor, Transbank indicará en la respuesta de la transacción de consulta valor cuota si a ésta se le debe aplicar una tasa de interés igual a cero de acuerdo a las características de la venta y los parámetros de las promociones activas.

1.7.8.7.2 Promociones comercio

Corresponde a las promociones ofrecidas por cada comercio al tarjeta habiente al momento de realizar una transacción de venta. Para este caso, Transbank valida que la transacción en curso no esté afecta a una promoción emisora, de forma tal de que la promoción sea única al tarjeta habiente de acuerdo a las características de la venta y los parámetros de la promoción ofrecida por el comercio.

En caso de existir una promoción del comercio, Transbank indicará en la respuesta de la transacción de consulta valor cuota si la transacción está afecta a este tipo de promoción de acuerdo a las características de la venta y los parámetros de las promociones activas.

1.7.8.8 PIN en Crédito

Este tipo de transacciones incorpora la funcionalidad de ingresar PIN en todos los productos soportados en una Transacción con Tarjeta de Crédito y bajo cualquier modalidad.

- Venta Normal.
- Venta Cuotas Normales.
- 2CSI (aplicable solo bajo modalidad Nuevas Cuotas).
- 3CSI.
- Cuotas Comercio.
- CIC, CIC Reload (aplicable solo bajo modalidad Nuevas Cuotas).
- N-Cuotas.

En términos generales la funcionalidad de ingreso de PIN para tarjetas de crédito, tiene la misma lógica que se utiliza para las tarjetas de débito. Es decir se desliza la tarjeta y cuando ésta es reconocida como tarjeta de crédito con PIN, se realizan las condiciones de venta de Crédito, luego se solicita confirmar monto e ingresar PIN (no se solicita los últimos 4 dígitos de la tarjeta de crédito).

A diferencia de las transacciones de Débito, en PIN en Crédito **no existen** reintentos de ingreso de PIN.

Se adjunta un ejemplo de la impresión del Voucher de Pin en Crédito, los vouchers son iguales a los informados para transacciones de crédito normal, con modificaciones en el **título**, **pie de firma** y **glosa de pie de voucher**. Adicionalmente, se explica la salvedad del período de carencia (**Referencia**: Diseño de comprobantes)

1.7.9 Transacciones financieras con tarjeta de débito

La operatoria de las transacciones de débito soportadas debe consultarse en el manual de Operaciones de Transbank. De tal manera de seguir con el flujo solicitado por Transbank.

1.7.9.1 Transacciones con Tarjeta de Débito - Venta Débito.

Alternativa que permite al comercio obtener autorización para ventas sin cuotas, con una tarjeta de débito.

Al ingresar el PIN en el PINPAD para las transacciones de Débito, el cliente puede realizar 3 intentos en forma errónea. Si el Pin no es ingresado correctamente en la tercera oportunidad, el aplicativo debe volver al menú de Medios de Pago.

1.7.9.2 Transacciones con Tarjeta de Débito - Venta Débito con Vuelto.

Alternativa que permite al comercio obtener autorización para ventas normales, por un monto superior al valor de los bienes o servicios adquiridos; y entregar al cliente, en efectivo, la diferencia entre el valor real de la compra y el monto de la transacción autorizada. Cabe señalar, que existe un monto límite, estipulado en el contrato, para las transacciones de venta con vuelto.

Por otra parte, el aplicativo despliega **"cuatro"** (4) diferentes alternativas de vuelto dentro de las cuales el cliente puede escoger el monto deseado, **las opciones desplegadas deben ser paramétricas**.

Referencia de flujo de transacciones: Transacción de débito

1.7.9.2.1 Operación en el Punto de Venta.

La operación en el punto de venta para esta transacción queda como sigue:

1. Presionar la tecla VENTA o deslizar la tarjeta del cliente.
2. Ingresar el Monto de Venta y presionar la tecla ENTER.
3. Desplegar Total y consultar si se desea vuelto
4. Si opción es NO, ir a paso 9.
5. Si la opción es SI, ir a paso 6.
6. Seleccionar Monto de Vuelto desde las "cuatro" opciones ya parametrizadas.
7. Desplegar en el visor Monto Vuelto y Monto Total.
8. Continuar operatoria venta normal, el monto a desplegar en el PINPAD corresponde al Monto Total, donde Monto Total = (Monto de Venta + Vuelto).

1.7.9.2.2 Transacciones de anulación

La anulación de transacciones no es aplicable para las transacciones con tarjeta de débito.

1.7.10 Transacciones administrativas

1.7.10.1 Carga de Llaves

Alternativa que permite cargar en línea en el aplicativo de Caja la llave (*working key*) generada por Transbank.

La Carga de Llave se debe realizar en forma automática al iniciar las operaciones del día. De tal manera que el POS tenga la llave, para realizar la primera transacción financiera del día.

Esto implica que debe existir un procedimiento de inicialización que se ejecuta en forma automática todos los días, el cual debe incluir la transacción Carga de Llaves.

1.7.10.2 Cierre Batch

Esta transacción permite al punto de venta intercambiar totales con el Host de Transbank. Junto con esto, en esta transacción el Host envía en la respuesta un nuevo juego de *working keys* (MAC) y los códigos de servicios actualizados. Esta transacción, al igual que las transacciones financieras, se solicita la mensajería y posteriormente se solicita la validación de la respuesta al PINPAD.

1.8 SUBMÓDULO DE HOST DE COMERCIO

1.8.1 Objetivo

El objetivo del sub-módulo de *Host* de Comercio es manejar y administrar la integridad de la mensajería de las transacciones administrativas. Adicionalmente, es el encargado de generar, establecer y mantener la comunicación con el *Host* de Transbank, así como de realizar el envío y recepción de mensajes en formato SPDH.

1.8.2 Consideraciones Generales

1.8.2.1 Habilitación de Conexiones a Transbank.

1.8.2.1.1 Especificaciones Técnicas de la Conexión.

- Router mínimo debe ser Cisco 1841 con IPSEC.
- Una LAN, se conecta en la red del cliente.
- Una LAN, servicio WAN, primario
- Una LAN, servicio WAN, secundario
- Enlace redundante, es decir, debe existir un primario y un secundario. Ambos enlaces deben ser contratados por el cliente.

Los enlaces deben cumplir con las siguientes características:

1. El proveedor del enlace secundario debe ser distinto al del enlace primario.
2. Poseer encriptación. Se establece una VPN (IPSEC 3DES) implementada por Transbank. se utiliza encriptación del enlace WAN.
3. Administración del router remoto la efectuará Transbank.
4. El cliente deberá instalar los enlaces en una DMZ.

Velocidades Fibra Oscura

1. Velocidad mínima de enlace primario **10mbps.**
2. Velocidad mínima de enlace secundario **10mbps**

Velocidades Red MPLS

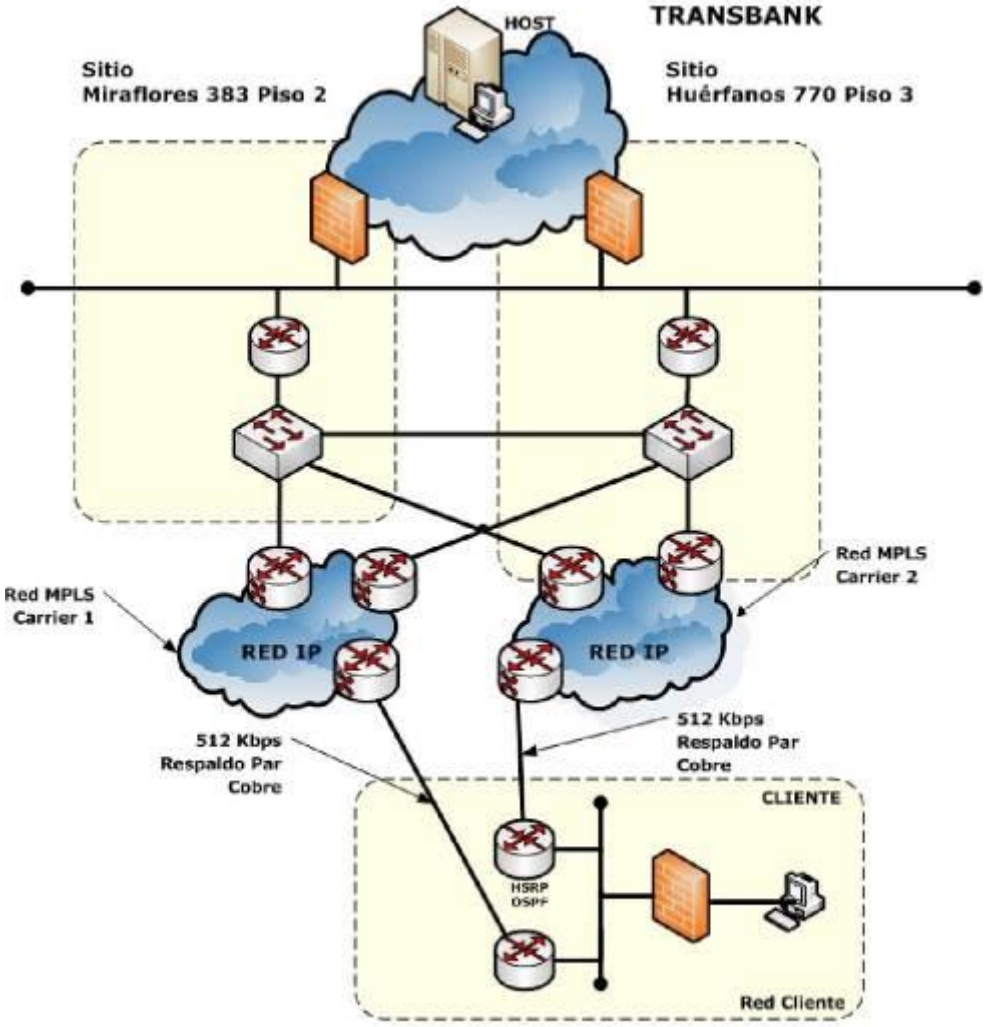
1. Velocidad mínima de enlace primario **256k.**
2. Velocidad mínima de enlace secundario **256 k**

1.8.2.1.2 Proveedores de enlace validados por Transbank - Servicio Host.

PROVEEDOR	RED
Telefónica	Fibra oscura
GTD	Fibra oscura
Telefónica	Red MPLS
Entel	Red MPLS

1.8.2.2 Alternativa de Conexión *Host to Host*

La alternativa de conexión que los comercios deben adoptar para conectarse modalidad *host to hos*t debe cumplir lo siguiente:



1.8.2.3 Servicio FTP

En este servicio se utilizará para la información que requieran nuestros clientes, este se activará en un horario el cual no presentará problema con el flujo de transacciones.

Este servicio funciona de la siguiente manera:

Se crea una casilla FTP en un servidor de Transbank. Donde se almacenan los archivos de cuadratura, el cliente se conecta a la casilla FTP que le fue asignada y descarga los archivos de cuadratura de sus transacciones.

1.8.2.4 Monitoreo Enlace

Transbank realiza un monitoreo de enlace, este será de 24 x 7. Este servicio es para apoyar a nuestros clientes ante reclamos de enlace. El área de Explotación de Sistemas se comunicará con el cliente para informar que efectúe el reclamo del servicio al carrier correspondiente.

1.8.2.5 Protocolos de Comunicación.

El protocolo de comunicación actualmente disponible para la **conexión *Host to Host*** con Transbank es **TCP/IP**, con el Host Comercio como cliente TCP o servidor TCP. La configuración por defecto es que el comercio opere como Cliente TCP.

1.8.2.6 Características de la Conexión TCP/IP.

Para la comunicación vía protocolo TCP/IP, se soporta en una conexión Cliente Servidor, donde:

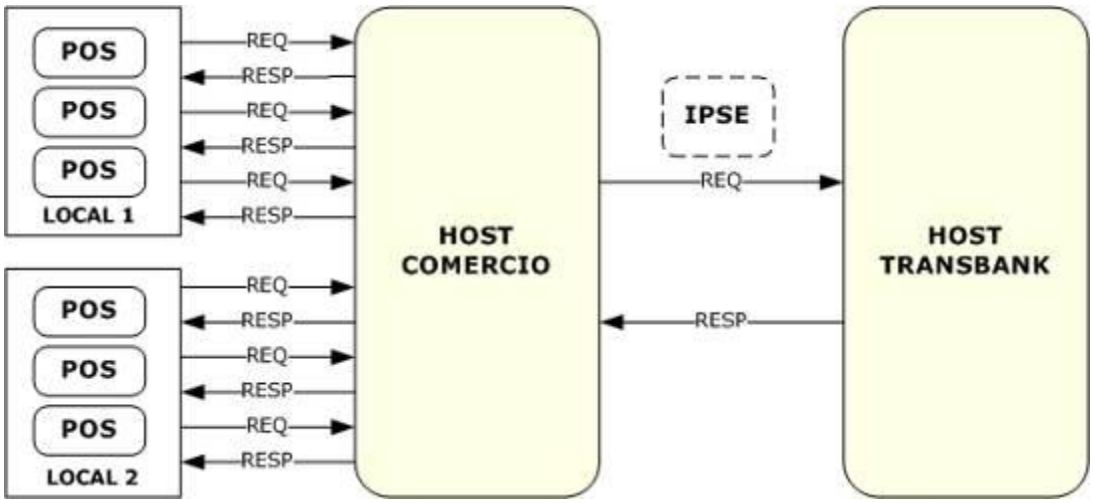
1. El Host de Transbank se comporta como Servidor.
2. El Host Comercio se comporta como Cliente.
3. Session (Socket) multi-thread.
4. La sesión del Cliente debe tener habilitado la opción de ***Keep-Alive.***

La encriptación de la data se realizará a través de **IPSEC** en los tramos comprendidos entre el computador central o Host comercio y el computador central o Host de Transbank.

Se considera establecer una "única sesión" (Socket) TCP/IP entre el Host de comercio y el Host de Transbank. Esta sesión debe ser **Multi - Thread.**

Dado que el Host de Transbank trabaja asincrónicamente, recibe múltiples requerimientos por un mismo socket, es **responsabilidad del Host de comercio multiplexar las transacciones de sus puntos de venta vía esta "única sesión" (Socket).**

Sólo en casos especiales, se re-evaluará el número de sesiones TCP/IP que podrán establecer el Host de comercio con el Host de Transbank, de acuerdo a los requerimientos y a las necesidades de cada comercio.



1.8.3 Consideraciones Generales

1.8.3.1 Características Exigidas a la Red de Comunicaciones del Comercio

Dado que las transacciones recibidas por Transbank atraviesan la red de comunicaciones del comercio, siendo ésta de su responsabilidad, se requiere que dicha red cumpla al menos con las siguientes características:

Los enlaces de comunicación, concentradores, equipos de comunicación y Host deben mantener un Uptime **superior al 99,8%.**

- El tiempo máximo para la transmisión de una transacción entre una caja y el Host del comercio no debe ser superior a 3 segundos.

- El Host del comercio así como los posibles concentradores que formen parte de la red del comercio deben administrar un tiempo máximo de espera (timeout) de la respuesta de Transbank. Este tiempo deben ser manejados por parámetros.

- El Punto de Venta debe administrar un timeout máximo desde que envió la transacción de requerimiento hasta recibir la respuesta de esta. Este timeout debe ser manejado por parámetro cuyo valor por defecto corresponde a 30 segundos.

- Deben existir operadores que controlen la red en todos sus nodos y administren la solución de eventuales problemas de comunicación entre los puntos de ventas y Transbank.

Para evaluar la red de comunicaciones del comercio, éste debe entregar a Transbank un informe que describa las características de su red, considerando:

- Topología de la red (Diagrama General).
- Nodos (Locales) y su ubicación geográfica.
- Número de puntos de venta por nodo.
- Disponibilidad de puertos de comunicación en puntos de venta para conectividad de PIN-PAD.
- Tipos de líneas de comunicación entre nodos (análogas y / o digitales).
- Velocidad de las líneas.
- Proveedor de las líneas.
- Respaldo de las líneas.
- Protocolos de comunicación.

1.8.3.1.1 Control de Acceso del Software de Caja

- El aplicativo Caja del comercio debe tener un control de acceso con restricciones y permisos definidos (usuario/contraseña) u otro control de acceso seguro y privado.
- Debe tener medidas de bloqueo de software malicioso y aplicaciones de terceros.
- En dispositivos móviles (Tablet) se recomienda automáticamente al encender iniciar el aplicativo de caja y bloquear el uso de otras aplicaciones.
- Es responsabilidad del comercio tener políticas de seguridad y control de acceso a sus aplicativos de caja.

1.8.3.1.2 Seguridad TLS 1.2

SSL (Secure Sockets Layer) o Capa de Conexiones Seguras. Es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de red. Desde el 2015 ha sido sustituido por TLS (Transport Layer Security) el cual está basado en SSL y son totalmente compatibles.
El comercio debe implementar seguridad interna en su red sobre todo para las conexiones por redes inalámbricas WIFI.

1.8.3.1.3 Seguridad en la Red WI-FI del Comercio
En el caso de que la red del Comercio requiera usar conexiones por WI-FI se exige que la red sea una red cifrada ***WPA2-PSK (AES)**.

Recomendaciones de seguridad para red WI-FI:

1) Cambiar regularmente la contraseña de red WI-FI
   Al cambiar regularmente la contraseña de red WI-FI evita que terceras personas puedan hacer uso de la red del comercio.

2) Configurar la red WI-FI como "No visible"
   Al ocultar la red WI-FI se evita que personas externas al comercio puedan encontrar e intentar acceder a la red del comercio.
   Ahora cada vez que se intente conectar un nuevo dispositivo, será necesario colocar primero la *SSID, para posteriormente ingresar la contraseña

3) Registrar y restringir las conexiones por MAC
   Al tener habilitadas las conexiones por MAC, se especifica que equipos pueden hacer uso de la red WI-FI, evitando que cualquier otro equipo haga uso de la red del comercio.

4) Restringir el acceso a la "Configuración del Router" desde WI-FI
   Al restringir el acceso a la configuración del Router desde conexiones WI-FI se evita que desde dispositivos WIFI se pueda acceder a esta configuración y se modifiquen sus parámetros.

5) Monitorear regularmente las conexiones WI-FI
   Los Router actuales permiten conocer los dispositivos que están conectados a la red WI-FI. Es recomendable monitorear para poder evitar algún dispositivo que esté conectado sin autorización.

**WPA2-PSK (AES): Sistema de protección para redes inalámbricas WI-FI. Es el último estándar de encriptación WI-FI y AES es el más reciente algoritmo de cifrado.*

**SSID: Difusión de un SSID de red. Un SSID es el nombre público de una red de área local inalámbrica (WLAN) que sirve para diferenciarla de otras redes inalámbricas en la zona. SSID es el nombre de la red que se especifica al configurar la red WI-Fi.*

1.8.3.2 Formato de Mensajes

Todos los mensajes de requerimiento de transacciones administrativas enviados por el terminal y las correspondientes respuestas entregadas por el módulo SPDH están compuestos por un *header* y campos adicionales que dependen del tipo de transacción.

Cada campo adicional está precedido de un carácter separador de campo (*FS*) y un carácter identificador de campo (*FID*). Los campos adicionales terminan con el próximo carácter separador de campo o un carácter de fin del texto (*ETX*), en el caso del último campo del mensaje.

El formato general de todos los mensajes en una conexión TCP/IP es:

b1	b1	TPDU	HEADER	FS	FID	DATO ADICIONAL	FS	FID	DATO ADICIONAL	ETX

Donde,

ETX	03h
FS	1Ch
b1,b2	En TCP/IP debe utilizarse dos Bytes con el equivalente binario del largo total del mensaje (incluyendo a estos dos Bytes)

Para el caso de las transacciones financieras (venta, anulación y reversas) y administrativas (cierre *batch*), el PINPAD entregará la mensajería correspondiente a:

HEADER	FS	FID	DATO ADICIONAL	FS	FID	DATO ADICIONAL

1.8.3.3 TPDU

El TPDU permite al Host de comercio parear requerimientos con respuestas en un modelo de múltiples transacciones simultáneas. El formato del TPDU es el siguiente:

- Byte 1 (no utilizado por esta solución, debe llevar valor cero (30H)). Este valor es asignado por Transbank y va expresado en formato hexadecimal.
- Bytes 2,3, identifica el origen del requerimiento y debe tener un valor expresado en formato hexadecimal. Este valor lo coloca el Host de comercio y lo usa para parear con la respuesta en un esquema de múltiples Transacciones simultáneas.
- Bytes 4,5, identifica el destino del requerimiento que en este caso es Transbank. Este campo debe llevar el valor fijo de 01 (3031 en hexadecimal).
- En el mensaje de respuesta, los campos origen y destino se invierten.

1.8.3.4 *Header*

El *header* debe ser incluido en todos los requerimientos de transacciones administrativas y será enviado con el mismo contenido en todas las respuestas. Si

en un requerimiento falta alguno de los datos del *header* la transacción es rechazada.

1.8.3.5 Campos Adicionales

Los campos adicionales dependen del tipo de transacción administrativa enviada. Para cada mensaje de requerimiento, Transbank valida la presencia de los campos adicionales definidos como obligatorios para la transacción. Si no se envían todos los campos requeridos, Transbank rechaza la transacción por error de formato.

En los mensajes de requerimiento, para mantener un estándar ***se exige que los campos adicionales deban venir en el mismo orden descrito en este manual***. En los mensajes de respuesta Transbank envía los campos adicionales en orden alfabético ascendente.

El detalle de la mensajería está en cada uno de los Submódulos del software de conectividad de Transbank.

1.8.4 Funcionalidades Soportadas

TIPO DE TRANSACCIONES	TRANSACCIONES	FUNCIONALIDADES SOPORTADAS
Transacciones de reversa	Reversa por *timeout* de una transacción financiera	**FT**
Transacciones Administración de Red	Echo Test (Handshake).	**Conexión con Transbank**

Las funcionalidades soportadas serán evaluadas por el área de Estándares de calidad de Transbank. Este proceso se denomina Certificación QA, la cual se realizará dependiendo de las funcionalidades soportadas por cada cliente.

1.8.4.1 Transacciones de reversa

Reversa por timeout de una transacción financiera

Se realiza con cualquier tipo de transacción financiera que no recibe respuesta del autorizador (Transbank).

Reversa por problemas de finalización de transacción en el punto de venta

Se realiza luego que el punto de venta ha recibido la respuesta aprobada de una transacción financiera y que por razones técnicas no es posible imprimirla.

Referencia de flujo de transacciones: Reversa FT

1.8.4.2 Transacciones de administración de red

Echo Test (*Handshake*). Esta transacción permite al Host del comercio comprobar el estado actual de la comunicación con el servidor Transbank (a nivel de aplicación). Debe ser utilizada, cuando el comercio desea verificar si el servidor de Transbank está atendiendo sus requerimientos.

Es la primera transacción que se intenta hacia el autorizador hasta recibir respuesta de Transbank

- Si la respuesta no es exitosa, el servicio se mantiene OFFLINE
- Si la respuesta es exitosa, se debe revisar la conectividad cada cierto intervalo de tiempo, recomendado de 180000 (milisegundos).
- Si la conexión se encuentra establecida, una transacción de EchoTest con resultado negativo:
    - Iniciará un ciclo de chequeo de la conexión más recurrente utilizando el tiempo recomendado de 5000 (milisegundos)
    - Se validará la cantidad de 2 intentos de transacciones con problemas de conexión antes de iniciar un ciclo de reconexión con el autorizador
    - Detendrá la programación del evento "EchoTest" hasta que se restablezca la conexión con el autorizador.
    - Durante el ciclo de reconexión, el servicio se encontrará OFFLINE para las consultas de POS, sin enviar requerimientos a Transbank

- Si la conexión se encuentra establecida, una transacción de EchoTest con resultado positivo gatilla un nuevo evento de EchoTest en el cierto intervalo de tiempo, recomendado de 180000 (milisegundos).

Una vez conectado con Transbank el componente Switch del Comercio realiza en forma periódica y configurable un testeo de la conexión a través de un comando "EchoTest" para lo cual requiere que se le asigne un único "Terminal ID" entregado por Transbank.

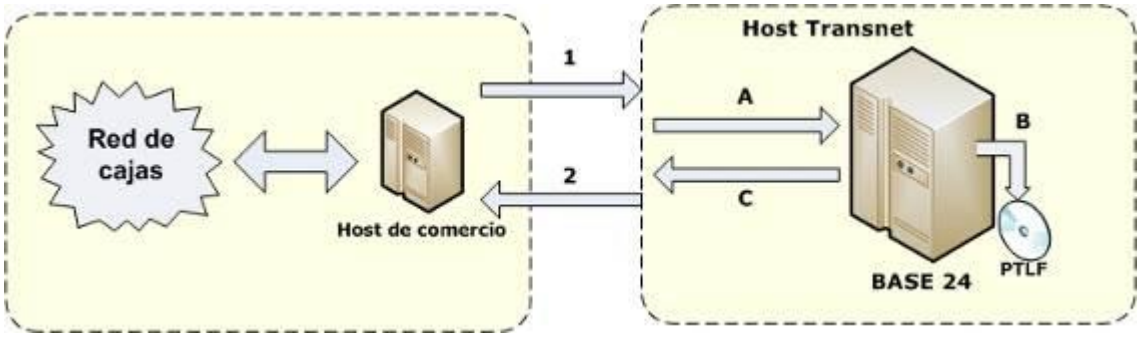
1.8.4.3 Flujo de los Mensajes.

El Submódulo de Host de Comercio como ya se indico es el encargado de conectarse a Transbank para enviar y recibir mensajes, como también mantener la integridad de la mensajería de las transacciones administrativas.

A continuación se describe el flujo de mensajes entre el Host del comercio y el Host de Transbank, para las distintas situaciones que se pueden dar en el ambiente transaccional, indicándose las acciones se que deben tomar dependiendo de los eventos que ocurran durante la comunicación.

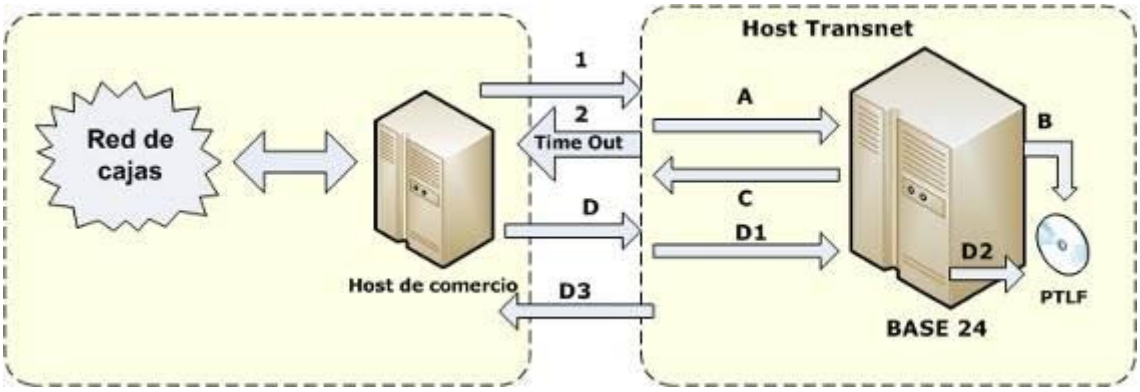
Desde este punto de vista se explicarán a continuación todos los tipos de transacciones (flujo de mensajes) que debe manejar, pero se especificarán solo las detalladas a continuación, por ser transacciones de Reversa (integridad) y de Administración de Red (conectividad).

1.8.4.3.1 Transacción Normal.



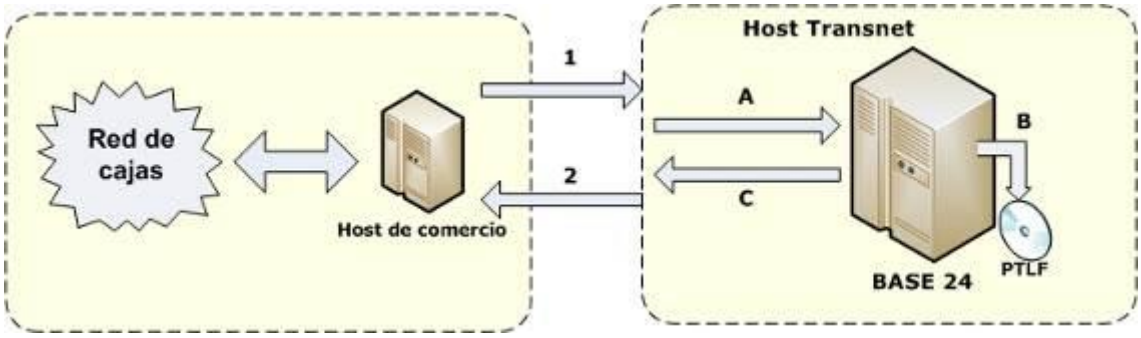
1	El Host del comercio envía el requerimiento al Host de Transbank.
A	El Host Transbank recibe el requerimiento del Host del comercio.
B	Base-24 procesa la transacción y la graba en su log (PTLF).
C	Base-24 responde al Host Transbank.
2	El Host Transbank envía la respuesta al Host del comercio.

1.8.4.3.2 Transacción con Reversa por timeout de la Caja.



1	El Host del comercio envía el requerimiento al Host de Transbank.
A	El Host Transbank recibe el requerimiento del Host del comercio.
B	Base-24 procesa la transacción y la graba en su log (PTLF).
C	Base-24 responde al Host Transbank.
2	El Host Transbank envía la respuesta (aprobada) fuera del tiempo máximo para este efecto o no fue contestada.
D	En el comercio, la caja al no recibir la respuesta o recibir respuesta para una transacción financiera aprobada fuera de tiempo envía una transacción de reversa al Host Transbank.
D1	El Host Transbank recibe la reversa y la envía a Base-24.
D2	Base-24 graba la transacción de reversa en su log.
D3	El Host Transbank envía la respuesta de la reversa al Host del comercio.

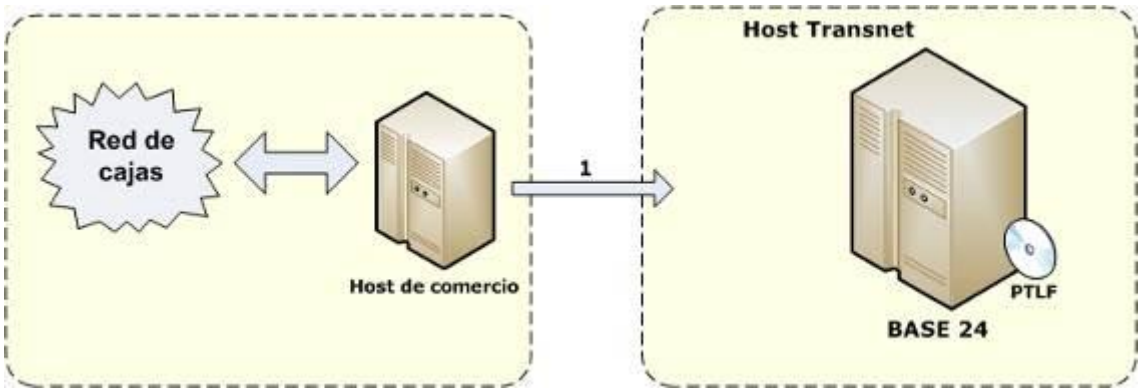
1.8.4.3.3 Transacción con Data Incorrecta.



1	El Host del comercio envía el requerimiento al Host de Transbank.
2	El Host Transbank envía la respuesta al Host del comercio indicando error de formato. Este rechazo no es registrado en el log (PTLF) de Base-24.

Nota: Se considera data incorrecta el orden de datos contenidos en el header.

1.8.4.3.4 Transacción con Formato Erróneo.



1	El Host del comercio envía el requerimiento al Host de Transbank.

Nota: Se entiende como formato erróneo uno o más campos del header con error de formato o datos inválidos o violación de protocolo. En este nivel es el protocolo el que se encarga de informar el rechazo del requerimiento mediante un mensaje con el código de **rechazo 810.**

1.8.4.3.5 Transacción Administración de red - Echo Test – Handshake

Esta transacción permite al Host del comercio comprobar el estado actual de la comunicación con el servidor Transbank (a nivel de aplicación). Debe ser utilizada, cuando el comercio desea verificar, si el servidor de Transbank está atendiendo sus requerimientos.

Lo que debe validar en este tipo de transacción es si Transbank responde la transacción. Esa es la manera de determinar que se tiene conexión con Transbank, y que se pueden realizar las transacciones Financieras y Administrativas.

Ejemplo:

Requerimiento:

001019.36S4CAJAHOST000010 200728164653AO95050000<fs>Q123456789012<fs>t00 00000000000000000000000000000000

<fs> byte "field separator"

PARÁMETROS	EJEMPLO	DESCRIPCIÓN
Terminal ID	S4CAJAHOST000010	Es el identificador del terminal que se utilizará en la caja. Largo máximo 16
Fecha y Hora	200728164653	Debe ir la fecha y hora en formato AAMMDDHHmmSS
Datos de Conteto	123456789012	Este campo es informativo y devuelto en la respuesta. Puede ser utilizado por el comercio para agregar información que le sirva a sus procesos internos. Largo máximo 16

Respuesta:

001019.36S4CAJAHOST000010
200728175134AO95000007<fs>HAC21B7CF735BC98FD0945F9AA7E51524<fs>M0000000000000000<fs>Q123456789012<fs>g
APROBADO<fs>h001180000

<fs> byte "field separator"

PARÁMETROS	EJEMPLO	DESCRIPCIÓN
Terminal ID	S4CAJAHOST000010	Es el identificador del terminal que se utilizará en la caja. Largo máximo 16
Fecha y Hora	200728164653	Debe ir la fecha y hora en formato AAMMDDHHmmSS
Datos de Contexto	123456789012	Este campo es informativo y devuelto en la respuesta. Puede ser utilizado por el comercio para agregar información que le sirva a sus procesos internos. Largo máximo 16
Glosa de Respuesta	APROBADO	Mensaje entregado desde Transabank
Numero de Secuencia	001180000	Número de secuencia de la transacción asignado por cada caja.

1.8.4.4 Tratamiento de Mensajes en el Host del Comercio.

1.8.4.4.1 Respuesta de Transacciones de Administración de Red

Si la respuesta corresponde a una transacción de administración de red, el Host del comercio no requiere ningún procesamiento adicional.

1.8.4.4.2 Mensaje de Reversa

El PINPAD puede generar una reversa en las siguientes situaciones:

- La caja envió el requerimiento, pero no recibe respuesta en el tiempo estipulado para ello.
- La caja recibe respuesta del Host de Transbank pero no puede finalizar la transacción o la validación de la respuesta en el PINPAD indica que se debe reversar.

Para ambos casos, la caja debe solicitar el mensaje de respuesta al PINPAD.

1.8.4.4.3 Parámetros de Comunicación

PARÁMETROS	TIPO DE DATO	DESCRIPCIÓN
Dirección_IP_Site_TBK	X(15)	Dirección IP del Host de Transbank
Puerto_Site_TBK	9(04)	Puerto del Host de Transbank asignado al comercio
Timeout_Respuesta_TBK	9(02)	Tiempo máximo que el Host de comercio espera por la respuesta del Host de Transbank a una transacción. El tiempo debe estar en segundos. Valor por defecto, 30 segundos.
Intervalo_Echo_Test_TBK	9(04)	Frecuencia en que el Submódulo del host de comercio envía transacción de eco test hacia el Host de Transbank. El valor debe estar en minutos. Valor por defecto es de 60 segundos.
Terminal_ID_Echo_Test	X(16)	Corresponde al Terminal ID a utilizar para generar los echo test hacia el Host de Transbank. Este ID debe corresponder a uno de los que componen la red del comercio.

2 CRITERIOS PARA LA GENERACIÓN DE REVERSAS

Los criterios que el terminal debe aplicar para la generación de una transacción de reversa son[3]:

- Si el terminal (punto de venta) no recibe una respuesta dentro del tiempo estipulado debe solicitar una reversa al PINPAD.
- Si la validación de la respuesta de una transacción financiera en el PINPAD indica que se debe enviar una reversa.
- Si el TPDU informado no corresponde a la caja qe efectuó la venta, el host del comercio no debe enviar la transacción al punto de venta, generándose de esta forma una solicitud de reversa por *timeout*.

3 INTERACCIÓN CON EL PINPAD

En este capítulo se describen las formas en cómo se desarrolla la interacción entre el PINPAD y la caja, esto incluye:
- Mensajes/acciones en la caja como en el PINPAD.
- Respuesta del PINPAD

Consideraciones:
- La velocidad de interacción con el PINPAD puede variar entre un sistema Operativo y otro. Por lo que debe ser paramétrico y/o configurable.
- El PIN a ingresar debe estar en el rango 4 a 12 dígitos.

3.1 Mensajes/acciones entre caja/PINPAD

3.1.1 Transacción con tarjeta de Débito

ACCIÓN EN LA CAJA	MENSAJE EN EL PINPAD	OBSERVACIÓN
ESTADO OCIOSO	"**TRANSBANK**" **Nota**: Esta glosa puede variar a criterio de Transbank.	
Selección Pago con tarjeta bancaria de débito	"**TRANSBANK**" **Nota**: Esta glosa puede variar a criterio de Transbank.	
Mensaje al operador "**OPERE TARJETA**"	**OPERE TARJETA** **MONTO $ xxxxxx**	En este punto el cliente debe deslizar, insertar o acercar la tarjeta, en caso de cancelación por parte del cliente el PINPAD acepta esta acción a través de la tecla <CANCEL>
	CONFIRME MONTO **$ xxxxxx**	En este punto el cliente debe confirmar el monto de la venta. Si el cliente quiere abortar la transacción en este punto, puede presionar la tecla <CANCEL>

[3] Cualquier otra condición determinada por la arquitectura de la solución debe ser presentada a Transbank y aprobada para su implementación.

	INGRESE SU CLAVE	En este punto el cliente debe ingresar su clave. Si el cliente quiere abortar la transacción en este punto, puede presionar la tecla <CANCEL> Si el cliente se equivoca al ingresar la clave y aún no ha presionado la tecla <ENTER> tiene la posibilidad de borrarla presionando <CLEAR> para luego volver a ingresar su clave.
Despliega mensaje informado por el PINPAD	De acuerdo al mensaje que recibe desde el punto de venta, el PINPAD valida y despliega el mensaje representativo del suceso Tx Aprobada, mensaje: **"TRANSACCIÓN APROBADA"** Tx rechazada, mensaje: **"<MOTIVO DEL RECHAZO>"**	

3.1.2 Transacción con tarjeta de Crédito nacional/internacional sin PIN

ACCIÓN EN LA CAJA	MENSAJE EN EL PINPAD	OBSERVACIÓN
ESTADO OCIOSO	**"TRANSBANK"** **Nota:** Esta glosa puede variar a criterio de Transbank.	
Selección pago con tarjeta bancaria de crédito	**"TRANSBANK"** **Nota:** Esta glosa puede variar a criterio de Transbank.	
Mensaje al operador "**OPERE TARJETA**"	**OPERE TARJETA MONTO $ xxxxxx**	En este punto el cliente debe deslizar, insertar o acercar la tarjeta, en caso de cancelación por parte del cliente el PINPAD acepta esta acción a través de la tecla <CANCEL>
"INGRESAR 4 ULTIMOS DIGITOS DEL NUMERO DE TARJETA"		En este punto se debe ingresar en el punto de venta los últimos 4 dígitos del número de la tarjeta de crédito.
Despliega mensaje informado por el PINPAD	De acuerdo al mensaje que recibe desde el punto de venta, el PINPAD valida y despliega el mensaje representativo del suceso Tx Aprobada, mensaje: **"TRANSACCIÓN APROBADA"** Tx rechazada, mensaje: **"<MOTIVO DEL RECHAZO>"**	

3.1.3 Transacción con tarjeta de Crédito nacional con PIN

ACCIÓN EN LA CAJA	MENSAJE EN EL PINPAD	OBSERVACIÓN
ESTADO OCIOSO	"**TRANSBANK**" **Nota**: Esta glosa puede variar a criterio de Transbank.	
Selección Pago Con tarjeta Bancaria de crédito	"**TRANSBANK**" **Nota**: Esta glosa puede variar a criterio de Transbank.	
Mensaje al operador "**OPERE TARJETA**"	**OPERE TARJETA** **MONTO $ xxxxxx**	En este punto el cliente debe deslizar, insertar o acercar la tarjeta, en caso de cancelación por parte del cliente el PINPAD acepta esta acción a través de la tecla <CANCEL>
	CONFIRME **MONTO/CUOTA** **$ xxxxxx**	En este punto el cliente debe confirmar el monto de la venta o el monto de la cuota, según sea el caso. Si el cliente quiere abortar la transacción en este punto, puede presionar la tecla <CANCEL>
	INGRESE SU CLAVE	En este punto el cliente debe ingresar su clave. Si el cliente quiere abortar la transacción en este punto, puede presionar la tecla <CANCEL> Si el cliente se equivoca al ingresar la clave y aún no ha presionado la tecla <ENTER> tiene la posibilidad de borrarla presionando <CLEAR> para luego volver a ingresar su clave.
Despliega mensaje informado por el PINPAD	De acuerdo al mensaje que recibe desde el punto de venta, el PINPAD valida y despliega el mensaje representativo del suceso Tx Aprobada, mensaje: **"TRANSACCIÓN APROBADA"** Tx rechazada, mensaje: **"<MOTIVO DEL RECHAZO>"**	

3.1.4 Transacción con tarjeta de Crédito nacional con PIN venta bajo modalidad Nuevas Cuotas

ACCIÓN EN LA CAJA	MENSAJE EN EL PINPAD	OBSERVACIÓN
ESTADO OCIOSO	"**TRANSBANK**" **Nota**: Esta glosa puede variar a criterio de Transbank.	
Selección Pago Con tarjeta Bancaria de crédito	"**TRANSBANK**" **Nota**: Esta glosa puede variar a criterio de Transbank.	
Mensaje al operador "**OPERE TARJETA**"	**OPERE TARJETA** **MONTO $ xxxxxx**	En este punto el cliente debe deslizar, insertar o acercar la tarjeta, en caso de cancelación por parte del cliente el PINPAD acepta esta acción a través de la tecla <CANCEL>
	[1] SIN CUOTAS **[2] CON CUOTAS**	En este punto el cliente selecciona una opción. Si el cliente quiere abortar la transacción en este punto, puede presionar la tecla <CANCEL>
	INGRESE NUMERO DE CUOTAS:	Solo se despliega si el cliente seleccionó la opción "[2] CON CUOTAS"
	CONFIRME MONTO/CUOTA **$ xxxxxx**	En este punto el cliente debe confirmar el monto de la venta o el monto de la cuota, según sea el caso. Si el cliente quiere abortar la transacción en este punto, puede presionar la tecla <CANCEL>
	INGRESE SU CLAVE	En este punto el cliente debe ingresar su clave. Si el cliente quiere abortar la transacción en este punto, puede presionar la tecla <CANCEL> Si el cliente se equivoca al ingresar la clave y aún no ha presionado la tecla <ENTER> tiene la posibilidad de borrarla presionando <CLEAR> para luego volver a ingresar su clave.
Despliega mensaje informado por el PINPAD	De acuerdo al mensaje que recibe desde el punto de venta, el PINPAD valida y despliega el mensaje representativo del suceso Tx Aprobada, mensaje: **"TRANSACCIÓN APROBADA"** Tx rechazada, mensaje: **"<MOTIVO DEL RECHAZO>"**	

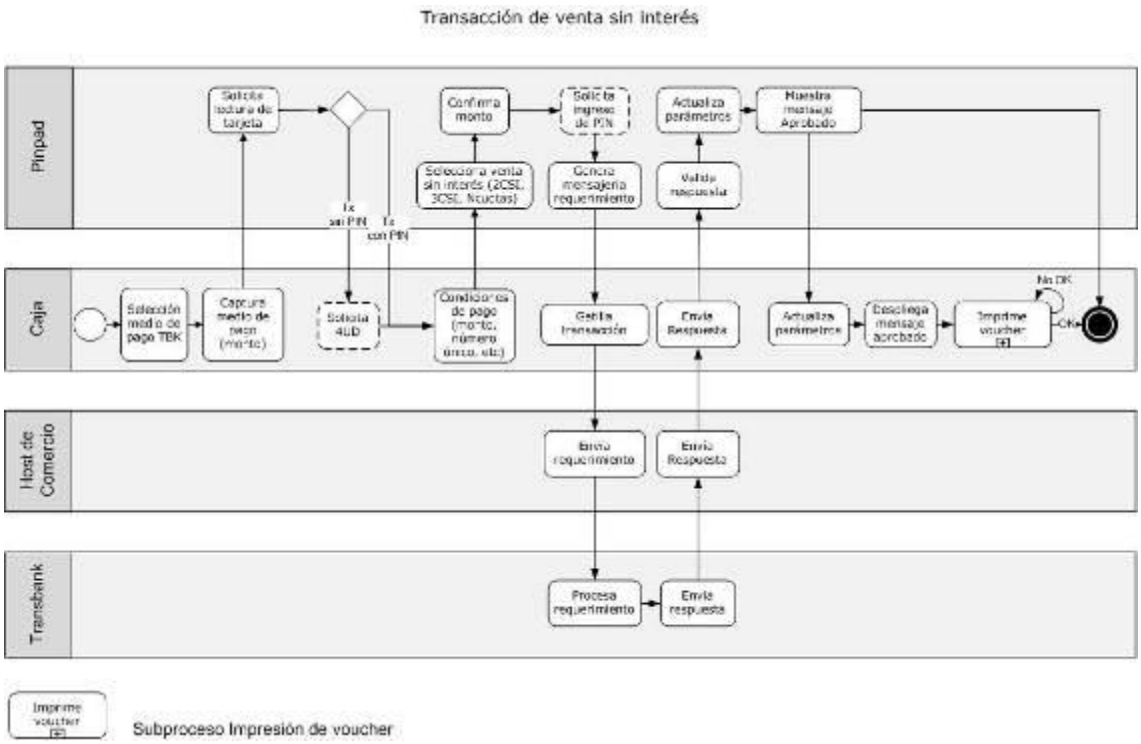
Para efectos de implementar la interacción con el PINPAD, se adjunta manual de comandos y comunicación del PINPAD (Referencia: `Manual de comandos pinpad Host to Host TRANSBANK - Comercio bajo protocolo SPDH 4.0`).

4 FLUJO DE TRANSACCIONES

A continuación se muestran los flujos de las transacciones al momento de realizar éstas. Cada uno de los flujos debe ser incorporado en la solución de caja del comercio, de acuerdo a la acción a realizar.

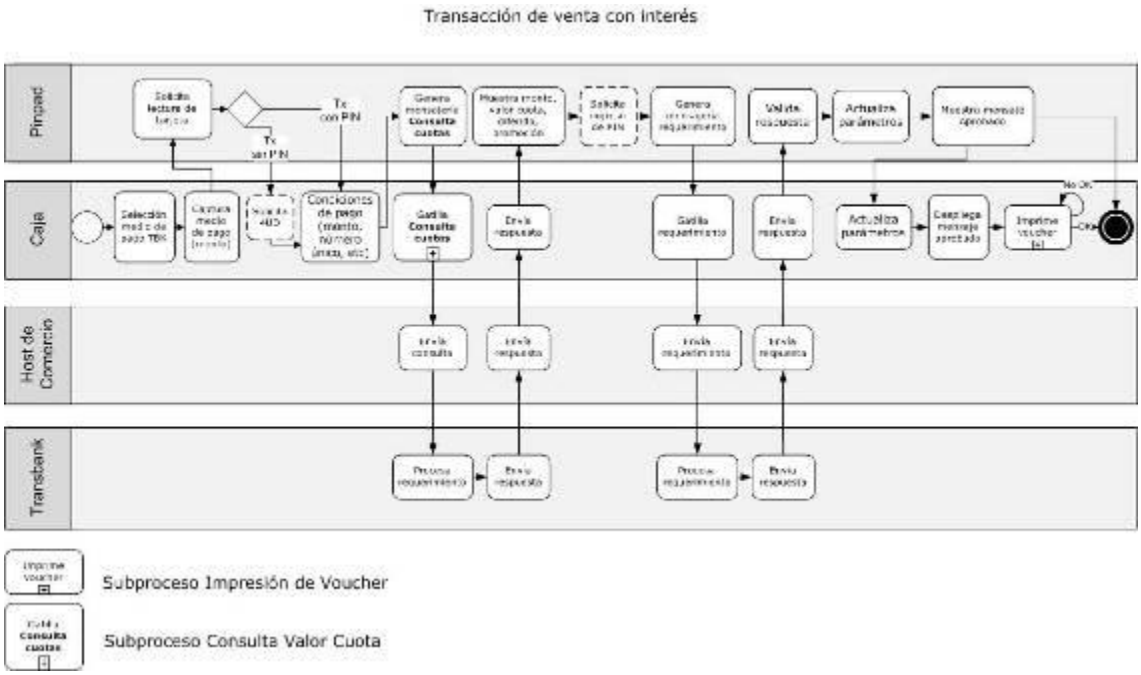
4.1 Transacción de venta con tarjeta de crédito sin Interés (NCuotas – 3CSI, 2CSI)

El flujo definido a continuación debe aplicarse bajo la modalidad Nuevas Cuotas. Para la modalidad SPDH 3.1 debe mantenerse el flujo actual de venta.



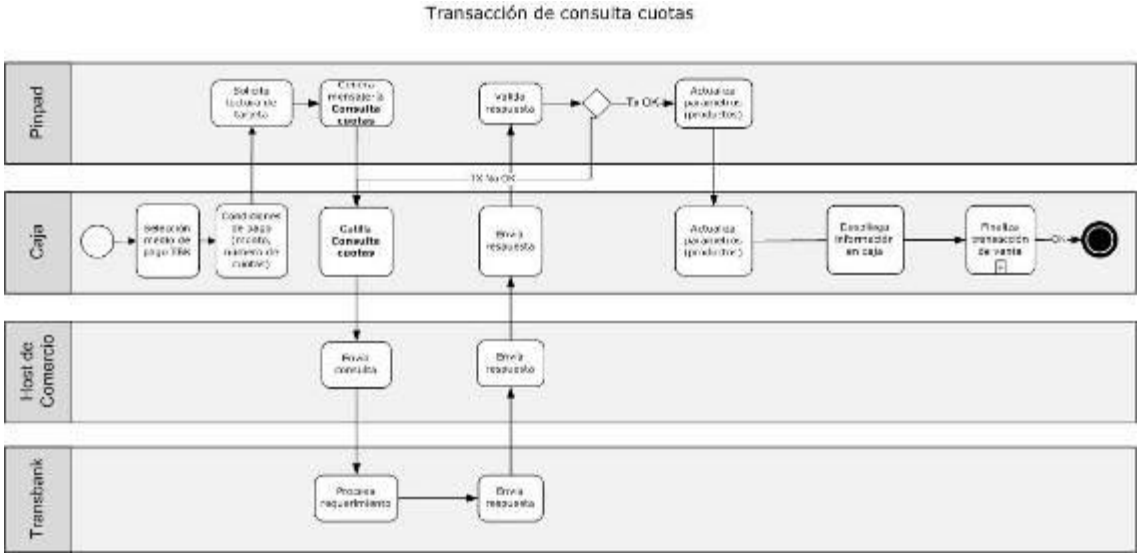
4.2 Transacción de venta con Interés (aplicable para CIC, CICR, Venta Normal)

El flujo definido a continuación debe aplicarse bajo la modalidad Nuevas Cuotas. Para la modalidad SPDH 3.1 debe mantenerse el flujo actual de venta.

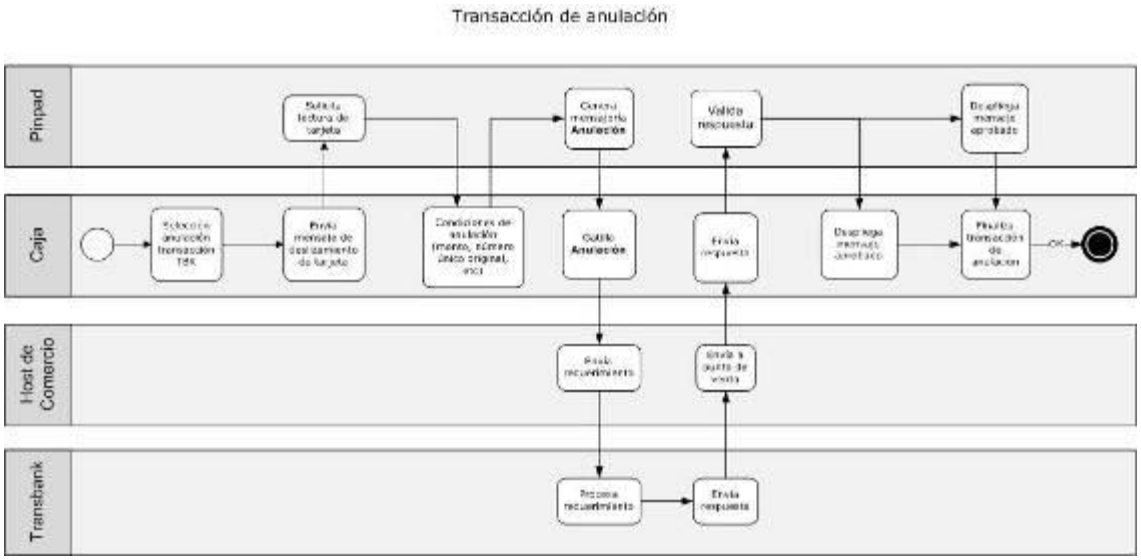


4.3 Consulta de valor cuota

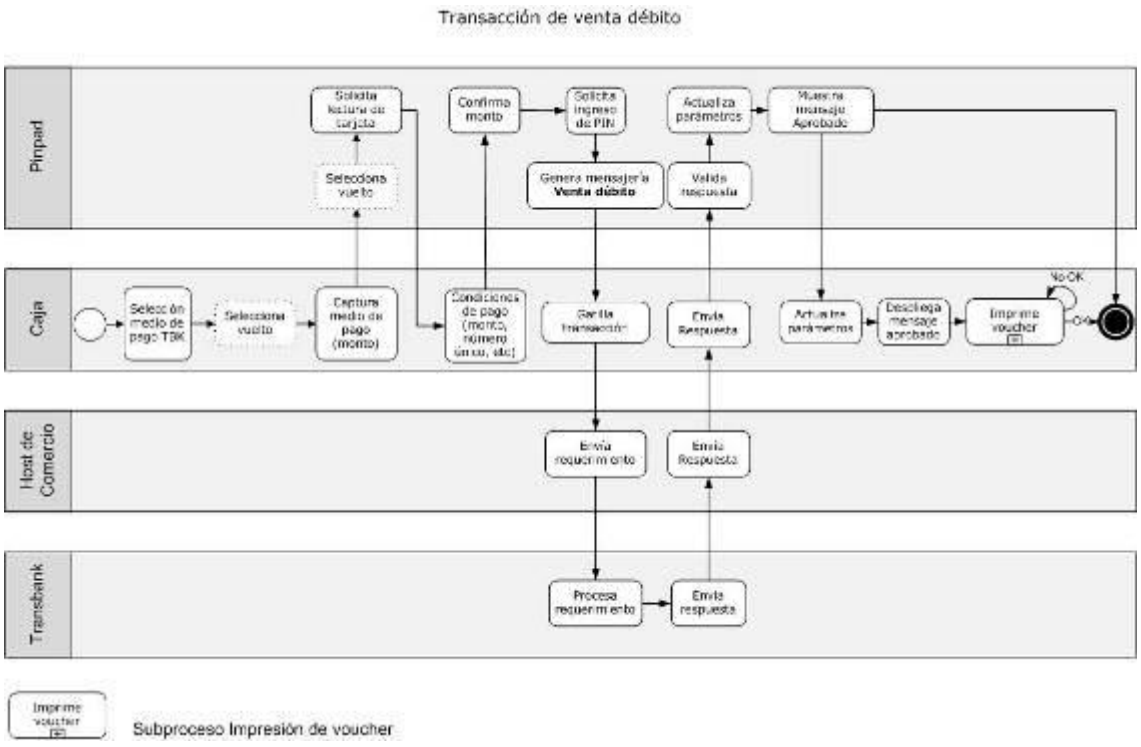
El flujo definido a continuación debe aplicarse bajo la modalidad Nuevas Cuotas. Para la modalidad SPDH 3.1 debe mantenerse el flujo actual de venta.



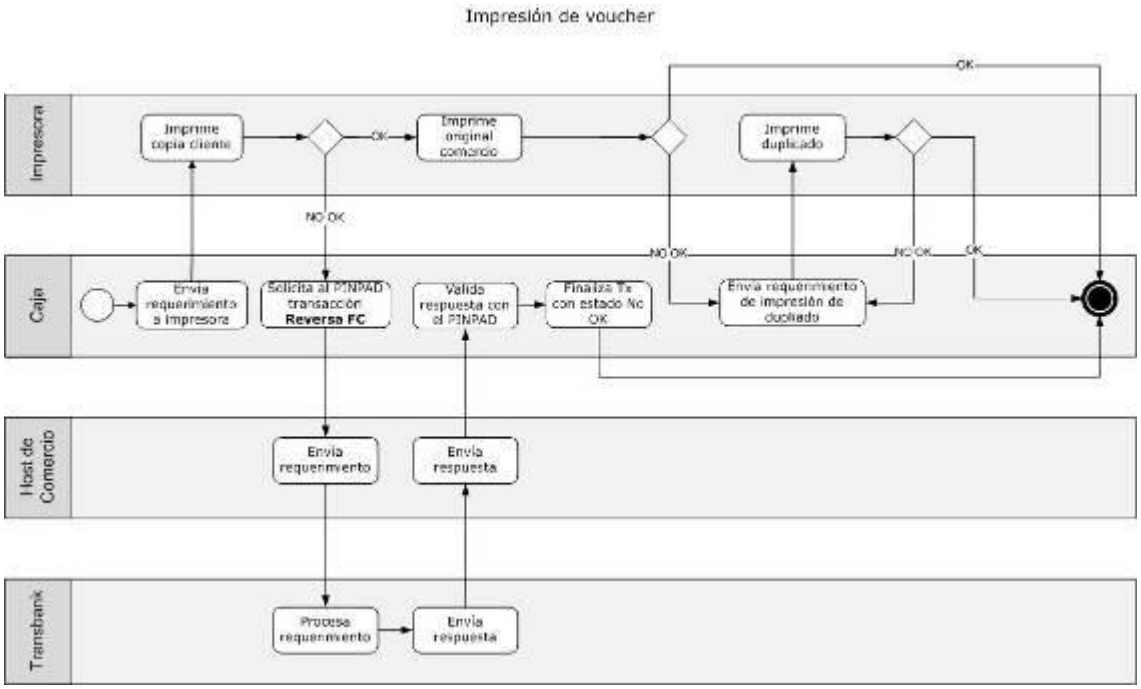
4.4 Anulación de transacciones



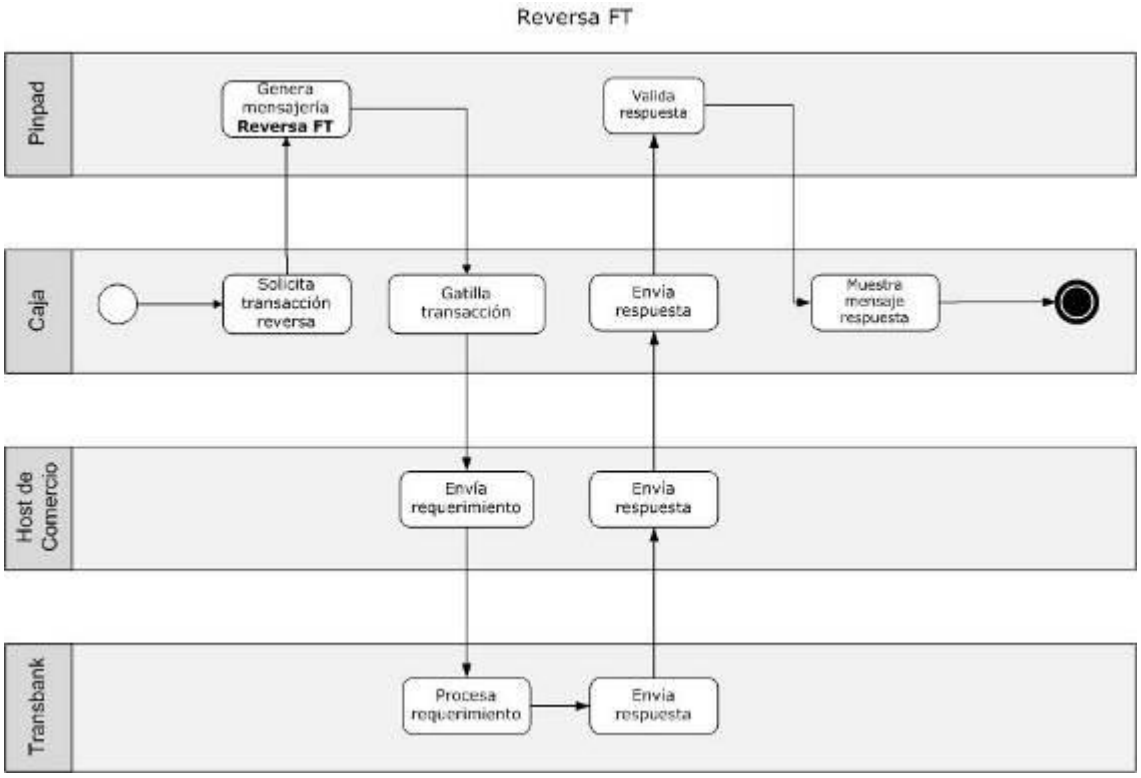
4.5 Transacción de débito



4.6 Impresión de voucher



4.7 Reversa FT



5 CONSIDERACIONES PARA EVALUACIÓN DE SOLUCIONES

Las consideraciones utilizadas por Transbank para evaluar la aplicación desarrollada por el comercio para atender las transacciones son:

5.1 Impresión de Comprobantes

Los datos impresos en el comprobante de venta se encuentran consistentes con los datos recibidos en la respuesta del requerimiento, por tanto se deben tener presente las siguientes consideraciones:

- Tipo de tarjeta corresponde a la utilizada en la venta.
- Monto de la venta corresponde a la venta.
- Número Único es único por punto de venta y corresponde a la venta.
- Número de Boleta corresponde a la venta.
- Tipo y Número de cuotas corresponde a la venta.
- Código de Autorización corresponde a la venta.

5.2 Aplicación de Caja

La secuencia en el proceso de venta utilizado para una venta con tarjeta de Crédito o Débito es simple y de fácil operatividad. Consideraciones a tener en cuenta:

- Mensajería desplegada para control de acciones en el punto de venta es suficientemente clara para el operador.
- La aplicación del punto de venta despliega la glosa de respuesta enviada por Transbank informada luego de la validación de la respuesta del PINPAD.

5.3 Mensaje de Requerimiento

- Los mensajes de requerimiento para las transacciones de ventas, anulaciones, reversas y cierre batch son generados por el PINPAD.

5.4 Administración de las comunicaciones

Desde el punto de vista de las comunicaciones, la aplicación de Transbank presenta una capa de comunicación (TCP/IP) y una capa de aplicación (Sistema autorizador BASE24).

- El Host comercio debe administrar una caída de la aplicación Transbank sin pérdida de enlace TCP/IP.
- La aplicación está administrando en forma adecuada el uso de transacciones de ECHOTEST para verificar que la aplicación autorizadora de Transbank se encuentra activa.
- Para una solución Cliente (Comercio) – Servidor (Transbank) con múltiples conexiones TCP/IP y aplicativas, se está administrando en forma adecuada la caída de algunas sesiones aplicativas sin pérdida de enlace TCP/IP.

- La comunicación que se establece desde el punto de venta del Cliente Comercio hacia el Servidor Transbank, mantiene un *uptime* de acuerdo a los estándares solicitados.

5.5 Pruebas PINPAD

- Cuando el PINPAD se desconecta de la caja, mantiene y recupera su funcionalidad al volver a conectarlo al punto de venta.

- Ante la cancelación de la transacción en el punto de venta o en el PINPAD, la aplicación del punto de venta recupera el flujo normal tanto en el punto de venta como en el PINPAD.

6 PA-DSS (NORMAS DE SEGURIDAD DE DATOS PARA LAS APLICACIONES DE PAGO)

Industria de Tarjetas de Pago (PCI) Normas de Seguridad de Datos para las Aplicaciones de Pago

Requisitos y procedimientos de evaluación de seguridad

Versión 1.2
Octubre 2008

6.1 Control de versiones

NOMBRE DOCUMENTO	VERSIÓN	FECHA LIBERACIÓN	AUTOR	REVISOR	PRINCIPALES CAMBIOS
Guía de Implementación Segura de la plataforma Host-to-Host para proveedores	1.0	11/01/08	P Calderón	MP. Aravena	Revisión del Documento
PA-DSS (NORMAS DE SEGURIDAD DE DATOS PARA LAS APLICACIONES DE PAGO	1.2	10/08/09	CCarnero	ABarrantes	Se reemplaza PABP por PADSS, añadiéndose observaciones Transbank y modificándose el formato del texto original para conservar el formato del resto de este documento.

6.2 Introducción

6.2.1 Finalidad de este documento

Los Asesores de Seguridad Certificados para las Aplicaciones de Pago (PA-QSA), quienes realizan las revisiones de la aplicación de pago, utilizarán este documento para que los proveedores de software puedan validar que una aplicación de pago cumpla con las Normas de Seguridad para las Aplicaciones de Pago (PA-DSS) de las PCI DSS. Este documento también tiene la finalidad de ser utilizado por los PA-QSA como plantilla para crear el informe de validación.

6.2.2 Relación entre PCI DSS y PA-DSS

Los requisitos de las Normas de Seguridad de Datos para las Aplicaciones de Pago (PA-DSS) se derivan de los Requisitos y Procedimientos de Evaluación de Seguridad de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) Este documento, que puede verse en www.pcisecuritystandards.org, detalla lo que se debe hacer para cumplir con las PCI DSS (y, por consiguiente, lo que debe admitir una aplicación de pago para facilitar el cumplimiento de las PCI DSS por parte de un cliente).

Es posible que el cumplimiento tradicional de las Normas de Seguridad de Datos de PCI no se aplique directamente a proveedores de aplicaciones de pago, dado que la mayoría de ellos no almacena, procesa ni transmite datos de titulares de tarjetas. Sin embargo, dado que los clientes utilizan estas aplicaciones de pago para almacenar, procesar y transmitir datos de titulares de tarjetas, y dichos clientes deben cumplir con las Normas de Seguridad de Datos de PCI, las aplicaciones de pago deben facilitar, y no entorpecer, el cumplimiento de las Normas de Seguridad de Datos de PCI por parte de los clientes. Algunas de las maneras en que las aplicaciones de pago pueden impedir el cumplimiento.

1. Almacenamiento de datos de banda magnética en la red de clientes después de la autorización.
2. Aplicaciones que les exigen a los clientes desactivar otras funciones requeridas por las Normas de Seguridad de Datos de PCI, como un software de antivirus o los sistemas de seguridad de tipo "firewalls", para que funcione adecuadamente la aplicación de pago.
3. El uso por parte del proveedor de métodos inseguros para conectarse a la aplicación a fin de proporcionar apoyo al cliente.

En el momento de implementarlas en un entorno que cumpla con las PCI DSS, las aplicaciones de pago seguro minimizarán la posibilidad de fallos de seguridad que comprometan todos los datos de banda magnética, los códigos y valores de validación de la tarjeta (CAV2, CID, CVC2, CVV2), los PIN y los bloqueos de PIN, y el fraude perjudicial derivado de tales fallos de seguridad.

6.2.3 Alcance de las PA-DSS

Las PA-DSS se aplican a proveedores de software y demás que desarrollan aplicaciones de pago que almacenan, procesan o transmiten datos de titulares de tarjetas como parte de la autorización o de la liquidación, siempre que dichas aplicaciones se vendan, distribuyan u otorguen bajo licencia a terceros.

Se puede utilizar la siguiente guía para determinar si las PA-DSS se aplican a una determinada aplicación de pago:

Nota:
Todos los productos de aplicaciones de pago validados no deben ser versiones beta.

- Las PA-DSS se atribuyen a las aplicaciones de pago que los proveedores de software generalmente venden e instalan "en forma estándar" sin demasiada personalización.

- Las PA-DSS rigen para las aplicaciones de pago suministradas en módulos, entre los que se incluyen un módulo "base" y otros módulos específicos para funciones o tipos de clientes, o personalizados según las solicitudes de los clientes. Es posible que las PA-DSS solo se apliquen al módulo "base", cuando ese módulo es el único que realiza las funciones de pago (una vez que lo confirmen las PA-DSS). Si existen otros módulos que también realizan las funciones de pago, las PA-DSS se aplicarán también a esos módulos. Tenga en cuenta que se considera una "mejor práctica" que los proveedores de software aíslen las funciones de pago en un solo módulo o en pocos módulos base y, de esa manera, se puedan reservar los demás módulos para funciones que no sean de pago. Si bien no es un requisito, esta mejor práctica puede limitar la cantidad de módulos sujetos a las PA-DSS.

- Las PA-DSS NO rigen para una aplicación de pago que se haya desarrollado para un solo cliente, o que se haya vendido a un solo cliente, dado que esta aplicación estará sujeta a la revisión normal de conformidad con las PCI DSS por parte del cliente. Tenga en cuenta que tal aplicación (a la que se puede denominar aplicación "personalizada") se vende a un solo cliente (por lo general, un gran comerciante o prestador de servicios), y está diseñada y desarrollada según las especificaciones provistas por el cliente.

- Las PA-DSS NO rigen para aplicaciones de pago desarrolladas por comerciantes y proveedores de servicios si sólo se utilizan internamente (no se venden, no se distribuyen ni se otorgan bajo licencia a terceros), dado que estas aplicaciones de uso interno deberían estar sujetas al cumplimiento normal de las PCI DSS por parte de los comerciantes o proveedores de servicios.

  Por ejemplo, para estos dos últimos casos, ya sea que la aplicación de pago desarrollada para uso interno o "personalizada" almacene datos de autenticación confiables prohibidos o permita contraseñas complejas, estarían consideradas como parte de los esfuerzos de cumplimiento habitual de las PCI DSS a cargo del comerciante o del prestador de servicios y no requerirían una evaluación de las PA-DSS por separado.

La siguiente lista, si bien no es del todo exhaustiva, detalla las aplicaciones que NO se consideran aplicaciones de pago a los fines de las PA-DSS (y, por lo tanto, no necesitan ser sometidas a revisiones según las PA-DSS):

- Sistemas operativos en los que se instala una aplicación de pago (por ejemplo, Windows, Unix).

- Sistemas de bases de datos que almacenan información de titulares de tarjetas (por ejemplo, Oracle).

- Sistemas de gestión operativa que almacenan datos de titulares de tarjetas (por ejemplo, para elaboración de informes o servicio al cliente).

Nota: PCI SSC SOLO enumerará las aplicaciones que sean aplicaciones de pago.

El alcance de la revisión según las PA-DSS debe incluir lo siguiente:

- Cobertura de todas las funciones de la aplicación de pago, incluidas, entre otras:
  1. Las funciones de pago completas (autorización y liquidación).
  2. Las entradas y las salidas de datos.
  3. Los estados de error.
  4. Las interfaces y las conexiones con otros archivos, sistemas y/o aplicaciones de pago o componentes de la aplicación.
  5. Todos los flujos de datos del titular de la tarjeta.
  6. Los mecanismos de cifrado.
  7. Los mecanismos de autenticación.

- Cobertura del asesoramiento que el proveedor de aplicaciones de pago debe brindarles a los clientes y a los revendedores/integradores (consulte la Guía de implementación de las PA-DSS más adelante en este documento) para asegurar:
  1. Que el cliente sepa cómo implementar la aplicación de pago de conformidad con las PCI DSS.
  2. Que se le diga al cliente con claridad que determinadas configuraciones del entorno y de la aplicación de pago pueden impedir que se cumpla las PCI DSS. Tenga en cuenta que es posible que el proveedor de aplicaciones de pago tenga que brindar ese asesoramiento incluso cuando la configuración específica:
     a. No pueda ser controlada por el proveedor de aplicaciones de pago una vez que el cliente haya instalado la aplicación, o
     b. Sea responsabilidad del cliente y no del proveedor de aplicaciones de pago.

- Cobertura de todas las plataformas seleccionadas para la versión revisada de la aplicación de pago (se deben especificar las plataformas incluidas).

- Cobertura de las herramientas utilizadas por la aplicación de pago, o dentro de ella, para acceder y/o visualizar los datos de titulares de tarjetas (herramientas de información, de registro, etc.)

6.3 Aplicabilidad de las PA-DSS a las terminales de hardware

Las terminales de hardware con aplicaciones de pago residentes (también denominadas terminales POS sin procesamiento o terminales independientes) no deben someterse a la revisión según las PA-DSS si se verifican todas las siguientes situaciones:

- El terminal no tiene conexiones con ningún sistema ni red del comerciante.

- El terminal se conecta únicamente con el adquirente o procesador.

- El proveedor de la aplicación de pago brinda, de manera segura y remota:
  1. Actualizaciones.
  2. Resolución de problemas.
  3. Acceso.
  4. Mantenimiento.

- No debe almacenarse la siguiente información después de la autorización: el contenido completo de toda pista de banda magnética (que se encuentra en el reverso de una tarjeta, en un chip o en cualquier otro dispositivo), el código de validación de la tarjeta o el valor (número de tres o cuatro dígitos en el anverso o reverso de la tarjeta de pago), el PIN o el bloqueo cifrado del PIN.

6.4 Funciones y responsabilidades

En la comunidad de las aplicaciones de pago, existen varias partes interesadas. Algunas de ellas poseen una participación más directa en el proceso de evaluación según las PA-DSS, como los proveedores, los QSA y el PCI SSC. Otras partes interesadas que no se encuentran directamente involucradas en el proceso de evaluación deben conocer todo el proceso para que la toma de decisiones comerciales relacionadas les resulte más fácil.

A continuación, se definen las funciones y las responsabilidades de las partes interesadas en la comunidad de las aplicaciones de pago. Las responsabilidades correspondientes a las partes interesadas que están involucradas en el proceso de evaluación se indican en una lista.

6.4.1 Marcas de pago

American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa Inc. son las marcas de pago que fundaron el PCI SSC. Estas marcas de pago son responsables de desarrollar y aplicar los programas relacionados con el cumplimiento de las PA-DSS, que incluye, a modo de ejemplo, lo siguiente:

- Los requisitos, los mandatos o las fechas que utilicen las aplicaciones de pago que cumplen con lo establecido en las PA-DSS.
- Las multas o las sanciones relacionadas con el uso de aplicaciones de pago que no cumplen con lo establecido en las PA-DSS.

Las marcas de pago pueden definir programas de cumplimiento, mandatos, fechas, etc., mediante las PA-DSS y aplicaciones de pago validadas que el PCI SSC establece. Mediante estos programas de cumplimiento, las marcas de pago promocionan el uso de dichas aplicaciones publicadas.

6.4.2 Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC)

El PCI SSC es el ente regulador que preserva las normas de la industria de tarjetas de pago, incluidas las PCI DSS y las PA-DSS. En relación con las PA-DSS, las PCI SSC:

- Forman un registro centralizado para los informes de validación (ROV) según las PA-DSS.
- Realiza revisiones de control de calidad (QA) del informe de validación según las PA-DSS para confirmar la coherencia y la calidad del informe.
- Coloca en una lista del sitio web las aplicaciones de pago validadas según las PA-DSS.
- Autoriza y capacita a los PA-QSA para que realicen revisiones según las PA-DSS.
- Mantiene y actualiza las PA-DSS y la documentación relacionada de acuerdo con un proceso de administración del ciclo de vida de las normas.

Observe que el PCI SSC no aprueba informes desde una perspectiva de validación. La función del PA-QSA es documentar la conformidad de las aplicaciones de pago con las PA-DSS a la fecha de la evaluación. Asimismo, el PCI SSC realiza un QA para garantizar que el PA-QSA documente de manera precisa y completa las evaluaciones según las PA-DSS.

6.4.3 Proveedores de software

Los proveedores de software ("proveedores") desarrollan aplicaciones de pago que almacenan, procesan o transmiten datos de titulares de tarjetas como parte de la autorización o de la liquidación y, luego, venden, distribuyen u otorgan estas aplicaciones de pago bajo licencia a terceros (clientes o revendedores/integradores). Los proveedores son responsables de:

- Crear aplicaciones de pago que cumplan con las PA-DSS y que faciliten, y no dificulten, el cumplimiento de las PCI DSS por parte de los clientes, (la aplicación no puede requerir un valor de implementación o configuración que viole un requisito de las PCI DSS).
- Cumplir los requisitos establecidos en las PCI DSS, siempre que el proveedor almacene, procese o transmita datos de titulares de tarjetas (por ejemplo, durante la resolución de problemas del cliente).
- Crear una Guía de implementación de las PA-DSS, específica para cada aplicación de pago, según los requisitos establecidos en este documento.
- Educar a los clientes, revendedores e integradores acerca de cómo instalar y configurar las aplicaciones de pago de conformidad con las PCI DSS.
- Asegurar que las aplicaciones de pago cumplan las PA-DSS y que aprueben satisfactoriamente una revisión según las PA-DSS, como se especifica en el presente documento.

6.4.4 PA-QSA

Los PA-QSA son QSA que han recibido la certificación y la capacitación del PCI SSC para realizar revisiones de PA-DSS. Observe que no todos los QSA son PA-QSA. El QSA debe cumplir con requisitos de autorización adicionales para poder ser un PA-QSA.

Los PA-QSA son responsables de:

- Realizar evaluaciones de las aplicaciones de pago de acuerdo con los Procedimientos de evaluación de seguridad y los Requisitos de validación para los PA-QSA.
- Proporcionar una opinión en cuanto a si la aplicación de pago satisface los requisitos de las PA-DSS.
- Proporcionar la documentación adecuada en el ROV para demostrar la conformidad de la aplicación de pago con las PA-DSS.
- Presentar el ROV al PCI SSC junto con la Declaración de validación (firmada por el PA-QSA y el proveedor).
- Mantener un proceso interno de control de calidad para sus tareas del PA-QSA.

Es responsabilidad del PA-QSA declarar si la aplicación de pago logró la debida conformidad. El PCI SSC no aprueba los ROV desde una perspectiva de cumplimiento técnico, sino que realiza revisiones de QA en los informes de validación para garantizar que los informes documenten de manera adecuada la evidencia de conformidad.

6.4.5 Revendedores e integradores

Los revendedores e integradores son entidades que venden, instalan o reparan aplicaciones de pago en representación de proveedores de software u otros. Los revendedores y los integradores son responsables de:
* Implementar una aplicación de pago que cumpla lo establecido en las PA-DSS dentro de un entorno que, a la vez, respete las PCI DSS (o debe instruir al comerciante para que lo haga).
* Configurar la aplicación de pago (cuando se proporcionen opciones de configuración) de acuerdo con la Guía de implementación de las PA-DSS suministrada por el proveedor.
* Configurar la aplicación de pago (o instruir al comerciante para que lo haga) de conformidad con las PCI DSS.
* Realizar el servicio técnico de las aplicaciones de pago (por ejemplo, resolución de problemas, entrega de actualizaciones remotas y prestación de asistencia remota) de acuerdo con la Guía de implementación de las PA-DSS y las PCI DSS.
Los revendedores e integradores no presentan aplicaciones de pago para la evaluación. Únicamente los proveedores pueden presentar productos.

6.4.6 Clientes

Los clientes son comerciantes, prestadores de servicios u otras personas que compran o reciben la aplicación de pago de un tercero con el fin de almacenar, procesar o transmitir datos de titulares de tarjetas como parte de una autorización o liquidación de transacciones de pago. Los clientes que desean utilizar aplicaciones que cumplen con las PA-DSS son responsables de:

- Implementar una aplicación de pago que cumpla lo establecido en las PA-DSS dentro de un entorno que, a la vez, respete las PCI DSS.
- Configurar la aplicación de pago (cuando se proporcionen opciones de configuración) de acuerdo con la Guía de implementación de las PA-DSS suministrada por el proveedor.

Nota:
La aplicación de pago que cumpla únicamente lo establecido en las PA-DSS no garantiza el cumplimiento de las PCI DSS.
- Configurar la aplicación de pago de conformidad con las PCI DSS.
- Mantener el estado de cumplimiento con las PCI DSS tanto para el entorno como para la configuración de la aplicación de pago.

7 Guía de Implementación de las PA-DSS

Las aplicaciones de pago validadas se deben poder implementar de conformidad con las PCI DSS. Los proveedores de software deben proporcionar una Guía de implementación de las PA-DSS para instruir a sus clientes y revendedores/integradores sobre la implementación de un producto seguro, documentar los detalles específicos de configuración segura mencionados en este documento, así como delinear claramente las responsabilidades del proveedor, el revendedor/integrador, y el cliente a fin de que cumplan los requisitos de las PCI DSS. Debe detallar la manera en que el cliente y/o el revendedor/integrador debería activar los valores de configuración de seguridad de la red del cliente. Por ejemplo, la Guía de implementación de las PA-DSS debe considerar las responsabilidades y las características básicas de seguridad de la contraseña de las PCI DSS aun cuando no esté controlada por la aplicación de pago, a fin de que el cliente pueda entender cómo implementar contraseñas seguras para cumplir con lo establecido en las PCI DSS.

Las aplicaciones de pago, cuando se implementan según la Guía de implementación de las PA-DSS y en un entorno que cumpla con las PCI DSS, deben facilitar y respaldar el cumplimiento de las PCI DSS por parte de los clientes.

Consulte el "Anexo A: Resumen de contenidos para la Guía de implementación de las PA-DSS" para comparar las responsabilidades de implementación de los controles que se especifican en la guía.

7.1 Requisitos del Asesor de Seguridad Certificado para las Aplicaciones de Pago (PA-QSA)

- Únicamente los Asesores de Seguridad Certificados para las Aplicaciones de Pago (PA-QSA) empleados por las empresas de Asesores de Seguridad Certificados (QSA) están autorizados para realizar las evaluaciones según las PA-DSS. Consulte la lista de Asesores de Seguridad Certificados en www.pcisecuritystandards.org si desea ver la lista de empresas certificadas para realizar las evaluaciones según las PA-DSS.
- El PA-QSA debe utilizar los procedimientos de pruebas detallados en este documento acerca de las Normas de Seguridad de Datos para las Aplicaciones de Pago.

7.2 Laboratorio de pruebas

- El PA-QSA debe tener acceso al laboratorio donde se lleva a cabo el proceso de validación. Este laboratorio debe poder simular el uso real de la aplicación de pago.
- Consulte el Anexo B: Confirmación de la configuración específica del laboratorio de pruebas de las PA-DSS que aparece en este documento, si desea ver los requisitos detallados de los procesos de laboratorio y los procesos relacionados.
- El PA-QSA debe completar y presentar el Anexo B, según el laboratorio específico utilizado para la aplicación de pago que está siendo revisada, como parte del informe completo de PA-DSS.

7.3 Información sobre la aplicabilidad de las DSS de la PCI

(Extraído de las PCI DSS v1.2)
La siguiente tabla proveniente de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) ilustra los elementos que habitualmente se utilizan

de los datos de titulares de tarjetas y los datos confidenciales de autenticación, independientemente de que esté permitido o prohibido el almacenamiento de dichos datos o de que esos datos deban estar protegidos. Esta tabla no intenta ser exhaustiva, sino que tiene como finalidad ilustrar distintos tipos de requisitos que se aplican a cada elemento de datos.

El número de cuenta principal (PAN) es el factor que define la aplicabilidad de los requisitos de las PCI DSS y las PA-DSS. Si no se almacena, procesa ni transmite el PAN, no se aplicarán las PCI DSS ni las PA-DSS.

	Elemento de datos	**Almacenamiento permitido**	**Protección requerida**	**PCI DSS req. 3, 4**
Datos del titular de la tarjeta	Número de cuenta principal	Si	Sí	Sí
	Nombre del titular de la tarjeta	Si	Si	No
	Código de servicio	Si	Si	No
	Fecha de vencimiento	Si	Si	No
Datos confidenciales de autenticación	Datos completos de la banda magnética	No	N/C	N/C
	CAV2/CID/CVC2/CVV2	No	N/C	N/C
	PIN/Bloqueo de PIN	No	N/C	N/C

7.4 Instrucciones y contenido para el informe de validación

Los PA-QSA utilizarán este documento como plantilla para crear el informe de validación. En el momento de completar el informe de validación, todos los PA-QSA deben seguir las instrucciones establecidas en el documento respecto del contenido y el formato del informe.

El informe de validación debe incluir la siguiente información como un prefacio de los Requisitos y Procedimientos de Evaluación de Seguridad detallados:

1. Descripción del alcance de la revisión
   - Describa el alcance de la cobertura de la revisión, según la sección anterior: Alcance de las PA-DSS.
   - Plazo de validación.
   - Versión de las PA-DSS que se utilizó para la evaluación.
   - Lista de la documentación revisada.

2. Resumen ejecutivo, Incluya lo siguiente:
   - Nombre del producto.
   - Versión del producto y plataformas afines consideradas.
   - Lista de revendedores o integradores para este producto.
   - Sistema/s operativo/s con que se probó la aplicación de pago.
   - Software de base de datos que utilizó o admitió la aplicación de pago.
   - Breve descripción de la aplicación de pago o de la familia de productos (2 ó 3 oraciones).
   - Diagrama de red de una implementación típica de la aplicación de pago (no es necesario que sea una implementación específica que esté en el sitio de un cliente) que incluya, de la manera más detallada posible, lo siguiente:
     - Las conexiones de entrada y salida de la red del cliente.
     - Los componentes que hay dentro de la red del cliente, incluidos los dispositivos POS, los sistemas, las bases de datos y los servidores web según corresponda.
     - Otras aplicaciones de pago o componentes necesarios, según corresponda.
   - Descripción o diagrama de cada pieza del vínculo de comunicación, que incluya: (1) LAN, WAN o Internet, (2) comunicación de software entre servidores y (3) comunicación dentro del servidor en el que se despliega el software (por ejemplo: cómo se comunican entre sí dos procesos diferentes en el mismo servidor).
   - Un diagrama de flujo de datos que muestre todos los flujos de datos de titulares de tarjetas, incluida la autorización, la captura, la liquidación y los flujos de reintegros de cobros, según corresponda.
   - Breve descripción de los archivos y las tablas que almacenan datos de titulares de tarjetas, respaldados por un inventario creado (u obtenido del proveedor de software) y retenido por el PA-QSA en los documentos de trabajo. Para cada almacenamiento (archivo, tabla, etc.) de datos de titulares de tarjetas, este inventario debe incluir:
     - Una lista de todos los elementos correspondientes a los datos almacenados de los titulares de tarjetas.
     - Cómo se asegura el almacenamiento de datos.
     - Cómo se registra el acceso al almacenamiento de datos.
   - Una lista de todos los componentes de software relacionados con la aplicación de pago, incluidos los requisitos y las dependencias de software de terceros.

- Una descripción de los métodos de autenticación completos de la aplicación de pago, incluido el mecanismo de autenticación de la aplicación, la base de datos de la autenticación y la seguridad del almacenamiento de datos.
- Una descripción de la función de la aplicación de pago ante una implementación típica y cuáles son los otros tipos de aplicaciones de pago necesarios para una implementación de pago completa.
- Una descripción del cliente típico al que se le venderá este producto (por ejemplo, una empresa grande o pequeña, ya sea específica de la industria, de Internet o con instalaciones físicas) y la base de clientes del proveedor (por ejemplo, segmento del mercado, nombres de grandes clientes).
- Definición de la metodología de control de versiones del proveedor para describir/ilustrar cómo indica el proveedor los cambios de versión importantes y menores por medio de números de versión, y para definir qué tipos de cambios incluye el proveedor en los cambios de versión importantes y menores.

Tenga en cuenta que el Anexo B: Confirmación de la configuración del laboratorio de pruebas específica para la evaluación de las PA-DSS también se debe completar y presentar junto con el informe completo de las PA-DSS.

3. Conclusiones y observaciones
   - Todos los PA-QSA deben utilizar la siguiente plantilla para proporcionar descripciones y conclusiones detalladas del informe.
   - Describa las pruebas realizadas que no se hayan incluido en la columna de procedimientos de prueba.

4. Información de contacto y fecha del informe
   - Información de contacto del proveedor de software (incluida la dirección URL, el número de teléfono y la dirección de correo electrónico).
   - Información de contacto del PA-QSA (incluido el nombre, el número de teléfono y la dirección de correo electrónico).
   - Información de contacto principal del control de calidad (QA) del PA-QSA (incluido el nombre de contacto del QA principal, el número de teléfono y la dirección de correo electrónico).
   - Fecha del informe

7.5 Pasos de conclusión de las PA-DSS

El presente documento contiene la tabla de Requisitos y Procedimientos de Evaluación de Seguridad y el Anexo B: Confirmación de la configuración del laboratorio de pruebas específica de la evaluación de las PA-DSS, y el Anexo C: Declaración de validación. Los Requisitos y Procedimientos de Evaluación de Seguridad detallan los procedimientos que debe realizar el PA-QSA. El Anexo B: Confirmación de la configuración del laboratorio de pruebas específica de la evaluación de las PA-DSS para confirmar el estado y las capacidades del laboratorio de pruebas que se utilizarán para realizar la evaluación de las PA-DSS. El Anexo C: Declaración de validación está dirigido al PA-QSA y al proveedor de software para que completen y firmen después de completar el informe de validación.

El PA-QSA debe realizar lo siguiente:

a. Completar el informe de validación y utilizar el presente documento como plantilla.
   a. Completar el prefacio del informe de validación, de acuerdo con la sección titulada "Instrucciones y contenido del informe de validación".

b. Completar y documentar todos los pasos detallados en los Requisitos y Procedimientos de Evaluación de Seguridad, incluidas las breves descripciones de los controles observados en la columna "Implementado", y anotar los comentarios necesarios. Tenga en cuenta de que un informe que contiene opiniones en la columna "No implementado" no se debe presentar ante el PCI SSC hasta que todos los elementos figuren en "Implementado".

b. Completar el Anexo B: Confirmación de la configuración específica del laboratorio de pruebas de la evaluación de las PA-DSS.
c. Completar y firmar el Anexo C: Declaración de validación (el PA-QSA y el proveedor de software).
d. Una vez completos, debe presentar todos los documentos mencionados anteriormente ante el PCI SSC según la Guía del programa PA-DSS.

7.6 Guía del programa PA-DSS

Consulte la Guía del programa PA-DSS para obtener información sobre la gestión del programa de las PA-DSS, incluidos los siguientes temas:

- Presentación del informe de PA-DSS y los procesos de aceptación.
- Proceso de renovación anual para las aplicaciones de pago incluidas en la lista de aplicaciones validadas según las PA-DSS.
- Transición de las aplicaciones validadas según las PABP a la lista de aplicaciones de pago validadas según las PA-DSS.
- Responsabilidades de notificación en caso de que se determine que una aplicación de pago publicada no cumple con algún compromiso.

El PCI SSC se reserva el derecho de requerir una revalidación por cambios significativos a las Normas de Seguridad de Datos para las Aplicaciones de Pago y/o por vulnerabilidad identificadas específicamente en una aplicación de pago publicada.

7.7 Requisitos y Procedimientos de Evaluación de Seguridad de de las PCI DSS

Requisitos de las PA-DSS	Procedimientos de prueba
1. No retenga toda la banda magnética, el código de validación de la tarjeta ni el valor (CAV2, CID, CVC2, CVV2), ni los datos de bloqueo del PIN.	
1.1 No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados): Los datos confidenciales de autenticación incluyen los datos mencionados en los requisitos 1.1.1 a 1.1.3 establecidos a continuación. *Requisito de las Normas de Seguridad de Datos PCI 3.2* *Nota: Al prohibir el almacenamiento de datos confidenciales de autenticación "después de la autorización", se considera que la transacción completó el proceso de autorización y que el cliente recibió la aprobación definitiva de la transacción. Una vez completa la autorización, no se podrán almacenar estos datos confidenciales de autenticación.*	1.1 Si se almacenan datos confidenciales de autenticación (vea los puntos 1.1.1 a 1.1.3 más adelante) antes de la autorización y, luego, se borran, revise la metodología para borrar los datos, a fin de determinar que los datos sean irrecuperables. Para cada rubro de datos confidenciales de autenticación que aparece a continuación, cumpla los siguientes pasos una vez que haya completado las numerosas transacciones de prueba que simulan todas las funciones de la aplicación de pago, a fin de incluir la generación de todas las condiciones de error y las entradas de registro.
1.1.1 Después de la autorización, no almacene contenidos completos de ninguna pista de la banda magnética (ubicada en el reverso de la tarjeta, en un chip o en cualquier otro dispositivo). Estos datos se denominan alternativamente, pista completa, pista, pista 1, pista 2 y datos de banda magnética. En el transcurso normal de los negocios, es posible que se deban retener los siguientes elementos de datos de la banda magnética: * El nombre del titular de la cuenta. * Número de cuenta principal (PAN). * Fecha de vencimiento. * Código de servicio. Para minimizar el riesgo, almacene solamente los elementos de datos que sean necesarios para el negocio. Nota: Consulte el Glosario de términos, abreviaturas y acrónimos de las PCI DSS para obtener más información. Requisito 3.2.1 de las Normas de Seguridad de Datos PCI	1.1.1 Utilice herramientas y/o métodos forenses (herramientas comerciales, secuencias de comandos, etc.) fn para examinar los resultados creados por la aplicación de pago y comprobar que todo el contenido de las pistas de la banda magnética que se encuentra en el reverso de la tarjeta no quede almacenado después de la autorización. Incluya los siguientes tipos de archivos (y cualquier otro resultado generado por la aplicación de pago): * Datos de transacciones entrantes * Todos los registros (por ejemplo, transacciones, historiales, depuración, error) * Archivos de historial * Archivos de seguimiento * Memoria no volátil, incluida la memoria caché no volátil * Esquemas de bases de datos * Contenidos de bases de datos

1.1.2 Después de la autorización, no almacene el valor ni el código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago) que se utiliza para verificar las transacciones de tarjetas ausentes. Nota: Consulte el Glosario de términos, abreviaturas y acrónimos de las PCI DSS para obtener más información. Requisito 3.2.2 de las Normas de Seguridad de Datos PCI	1.1.2 Utilice herramientas y/o métodos forenses (herramientas comerciales, secuencias de comandos, etc.)fn para examinar los resultados creados por la aplicación de pago y verificar que el código de validación de la tarjeta de tres o cuatro dígitos impreso en el anverso de la tarjeta o en el panel de firma (datos CVV2, CVC2, CID, CAV2) no quede almacenado después de la autorización. Incluya los siguientes tipos de archivos (y cualquier otro resultado generado por la aplicación de pago): * Datos de transacciones entrantes * Todos los registros (por ejemplo, transacciones, historiales, depuración, error) * Archivos de historial * Archivos de seguimiento * Memoria no volátil, incluida la memoria caché no volátil * Esquemas de bases de datos * Contenidos de bases de datos
1.1.3 Después de la autorización, no almacene el número de identificación personal (PIN) ni el bloqueo del PIN cifrado. Nota: Consulte el Glosario de términos, abreviaturas y acrónimos de las PCI DSS para obtener más información. Requisito 3.2.3 de las Normas de Seguridad de Datos PCI	1.1.3 Utilice herramientas y métodos forenses (herramientas comerciales, secuencias de comandos, etc.)5 para examinar los resultados creados por la aplicación de pago y comprobar que los PIN y los bloqueos de PIN cifrados no queden almacenados después de la autorización. Incluya los siguientes tipos de archivos (y cualquier otro resultado generado por la aplicación de pago): * Datos de transacciones entrantes * Todos los registros (por ejemplo, transacciones, historiales, depuración, error) * Archivos de historial * Archivos de seguimiento * Memoria no volátil, incluida la memoria caché no volátil * Esquemas de bases de datos * Contenidos de bases de datos
1.1.4 Borre de manera segura los datos que haya en la banda magnética, los valores o los códigos de validación de la tarjeta y los PIN o los datos de bloqueo de PIN almacenados por versiones anteriores de la aplicación de pago de acuerdo con las normas aceptadas de la industria para una eliminación segura y según se define, por ejemplo, en la lista de productos aprobados de la Agencia de Seguridad Nacional u otra norma o reglamentación estatal o nacional. Requisito de las Normas de Seguridad de Datos PCI 3.2 Nota: Este requisito solamente se implementa cuando existen versiones anteriores de la aplicación de pago que hayan almacenado datos confidenciales de autenticación.	1.1.4.a Revise la Guía de implementación de las PA-DSS preparada por el proveedor y compruebe que la documentación incluya las siguientes instrucciones para los clientes y los revendedores/integradores: * Se deben eliminar los datos históricos (datos de la banda magnética, códigos de validación de la tarjeta, PIN o bloqueos de PIN almacenados por versiones anteriores de la aplicación de pago). * Se deben explicar cómo eliminar los datos históricos. * Se debe explicar que dicha eliminación es absolutamente necesaria para cumplir lo establecido en las PCI DSS. 1.1.4.b Verifique que el proveedor proporcione una herramienta o un procedimiento de limpieza seguro para eliminar los datos. 1.1.4.c Verifique que, mediante el uso de herramientas y/o métodos forenses, la herramienta o procedimiento de limpieza seguro elimine el material criptográfico de manera segura.
1.1.5 Borre de manera segura los datos confidenciales de autenticación (datos previos a la autorización) que se utilizan con fines de depuración o resolución de problemas desde los archivos de registro, los archivos de depuración y otras fuentes de datos que se reciben de parte de	1.1.5.a Examine los procedimientos del proveedor de software para solucionar los problemas de los clientes y verifique que se realice lo siguiente en los procedimientos: * Reúna datos confidenciales de autenticación cuando sea necesario resolver un problema

los clientes, a fin de asegurar que los datos de banda magnética, los códigos o valores de validación de la tarjeta y los PIN o los datos de bloqueo de PIN no queden almacenados en los sistemas del proveedor de software. Estas fuentes de datos se deben recopilar en cantidades limitadas y solo cuando sea necesario para resolver un problema, se deben cifrar cuando se almacenan y se deben borrar inmediatamente después de ser utilizadas. Requisito de las Normas de Seguridad de Datos PCI 3.2	específico. * Almacene dichos datos en ubicaciones específicas y conocidas que tengan acceso limitado. * Reúna una cantidad limitada de datos necesarios para resolver un problema específico. * Cifre datos confidenciales de autenticación cuando los almacena. * Borre de manera segura dichos datos inmediatamente después de utilizarlos. 1.1.5.b Seleccione una muestra de pedidos de resolución de problemas que los clientes hayan realizado recientemente y verifique que cada acontecimiento haya seguido el procedimiento analizado en el punto 1.1.5.a.
	1.1.5.c Revise la Guía de implementación de las PA-DSS preparada por el proveedor y compruebe que la documentación incluya las siguientes instrucciones para los clientes y los revendedores/integradores: * Reúna datos confidenciales de autenticación cuando sea necesario resolver un problema específico. * Almacene dichos datos en ubicaciones específicas y conocidas que tengan acceso limitado. * Reúna solamente una cantidad limitada de datos necesarios para resolver un problema específico. * Cifre datos confidenciales de autenticación cuando los almacena. * Borre de manera segura dichos datos inmediatamente después de utilizarlos.
2. Proteja los datos del titular de la tarjeta que fueron almacenados	
2.1 El proveedor de software debe guiar a los clientes sobre cómo purgar los datos del titular de la tarjeta después de que haya caducado el período de retención definido por el cliente. Requisito de las Normas de Seguridad de Datos PCI 3.1	2.1.a Revise la Guía de implementación de las PA-DSS preparada por el proveedor y compruebe que la documentación incluya las siguientes instrucciones para los clientes y los revendedores/integradores: * Se deben purgar los datos del titular de la tarjeta que excedan el período de retención definido por el cliente. * Se deben incluir todas las ubicaciones en las que la aplicación de pago almacena datos del titular de la tarjeta (para que el cliente conozca las ubicaciones de los datos que deben ser borrados).
2.2 Oculte el PAN cuando aparezca (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá). Notas: * Este requisito no se aplica a esos trabajadores y a otras partes que posean una necesidad comercial legítima de conocer el PAN completo. * Este requisito no reemplaza los requisitos más estrictos que fueron implementados y que aparecen en los datos del titular de la tarjeta (por ejemplo, los recibos de puntos de venta [POS]). Requisito de las Normas de Seguridad de Datos PCI 3.3	2.2 Revise las vistas de datos de la tarjeta, incluidos, por ejemplo, los dispositivos de POS, las pantallas, los registros y los recibos, para determinar que los números de la tarjeta de crédito se oculten en el momento de visualizar los datos del titular de la tarjeta, salvo quienes estén por razones comerciales legítimas deban ver todos los números de la tarjeta de crédito.
2.3 Haga que el PAN quede, como mínimo, ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles y en registros) utilizando cualquiera de los siguientes métodos: * Valores hash de una vía en criptografía sólida * Truncamiento. * Token y ensambladores de índices (los ensambladores se deben almacenar de manera segura). * Criptografía sólida con procesos y procedimientos de gestión de claves relacionadas.	2.3.a Verifique que el PAN quede ilegible en todo lugar donde se almacene, de acuerdo con el requisito 3.4. de las PCI DSS. 2.3.b Si el proveedor de software almacena el PAN por alguna razón (por ejemplo, porque se recibieron de parte de los clientes archivos de registro, de depuración y otras fuentes de datos para fines de depuración o resolución de problemas), verifique que el PAN quede ilegible de acuerdo con el requisito 3.4. de las PCI DSS.

La información de cuenta MÍNIMA que se debe dejar ilegible es el PAN. Requisito de las Normas de Seguridad de Datos PCI 3.4 Se debe dejar ilegible el PAN en todo lugar donde se almacene, incluso fuera de la aplicación de pago. Nota: La "criptografía sólida" se define en el Glosario de términos, abreviaturas y acrónimos de las PCI DSS.	
2.4 Si se utiliza cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independientemente de los mecanismos de control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales). Las claves de descifrado no deben estar vinculadas a cuentas de usuarios. Requisito de las Normas de Seguridad de Datos PCI 3.4.1	2.4 Si se utiliza el descifrado de disco, verifique que se implemente de acuerdo con los requisitos 3.4.1.a a 3.4.1.c. de las PCI DSS.
2.5 La aplicación de pago debe proteger las claves de cifrado que se utilizan para cifrar los datos los titulares de tarjetas contra su posible divulgación o uso indebido. Requisito de las Normas de Seguridad de Datos PCI 3.5	2.5 Compruebe que la aplicación de pago proteja las claves contra su divulgación o uso indebido, según los requerimientos de las PCI DSS 3.5.1 y 3.5.2.
2.6 La aplicación de pago debe implementar procesos y procedimientos de gestión de las claves criptográficas utilizadas en el cifrado de datos de titulares de tarjetas. Requisito de las Normas de Seguridad de Datos PCI 3.6	2.6 Verifique que las aplicaciones de pago implementen técnicas de gestión de claves para claves criptográficas, según los requerimientos de las PCI DSS 3.6.1 a 3.6.8.
2.7 Borre de manera segura todo material criptográfico clave o criptograma almacenado por versiones anteriores de la aplicación de pago de acuerdo con las normas aceptadas de la industria para una eliminación segura y según se define, por ejemplo, en la lista de productos aprobados de la Agencia de Seguridad Nacional u otra norma o reglamentación estatal o nacional. Estas son las claves criptográficas que se utilizan para cifrar o verificar los datos de titulares de tarjetas.	2.7 a Revise la Guía de implementación de las PA-DSS preparada por el proveedor y compruebe que la documentación incluya las siguientes instrucciones para los clientes y los revendedores/integradores: * Se debe eliminar el material criptográfico. * Se debe explicar cómo eliminar el material criptográfico. * Se debe explicar que dicha eliminación es absolutamente necesaria para cumplir lo establecido en las PCI DSS. * Cómo volver a cifrar datos históricos con claves nuevas.
Requisito de las Normas de Seguridad de Datos PCI 3.6 Nota: Este requisito solamente se pondrá en práctica en caso de que haya versiones anteriores de la aplicación de pago que hayan utilizado materiales criptográficos clave o criptogramas para cifrar datos de titulares de tarjetas.	2.7.b Verifique que el proveedor proporcione una herramienta o un procedimiento de limpieza seguro para eliminar el material criptográfico. 2.7.c Verifique, mediante el uso de herramientas y/o métodos forenses, que la herramienta o el procedimiento de limpieza seguro elimine el material criptográfico de manera segura de acuerdo con las normas aceptadas en la industria para una eliminación segura de los datos.
3. Provea las funciones de autenticación segura[4]	
3.1 La instalación simple de la aplicación de pago implementada al completarse el proceso de instalación debe facilitar el uso de ID de usuario únicas y una autenticación segura (definida en los requisitos 8.1, 8.2 y 8.5.8 a 8.5.15 de las PCI DSS) para el acceso administrativo y para el acceso a los datos de titulares de tarjetas.	3.1.a Pruebe la aplicación de pago para verificar si se requieren ID de usuario únicas y una autenticación segura para todo el acceso administrativo y para todo el acceso a los datos de titulares de tarjetas, de acuerdo con los requisitos 8.1, 8.2 y 8.5.8 a 8.5.15 de las PCI DSS.

[4] En los procedimientos de prueba fueron cambiadas las referencias a contraseñas "fuertes" o "complejas" por "autenticación segura" a fin de incluir otras formas de autenticación (tokens, biometría, etc...)

Requisitos 8.1, 8.2 y 8.5.8 a 8.5.15 de las Normas de Seguridad de Datos PCI	3.1.b Pruebe la aplicación de pago para verificar que se no utilicen cuentas administrativas predeterminadas para otro software necesario y que no se requiera su uso (por ejemplo, la aplicación de pago no debe utilizar la cuenta administrativa para el software de base de datos).
Nota: No se intenta que los controles de contraseña sean aplicados a los empleados que únicamente tienen acceso a un solo número de tarjeta por vez para facilitar una sola transacción. Estos controles son aplicables para el acceso de los empleados con habilitaciones administrativas, para el acceso a servidores con datos de titulares de tarjetas y para el acceso controlado por la aplicación de pago. Este requisito debe implementarse en la aplicación de pago y en todas las herramientas relacionadas que se utilizan para ver o acceder a los datos de titulares de tarjetas.	3.1.c Consulte la Guía de implementación de las PA-DSS creada por el vendedor para verificar lo siguiente: * Se les aconseja a los clientes y los revendedores/ integradores no utilizar cuentas administrativas predeterminadas para los inicios de sesión de la aplicación de pago (por ejemplo, no utilice la cuenta "sa" para el acceso de la aplicación de pago a la base de datos). * Los clientes y los revendedores/integradores deben asignar una autenticación segura a estas cuentas predeterminadas (aun cuando no se utilicen) y, luego, debe desactivar las cuentas o no utilizarlas. * Siempre que sea posible, los clientes y los revendedores/ integradores deben asignar una autenticación segura para las aplicaciones y los sistemas de pago. * A los clientes y a los revendedores/integradores se los asesora sobre cómo crear una autenticación segura que cumpla lo establecido en las PCI-DSS para acceder a la aplicación de pago de conformidad con los requisitos 8.5.8 a 8.5.15 de las PCI DSS. * A los clientes y revendedores/integradores se les aconseja que si cambian los valores de configuración de la instalación simple para las ID únicas y una autenticación segura se violarán las PCI-DSS.
3.2 El acceso a computadoras, servidores y bases de datos con aplicaciones de pago debe requerir una ID única y una autenticación segura. Requisitos de las Normas de Seguridad de Datos PCI 8.1 y 8.2	3.2 Consulte la Guía de implementación de las PA-DSS creada por el proveedor para verificar que se les sugiera firmemente a los clientes y los revendedores/integradores que controlen el acceso a cualquier computadora, servidor y base de datos que tenga aplicaciones de pago y datos de titulares de tarjetas por medio de una ID única y una autenticación segura que cumpla con las PCI DSS.
3.3 Durante la transferencia y el almacenamiento de datos, haga ilegibles las contraseñas de aplicaciones de pago mediante la criptografía sólida basada en normas aprobadas Nota: La "criptografía sólida" se define en el Glosario de términos, abreviaturas y acrónimos de las PCI DSS. Requisito de las Normas de Seguridad de Datos PCI 8.4	3.3 Controle los archivos de contraseña de la aplicación de pago durante el almacenamiento y la transmisión a fin de verificar que las contraseñas sean ilegibles en todo momento.
4. Registre la actividad de la aplicación de pago	
4.1 En el momento de completarse el proceso de instalación, la instalación simple predeterminada de la aplicación de pago debe registrar todos los accesos de los usuarios (en especial de los que tienen privilegios administrativos), y debe poder vincular todas las actividades con usuarios individuales. ***Requisito de las Normas de Seguridad de Datos PCI 10.1***	4.1 Controle los valores de configuración de la aplicación de pago para verificar que las pistas de auditoría se activen automáticamente o estén a disposición de los clientes para ser activadas.
4.2 La aplicación de pago debe implementar una pista de auditoría automatizada para rastrear y supervisar el acceso. *Requisitos de las Normas de Seguridad de*	4.2.a Consulte los parámetros de registro de la aplicación de pago y verifique que los registros contengan los datos exigidos en los requisitos 10.2.1 a 10.2.7 y 10.3.1 a 10.3.6.

Datos PCI 10.2 y 10.3	4.2.b Si los valores de configuración del registro de la aplicación de pago pueden ser configurados por el cliente y los revendedores/integradores, o los clientes o los revendedores/integradores son responsables de implementar el registro, repase la *Guía de implementación de las PA-DSS* preparada por el proveedor para comprobar que la documentación incluya lo siguiente: Cómo configurar los valores de configuración del registro para que cumplan con lo establecido en las PCI DSS según los requisitos 10.2.1 a 10.2.7 y 10.3.1 a 10.3.6 de las PCI DSS. Que no se desactiven los registros y que no se incumplan las PCI DSS.
5. Desarrolle aplicaciones de pago seguras	
5.1 Desarrolle aplicaciones de software conforme a las DSS de la PCI (por ejemplo, registro y autenticación seguros) sobre la base de las mejores prácticas de la industria e incorpore la seguridad de la información en todo el ciclo de desarrollo de software. Los procesos deben incluir lo siguiente: ***Requisito de las Normas de Seguridad de Datos PCI 6.3***	5.1. Obtenga los procesos de desarrollo del software escritos y examínelos para verificar que estén basados en las normas de la industria y que se considere la seguridad en todo su ciclo de vida y que se desarrollen las aplicaciones de software conforme a las DSS de la PCI. A partir de un examen de los procesos de desarrollo del software escritos, las entrevistas con los desarrolladores de software y la inspección de los datos relevantes (documentación de la configuración de la red, los datos de producción y prueba, etc.), verifique lo siguiente:
5.1.1 Las pruebas de todos los parches de seguridad y la configuración del sistema y del software cambian antes de su despliegue, incluidas, entre otras, las pruebas de lo siguiente.	5.1.1 Se prueben, antes de su despliegue, todos los cambios en los parches de seguridad y en la configuración del sistema y del software, incluidas, entre otras, las pruebas de lo siguiente.
5.1.1.1 Validación de todas las entradas (para prevenir el lenguaje de comandos entre distintos sitios, los errores de inyección, la ejecución de archivos maliciosos, etc.).	5.1.1.1 Validación de todas las entradas (para prevenir el lenguaje de comandos entre distintos sitios, los errores de inyección, la ejecución de archivos maliciosos, etc.).
5.1.1.2 Validación de un correcto manejo de los errores.	5.1.1.2 Validación de un correcto manejo de los errores.
5.1.1.3 Validación del almacenamiento criptográfico seguro.	5.1.1.3 Validación del almacenamiento criptográfico seguro.
5.1.1.4 Validación de las comunicaciones seguras.	5.1.1.4 Validación de las comunicaciones seguras.
5.1.1.5 Validación de un correcto control del acceso basado en funciones (RBAC).	5.1.1.5 Validación de un correcto control del acceso basado en funciones (RBAC).
5.1.2 Desarrollo/prueba por separado y entornos de producción.	5.1.2 Los entornos de prueba/desarrollo están separados del entorno de producción y se implementa un control del acceso para reforzar la separación.
5.1.3 Separación de funciones entre desarrollo/ prueba y entornos de producción.	5.1.3 Existe una separación de funciones entre el personal asignado a los entornos de desarrollo/prueba y los asignados al entorno de producción.
5.1.4 Los PAN activos no se utilizan para las pruebas ni para el desarrollo.	5.1.4 Los PAN activos no se utilizan para las pruebas ni para el desarrollo ni se desinfectan antes de ser utilizados.
5.1.5 Eliminación de datos y cuentas de prueba antes de que se activen los sistemas de producción	5.1.5 Los datos y las cuentas de prueba se eliminan antes de que se active el sistema de producción.
5.1.6 Eliminación de las cuentas, las ID de usuario y las contraseñas personalizadas de la aplicación de pago antes de que se les envíen a los clientes las aplicaciones de pago.	5.1.6 Personalización de las cuentas, las ID de usuario y las contraseñas de la aplicación de pago antes de que se les envíen a los clientes las aplicaciones de pago.
5.1.7 Revisión del código de la aplicación de pago antes del envío a los clientes después de que surja algún cambio significativo, a fin de identificar la potencial vulnerabilidad de la codificación. Nota: Este requisito de revisión de códigos se aplica a todos los componentes de las aplicaciones da pago (tanto internos como públicos) como parte del ciclo de vida de desarrollo del sistema	5.1.7.a Confirme que el proveedor realice revisiones de códigos de todos los cambios de código de aplicación de las aplicaciones internas (ya se mediante proceso automáticos o manuales) de la siguiente manera: * Los cambios a los códigos se revisan por individuos distintos al autor que originó el código y por individuos con conocimiento en técnicas de revisión de código y prácticas seguras de

que exige el requisito 5.1 de las normas PA-DSS y el 6.3 de las PCI DSS. Las revisiones de los códigos se pueden realizar por terceros o personal interno con conocimiento.	codificación. * Las correcciones pertinentes se implementan antes de su lanzamiento. * La gerencia revisa y aprueba los resultados de la revisión de códigos antes de su lanzamiento
	5.1.7.b Confirme que el proveedor realice revisiones de códigos de todos los cambios de código de aplicación de las aplicaciones web (ya se mediante procesos automáticos o manuales) de la siguiente manera: * Los cambios a los códigos se revisan por individuos distintos al autor que originó el código y por individuos con conocimiento en técnicas de revisión de código y prácticas seguras de codificación. * Las revisiones de los códigos aseguran que los códigos se desarrollen conforme a lineamientos de codificación segura como la Guía para proyectos abiertos de seguridad web. (Consulte los requisitos de las normas PA-DSS 5.2 y los correspondientes a las normas PCI DSS 6.5.) * Las correcciones pertinentes se implementan antes de su lanzamiento. * La gerencia revisa y aprueba los resultados de la revisión de códigos antes de su lanzamiento.
5.2 Desarrolle todas las aplicaciones de pago web (internas y externas, que incluyan acceso administrativo web al producto) basadas en las directrices de codificación segura, como la Guía para proyectos de seguridad de aplicaciones web abiertas. Considere la prevención de las vulnerabilidades de codificación comunes en los procesos de desarrollo de software, a fin de incluir: Nota: Las vulnerabilidades enumeradas en los requisitos PA DSS 5.2.1 a 5.2.10 y en las normas PCI DSS 6.5.1 a 6.5.10 de la guía OWASP eran actuales en el momento de publicación de las normas PCI DSS v1.2. Sin embargo, al actualizar la guía OSWAP, y si se actualiza, la versión actual se debe utilizar para estos requisitos. Requisito de las Normas de Seguridad de Datos PCI 6.5	5.2.a. Obtenga los procesos de desarrollo de software y revíselos para las aplicaciones basadas en la web (internas y externas, que incluyen acceso administrativo web al producto). Compruebe que el proceso incluya capacitación acerca de las técnicas de codificación segura para desarrolladores y que esté basado en una guía, como la Guía de OWASP (http://www.owasp.org). Entreviste a un grupo modelo de desarrolladores y obtenga evidencias de que son expertos en técnicas de codificación segura.
	5.2.b. Respecto de las aplicaciones de pago web incluidas en la revisión, compruebe que no queden desprotegidas ante las vulnerabilidades de codificación habituales mediante una prueba de penetración manual o automática que específicamente intente aprovechar cada una de las siguientes situaciones:
5.2.1. Lenguaje de comandos entre distintos sitios (XSS).	5.2.1 Lenguaje de comandos entre distintos sitios (XSS) (valide todos los parámetros antes de su inclusión).
5.2.2 Errores de inyección, en especial, errores de inyección SQL También considere los errores de inyección LDAP y Xpath, así como otros errores de inyección.	5.2.2 Errores de inyección, en especial, errores de inyección SQL (valide la entrada para verificar que los datos del usuario no pueden modificar el significado de los comandos ni el de las consultas).
5.2.3. Ejecución de archivos maliciosos.	5.2.3 Ejecución de archivos maliciosos (valide la entrada para verificar que la aplicación no acepte nombres de archivos ni archivos de los usuarios).
5.2.4 Referencias inseguras a objetos directos	5.2.4 Referencias inseguras a objetos directos (no exponga a los usuarios las referencias a objetos internos).
5.2.5 Falsificación de solicitudes entre distintos sitios (CSRF).	5.2.5 Falsificación de solicitudes entre distintos sitios (CSRF) (no confíe en las credenciales de autorización ni en los tokens que los exploradores presentan automáticamente)
5.2.6 Filtración de información y manejo inadecuado de errores	5.2.6 Filtración de información y manejo inadecuado de errores (no filtre información por

	medio de mensajes de error u otros medios).
5.2.7 Autenticación y administración de sesión interrumpidas.	5.2.7 Autenticación y administración de sesión interrumpidas (autentique correctamente a los usuarios y proteja las credenciales de cuentas y los tokens de sesión).
5.2.8 Almacenamiento criptográfico inseguro	5.2.8 Almacenamiento criptográfico inseguro (prevenga errores criptográficos).
5.2.9 Comunicaciones inseguras	5.2.9 Comunicaciones inseguras (cifre correctamente todas las comunicaciones autenticadas y confidenciales).
5.2.10 Omisión de restringir el acceso URL	5.2.10 Omisión de restringir el acceso a URL (refuerce constantemente el control del acceso en la capa de presentación y la lógica comercial para todas las URL).
5.3 El proveedor de software debe seguir los procedimientos de control de cambios para todos los cambios que surjan en la configuración del software de productos. Los procedimientos deben incluir lo siguiente: Requisito de las Normas de Seguridad de Datos PCI 6.4	5.3.a Obtenga y consulte los procedimientos de control de cambios del proveedor para las modificaciones del software y verifique que los procedimientos exijan los puntos 5.3.1 a 5.3.4 que aparecen a continuación.
	5.3.b Examine los cambios recientes en la aplicación de pago y realice un seguimiento de los cambios relacionados con la documentación de control de cambios. Verifique que, para cada cambio examinado, se haya documentado lo siguiente de acuerdo con los procedimientos de control de cambios:
5.3.1 Documentación de incidencia	5.3.1 Verifique que la documentación que tiene incidencia en el cliente se incluya en la documentación de control de cambios de cada cambio.
5.3.2 Aprobación de la gerencia a cargo de las partes pertinentes	5.3.2 Verifique que la aprobación de la gerencia a cargo de las partes pertinentes esté presente en cada cambio.
5.3.3 Pruebas de la funcionalidad operativa	5.3.3 Verifique que se hayan realizado las pruebas de funcionalidad operativa para cada cambio.
5.3.4 Procedimientos de detención o desinstalación del producto	5.3.4 Verifique que los procedimientos de detención o desinstalación del producto estén preparados para cada cambio.
5.4 La aplicación de pago no debe utilizar ni requerir el uso de servicios y protocolos innecesarios e inseguros (por ejemplo, NetBIOS, posibilidad de compartir archivos, Telnet, FTP descifrada, etc.). Requisito de las Normas de Seguridad de Datos PCI 2.2.2	5.4 Consulte los servicios de sistema, los daemons y los protocolos activados o requeridos por la aplicación de pago. Verifique que los servicios o protocolos innecesarios e inseguros no queden activados de manera predeterminada ni sean requeridos por la aplicación de pago (por ejemplo, no está activado el FTP o está cifrado por medio de una SSH u otra tecnología).
6. Proteja las transmisiones inalámbricas	
6.1 En cuanto a las aplicaciones de pago que utilizan tecnología inalámbrica, la tecnología inalámbrica se debe implementar de manera segura. Requisito de las Normas de Seguridad de Datos PCI 1.2.3 y 2.1.1	6.1.a En cuanto a las aplicaciones de pago desarrolladas por el proveedor con tecnología inalámbrica y otras aplicaciones inalámbricas combinadas con la aplicación de pago, verifique que las aplicaciones inalámbricas no utilicen los valores de configuración predeterminados por el proveedor y que se configuren de acuerdo con el requisito de la norma de seguridad de datos PCI
	6.1.b Consulte la Guía de implementación de las PA-DSS preparada por el proveedor para verificar que los clientes y los revendedores/integradores

	reciban instrucciones, cuando se utilice la modalidad inalámbrica, para instalar un firewall según el requisito 1.3.8 de las PCI DSS.
6.2 Para las aplicaciones de pago que utilizan tecnologías inalámbricas, estas aplicaciones deben facilitar el uso de las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) a los efectos de implementar cifrados sólidos para la autenticación y transmisión. Con el fin de simplificar la utilización de WEP, las aplicaciones de pago que usen tecnologías inalámbricas deberán facilitar lo siguiente: * En el caso de nuevas implementaciones inalámbricas, se prohíbe la implementación WEP después del 31 de marzo de 2009. * En el caso de actuales implementaciones inalámbricas, se prohíbe la implementación WEP después del 30 de junio de 2010. Requisito de las Normas de Seguridad de Datos PCI 4.1.1	6.2.a En cuanto a las aplicaciones de pago desarrolladas por el proveedor con tecnología inalámbricas y otras aplicaciones inalámbricas combinadas con la aplicación del proveedor, verifique se hayan utilizado las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) para incluir o facilitar el cifrado sólido para la autenticación y transmisión, de acuerdo con el requisito 4.1.1. de las PCI DSS.
	6.2.b Si los clientes pudieran implementar la aplicación de pago en un entorno inalámbrico, consulte la Guía de implementación de las PA-DSS preparada por el proveedor para verificar si los clientes y los revendedores/integradores han recibido instrucciones sobre los valores de configuración inalámbricos que cumplen con las PCI DSS, según los requisitos 1.3.8, 2.1.1 y 4.1.1. de las PCI DSS.
7. Pruebe las aplicaciones de pago para tratar las vulnerabilidades	
7.1 Los proveedores de software deben establecer un proceso para identificar las vulnerabilidades de seguridad que se hayan descubierto recientemente (por ejemplo, suscribirse a servicios de alerta gratuitos por Internet) y para realizar pruebas en las aplicaciones de pago a fin de advertir vulnerabilidades. En este proceso, se debe incluir todo software o sistema subyacente que provea o requiera la aplicación de pago (por ejemplo, los servidores web, programas y bibliotecas de terceros). Requisito de las Normas de Seguridad de Datos PCI 6.2	7.1.a Obtenga y consulte los procesos para identificar las nuevas vulnerabilidades y para probar las aplicaciones de pago respecto de nuevas vulnerabilidades. Verifique que los procesos incluyan: * El uso de fuentes externas para obtener información sobre vulnerabilidad de la seguridad. * Las pruebas de aplicaciones de pago respecto de nuevas vulnerabilidades.
	7.1.b Verifique que los procesos para identificar las nuevas vulnerabilidades e implementar correcciones en la aplicación de pago sean de aplicación en todo el software que provee o exige la aplicación de pago (por ejemplo, servidores web, programas y bibliotecas de terceros).
7.2 Los proveedores de software deben establecer un proceso para el desarrollo y la implementación oportunos de parches y actualizaciones de seguridad, que incluya la entrega de actualizaciones y parches de manera segura con una conocida cadena de confianza, y el mantenimiento de la integridad del código de parche y actualización durante la entrega y la implementación.	7.2.a Obtenga los procesos y examínelos para desarrollar e implementar los parches y las actualizaciones de seguridad para el software. Verifique que los procesos incluyan: * Desarrollo e implementación oportunos de parches dirigidos a los clientes. * Entrega de parches y actualizaciones de manera segura con una conocida cadena de confianza. * Entrega de parches y actualizaciones a fin de mantener la integridad de lo que se entrega. * Pruebas de la integridad del parche o actualización a cargo del sistema objetivo antes de la instalación.
	7.2.b Para verificar que se mantenga la integridad del código del parche y la actualización, ejecute el proceso de actualización con código arbitrario y determine si el sistema permitirá que se lleve a cabo la actualización.
8. Facilite la implementación de una red segura	
8.1 La aplicación de pago debe ser capaz de implementarse en un entorno de red seguro. La aplicación no debe interferir con el uso de dispositivos, aplicaciones ni configuraciones que se requieran para cumplir con las PCI-DSS (por ejemplo, la aplicación de pago no puede interferir en la protección antivirus, las configuraciones de firewall ni ningún otro dispositivo, aplicación o	8.1 Pruebe la aplicación de pago en un laboratorio para obtener pruebas de que se puede ejecutar en una red que cumple plenamente con lo establecido en las PCI DSS. Verifique que la aplicación de pago no inhiba la instalación de parches ni actualizaciones a otros componentes del entorno.

configuración que se requiera para cumplir en las PCI-DSS). Requisitos 1, 3, 4, 5, y 6.6 de las Normas de Seguridad de Datos PCI	
9. Los datos de titulares de tarjetas nunca se deben almacenar en un servidor conectado a Internet	
9.1 La aplicación de pago se debe desarrollar de manera que el servidor de base de datos y el servidor web no tengan que estar en el mismo servidor ni se requiera que el servidor de base de datos se encuentre en la DMZ del servidor web. Requisito de las Normas de Seguridad de Datos PCI 1.3.2	9.1.a Para verificar si la aplicación de pago almacena los datos de titulares de tarjetas en la red interna, y nunca en la DMZ, obtenga evidencia de que la aplicación de pago no requiere el almacenamiento de datos en la DMZ y de que permitirá el uso de una DMZ para separar Internet de los sistemas que almacenan los datos de titulares de tarjetas (por ejemplo, la aplicación de pago no debe requerir que el servidor de la base de datos y el servidor web estén en el mismo servidor ni en la DMZ del servidor web).
	9.1.b Si los clientes pudieran almacenar datos de titulares de tarjetas en un servidor conectado a Internet, consulte la Guía de implementación de las PA-DSS preparada por el proveedor para verificar si a los clientes y revendedores/integradores se les informó que no deben almacenar estos datos en sistemas a los que se pueda acceder desde Internet (por ejemplo, el servidor web y el servidor de la base de datos no deben estar en el mismo servidor).
10. Facilite actualizaciones de software remotas y seguras	
10.1 Si las actualizaciones de la aplicación de pago se entregan mediante acceso remoto a los sistemas de los clientes, los proveedores de software deben informales a los clientes que enciendan las tecnologías de acceso remoto solamente cuando sea necesario para realizar descargas desde el proveedor y que lo apaguen inmediatamente después de finalizada la descarga. De manera alternativa, si se entregan por medio de VPN u otra conexión de alta velocidad, los proveedores de software deben sugerirles a sus clientes cómo configurar correctamente un firewall o un producto firewall personal a fin de asegurar conexiones "siempre activas". Requisitos de las Normas de Seguridad de Datos PCI 1 y 12.3.9	10.1 Si el proveedor entrega la aplicación de pago y/o las actualizaciones por medio de un acceso remoto a las redes del cliente, consulte la Guía de implementación de las PA-DSS preparada por el proveedor y verifique que contenga lo siguiente: * Las instrucciones para los clientes y revendedores/integradores con relación al uso de tecnologías de acceso remoto, según el requisitos 12.3.9 de las PCI DSS * La recomendación para los clientes y los revendedores/integradores de que utilicen un firewall o un producto firewall personal en caso de que la computadora esté conectada por VPN u otra conexión de alta velocidad, a fin de asegurar estas conexiones "siempre activas" de conformidad con el requisito 1 de las PCI DDS.
11. Facilite un acceso remoto seguro a la aplicación de pago	
11.1 La aplicación de pago no debe interferir con el uso de un mecanismo de autenticación de dos factores. La aplicación de pago debe admitir tecnologías como RADIUS o TACACS con tokens o VPN con certificados individuales. Requisito de las Normas de Seguridad de Datos PCI 8.3	11.1 Pruebe la aplicación de pago en un laboratorio para obtener evidencias de que puede ejecutarse con un mecanismo de autenticación de dos factores(la aplicación de pago no debe prohibir la habilidad de una organización de implementar una autenticación de dos factores).
11.2 Si se puede acceder a la aplicación de pago de manera remota, el acceso remoto debe ser autenticado mediante el uso de un mecanismo de autenticación de dos factores. Requisito de las Normas de Seguridad de Datos PCI 8.3	11.2 Si se puede acceder a la aplicación de pago de manera remota, consulte la Guía de implementación de las PA-DSS preparada por el proveedor de software y verifique que contenga las instrucciones para los clientes y revendedores/integradores respecto del uso requerido de la autenticación de dos factores (ID de usuario y contraseña, además de un elemento de autenticación adicional, como una tarjeta inteligente, token o PIN).
11.3 Si los proveedores,	11.3.a Si el proveedor de software utiliza

revendedores/integradores o clientes pueden acceder de manera remota a las aplicaciones de pago de los clientes, el acceso remoto se debe implementar de manera segura. Requisito de las Normas de Seguridad de Datos PCI 8.3	productos de acceso remoto para acceder de manera remota a la aplicación de pago de los clientes, verifique que el personal del proveedor implemente y utilice las funciones de seguridad para acceso remoto. Nota: Algunos ejemplos de funciones de seguridad para acceso remoto son: * Cambiar los valores de configuración predeterminados en el software de acceso remoto (por ejemplo, cambiar las contraseñas predeterminadas y utilizar contraseñas únicas para cada cliente). * Permitir conexiones únicamente provenientes de direcciones IP/MAC (conocidas) específicas. * Utilizar una sólida autenticación y contraseñas complejas para inicios de sesión de acuerdo con los Requisitos 8.1, 8.3, y 8.5.8 a 8.5.15 de las PCI DSS. * Activar la transmisión de datos cifrados de acuerdo con el requisito 4.1 de las PCI DSS * Activar el cierre de cuenta después de un determinado número de intentos fallidos de inicio de sesión de acuerdo con el requisito 8.5.13 de las PCI DSS. * Configurar el sistema de manera que un usuario remoto deba establecer una conexión de red privada virtual (VPN) mediante un firewall antes de que se le permita el acceso. * Activar la función de inicio de sesión. * Restringir el acceso a las contraseñas del cliente únicamente a personal autorizado del revendedor/integrador. * Establecer contraseñas para clientes de acuerdo con los requisitos 8.1, 8.2, 8.4 y 8.5. de las PCI DSS.
	11.3.b Si los revendedores/integradores o clientes pueden utilizar un software de acceso remoto, consulte la Guía de implementación de las PA-DSS preparada por el proveedor de software y verifique que los clientes y revendedores/integradores hayan recibido instrucciones para utilizar e implementar funciones de seguridad para acceso remoto. Nota: Algunos ejemplos de funciones de seguridad para acceso remoto son: * Cambiar los valores de configuración predeterminados en el software de acceso remoto (por ejemplo, cambiar las contraseñas predeterminadas y utilizar contraseñas únicas para cada cliente). * Permitir conexiones únicamente provenientes de direcciones IP/MAC (conocidas) específicas. * Utilizar una sólida autenticación y contraseñas complejas para inicios de sesión de acuerdo con los Requisitos 8.1, 8.3, y 8.5.8 a 8.5.15 de las PCI DSS. * Activar la transmisión de datos cifrados de acuerdo con el requisito 4.1 de las PCI DSS. * Activar el cierre de cuenta después de un determinado número de intentos fallidos de inicio de sesión de acuerdo con el requisito 8.5.13 de las PCI DSS. * Configurar el sistema de manera que un usuario remoto deba establecer una conexión de red privada virtual (VPN) mediante un firewall antes de que se le permita el acceso. * Activar la función de inicio de sesión. * Restringir el acceso a las contraseñas del cliente únicamente a personal autorizado del revendedor/integrador. * Establecer contraseñas para clientes de acuerdo

	con los requisitos 8.1, 8.2, 8.4 y 8.5. de las PCI DSS.
12. Cifre el tráfico sensitivo de las redes públicas	
12.1 Si la aplicación de pago envía o facilita el envío de datos de titulares de tarjetas mediante redes públicas, debe admitir el uso de protocolos seguros y criptografía sólida, como /TLS y el protocolo de seguridad de Internet (IPSEC) para proteger los datos confidenciales de titulares de tarjetas durante la transmisión a través de redes públicas abiertas. Ejemplos de redes públicas abiertas que se encuentran dentro del alcance de las DSS de la PCI son: * Internet * Tecnologías inalámbricas * Sistema global de comunicaciones móviles (GSM) * Servicio de radio paquete general (GPRS) Requisito de las Normas de Seguridad de Datos PCI 4.1	12.1.a Si la aplicación de pago envía o facilita el envío de datos de titulares de tarjetas mediante de redes públicas, verifique que se provea la tecnología de transmisión de cifrado seguro (por ejemplo, IPSEC, VPN o SSL/TLS) o que se especifique cómo utilizarla.
	12.1.b Si la aplicación de pago permite la transmisión de datos mediante redes públicas, consulte la Guía de implementación de las PA-DSS preparada por el proveedor y verifique que se incluyan las directivas para los clientes y revendedores/integradores sobre cómo utilizar la tecnología de transmisión de cifrado seguro (por ejemplo, IPSEC, VPN o SSL/TLS).
12.2 La aplicación de pago nunca debe enviar PAN no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea o el chat). Requisito de las Normas de Seguridad de Datos PCI 4.2	12.2.a Si la aplicación de pago permite y/o facilita el envío de PAN por medio de tecnologías de mensajería de usuario final, verifique que se le provea una solución de cifrado sólido, o bien que se le especifique cómo utilizarla.
	12.2.b Si la aplicación de pago permite y/o facilita el envío de PAN por medio de tecnologías de mensajería de usuario final, consulte la Guía de implementación de las PA-DSS preparada por el proveedor y compruebe que se incluyan las directivas para los clientes y revendedores/integradores sobre cómo utilizar una solución de cifrado sólido.
13. Cifre el acceso administrativo que no sea de consola.	
13.1 Instruya a los clientes para que cifren todo el acceso administrativo que no sea de consola con tecnologías como SSH, VPN o SSL/TLS para la administración basada en la web u otro acceso administrativo que no sea de consola. Requisito de las Normas de Seguridad de Datos PCI 2.3 Nunca se deben utilizar Telnet ni rlogin para un acceso administrativo.	13.1 Si la aplicación de pago o el servidor permite la administración que no sea de consola, consulte la Guía de implementación de las PA-DSS preparada por el proveedor y compruebe si se recomienda el uso de SSH, VPN o SSL/TLS para el cifrado del acceso administrativo que no sea de consola.
14. Mantenga la documentación instructiva y los programas de capacitación para clientes, revendedores e integradores	
14.1 Desarrolle, mantenga y difunda una Guía de implementación de las PA-DSS para clientes, revendedores e integradores que cumpla con lo siguiente:	14.1 Consulte la Guía de implementación de las PA-DSS y sus procesos afines, y compruebe que se difunda la guía entre todos los usuarios de la aplicación de pago (incluidos los clientes, revendedores e integradores).
14.1.1 Aborda todos los requisitos del presente documento siempre que se haga referencia a la Guía de implementación de las PA-DSS.	14.1.1 Verifique que la Guía de implementación de las PA-DSS considere todos los requisitos relacionados del presente documento.
14.1.2 Incluye una revisión anual, como mínimo, y actualizaciones para mantener al día la documentación de acuerdo con los cambios de software importantes y menores, y los cambios relacionados con los requisitos establecidos en el presente documento.	14.1.2.a Verifique que la Guía de implementación de las PA-DSS se revise con una frecuencia anual y se actualice según sea necesario para documentar todos los cambios importantes y menores de la aplicación de pago.
	14.1.2.b Verifique que la Guía de implementación de las PA-DSS se revise con una frecuencia anual y se actualice según sea necesario para

	documentar los cambios a los requisitos de las PA-DSS.
14.2 Desarrolle e implemente los programas de capacitación y comunicación para asegurar que los revendedores e integradores sepan cómo implementar la aplicación de pago y los sistemas y las redes afines de acuerdo con la Guía de implementación de las PA-DSS de conformidad con las PCI DSS.	14.2 Examine los materiales de capacitación y el programa de comunicación para revendedores e integradores y confirme si los materiales consideran todos los rubros analizados en la Guía de implementación de las PA-DSS en todo el documento.
14.2.1 Actualice los materiales de capacitación en forma anual y cada vez que se lancen nuevas versiones de la aplicación de pago.	14.2.1.a Consulte los materiales de capacitación para revendedores e integradores y verifique que se revisen en forma anual y cada vez que se lancen nuevas versiones de la aplicación de pago, y que, además, se actualicen según sea necesario.
	14.2.1.b Examine el proceso de distribución para las nuevas versiones de la aplicación de pago y verifique que la documentación actualizada se distribuya junto con la aplicación de pago actualizada.
	14.2.1.c Seleccione una muestra de revendedores e integradores y entrevístelos para comprobar que hayan recibido los materiales de capacitación.

7.8 Anexo A: Resumen de contenidos para la Guía de implementación de las PA-DSS

Este Anexo fue redactado con el propósito de resumir los requisitos de las PA-DSS que tienen temas relacionados con la Guía de implementación de las PA-DSS, a fin de explicar el contenido de la Guía y describir las responsabilidades de implementar los controles relacionados.

Requisito PA-DSS	Tema de las PA-DSS	Contenido de la Guía de implementación	Responsable de la implementación de controles
1.1.4	Borre los datos confidenciales de autenticación almacenados por las versiones anteriores de la aplicación de pago.	* Se deben eliminar los datos históricos (datos de la banda magnética, códigos de validación de la tarjeta, PIN o bloqueos de PIN almacenados por versiones anteriores de la aplicación de pago). * Se deben explicar cómo eliminar los datos históricos. * Se debe explicar que dicha eliminación es absolutamente necesaria para cumplir lo establecido en las PCI DSS.	Proveedor de software: Proporcione la herramienta o el procedimiento para que los clientes puedan eliminar con seguridad los datos almacenados por versiones anteriores de acuerdo con el Requisito 1.1.4. de las PA-DSS. Clientes y revendedores/integradores: Borre todos los datos históricos de acuerdo con la Guía de implementación de las PA-DSS y el requisito 1.1.4 de las PA-DSS.
1.1.5	Borre todos los datos confidenciales de autenticación (autorización previa) reunidos como consecuencia del proceso de resolución de problemas de la aplicación de pago.	* Los datos confidenciales de autenticación (autorización previa) solamente se deben reunir cuando sea necesario resolver un problema específico. * Dichos datos deben ser almacenados solamente en ubicaciones específicas, conocidas y con acceso limitado. * Reúna sólo una cantidad limitada de datos necesarios	Proveedor de software: Resuelva los problemas del cliente de acuerdo con el requisito 1.1.6.a. de las PA-DSS. Clientes y revendedores/integradores: Resuelva todos los problemas de acuerdo con la Guía de implementación de las PA-DSS y el requisito 1.1.6.a. de las PA-DSS.

		para resolver un problema específico. * Los datos confidenciales de autenticación se deben cifrar en el momento de almacenarlos. * Dichos datos se deben borrar de manera segura e inmediatamente después de utilizarlos.	
2.1	Purgue los datos de titulares de tarjetas después del período de retención definido por el cliente.	* Los datos de titulares de tarjetas se deben purgar después de superar el período de retención definido por el cliente. * Todas las ubicaciones en que la aplicación de pago almacena datos de titulares de tarjetas.	Proveedor de software: Infórmeles a los clientes que deben purgar los datos de titulares de tarjetas que superen los períodos de retención definidos por el cliente y las ubicaciones donde la aplicación de pago almacene dichos datos. Clientes y revendedores/integradores: Purgue los datos de titulares de tarjetas que superen el período de retención definido por el cliente.
2.7	Borre el material clave criptográfico o los criptogramas almacenados por las versiones anteriores de la aplicación de pago.	* Se debe eliminar el material criptográfico. * Se debe explicar cómo eliminar el material criptográfico. * Se debe explicar que dicha eliminación es absolutamente necesaria para cumplir lo establecido en las PCI. * Cómo volver a cifrar datos históricos con claves nuevas.	Proveedor de software: Proporcione la herramienta o el procedimiento para eliminar con seguridad el material clave criptográfico o los criptogramas almacenados por las versiones anteriores, de conformidad con el requisito 1.1.5 de las PA-DSS y facilite la herramienta o el procedimiento para volver a cifrar los datos históricos con nuevas claves. Clientes y revendedores/integradores: Borre todo el material criptográfico histórico de acuerdo con la Guía de implementación de las PA-DSS y el requisito 1.1.5 de las PA-DSS.
3.1	Utilice ID de usuario únicos y una autenticación segura, tanto para el acceso administrativo como para el acceso a datos de titulares de tarjetas.	* No utilice cuentas administrativas predeterminadas para los inicios de sesión de la aplicación de pago. * Asigne una autenticación segura a las cuentas predeterminadas (incluso si estas no se utilizan) y desactive o no utilice las cuentas. * Utilice una autenticación segura para el sistema y la aplicación de pago siempre que sea posible. * Cómo crear una autenticación segura para acceder a la aplicación de pago según los requisitos 8.5.8 a 8.5.15. de las PCI DSS.	Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente utilice ID de usuario únicas y una autenticación segura para las cuentas/contraseñas de la aplicación de pago según los requisitos 8.1 y 8.2 de las PCI DSS. Clientes y revendedores/integradores: Establezca y mantenga ID de usuario únicas y una autenticación segura de acuerdo con la Guía de implementación de las PA-DSS y los requisitos 8.1 y 8.2 de las PCI DSS.
3.2	Utilice ID de usuario	Utilice nombres de usuario	Proveedor de software:

	únicas y una autenticación segura para acceder a computadoras, servidores y bases de datos con aplicaciones de pago.	únicos y una autenticación segura para acceder a computadoras, servidores y bases de datos con aplicaciones de pago y/o datos de titulares de tarjetas de acuerdo con los requisitos 8.5.8 a 8.5.15 de las PCI DSS.	Asegúrese de que la aplicación de pago admita que el cliente utilice nombres de ID de usuario únicas y una autenticación segura para las cuentas/contraseñas (cuando estén determinadas por el proveedor) a fin de acceder a computadoras, servidores y bases de datos según los requisitos 8.1, 8.2, y 8.5.8 a 8.5.15 de las PCI DSS. Clientes y revendedores/integradores: Establezca y mantenga ID de usuario únicas y una autenticación segura de acuerdo con la Guía de implementación de las PA-DSS y los requisitos 8.1, 8.2 y 8.5.8 a 8.5.15 de las PCI DSS.
4.2	Implemente pistas de auditoría automatizadas.	* Establezca valores de configuración de registro que cumplan con las PCI DSS, de conformidad con el requisito 10 de las PCI DSS. * Se deben activar los registros, ya que desactivarlos provocará un incumplimiento de las PCI DSS.	Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente utilice registros compatibles, de conformidad con el requisito 10 de las PCI DSS. Clientes y revendedores/integradores: Establezca y mantenga registros que cumplan con las PCI DSS de conformidad con la Guía de implementación de las PA-DSS y el requisito 10 de las PCI DSS.
6.1	Implemente tecnología inalámbrica de manera segura.	Si se utiliza tecnología inalámbrica en un entorno de pagos, instale un firewall según el requisito 1.3.8 de las PCI DSS.	Proveedor de software: Asesore a los clientes y revendedores/integradores para que, de conformidad con el requisito 2.1.1 de las PCI DSS, cambien los valores de configuración predeterminados del proveedor de tecnología inalámbrica cuando se utilice esta tecnología con la aplicación de pago. Clientes y revendedores/integradores: Para la tecnología inalámbrica implementada por clientes o revendedores/integradores dentro del entorno de pagos, instale un firewall según la Guía de implementación de las PA-DSS y el requisito 2.1.1 de las PCI DSS.
6.2	Asegure las transmisiones de datos de titulares de tarjetas que se realizan mediante redes inalámbricas.	Si la aplicación de pago se implementa dentro de un entorno inalámbrico, utilice valores de configuración inalámbrica que cumplan con las PCI DSS de conformidad con el requisito 4.1.1 de las PCI DSS.	Proveedor de software: Asesore a los clientes y revendedores/integradores para que, de conformidad con el requisito 4.1.1 de las PCI DSS, implementen transmisiones cifradas seguras, en caso de que se utilice tecnología inalámbrica con la aplicación de pago. Clientes y revendedores/integradores:

			Para la tecnología inalámbrica implementada en el entorno de pagos por clientes o revendedores/integradores, utilice transmisiones cifradas seguras de conformidad con la Guía de implementación de las PA-DSS y el requisito 4.1.1 de las PCI DSS.
9.1	Almacene datos de titulares de tarjetas únicamente en los servidores que no estén conectados a Internet.	No almacene datos de titulares de tarjetas en sistemas a los que se pueda acceder desde Internet (por ejemplo, el servidor web y el servidor de base de datos no deben estar en el mismo servidor).	Proveedor de software: Asegúrese de que la aplicación de pago no requiera el almacenamiento de datos en la DMZ ni en sistemas accesibles desde Internet, ni permita el uso de una DMZ de conformidad con el requisito 1.3.4 de las PCI DSS. Clientes y revendedores/integradores: Establezca y mantenga las aplicaciones de pago de manera que los datos de titulares de tarjetas no se almacenen en sistemas a los que se pueda acceder desde Internet, de conformidad con la Guía de implementación de las PA-DSS y el requisito 1.3.4 de las PCI DSS.
10.1	Entregue de manera segura las actualizaciones de la aplicación de pago.	* Reciba actualizaciones remotas de la aplicación de pago por medio de módems seguros, de conformidad con el requisito 12.3 de las PCI DSS. * Si la computadora está conectada mediante una VPN u otra conexión de alta velocidad, reciba actualizaciones remotas de la aplicación de pago por medio de un firewall o un firewall personal, de conformidad con el requisito 1 ó 1.3.9 de las PCI DSS.	Proveedor de software: Entregue de manera segura actualizaciones remotas de la aplicación de pago de conformidad con los requisitos 1, 1.3.9, y 12.3.9 de las PCI DSS. Clientes y revendedores/integradores: Reciba de manera segura de parte del proveedor las actualizaciones de la aplicación de pago, de conformidad con la Guía de implementación de las PA-DSS y los requisitos 1, 1.3.9, y 12.3.9 de las PCI DSS.
11.2	Implemente una autenticación de dos factores para el acceso remoto a la aplicación de pago.	Utilice una autenticación de dos factores (ID de usuario y contraseña, además de un rubro de autenticación adicional, como un token) si es posible acceder a la aplicación de pago de manera remota.	Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente utilice una autenticación de dos factores, de conformidad con el requisito 8.3 de las PCI DSS. Clientes y revendedores/integradores: Establezca y mantenga una autenticación de dos factores para el acceso remoto a la aplicación de pago, de conformidad con la Guía de implementación de las PA-DSS y el requisito 8.3 de las PCI DSS.
11.3	Implemente de manera segura un software de acceso remoto.	Implemente y utilice funciones de seguridad del software de acceso remoto en caso de utilizarlo para acceder de manera remota a la aplicación	Proveedor de software: (1) Si el proveedor utiliza productos de acceso remoto para acceder a sitios de clientes, utilice las funciones de seguridad de

		de pago o al entorno de pago.	acceso remoto, como las que se especifican en el requisito 11.3.a de las PA-DSS. (2) Asegúrese de que la aplicación de pago admita que el cliente utilice funciones de seguridad de acceso remoto. Clientes y revendedores/integradores: Utilice funciones de seguridad de acceso remoto, si usted permite el acceso remoto a las aplicaciones de pago, de conformidad con la Guía de implementación de las PA-DSS y el requisito 11.3.b de las PA-DSS.
12.1	Asegure las transmisiones de datos de titulares de tarjetas que se realizan mediante redes públicas.	Implemente y utilice la SSL para una transmisión segura de datos de titulares de tarjetas mediante redes públicas, de conformidad con el requisito 4.1 de las PCI DSS.	Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente utilice transmisiones seguras de datos de titulares de tarjetas mediante redes públicas, de conformidad con el requisito 4 de las PCI DSS. Clientes y revendedores/integradores: Establezca y mantenga transmisiones seguras de datos de titulares de tarjetas, de conformidad con la Guía de implementación de las PA-DSS y el requisito 4 de las PCI DSS.
12.2	Cifre los datos de titulares de tarjetas por medio de tecnologías de mensajería de usuario final.	Implemente y utilice una solución de cifrado en caso de que se puedan enviar los PAN mediante tecnologías de mensajería de usuario final.	Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente cifre los PAN en caso de enviarlos por medio de tecnologías de mensajería de usuario final, de conformidad con el requisito 4.2 de las PCI DSS. Clientes y revendedores/integradores: Cifre todos los PAN enviados por medio de tecnologías de mensajería de usuario final, de conformidad con la Guía de implementación de las PA-DSS y el requisito 4.2 de las PCI DSS.
13.1	Cifre el acceso administrativo que no sea de consola.	Implemente y utilice SSH, VPN, o SSL/TLS para el cifrado de todo acceso administrativo que no sea de consola a la aplicación de pago o servidores que se encuentran en el entorno de datos de titulares de tarjetas.	Proveedor de software: Asegúrese de que la aplicación de pago admita que el cliente cifre todo acceso administrativo que no sea de consola, de conformidad con el requisito 2.3 de las PCI DSS. Clientes y revendedores/integradores: Cifre todo el acceso administrativo que no sea de consola, de conformidad con la Guía de implementación de las PA-DSS y el requisito 2.3 de las PCI DSS.