BANORTE

MANUAL DE INTEGRACIÓN API PAYWORKS SEGURO

Diciembre 2019

Versión 2.2

Contenido

Figuras

Tablas

Versiones

Tabla 1. Versiones de actualización del manual

Versión	Descripción de última modificación	Fecha
1.0	Primera versión.	17 de Octubre del 2014
1.1	Corrección de errores en texto	6 de Noviembre del 2014
1.2	Corrección de Tags EMV Especificación de Frameworks para desarrollos .NET	27 de Noviembre del 2014
1.3	Se agregó el apéndice de certificación y liberación a producción.	19 de Diciembre de 2014
1.4	Se agregó la información para la impresión de voucher cuando en la transacción se solicite el PIN Offline.	30 de Enero de 2014
1.5	Se remueve el ARQC de la impresión de los Vouchers VISA y MASTER CARD	25 julio 2016
1.6	Actualización de URL de pagos Banorte	Noviembre 2016
1.7	Nota para gestión de usuarios	Noviembre 2017
1.8	Nota Caracteres Especiales en valores de parámetros	Diciembre 2017
2.0	Actualización para la inclusión de Operativa Contactless	Noviembre 2018
2.1	Actualización de Códigos de rechazo	Febrero 2019
2.2	Actualización Nota en Preautorización	Diciembre 2019

Introducción

En este capítulo daremos una idea general con la finalidad de familiarizar al usuario con la API para el cobro mediante presencia de plástico en sus puntos de venta.

¿Qué es Interredes?

Este esquema surge de la necesidad de integrar más de un punto de venta en el sistema del comercio con el motor de pagos Banorte a fin de procesar transacciones de tarjetas de crédito y débito.

El concepto de Interredes permite la centralización de todas las transacciones de las sucursales en un sólo punto, o bien, la intercomunicación con cada uno de los puntos de venta en las diferentes sucursales.

Es posible integrar a la Interred cualquier dispositivo de lectura de banda magnética, PIN Pads, kioscos, terminales, lectores de tarjeta, etc.

Para realizar la lectura del plástico en el punto de venta, se requiere un dispositivo certificado en los estándares de la industria, como se describe a continuación.

¿Qué es un PIN Pad?

Un PIN Pad es un dispositivo electrónico que provee diversas funciones:

- Lectura de tarjetas con banda magnética.
- Lectura de tarjetas con chip que cumplan con estándares EMV.
- Lectura de tarjetas contactless que cumplan con estándares EMV.
- Implementación interna de estándares EMV.
- Captura y codificación de números de identificación personal (NIP).

Es una alternativa al pago de efectivo. Se utiliza con alguna aplicación para recibir pagos con tarjetas de débito, crédito o monedero electrónico.

La aplicación normalmente se ejecuta en alguna computadora e interactúa con el PIN Pad a través de comandos de software. Físicamente, éste se encuentra conectado a alguno de los puertos del equipo, donde se ejecuta la aplicación, generalmente puerto serial o USB.

El PIN Pad cuenta con los lectores necesarios, tanto de banda magnética, chip como contactless, para poder leer las tarjetas de los clientes en el momento en que la aplicación lo indique. También cuenta con una pequeña pantalla para poder desplegar textos enviados desde la aplicación. Finalmente, para aquellas tarjetas emitidas por instituciones que requieran validación del número de identificación personal del tarjetahabiente, el PIN Pad provee un pequeño teclado numérico por medio del cual el cliente puede autentificarse.

Además, el PIN Pad posee internamente una aplicación responsable de administrar los componentes de hardware presentes en el dispositivo, así como de implementar el protocolo de comunicación con la aplicación controladora, a fin de poder recibir e interpretar correctamente los comandos enviados por ésta, cuando se desea que el PIN Pad ejecute tal o cual función. Actualmente Banorte maneja los PIN Pads Vx810 y Vx820 del fabricante VeriFone.

La Figura 1 Ilustra la instalación de un PIN Pad en un equipo con aplicación de punto de venta:

Figura 1. Instalación de PIN Pad

Seguridad

El PIN Pad encripta los datos sensibles, al momento de enviar una transacción hacia Banorte. Esto con la finalidad de que la información viaje de forma segura hacia el emisor para su autorización. Los datos que se encriptan al ser enviados hacia Banorte son los siguientes:

- Track 1
- Track 2
- Código de seguridad (CVC2, CVV2, 4DBC)

Cada dispositivo recibirá una llave única de cifrado, por lo tanto es necesario realizar la carga del dispositivo de forma individual. Cada dispositivo estará enlazado a una afiliación. Si se requiere mover el dispositivo para ser utilizado en una afiliación diferente, será necesario realizar nuevamente una carga de la llave de encriptación. Los PIN Pad de Banorte que cuentan con la aplicación segura, no podrán transaccionar hasta que realicen la inyección de la llave de cifrado.

La inyección de la llave de encriptación es requerida para el funcionamiento del dispositivo. Cuando al comercio se le haga entrega de un dispositivo, únicamente recibirá los comandos para la inyección de llave. Mientras no se realice la inyección de llave el PIN Pad no realizará ningún comando o transacción. Si el comercio cree que la seguridad de la información que

procesa el dispositivo es comprometida, podrá solicitar nuevamente la carga de llave. Para esto es necesario solicitar el cambio de la llave de encriptación a su ejecutivo.

NOTA: Si actualmente ya se tiene una integración con Banorte y realizará el cambio a la versión segura, es necesario crear un plan de "rollout" debido a que el dispositivo debe darse de alta en la afiliación. Además, los nuevos dispositivos no funcionarán con la integración anterior.

Interfaz de programación (API)

Pensando en simplificar el trabajo a nuestros clientes e integradores, Banorte ha desarrollado una interfaz de programación (también conocida como API, siglas del inglés Application Program Interface) que internamente se hace cargo de la complejidad técnica del protocolo de comunicación con el PIN Pad, y provee a cambio, una serie de funciones de muy fácil uso que la aplicación puede ejecutar desde su propio código, a fin de instruir al PIN Pad a realizar determina función, en un punto preciso de la operación.

Además, la función de lectura de tarjetas, la interfaz de programación desarrollada por Banorte, permite al cliente que así lo desee, efectuar la autorización en línea de la transacción, entregándole como salida la información necesaria para su aplicación de punto de venta, tal como el resultado (si la operación fue aceptada o declinada), el código de autorización (en caso de haber sido aceptada), el nombre del tarjetahabiente, y toda la información adicional que normalmente se requiere para este tipo de aplicaciones.

Obsérvese que integrado de esta forma, el PIN Pad se convierte en una especie de terminal de punto de venta tradicional, pero con la ventaja de que es la aplicación del propio cliente quien lo controla.

Esta serie de funciones está disponible para diversos lenguajes y plataformas de programación, y se describen en forma detallada dentro del presente manual.

Modos de operación

La interfaz de programación Banorte PIN Pads posee dos modalidades de operación:

1. PROCESAR TRANSACCIÓN - Lectura de tarjeta con procesamiento de transacción incluido (Envió a Banorte de datos de operación y respuesta de la transacción)
2. LEER, ENVIAR Y NOTIFICAR - Sólo lectura de tarjeta para procesamiento interno de la información.

Bajo la primera modalidad, al momento de efectuar una transacción, el PIN Pad no sólo leerá la tarjeta del cliente, sino que enviará la información de entrada suministrada por la aplicación, así como la información recopilada de la tarjeta hacia el procesador central de pagos de Banorte

con el fin de efectuar la autorización de la misma. Una vez recibida la respuesta del procesador central, la información será entregada a la aplicación del cliente en los parámetros de salida de la misma llamada.

Esta modalidad se recomienda para aquellos clientes que por la arquitectura de su aplicación, pueden enviar directamente la transacción a Banorte sin requerir de la intervención de un tercer componente de software.

Sin embargo, para aquellos clientes que por necesidades de arquitectura requieren hacer llegar la transacción a Banorte por un medio alterno (por ejemplo, clientes con un servidor de transacciones ISO 8583, los cuales requieren sólo la información leída de la tarjeta para formar el mensaje de la transacción), la interfaz de programación provee la segunda modalidad, en la que únicamente se regresan a la aplicación del cliente los datos de la tarjeta leída sin enviar ningún requerimiento de autorización al procesador central de pagos de Banorte. Se asume, por supuesto, que el cliente se hará cargo de hacer llegar la transacción al banco a través de su medio alterno.

Esta segunda modalidad puede ser también de utilidad para aquellos clientes que deseen implantar algún esquema de tarjeta propia, en la que únicamente requieren de la función de lectura de la misma. Por supuesto, las tarjetas deberán cumplir con los estándares mínimos necesarios para poder ser leídas por los dispositivos PIN Pads.

El usar la interfaz de programación en una modalidad u otra, es simplemente cuestión de hacer llamadas a diferentes funciones incluidas dentro del propio API; no hay necesidad de hacer uso de configuraciones o instalaciones especiales. La aplicación puede decidir en cualquier momento, de acuerdo a la operación, cuándo usar el API, de un modo o de otro.

Instrucciones Básicas para operar con la API

En esta sección se detallarán las operaciones básicas de la API ejemplificando el proceso completo desde la lectura de la tarjeta hasta el envío de la operación a Banorte.

Inicialización y liberación del PIN Pad

Los PIN Pads proporcionados por Banorte utilizan una interfaz virtual de bajo nivel basada en puerto serial. Esto significa que aún cuando el puerto físico utilizado sea un USB, el controlador instalado para el dispositivo crea un puerto serial virtual, mediante el cual la API puede interactuar con el PIN Pad.

Banorte provee a sus clientes el controlador necesario para los PIN Pads; los cuales deberán solicitarse vía correo electrónico a las direcciones de contacto descritas en la última sección de este manual, especificando el modelo de dispositivo que le fue entregado.

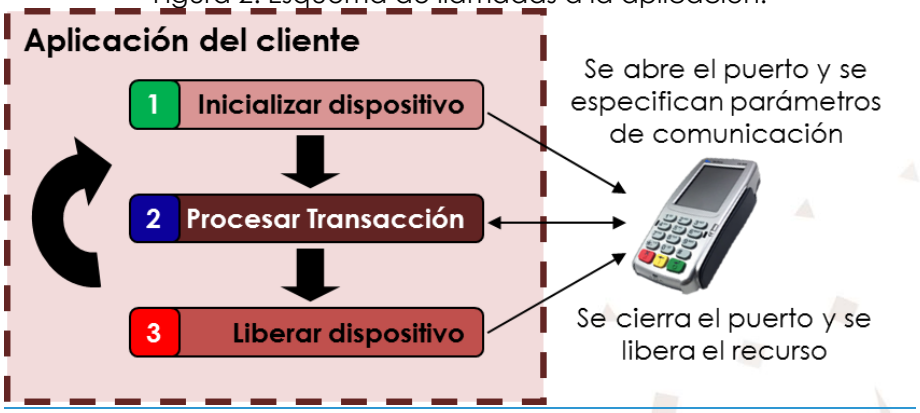
Como en el caso de cualquier otro puerto serial, ya sea virtual o físico, es necesario garantizar que el puerto designado para usarse con el PIN Pad se encuentre disponible para uso de la API.

La interfaz de programación provee dos llamadas, denominadas ***prepareDevice*** y ***releaseDevice***, las cuales deberán ser ejecutadas, la primera al inicio de operaciones para realizar la inicialización del puerto serial asignado, y la segunda al término de la ejecución de la aplicación para garantizar que el puerto quede libre para un eventual uso de otras aplicaciones.

No se recomienda llamar estas dos operaciones por transacción, ya que se estaría haciendo la inicialización y la liberación del puerto innecesariamente múltiples veces. Sin embargo es de mucha importancia que dentro del manejo de excepciones se establezca el procedimiento para liberar el dispositivo.

La Figura 2 esquematiza el uso de estas llamadas por la aplicación:

Figura 2. Esquema de llamadas a la aplicación.



Inicio y fin de transacciones

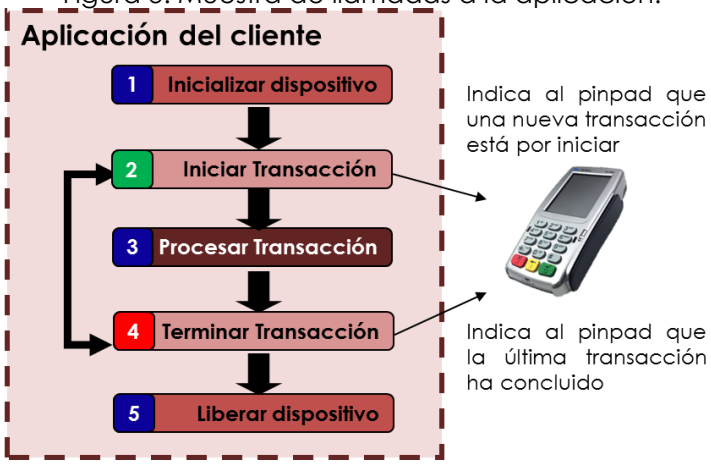
La API provee dos llamadas, denominadas ***startTransaction*** y ***endTransaction***, las cuales deberán ser ejecutadas por la aplicación al inicio y al término de una transacción, respectivamente. Internamente, estas llamadas se utilizan para realizar los pasos necesarios en el PIN Pad de modo que éste sepa cuándo está por iniciar una transacción y cuándo se ha completado.

Estas llamadas deberán hacerse por cada transacción efectuada con el PIN Pad, ya que es necesario informar a éste sobre los eventos de inicio y fin, para que la aplicación residente en el dispositivo se sincronice adecuadamente.

Es importante comentar que ambas llamadas son necesarias aún cuando la API se utilice en modalidad de sólo lectura de tarjetas. En ese caso, la operación de lectura de tarjeta (y eventual notificación del resultado de la transacción) se considera como una transacción, aún cuando ésta no se haga llegar a Banorte por medio de la API.

La Figura 3 muestra el uso de estas llamadas por parte de la aplicación:

Figura 3. Muestra de llamadas a la aplicación.



Carga de llaves de Encriptación

Para la seguridad de los comercios y de los tarjetahabientes, la información viaja de forma encriptada desde el dispositivo hacia Banorte. Para esto, es necesario realizar la carga de la llave de encriptación en el dispositivo. Dependiendo la forma en que se realice la conexión entre el punto de venta y Banorte, será la llamada a efectuarse a la API para la carga de la llave. Se recomienda al desarrollador generar un módulo o una aplicación por separado para la carga de llaves del dispositivo.

Modo de Operación: Procesar Transacción

Dando como hecho que el punto de venta tiene conexión directa a Internet y a Banorte, la aplicación del cliente deberá solicitar la información del PIN Pad mediante la llamada ***getInformation***. Esta llamada como parámetros de salida entregará la información del dispositivo que incluirá el número de serie y la versión de la aplicación instalada en el dispositivo.

Con la información obtenida de la llamada ***getInformation***, se realizará la llamada ***updateMasterKey***, la cual irá a Banorte y solicitará la llave de encriptación y la inyectará en el dispositivo. Después de que la llave se inyecte, el dispositivo podrá realizar transacciones financieras.

Modo de Operación: Leer, Enviar y Notificar Transacción

Cuando el punto de venta no tiene acceso directo a la nube y por ende no tiene acceso directo a Banorte, sino que se conecta a un servidor antes de enviar la transacción a Banorte, la aplicación tiene llamadas específicas para estos casos. La aplicación de punto de venta del cliente deberá solicitar la información del dispositivo mediante la llamada ***getInformation***. Este comando entregará la información del dispositivo que incluye el número de serie del dispositivo y la versión de la aplicación instalada en el dispositivo.

Para obtener la llave de encriptación Banorte solicita un selector del dispositivo. Este selector se obtiene realizando la llamada ***getSelector***. Esta llamada retornará el selector necesario para

solicitar la llave de encriptación a Banorte. Ya con el selector se enviará el comando **GET_KEY** utilizando la llamada ***sendTransaction***. Banorte retornará la llave de encriptación que se inyectará en el dispositivo mediante la llamada ***loadMasterKey***. Después de la inyección de la llave el dispositivo podrá realizar transacciones.

Procesamiento de transacciones

La API provee la funcionalidad para enviar a procesar las transacciones al emisor mediante Payworks. Existe dos maneras de procesar las transacciones: **Proceso integrado de transacciones** y **Proceso independiente de transacciones** o por módulos.

Modo de operación Procesar Transacción

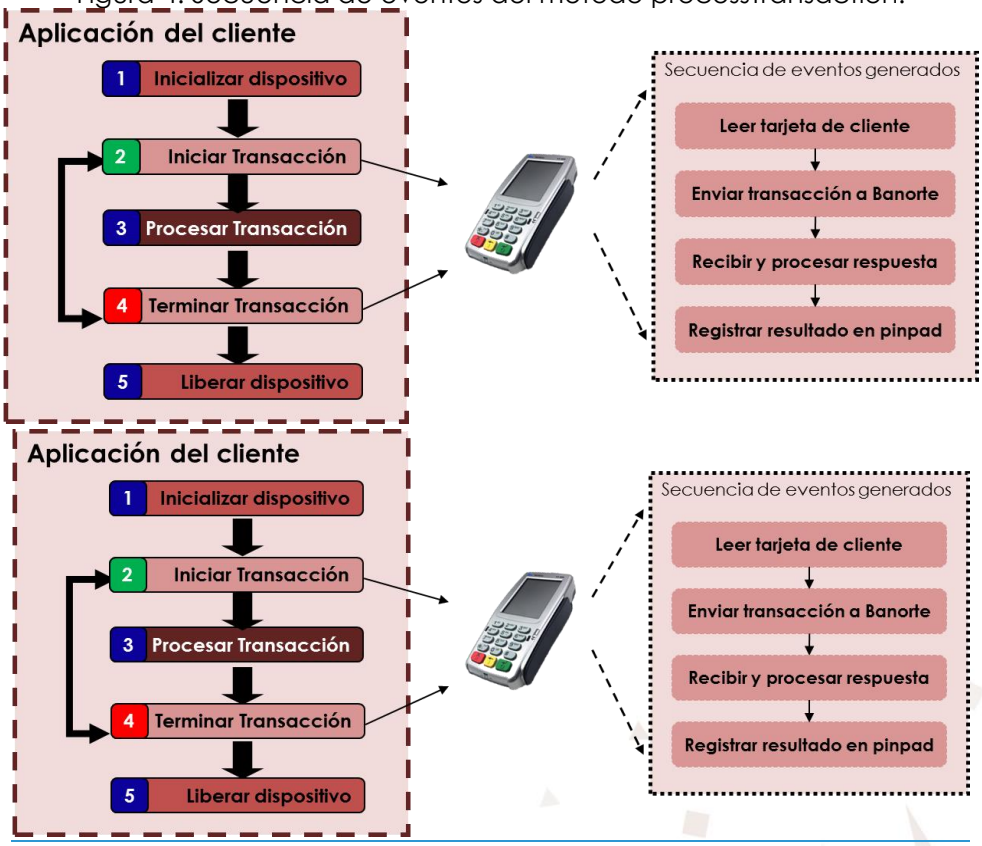
La API de Banorte está diseñado para trabajar en una modalidad que permita en una sola llamada hacer llegar la transacción al procesador central de pagos de Banorte para su autorización. Esta es la modalidad generalmente recomendada a los clientes, a menos que por motivos de su arquitectura requieran hacer llegar la transacción a Banorte por otro medio.

Para utilizar la API en este modo, la aplicación del cliente deberá ejecutar la llamada ***processTransaction***. En ese momento, el PIN Pad se preparará para recibir la tarjeta del cliente (ya sea de banda magnética o de chip), la leerá, generará la información necesaria para enviar la información a Banorte, recibirá la respuesta y entregará el resultado a la aplicación del cliente en los parámetros de salida de esta misma llamada.

La llamada espera ciertos parámetros de entrada que indican, entre otras cosas, el tipo de transacción, el importe de la misma, etc.

La Figura 4 ilustra la secuencia de eventos que se llevan a cabo al momento de ejecutar la llamada ***processTransaction***:

Figura 4. Secuencia de eventos del método processTransaction.



Cuando la API intente enviar la transacción hacia Banorte, se requerirá que las aplicaciones que utilice tengan disponible la conexión necesaria al momento de ejecutar la llamada. La conexión a Banorte puede estar disponible en diferentes modos: internet, línea dedicada, VPN, etc., y normalmente es gestionada por el cliente al momento de tramitar su afiliación.

Al momento de ejecutar esta llamada, el cliente observará que en la pantalla del PIN Pad se despliega la leyenda "Inserte tarjeta". En este momento el cliente podrá deslizar su tarjeta (si es de banda magnética) o insertarla (si es de chip). En el caso de una tarjeta de chip, ésta **NO DEBERÁ SER RETIRADA** hasta que la transacción se complete, ya que de lo contrario ésta no podrá concluirse satisfactoriamente.

La Figura 5 muestra un tipo de PIN Pad provisto por Banorte, el VX820, en donde se señalan claramente los lectores correspondientes a cada tipo de tarjeta (banda y chip); otros modelos contarán con lectores similares:

Figura 5. PIN Pad VeriFone Vx820.

La llamada a ***processTransaction*** entregará como parámetros de salida a la aplicación del cliente la información necesaria para que ésta pueda proceder a hacer sus registros en la base de datos, efectuar impresión de ticket, etc.

Modo de Operación Leer, Enviar y Notificar Transacción

En el caso de aplicaciones que requieran hacerse cargo de la transacción directamente, la API provee dos llamadas: ***readCard*** y ***notifyResult***.

Como su nombre lo indica, la primera llamada se utiliza exclusivamente para realizar el proceso de lectura de una tarjeta del cliente, sea de banda, ~~o~~ chip o contactless, y entregará como parámetros de salida la información necesaria para que la aplicación del cliente, o un tercer componente de software, pueda construir el mensaje de la transacción y enviarlo a Banorte.

En el caso de tarjetas con banda magnética, la API internamente detecta cuando una tarjeta leída es bancaria, y en ese caso entrega como parámetros de salida los datos desglosados del nombre del tarjetahabiente, el número de tarjeta y la fecha de expiración. Si la tarjeta no es reconocida como bancaria (Visa, MasterCard o American Express), la llamada devolverá únicamente el contenido de los tracks 1 y 2 que se hubieren reconocido en la lectura.

Es importante mencionar en este punto, que el mecanismo de lector del PIN Pad está diseñado para leer tarjetas que cumplen con los estándares **ISO 7810**, **7811** y **7813** que reglamentan el diseño de las tarjetas, las características del material magnético de la banda, el formato de grabación de los tracks, el contenido de los mismos, etc. **No se garantiza la lectura de tarjetas de Banda que no se adhieran a dichos estándares.**

Para el caso de tarjetas con chip y contactless, el equipo podrá leer sin problema todas aquellas tarjetas que cumplan con los estándares de EMVCo publicados sobre la materia. **No se garantiza la lectura de tarjetas de chip que no cumplan con dichos estándares**. Cuando la lectura se ha realizado sin problema, la llamada devolverá igualmente a la aplicación del cliente la información desglosada del nombre del tarjetahabiente, el número de tarjeta y la fecha de expiración para facilitar el proceso de la transacción en el punto de venta.

En el caso de tarjetas que posean tanto chip como banda magnética, la aplicación del PIN Pad considerará al chip como el medio de lectura preferido, ya que se considera más seguro. Si la tarjeta tiene Chip, Contactlees y Banda Magnética, la aplicación del PIN Pad considera al Chip y Contactless como lecturas preferidas. Por tanto, si el cliente intenta deslizar por el lector de banda una tarjeta de chip, la lectura será rechazada y se invitará al cliente a que utilice el lector de chip.

Como parte de la información de salida suministrada por esta llamada, la aplicación del cliente podrá determinar cuál fue el medio por el que se leyó la tarjeta, a saber: banda magnética, chip ~~o~~, o contactless. Esta información requiere ser enviada al banco emisor, por lo que si el cliente se está haciendo cargo de la transacción, deberá informar a Banorte sobre el tipo de lectura realizada, lo cual se hará dependiendo del medio que se utilice para hacer llegar la transacción a Banorte. Por ejemplo, aquellos clientes que cuentan con un servidor de transacciones ISO 8583

deberán generar el campo 22 (POS Entry Mode) con los valores adecuados dependiendo de la salida que entregue esta llamada.

Para el caso de las tarjetas de chip, la llamada a ***readCard*** devolverá igualmente la información de Tags EMV que la especificación define como requisito para ser enviados al banco emisor para su validación. Esta es una cadena ASCII de dígitos hexadecimales que la aplicación del cliente deberá hacer llegar a Banorte dependiendo del medio que utilice para tal fin. Por ejemplo, si se tiene un servidor de transacciones ISO 8583, la cadena entregada por esta llamada deberá ser convertida a la secuencia binaria respectiva y colocada en el campo 55 del mensaje ISO 8583 como lo señala la especificación Terminal To Host.

Es importante comentar que el procesador central de pagos de Banorte puede rechazar aquellas transacciones que no cumplan con la información necesaria requerida por los estándares de transacciones financieras vigentes en el momento.

La llamada a ***notifyResult*** se requiere **ÚNICAMENTE PARA TARJETAS CON CHIP O CONTACTLESS CHIP**, ya que la especificación EMV obliga a la aplicación del cliente a informar al dispositivo sobre el resultado de la transacción.

Esta llamada deberá hacerse una vez que ya se tiene el resultado de la transacción, informando de ésta a la API a través de los parámetros de entrada que dicha llamada espera. Obsérvese que esta llamada deberá hacerse independientemente del resultado de la transacción; es decir, deberá ejecutarse para transacciones aprobadas, declinadas, e inclusive para aquellas en las que no se recibió respuesta por parte del emisor (siempre asumiendo que se trata de transacciones con lectura de chip, o contactless chip). Al momento de ejecutarse la llamada a ***notifyResult***, el PIN Pad completa los registros necesarios en el chip de la tarjeta, y despliega el mensaje respectivo invitando al tarjetahabiente o al cliente a retirar su tarjeta, una vez que el proceso de la transacción ha concluido. Esta es la razón por lo que la tarjeta no debe retirarse anticipadamente.

El usuario podrá apreciar en este punto la diferencia entre las dos modalidades de operación ~~provistas porque~~ provee la API: Mientras que en la modalidad con ~~proceso de transacción~~procesar transacción ~~incluido el API~~ se encarga de suministrar todos los datos requeridos a Banorte y completar la transacción con una sola llamada, en la segunda modalidad, con Leer, Enviar y Notificar transacción es la aplicación del cliente la que con base a la información de salida proporcionada por la llamada a ***readCard***, deberá ser responsable de formar el mensaje correspondiente, hacer llegar la transacción a Banorte, recibir la respuesta, procesar el resultado de la respuesta y notificar la API del resultado final por medio de una llamada a ***notifyResult***.

Despliegue de mensajes en pantalla

Para aquellos clientes que deseen personalizar los mensajes desplegados en la pantalla del PIN Pad, la API incluye una llamada ***desplegarTexto***, que permite pasar como parámetro de entrada el texto deseado e internamente se encarga de que éste sea desplegado en el dispositivo.

Esta llamada puede ejecutarse antes de procesar una transacción, o bien una vez que ésta ha sido completada.

Selección de idioma

La API permite especificar el idioma que se usará para los nombres de variables, valores de éstas y textos de los posibles mensajes de error. Los idiomas actualmente soportados son español e inglés. La forma específica en que el idioma se selecciona depende del lenguaje de programación.

Igualmente, cada una de las llamadas de la API tiene un nombre en inglés y en español. Por ejemplo, existe ***displayText*** equivalente a ***desplegarTexto***.

Arquitectura

En este capítulo, se proporciona un panorama general de la construcción de la interfaz de programación para PIN Pad de Banorte, así como diversos aspectos técnicos que ayudarán a los consultores especializados a facilitarles el trabajo de integrar la API a las aplicaciones.

Estructura

La API de Banorte está estructurado por niveles, para facilitar así la futura integración de nuevos modelos y/o marcas de dispositivos, evitando así trasladar al cliente las complejidades técnicas internas requeridas por el esquema de comunicación de cada dispositivo.

Es importante enfatizar que la aplicación del cliente no tiene que involucrarse en los detalles de bajo nivel, y que la arquitectura anterior tiene por objetivo hacer lo más transparente posible a los clientes un posible cambio de equipo a futuro.

Físicamente, la API se entrega como una **biblioteca de carga dinámica** (DLL para usuarios Windows, SO para usuarios UNIX). Las llamadas disponibles en la API se encuentran convenientemente exportadas para facilitar su localización desde el código de la aplicación. Dependiendo del lenguaje de programación seleccionado, es posible que se entregue algún componente adicional de software (por ejemplo, para usuarios Java se entrega un archivo .jar que expone la interfaz de programación como un conjunto de clases que son fácilmente utilizables por usuarios de dicho lenguaje).

Parámetros de entrada y salida

Tratando de seleccionar un esquema que resultara fácil de utilizar para los clientes, considerando la diversidad de lenguajes de programación y plataformas existentes, se adoptó un esquema de comunicación para las llamadas la API basado en parámetros, tanto de entrada como de salida. Por medio de ciertos parámetros de entrada la aplicación puede proporcionar a la llamada específica la API la información que requiere para hacer su trabajo, y es también por medio de parámetros de salida que la aplicación del cliente puede recibir retroalimentación de la API, sobre el resultado de una llamada en particular.

Cada parámetro, tanto de entrada como de salida, está identificado por un nombre que es representativo de su uso. Este nombre puede estar en inglés o en español, dependiendo del lenguaje seleccionado al momento de iniciar la operación con la API.

Los valores de cada parámetro invariablemente serán de tipo texto, para evitar las complejidades que implica la implementación de otros tipos de lenguajes de programación y/o plataformas. Será responsabilidad de la aplicación del cliente realizar las conversiones necesarias entre su propio código y el API cuando maneje algún parámetro con un tipo de dato diferente a texto.

Cada llamada específica de la API señala sus parámetros de entrada y/o de salida. La estructura de datos específica para pasarlos depende del lenguaje de programación; en el presente documento puede hallarse la implementación para cada lenguaje soportado.

Instalación del dispositivo PIN Pad

El presente capítulo explica los pasos a seguir para conectar los dispositivos PIN Pad, así como para instalar los componentes de software requeridos, a fin de integrar éstos adecuadamente a la aplicación de punto de venta del cliente.

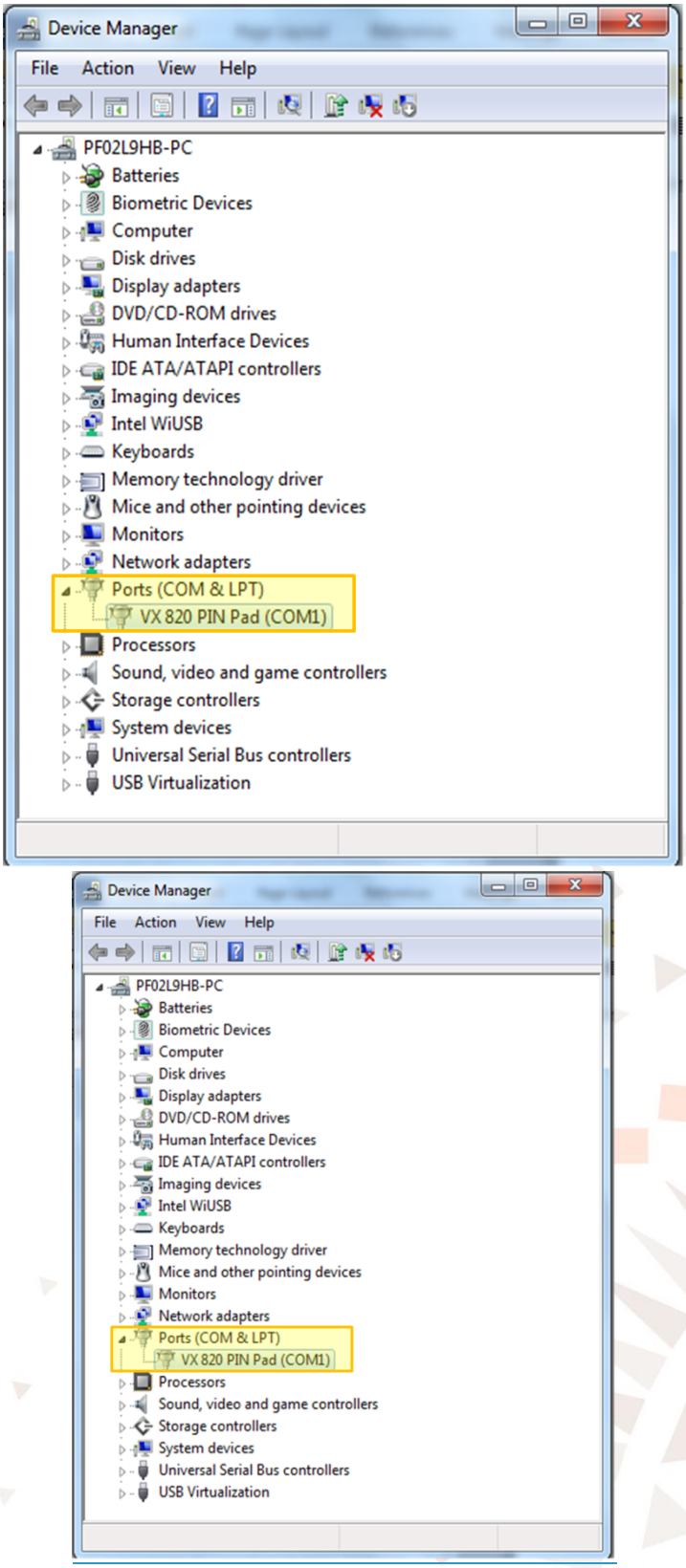
Conexiones Físicas

PIN Pads con Interfaz USB

Actualmente todos nuestros PIN Pad cuentan con cable para conexión a puerto USB, entonces es necesario seguir los siguientes pasos:

- Instalar primeramente el controlador (driver) proporcionado por Banorte para virtualizar el puerto serial que utilizará la API para manipular el dispositivo. Solicite la guía detallada sobre la instalación de cada controlador esto depende de cada marca y modelo de equipo. Es importante realizar primero la instalación antes de conectar físicamente el dispositivo.
- Comprobar que la instalación del controlador se ha realizado con éxito. Si esto es así, el nuevo puerto serial virtual instalado por el controlador debe aparecer en la lista de dispositivos de hardware del sistema operativo. En Windows, esta lista puede obtenerse haciendo clic con el botón derecho en el ícono correspondiente a Mi PC y luego seleccionando la opción “Propiedades”, la pestaña “Hardware” y finalmente el botón Administrador de Dispositivos. Deberá encontrarse una lista similar a la que se muestra en la Figura 6:

Figura 6. Instalación de PIN Pad en la ventana del Administrador de Dispositivos.



Obsérvese que en el ejemplo, el puerto virtual serial asignado es el COM1; este es el identificador de puerto que deberá pasarse como parámetro la API al momento de ejecutar la inicialización del dispositivo (Véase el apartado **Funciones de API**).

Referencias de Implementación

En este apartado, se revisarán los tipos de operaciones permitidas, así como algunos ejemplos en diferentes lenguajes de programación de los métodos contenidos en la API.

Incluso si el lenguaje de programación no se encontrara en este manual, esto no significa que la integración no se pueda realizar, es probable que solo se requiera realizar un poco más de investigación técnica, por lo cual se le sugiere que contacte a su ejecutivo para validar las opciones que podemos ofrecer para llevar a cabo su integración.

Funciones de API

El presente capítulo proporciona la información detallada sobre el uso de cada una de las llamadas disponibles en la interfaz de programación para PIN Pads de Banorte. Ya que los detalles específicos son dependientes del lenguaje y/o de la plataforma utilizada por el cliente, se ha considerado conveniente subdividir este capítulo en secciones, una por cada uno de los lenguajes directamente soportados por la versión actual de la API. De esta forma, los usuarios familiarizados con algún lenguaje en particular encontrarán la información buscada mucho más comprensible.

~~Si algún lenguaje en particular no apareciera en la presente referencia, esto no significa necesariamente que el API no pueda integrarse con aplicaciones desarrolladas en dicho lenguaje; sin embargo, será necesario realizar una investigación técnica adicional para estudiar la manera de llevar a cabo esa integración. Para ello el usuario que así lo requiera puede contactar a su ejecutivo Banorte indicándole las características de su plataforma y aplicación.~~

En la Tabla 2. Funciones en español e inglés y su descripción. Se muestra una breve descripción de las funciones en inglés y español.

Tabla 2. Funciones en español e inglés y su descripción.

Función	Nombre Español	Nombre en Inglés	Descripción
Desplegar texto	*desplegarTexto*	*displayText*	Despliega un mensaje de texto en la pantalla de la PIN Pad.
Inicializar dispositivo	*inicializarDispositivo*	*prepareDevice*	Prepara al PIN Pad para recibir instrucciones.
Liberar dispositivo	*liberarDispositivo*	*releaseDevice*	Al término de la ejecución de la aplicación para garantizar que el puerto quede libre.
Iniciar transacción	*iniciarTransaccion*	*startTransaction*	Le indica al PIN Pad que iniciará una transacción.
Terminar transacción	*terminarTransaccion*	*endTransaction*	Indica la finalización de una transacción.
Obtener información	*obtenerInformacion*	*getInformation*	Obtiene la información del dispositivo.

Obtener selector	*obtenerSelector*	*getSelector*	Retorna el selector necesario para solicitar la llave de encriptación.
Cargar llave	*cargarLlaveMaestra*	*loadMasterKey*	Inyecta la llave de encriptación en el dispositivo.
Cancelar carga de llave	*cancelarCargaLlave*	*cancelLoadKey*	Cancela la inyección de la llave de encriptación.
Actualizar llave	*actualizarLlaveMaestra*	*updateMasterKey*	Realiza la obtención del selector y la carga de la llave en un solo
Leer Tarjeta	*leerTarjeta*	*readCard*	Le indica al PIN Pad que se leerá una tarjeta.
Enviar Transacción	*enviarTransaccion*	*sendTransaction*	Envía una transacción al motor de Pagos Payworks.
Notificar Resultado	*notificarResultado*	*notifyResult*	Notifica al PIN Pad el resultado de una transacción Chip.
Procesar Transacción	*procesarTransaccion*	*processTransaction*	Es una función que realiza las 3 funciones anteriores en un solo paso, genera la Lectura de la tarjeta, el envío de la transacción al motor de Pagos y la notificación al Chip del resultado de la transacción
Obtener Versión	*obtenerVersion*	*getVersion*	Regresa la versión de DLL que está siendo utilizada.

Tipos de Transacciones

En esta sección analizaremos de los tipos de operación que soporta Payworks Seguro mostrando ejemplos de operativas e información requerida en cada una de las transacciones, así como una breve explicación de su uso para un mayor entendimiento.

Los tipos de operación que podemos utilizar en Payworks Seguro son:

- Venta ~~normal~~ (con plástico presente o Pago Móvil).
- Venta con promoción (con plástico presente).
- Venta forzada (con plástico presente).
- Preautorización (con plástico presente).
- Reautorización.
- Postautorización.
- Devolución ~~referenciada~~ (parcial o total).
- ~~de venta~~Cashback (solicitar anexo al **Laboratorio de Payworks**).
- Reversa.

De acuerdo al tipo de transacción deberán incluirse cada uno de los posibles campos en el envío de la operación a Banorte. El motor reconocerá las variables dependientes para cada

una de las operaciones y si es necesario enviara una respuesta de error con el nombre de la variable faltante en el envío.

Venta

Como venta se identifican aquellas transacciones que se aplican directamente a la cuenta del tarjetahabiente. Los tipos de ventas son:

- Venta ~~normal~~ (con plástico presente o Pago Móvil).
- Venta con promoción (con plástico presente).
- Venta forzada (con plástico presente): Por venta forzada se entiende como una transacción en la que el comercio solicita autorización telefónica al emisor y obtiene un código de autorización, el cual es proporcionado como parte de la transacción. El plástico debe de estar presente.
- Venta QPS (Quick Payment Service): Por venta QPS se entiende una transacción en la que no es necesario que el tarjetahabiente firme un comprobante. Se envía el parámetro QPS en la transacción.

NOTA: La venta QPS es únicamente para transacciones por montos de $250.00 o menores; y es aplicable únicamente a ciertos giros de comercios. Para mayor información comunicarse con su ejecutivo de E-banking Banorte.

Se consideran ventas ~~"normales"~~ aquellas en las que el cargo será aplicado en una sola exhibición al tarjetahabiente. Se consideran ventas con promoción aquellas en las que aplica una o más de las siguientes modalidades:

Venta con promoción

Se consideran ventas con promoción aquellas en las que aplica una o más de las siguientes modalidades:

- Pago diferido ~~diluido~~ a meses sin intereses
- Pago diferido ~~diluido~~ a meses con intereses
- Pago diferido (compre hoy y pague después)
- Esquema mixto (pago diferido y ~~diluido~~ a meses con o sin intereses).

Existen 3 identificadores para reconocer una venta ~~como Q6~~con promoción, estos son PLAN_TYPE, PAYMENTS_NUMBER e INITIAL_DEFERMENT, los diferentes valores entre estas variables indicarán a la venta si es con o sin intereses, el plazo de diferimiento y el número de pagos a realizar. Más adelante se detallará esta información.

Preautorización - Reautorización - Postautorización

La preautorización es una operación que genera una reserva sobre el saldo del tarjetahabiente, en caso de querer hacerlo efectivo, el comercio deberá enviar el cierre de esta operación de diversas formas. Esto pude ser a través de una postautorización, de un comando como el cierre de lote o cierre de afiliación, que se detallarán más adelante. Algunos emisores en lugar de reservar el saldo realizan el cargo directo en sus tarjetas de débito.

La reautorización es una transacción referenciada que tiene por objetivo solicitar una retención adicional de saldo en la cuenta del tarjetahabiente, sin necesidad de enviar de nuevo los datos de la tarjeta. La referencia que debe proporcionarse es la de la preautorización sobre la que originalmente se hizo la retención de saldo inicial. Las reautorizaciones están disponibles normalmente sólo para aquellos puntos de venta o terminales registradas con la operativa de hoteles o renta de autos. Pueden hacerse tantas reautorizaciones como se desee, mientras el emisor de la tarjeta lo apruebe.

La postautorización es una transacción referenciada en la que se cierra una preautorización previa, proporcionándose el monto definitivo. La preautorización cuya referencia se provee, podría tener una cadena de varias reautorizaciones previas, pero por estándar de intercambio bancario sólo se cerrará la original. El monto de la postautorización está sujeto a las siguientes reglas:

- Hasta por un monto igual al de la preautorización original, para operativa de retail.
- Hasta por el doble de la preautorización original, para operativa de restaurante.
- Hasta por la suma de la preautorización original más la suma de las posibles reautorizaciones adicionales, para operativas de hoteles y renta de autos.
- La postautorización debe ser menor a 30 días naturales de la fecha de la preautorización.

A continuación se muestra un ejemplo de cómo encadenar estos mensajes:

La preautorización solicita un monto (inicial o definitivo) al autorizador ~~en este caso~~para este ejemplo de 10 pesos.

```
**********************************************************************
-[24/01/2012 13:17:53] SE RECIBIO POST HTTP DESDE LA IP:
GROUP:     [TESTER]
TERMINAL_ID:       [327782962]
PASSWORD:          [a7395007********]
USER:      [a7395007]
MERCHANT_ID:       [7395007]
CMD_TRANS:         [PREAUTH]
TRACK2:
[6F022E3ACA4E4E420E5EB126DF96A6F2F4AFFC35195B8253ED5F089147FF0AF5]
CONTROL_NUMBER:          [A-1787715971]
ENTRY_MODE:        [MAGSTRIPE]
AMOUNT:    [10]
MODE:      [AUT]
```

```
**********************************************************************
```

El comercio recibe por respuesta un código de autorización y una referencia que deberá guardar para realizar el cierre de esta operación.

```
**********************************************************************
[24/01/2012 13:17:53] SE ENVIO RESPUESTA HTTP HACIA LA IP:
NUMERO_CONTROL:          [A-1787715971]
REFERENCIA:              [327346348261]
FECHA_RSP_CTE:    [20120124 13:17:53.158]
TEXTO:       [Aprobada+por+Payworks+%28modo+prueba%29]
RESULTADO_PAYW: [A]
FECHA_REQ_CTE:    [20120124 13:17:53.111]
CODIGO_AUT:       [254131]
ID_AFILIACION:    [7395007]

**********************************************************************
```

El comercio puede (en caso de ser operativa Hotel o Renta de autos) solicitar una reautorización para reservar más saldo en la cuenta del tarjetahabiente. En este caso se hace una reautorización por 5 pesos adicionales.

```
**********************************************************************
[24/01/2012 13:25:05] SE RECIBIO POST HTTP DESDE LA IP:
GROUP:              [TESTER]
TERMINAL_ID:        [327782962]
REFERENCE:          [327346348261]
PASSWORD:           [a7395007********]
USER:               [a7395007]
MERCHANT_ID:        [7395007]
CMD_TRANS:          [REAUTH]
CONTROL_NUMBER:     [A-21944831]
MODE:               [AUT]
AMOUNT:             [5]

**********************************************************************
```

Observe que se entrega la referencia de la operación original y únicamente el importe adicional que se solicita. El último paso sería la solicitud de cierre de esta operación.

```
**********************************************************************
[24/01/2012 13:28:02] SE RECIBIO POST HTTP DESDE LA IP:
GROUP:              [TESTER]
TERMINAL_ID:        [327782962]
REFERENCE:          [327346348261]
PASSWORD:           [a7395007*******]
```

USER: [a7395007]
MERCHANT_ID: [7395007]
CMD_TRANS: [POSTAUTH]
CONTROL_NUMBER: [A-1548305838]
MODE: [AUT]
AMOUNT: [15]

****
****
[24/01/2012 13:28:02] SE ENVIO RESPUESTA HTTP HACIA LA IP
NUMERO_CONTROL: [A-1548305838]
REFERENCIA: [327346348381]
FECHA_RSP_CTE: [20120124 13:28:02.591]
TEXTO: [Aprobada+por+Payworks+%28modo+prueba%29]
RESULTADO_PAYW: [A]
FECHA_REQ_CTE: [20120124 13:28:02.551]
CODIGO_AUT: [713967]
ID_AFILIACION: [7395007]

****

Se envía la postautorización para concluir la operación y enviarla a cobro. La transacción se depositará en la cuenta del comercio al día hábil siguiente de la fecha de postautorización.

NOTA: Es responsabilidad del comercio asegurar el correcto cierre de la Preautorización, validando el resultado de la Postautorización.

En caso de que la Postautorización tenga un resultado diferente a Aprobado el comercio debe realizar un reintento de la transacción. Banorte no se hará responsable de las transacciones no cerradas correctamente por el comercio

Devolución ~~Referenciada~~

Por ~~devolución~~ operación referenciada se entiende como una bonificación que se hace al tarjetahabiente hasta por el 100% de una venta o preautorización previa, para lo cual el comercio deberá enviar la referencia de dicha venta o preautorización sobre la que se desea hacer la devolución.

En el caso de preautorizaciones, éstas deberán haber sido ya cerradas, y el importe de la devolución no podrá exceder del importe final con el que se cerró dicha preautorización. Una venta o preautorización cerrada puede tener cualquier número de devoluciones parciales, siempre que el emisor lo autorice y el monto remanente de la transacción original no llegue a cero.

~~**Cancelación**~~

~~Por cancelación se entiende una transacción referenciada que solicita la anulación de una transacción previa, la cual puede ser una venta, preautorización, crédito directo o cashback. Nuevamente, el comercio enviará la referencia de la transacción que desea cancelar, sin necesidad de enviar un monto, ya que éste es calculado automáticamente por Payworks, de acuerdo a las siguientes reglas:~~

~~Si la transacción referenciada es una preautorización abierta:~~

~~1. Si el punto de venta o terminal tiene el permiso necesario:~~
~~• Para las operativas de retail y restaurante, el monto de la cancelación será igual al monto de la preautorización original.~~
~~• Para las operativas de hotel y renta de autos, el monto de la cancelación será igual a la suma de la preautorización original, más la suma de todas la posibles reautorizaciones que pudiera haber.~~
~~Si el punto de venta o terminal no cuenta con el permiso necesario, la transacción se declina.~~
~~2. En cualquier otro caso, la cancelación se efectúa por el monto remanente de la transacción original.~~

Reversa

Por reversa se entiende como una transacción referenciada que es generada por el comercio para anular una transacción enviada cuando no se reciba respuesta de Payworks, o bien cuando se haya experimentado alguna falla en la comunicación. La reversa se diferencia de la devolución fundamentalmente en que la primera es ~~causada por~~a causa de una falla, mientras que la segunda es por voluntad ~~explícita del~~del comercio.

Para efectuar una reversa, el comercio tiene las siguientes alternativas:

- Proporcionando la referencia de la transacción que se desea reversar
- Proporcionando el número de control de la transacción que se desea reversar~~Si maneja números de control para cada transacción, podrá enviar el número de control de la transacción que desea reversar como dato de entrada.~~
- ~~Si no maneja números de control pero conoce la referencia de la transacción que desea reversar, podrá enviarla como dato de entrada en la solicitud de reversa.~~
- ~~Si maneja números de control para cada transacción, podrá enviar el número de control de la transacción que desea reversar como dato de entrada.~~
- Si ~~se proporcionan~~conocen ambos datos (referencia y número de control~~), y~~ en la solicitud de reversa, tomará precedencia sobre la referencia~~el primero)~~.

- ~~En cualquier caso,~~ Payworks verificará el estado de la transacción: si ésta había sido procesada y aprobada, se procederá a generar el mensaje de reversa hacia el autorizador respectivo; si la transacción no se localiza o no había sido aprobada, se rechazará la reversa sin ejercer acción alguna hacia el autorizador. El comercio podrá comprobar el resultado de la

reversa como usualmente lo haría con cualquier otra transacción, verificando el código de resultado Payworks y el texto adicional.

> **NOTA:** Es obligatorio enviar el número de control de la transacción y/o la referencia de la misma para poder realizar la reversa de la transacción.

Por restricciones en la mensajería de los diferentes autorizadores, no todas las transacciones son reversibles. Generalmente se podrán reversar ventas, preautorizaciones y reautorizaciones.

La reversa no aplica para operaciones de cierre de lote o cierre de afiliación; estas operaciones son irreversibles y están a total control del comercio.

Cashback

Por cashback se entiende la disposición de efectivo en el punto de venta por parte del tarjetahabiente. No se podrá realizar una devolución o reversa a una transacción enviada como cashback. Para recibir más información sobre la integración de cashback favor de comunicarse con el **laboratorio de soporte** de Payworks.

Comandos

Los comandos son operaciones disponibles en Payworks Seguro que proveen funcionalidad expandida a la plataforma y permiten al comercio tener un mejor control de su flujo de transacciones.

Los comandos disponibles en Payworks Seguro son los siguientes:

Obtención de llave

Una obtención de llave es un comando que indica a Payworks que se está solicitando una llave de encriptación para un dispositivo en específico. Antes de enviar el comando para la obtención de la llave, es necesario realizar la solicitud de la información de dispositivo y del selector. Después de recibir la llave se debe inyectar en el dispositivo. Este comando es necesario únicamente cuando el punto de venta no tiene conexión directa a Banorte.

Cierre de afiliación

Un cierre de afiliación es un comando que solicita a Payworks el cierre masivo de todas aquellas preautorizaciones/reautorizaciones se encuentren abiertas y que correspondan a la afiliación de la que procede el comando recibido. Internamente esto originará que Payworks genere las postautorizaciones respectivas hacia el autorizador, evitando así ~~e~~al comercio la necesidad de enviar una por una. Las reglas para cerrar las preautorizaciones son exactamente las mismas descritas en la información correspondiente a la transacción de postautorización.

Adicional, el comercio deberá tomar en cuenta que el cierre únicamente se procesará por el importe realizado en la preautorización original o por la suma total de todas las reautorizaciones realizadas sobre la misma. En esta situación, no le será posible cerrar por un importe menor una transacción. En tal caso, deberá realizarlo previamente al cierre de afiliación de forma individual o suspender la transacción (Ver **Suspensión de transacción/Reactivación de transacción**).

Cierre de lote

Un cierre de lote es un comando que solicita a Payworks el cierre masivo de todas aquellas preautorizaciones/reautorizaciones se encuentren abiertas y que tengan el lote indicado como dato de entrada en el comando. Un lote es un identificador administrado por el comercio, enviado opcionalmente como dato de entrada en cada transacción, y que sirve para agrupar lógicamente un conjunto de transacciones. El comando de cierre de lote puede ser enviado cualquier número de veces, y cada vez que lo reciba, Payworks localizará en su base de datos todas aquellas preautorizaciones abiertas que tengan dicho lote, procediendo a generar las postautorizaciones respectivas. Las reglas de cierre son exactamente las mismas, descritas en la información correspondiente a la transacción de postautorización y cierre de lote.

Es responsabilidad del cliente la administración del lote en las transacciones. Por ejemplo, si ya ha efectuado el cierre para un lote en particular, y posteriormente envía una nueva preautorización con ese mismo lote, dicha preautorización ya no será tomada en cuenta sino hasta que envíe un nuevo comando de cierre de lote.

Verificación

Una verificación es un comando que solicita a Payworks información sobre una transacción previa (status, código de autorización, fechas, etc.). Al igual que en el caso de las transacciones de reversa, el comando de verificación podrá hacerse por cualquiera de los siguientes criterios:

- Proporcionando la referencia de la transacción que se desea verificar
- Proporcionando el número de control de la transacción que se desea verificar
- Si conocen ambos datos (referencia y número de control), en la verificación tomará precedencia sobre la referencia.
- ~~Enviando simplemente la solicitud de verificación, con lo cual Payworks asumirá que se desea verificar la última transacción recibida del usuario y afiliación especificados en el comando.~~

Obsérvese que la transacción de reversa y el comando de verificación parecen similares a primera vista. Sin embargo, por ser una transacción, la primera ejerce una acción hacia el autorizador, mientras que la segunda sólo sirve para informar al comercio sobre el estado de una transacción. Por tanto, el comercio podrá utilizar cualquiera de las dos operaciones cuando no esté seguro del estado de una transacción, pero sólo debería usar la reversa cuando realmente desee solicitar al emisor la anulación de una transacción.

Ejemplo:

VTA | 333069450547 | 5256781385544494 | 400.00 | C | A | 00 | 021302 | 20180801 14:13:01.865 | 20180801 14:13:02.461 | 20180801 14:13:02.507 | 20180801 14:13:02.508 | EXTRANJERA | MASTERCARD | CREDITO | 1902 | 1E0300

VTA|290444177992|4931720020996319|10.00|C|A|null|819509|20101122 11:48:39.652|null|null|20101122 11:48:39.762

Tabla 3. Información retornada en una transacción de verificación

Información Retornada	Descripción	Formato	Ejemplo
Tipo de Transacción Original	• VTA: Venta estándar • VPR: Venta con promoción • VFZ: Venta forzada • PRE: Preautorización • REA: Reautorización • POS: Postautorización • CRD: Crédito • DEV: Devolución estándar • CSB: Cashback • REV: Reversa	Caracter	VTA
Referencia	Se genera en forma automática por el motor	Numérico	333069450547290444177992
Tarjeta	Ingresada al momento de la compra	Número de tarjeta	5256781385544494493172020020996310
Monto	Monto de transacción	Formato: ####.##	400.0010
Código Payworks	Estatus de la transacción. **A**: Abierta (por ejemplo, una preautorización que no se ha cerrado). **C**: Cerrada (por ejemplo, una preautorización ya cerrada, o cualquier otra transacción que no requiere un cierre). **P**: Con devolución parcial (por ejemplo, una venta a la que se le ha hecho por lo menos una devolución parcial). **R**: Reversada (cualquier transacción para la que se ha procesado una reversa). **T**: Con devolución total (por ejemplo, una venta en la que ya se han hecho una o más devoluciones, y la suma de éstas coincide con el importe de la venta). **X**: Indefinida (transacciones que fueron enviadas al autorizador, pero no recibieron respuesta o fueron declinadas).	Caracter	C
Resultado Payworks	Resultado de la transacción. Valores posibles: **A** = Aprobada **D** = Declinada **R** = Rechazada **T** = Sin Respuesta	Caracter	A
Resultado de Autorizador	Código de respuesta retornado por el Autorizador. Únicamente en transacciones productivas.	Numérico	00 (n/a modo prueba)
Código de Autorización	Código entregado por el Autorizador, Variable	Alfanumérico	021302819509

Fecha y hora transacción Banorte	Fecha y hora en que la transacción llegó a Banorte	AAAAMMDD HH:MM:SS.sss	20180801 14:13:01.86520101122 11:48:38.473
Fecha y hora transacción prosa	Fecha y hora en que la transacción llegó a PROSA. Solamente se retorna en transacciones productivas.	AAAAMMDD HH:MM:SS.sss	20180801 14:13:02.46120101122 11:48:38.936
Fecha y hora salida transacción prosa	Fecha y hora en que la transacción fue retornada por PROSA. Solamente aparece en transacciones productivas.	AAAAMMDD HH:MM:SS.sss	20180801 14:13:02.50720101122 11:48:39.380
Fecha y hora salida transacción Banorte	Fecha y hora en que la transacción fue retornada por Banorte.	AAAAMMDD HH:MM:SS.sss	20180801 14:13:02.50820101122 11:48:39.762
Banco Emisor	Nombre del Banco Emisor de la tarjeta. Opcionalmente entregado por el autorizador para una transacción aprobada	Caracter	EXTRANJERA
Marca Tarjeta	Marca de la tarjeta. Opcionalmente entregado por el autorizador para una transacción aprobada	Caracter	MASTERCARD
Tipo Tarjeta	Indica si la tarjeta es de débito o de crédito. Opcionalmente entregado por el autorizador para una transacción	Carácter	CREDITO
Fecha de Expiración	Fecha de Expiración de la tarjeta con la que se realiza la transacción. Si la transacción es manual (pago móvil) el formato es MMAA	AAMM	1902
TAG 9F34	Tag 9F34 de la cadena de EMV, como soporte para revisar si la transacción original solicitó o no firma electrónica	Alfanumérico	1E0300

Suspensión de transacción/Reactivación de transacción

Una suspensión de transacción es un comando que indica a Payworks que una transacción de venta o preautorización no podrá ser referenciada posteriormente por otra transacción (devolución, reautorización, postautorización, etc.), ni podrá participar en cierres masivos, en tanto no se reciba la correspondiente reactivación.

Una reactivación de transacción es un comando que indica a Payworks que una transacción que se encontraba en estado de suspensión podrá volver a ser referenciada por una nueva transacción y podrá asimismo considerarse para futuros cierres masivos.

~~De acuerdo al tipo de transacción deberán incluirse cada uno de los posibles campos en el envío de la operación a Banorte. El motor reconocerá las variables dependientes para cada una de las operaciones y si es necesario enviara una respuesta de error con el nombre de la variable faltante en el envío.~~

Referencias

El motor de pagos permite el envío de diferentes variables que pueden ser utilizadas como referencias. Las variables son:

Tabla 4. Referencias del cliente

Nombre Español	Nombre Inglés	Descripción
REF_CLIENTE1	**CUSTOMER_REF1**	Dato para uso exclusivo del cliente.
REF_CLIENTE2	**CUSTOMER_REF2**	Dato para uso exclusivo del cliente.
REF_CLIENTE3	**CUSTOMER_REF3**	Dato para uso exclusivo del cliente.
REF_CLIENTE4	**CUSTOMER_REF4**	Dato para uso exclusivo del cliente.
REF_CLIENTE5	**CUSTOMER_REF5**	Dato para uso exclusivo del cliente.

Tipos de Moneda

Los tipos de moneda que soportan el motor de Pagos Payworks son pesos y dólares. Este se especifica en la configuración interna, por lo tanto, no es necesario enviar una variable para especificar este valor.

Es importante aclarar que las afiliaciones en dólares solo aceptan pagos de tarjetas emitidas en el extranjero y el monto deberá ser enviado únicamente en dólares y no en pesos. Es decir, si el cliente quiere cobrar 10 USD, el monto que deberá enviar es 10.00.

NOTA: Recordar que cada afiliación únicamente puede ser configurada en pesos o dólares, no existe una operativa dual.

Pagos Diferidos

Para Pagos Diferidos Q6 se utiliza la misma afiliación normal, solo se adiciona configuración para también enviar una transacción con diferimiento o promoción. A continuación se muestran las tres variables para operar las transacciones en los pagos diferidos.

Tabla 5. Parámetros para pagos diferidos

Variable español	Variable inglés	Descripción
DIFERIMIENTO_INICIAL	**INITIAL_DEFERMENT**	Indica el no. de meses a los que se difiere el pago (compre hoy y pague después). Si no hay diferimiento inicial, el valor reportado deberá ser 00.
NUMERO_PAGOS	**PAYMENTS_NUMBER**	Indica el no. de meses en los que se diluye el pago. Si sólo hay diferimiento inicial, el valor reportado deberá ser 00.

TIPO_PLAN	**PLAN_TYPE**	Indica el tipo de plan de la promoción sobre la que se hace la transacción. Valores posibles: Si hay diferimiento inicial: 07 - Si hay no. de pagos: 03 - sin intereses 05 - con intereses

NOTA: Para realizar un pago con promociones es necesario contar con un contrato con los Bancos Emisores para que estos acepten el diferimiento y/o promoción de los pagos.

Solicitud de PIN

Algunos emisores, tanto nacionales como extranjeros, emiten tarjetas de chip que al momento de ser insertadas solicitan un PIN para la autenticación del tarjetahabiente. Como en México no se utiliza el PIN Online para realizar transacciones bancarias, el dispositivo solicitará el PIN Offline para la validación del tarjetahabiente si la tarjeta así lo requiererierá. La validación del PIN Offline no es indicador de que el voucher no requiere ser firmado. En algunos casos, al insertar el PIN en el dispositivo al momento de realizar una transacción, no será requerida la firma autógrafa del tarjetahabiente. Para saber si solicitar o no solicitar la firma del tarjetahabiente en el voucher, la aplicación de punto de venta del comercio deberá analizar el Cardholder Verification Method (CVM) Results. Ver **APÉNDICE D: Validación de PIN Offline**.

Si en la transacción se solicita el PIN offline y no se solicita la firma autógrafa, deberá aparecer en el comprobante de pago la leyenda: **AUTORIZADO CON FIRMA ELECTRÓNICA**. Si en la transacción se solicita el PIN Offline, y además se solicita la firma autógrafa se debe desplegar el mensaje **PIN VERIFICADO** y el espacio para que el tarjetahabiente firme el comprobante de pago. Si la transacción es una venta QPS, se deberá imprimir el mensaje de una venta QPS en lugar de las leyendas antes mencionadas.

NOTA: Si en una transacción se inserta el PIN y no es requerida la firma autógrafa del tarjetahabiente, no deberá aparecer la línea para firmar el comprobante. Si aparece la línea, además del mensaje indicado que se validó el PIN y el comprobante no está firmado, el vocuher quedará **invalidado** para un contracargo.

Transacciones a modo de Prueba

El motor de pagos permite ejecutar transacciones en Modo de Prueba (para simular el comportamiento de la aplicación del comercio) y en Modo Producción. Esto se define en la variable MODE. Los diferentes valores que se pueden definir en la variable **MODE** son los siguientes:

- **MODO (MODE)= PRD** (Producción), la transacción es procesada en modo real.
- **MODO (MODE)= AUT** (Autorización), modo de simulación, la transacción enviada en este modo siempre es aceptada.
- **MODO (MODE)= DEC** (Declinado), modo de simulación, la transacción enviada en este modo siempre es rechazada.
- **MODO (MODE)= RND** (Random), modo de simulación, la transacción enviada en este modo es aceptada o rechazada aleatoriamente.

Si lo que se desea es simplemente verificar la conexión con la aplicación Payworks puede establecer la variable Modo en modo de prueba (valor AUT, DEC o RND), considerando que todas las transacciones generadas en este modo no llegarán hasta el procesador de tarjetas y por lo tanto, no se hará ningún cargo a la tarjeta y ningún abono al estado de cuenta.

NOTA: Es importante que al momento de terminar las pruebas y empezar a transaccionar en producción, establecer esta variable en **MODO = PRD** para indicar al motor que su integración ya se encuentra en producción, ya que si la aplicación del comercio envía por error las transacciones a modo de prueba no existe forma de reprocesar estas ventas.

Credenciales

Para que el comercio pueda realizar transacciones mediante el motor de pagos de Payworks, es necesario que cuente con un conjunto de credenciales que identificarán la afiliación. Estas credenciales serán entregadas por el área de Originación de Banorte. Las credenciales proporcionadas por Banorte son las siguientes:

- **Número de Afiliación:** Es el número que identifica al comercio y es proporcionado al momento de realizar el contrato con Banorte. Si el comercio desea realzar transacciones de American Express mediante Payworks, no será necesario cambiar la afiliación por la proporcionada por American Express, se continuará enviando la afiliación de Banorte en las transacciones y comandos.
- **Usuario:** A cada afiliación se le asigna un usuario administrador predeterminado con la cual podrán realizar transacciones. ~~Si se desea~~Es recomendable generar un usuario con permisos ~~o propiedades diferentes~~de acuerdo a sus actividades (ejecución, reportes, etc.), será necesario solicitar al ejecutivo del comercio que habilite el módulo de usuarios en la Herramienta Administrativa.
- **Contraseña:** Contraseña asociada al usuario. Proporcionada únicamente por el área de Originación de Banorte y será enviado al correo electrónico otorgado al momento del alta de la afiliación. El ejecutivo de Banorte y el personal del Laboratorio de Payworks no tienen acceso a este dato.
- **Terminal:** Identificador del dispositivo con el que se realizan las transacciones, ~~regularmente~~ asociado al número de afiliación del comercio.

Estas credenciales son proporcionadas al comercio mediante un correo de bienvenida por parte de Banorte. Las contraseñas de los usuarios no serán entregadas en el mismo correo en el cual se entregan el resto de las credenciales, sino que serán entregadas en un segundo mensaje de correo electrónico y serán enviados **ÚNICAMENTE** al correo proporcionado al momento de dar de alta la afiliación.

Si por alguna razón, el comercio ya no tiene acceso a la cuenta de correo con la que se dió el alta de la afiliación y desea cambiarlo, será necesario que sea solicitado a su ejecutivo para que a su vez, sea solicitado al área de Originación el cambio.

Ejemplos de Integración

Integración basada en Java

Banorte le ofrecerá como input para este tipo de operaciones, una biblioteca dinámica (dll) BanortePinpadSeguro.dll y BanortePinpadSeguro.jar, los cuales contienen las llamadas a los métodos proporcionados en la API.

Será necesario que el usuario establezca el ambiente de ejecución, adecuado en su entorno de Java para ajustar las referencias a las bibliotecas. Para realizar esto usted puede:

1. Instalar el archivo BanortePinPad.jar (entregado por Banorte) en una ubicación para que pueda ser localizable por el JRE. Esto puede hacerse de varias maneras, dependiendo de las características específicas de la aplicación del cliente:
   - Incluyendo el archivo BanortePinPad.jar, en la variable de entorno CLASSPATH. Por ejemplo:

```
CLASSPATH=C:\AplicPuntoVenta\AplicPuntoVenta.jar;
C:\AplicPuntoVenta\Banorte\BanortePinPadSeguro.jar
```

   - Incluyendo el archivo BanortePinPad.jar como referencia en el manifiesto de la aplicación, si ésta se encuentra contenida en un archivo JAR autoejecutable. Por ejemplo:

```
Manifest-Version: 1.0
Main-Class: com.miempresa.puntoventa.Main Class-
Path: PuntoVenta.jar BanortePinPadSeguro.jar
```

   - Copiando el archivo BanortePinPad.jar al directorio de extensiones del JRE utilizado, típicamente lib/ext (no recomendado).

2. Copiar el archivo BanortePinPad.dll a alguna ubicación deseada, y poner visible dicha ubicación al JRE para que pueda cargar la biblioteca dinámica en tiempo de ejecución. Esto puede hacerse típicamente de varias maneras:
   - Especificando en la propiedad **java.library.path** la ubicación donde se copió el archivo BanortePinPad.dll. Esta propiedad deberá pasarse al JRE al momento de ejecutar la aplicación principal. Por ejemplo:

```
Java –cp
C:\AplicPuntoVenta\AplicPuntoVenta.jar;C:\AplicPuntoVenta\Ba
norte\BanortePinPadSeguro.jar
-D java.library.path=C:\AplicPuntoVenta\Banorte
```

   - Especificando la ubicación donde se copió el archivo BanortePinPadSeguro.dll en la variable de entorno LIBRARY_PATH. Por ejemplo:

```
LIBRARY_PATH=C:\AplicPuntoVenta\Banorte
```

   - Copiando el archivo DLL a la ubicación por defecto del sistema operativo (Por ejemplo, C:\Windows\System32).
   - Si el integrador desea hacer uso de alguna herramienta IDE (tal como Eclipse o NetBeans) para probar la aplicación con la API de Banorte, entonces será suficiente indicar en el proyecto creado en el IDE la ubicación del archivo BanortePinPadSeguro.jar en el CLASSPATH asignado a dicho proyecto.

El paquete de clases preparado para usuarios Java consta de una serie de clases e interfaces, cuyo detalle de utilización se describe en las siguientes subsecciones. La mayoría de los métodos ofrecidos por las clases pueden eventualmente lanzar la excepción ***BanorteException*** en caso de un problema; la aplicación del cliente deberá considerar esta situación para poder atrapar posibles excepciones y en su caso, tomar la acción correspondiente. La totalidad de clases e interfaces se encuentran dentro del paquete **com.banorte.pinpad**, el cual deberá ser referenciado por la aplicación del cliente por medio del estatuto **import**.

Para aquellos usuarios familiarizados con la documentación tipo **Javadoc**, se ofrece una ayuda en este formato, la cual se entrega junto con el archivo **BanortePinPadSeguro.jar**.

> **NOTA:** Para el uso del archivo **BanortePinPadSeguro.jar** y de la Dll es necesario contar con Java JDK 1.5 o superior.

Interfaz PIN Pad

La API para Java contiene una interfaz que define ciertos métodos que todo dispositivo PIN Pad provisto por Banorte deberá proporcionar. Dentro del mismo paquete existirá una clase por cada

diferente tipo de dispositivo soportado por Banorte. En la versión actual de la API, se ofrecen las clases Vx810Segura y Vx820Segura.

Aún cuando la creación del objeto PIN Pad se haga sobre una versión en particular de dispositivo, se recomienda al diseñador de la aplicación del cliente tratar de usar la interfaz genérica, para simplificar el mantenimiento en caso de un eventual cambio de dispositivo.

Así, en vez de hacer esto:

```
Vx810 pinpad = new Vx810();
```

Se recomienda hacer esto:

```
Vx810Segura pinpad = new Vx810Segura();
```

De esta forma, la aplicación del cliente puede dinámicamente instanciar el PIN Pad a utilizar (probablemente con base a un archivo de configuración), y el código que haga uso de los servicios del PIN Pad será **independiente del** ~~dispositivo específico~~modelo del dispositivo.

Creación de objeto PIN Pad Java

Para comenzar a utilizar el PIN Pad, será necesario instanciar un objeto de tipo PIN Pad usando algunas de las clases concretas disponibles en el paquete. Como parámetro opcional, el usuario puede especificar una cadena de caracteres que indique el idioma deseado. Recuérdese que los textos de los parámetros de entrada y salida, así como los textos de los mensajes de error reportados por las excepciones varían en función del idioma seleccionado.

Ejemplos:

```
//Crea el objeto pinpad en Español
Vx810Segura pinpad = new Vx810Segura("ES")

//Crea el objeto pinpad en Inglés
Vx810Segura pinpad = new Vx810Segura("EN")
```

Este paso deberá hacerse una vez por cada PIN Pad conectada físicamente al equipo de punto de venta; la referencia devuelta será utilizada más adelante para solicitar servicios al objeto creado.

Inicialización de dispositivo

Una vez creado el objeto PIN Pad, el paso siguiente consiste en inicializar el dispositivo. Recuérdese que el PIN Pad se conecta por medio de un puerto serial, físico o virtual, por lo que será necesario definir los parámetros de configuración de dicho puerto.

El PIN Pad originalmente entregado de fábrica cuenta con la siguiente configuración:

Tabla 6. Configuración de PIN Pad

Parámetro	Valor
Velocidad	19200 bps
Paridad	Ninguna
Bits de datos	8
Bits de paro	1

Para inicializar el dispositivo, deberá ejecutarse una llamada al método ***prepareDevice***, pasando como parámetro de entrada un objeto de tipo **java.util.Map**. Este objeto deberá tener una entrada por cada combinación (parámetro, valor) que se requiera. Tanto el nombre del parámetro, como el valor deberán ser de tipo **java.lang.String**. La tabla con los parámetros necesarios se presenta en la subsección Parámetros de Inicialización.

Ejemplo:

```
//Se crea la tabla con los parámetros de inicialización
HashMap config = new HashMap(5);

config.put("PORT", "COM5");
config.put("BAUD_RATE", "19200");
config.put("PARITY", "N");
config.put("STOP_BITS", "1");
config.put("DATA_BITS", "8");

//Se inicializa la pinpad con los parámetros de la tabla
try {
pinpad.prepareDevice(config);
}
catch(BanorteException e) {
System.out.println("Falla al inicializar Pinpad: " + e.getMessage());
}
```

La llamada anterior deberá hacerse solamente una sola vez, durante el tiempo de vida de la aplicación.

Inicio de transacción Java

Por cada transacción que se desee ejecutar, será necesario primero hacer una llamada al método ***startTransaction*** del objeto PIN Pad. Esto se requiere para preparar el hardware del dispositivo para una nueva operación.

Este método no requiere parámetros.

Ejemplo:

```
//Se inicia la transacción
```

```
try{
pinpad.startTransaction();
} catch (BanorteException e) {
System.out.println("Falla al inicializar transacción: " + e.getMessage());
}
```

Obtener la información del PIN Pad

Esta función realiza la petición al dispositivo para que provea la información de la versión del dispositivo. La llamada ***getInformation*** retorna el número de serie del dispositivo y la versión de la aplicación financiera instalada en el mismo. Esta llamada se ejecuta antes de realizar una carga de llave de cifrado o de una actualización de la llave. A continuación se muestra el procedimiento:

```
//Creamos el HashMap para obtener la información
HashMap informacion = new HashMap(5);
String numeroSerie = "";

try {
pinpad.getInformation(parametrosSalida);
numeroSerie = informacion.get("NUMERO_SERIE");
} catch (BanorteException e) {
System.out.println("Falla al obtener la información: " + e.getMessage());
}
```

Carga de llaves

Carga de llaves con Modo de Operación: Procesar Transacción

Esta función será utilizada exclusivamente por comercios en el que su punto de venta tiene acceso directo a Banorte mediante la Internet. Mediante la llamada ***updateMasterKey*** se realizará la carga de la llave de encriptación en el dispositivo. A continuación se muestra un ejemplo:

```
//Creamos el HashMap para realizar la carga de llave
HashMap cargarEntrada = new HashMap();

cargarEntrada.put("MERCHANT_ID", "7395007");
cargarEntrada.put("USER", "a7395007");
cargarEntrada.put("PASSWORD", "a7395007********");
cargarEntrada.put("CONTROL_NUMBER", "CARGALLAVE001");
cargarEntrada.put("RESPONSE_LANGUANGE", "EN");
cargarEntrada.put("BANORTE_URL", "https://via.pagosbanorte.com/InterredesSeguro");
cargarEntrada.put("SERIAL_NUMBER", numeroSerie);

//Realizamos la carga de la llave
try {
```

```
pinpad.updateMasterKey(parametrosEntrada);
} catch (BanorteException e) {
System.out.println("Falla al cargar llave: " + e.getMessage());
}
```

Si la seguridad de la información del dispositivo pudiera llegar a estar comprometida, puede solicitarse la regeneración de una llave de encriptación y volver a ejecutar la llamada ***updateMasterKey***.

Carga de llave con Modo de Operación: Leer, Enviar y Notificar Transacción

Para los usuarios que desde su punto de venta no cuenten con acceso directo a Banorte será necesario realizar los siguientes pasos:

Obtención del selector

Es necesario solicitar el selector del dispositivo para obtener de Banorte la llave que el dispositivo específico requiere. Mediante la llamada ***getSelector*** se obtienes este dato. Por ejemplo:

```
//Se crea el HashMap para obtener el selector
HashMap selectorSalida = new HashMap();

//Se solicita el selector al pinpad
try {
pinpad.getSelector(selectorSalida);
String selector = selectorSalida("SELECTOR");
} catch (BanorteException e) {
System.out.println("Falla al obtener selector: " + e.getMessage());
}
```

Solicitud de la llave de encriptación

Como el punto de venta no tiene acceso directo a Banorte, la solicitud de la llave de encriptación se puede realizar utilizando la clase ***ConectorBanorte***, la cual contiene un único método estático llamado ***sendTransaction***. Este método utiliza dos **HashMap**, uno de parámetros de entrada y otro de parámetros de salida. Este método no realiza una conexión con el PIN Pad, sino que envía una transacción o un comando hacia Banorte, por lo tanto puede ser utilizado en una ubicación diferente al punto de venta, por ejemplo un servidor. A continuación se presenta un ejemplo:

```
//Se crean los HashMaps para solicitor la llave a Banorte
HashMap llaveEntrada = new HashMap();
HashMap llaveSalida = new HashMap();

//Llenamos los parámetros de la table
llaveEntrada.put("MERCHANT_ID", "7395007");
llaveEntrada.put("USER", "a7395007");
llaveEntrada.put("PASSWORD", "a7395007********");
llaveEntrada.put("RESPONSE_LANGUAGE", "EN");
```

```
llaveEntrada.put("CMD_TRANS", "GET_KEY");
llaveEntrada.put("CONTROL_NUMBER", "SOLICITARLLAVE001");
llaveEntrada.put("BANORTE_URL", "https://via.pagosbanorte.com/InterredesSeguro");
llaveEntrada.put("SELECTOR", selector);

//Utilizamos el método sendTransaction para solicitar la llave a Banorte
try {
ConectorBanorte.sendTransaction(llaveEntrada, llaveSalida);
} catch (BanorteException e) {
System.out.println("Falla al obtener llave: " + e.getMessage());
}

//Obtenemos los datos de la respuesta
String resultadoPayw = get.llaveSalida("PAYW_RESULT");
String codigoPayw = get.llaveSalida("PAYW_CODE");
String llaveMaestra = get.llaveSalida("TEXT");
```

Carga de llave de encriptación

Ya que se tiene la llave de encriptación se procede a cargar la llave en el dispositivo. Para realizar la carga en el dispositivo se realizan los siguientes pasos:

```
//Se valida que se haya obtenido correctamente la llave resutadoPayw = "A"
if (!"A".equals(resultadoPayw)) {
HashMap cancelarCarga = new HashMap()
cancelarCarga.put("SERIAL_NUMBER", numeroSerie);

//Se cancela carga de la llave
try {
pinpad.cancelarCargaLlave(parametrosEntrada);
} catch (BanorteException e) {
System.out.println("Falla al cancelar la carga: " + e.getMessage());
}
} else {

//Se crea el HashMap para cargar la llave en el pinpad
HashMap cargarLlave = new HashMap();

cargarLlave.put("SERIAL_NUMBER", numeroSerie);
cargarLlave.put("MASTER_KEY", llaveMaestra);

//Realizamos la carga de la llave en el pinpad
try {
pinpad.loadMasterKey(cargarLlave);
} catch (BanorteException e) {
System.out.println("Falla al cargar llave: " + e.getMessage());
}
}
```

Si el comercio cree que la llave de encriptación del dispositivo está comprometida deberá solicitar a su ejecutivo que genere una nueva llave de encriptación. Después el comercio realizará nuevamente los pasos para la carga de la llave, desde la obtención del selector hasta la carga de la llave.

Procesamiento de transacciones

Proceso autónomo de transacción (Procesar Transacción)

Para aquellos usuarios que prefieran dejar a cargo de la API el envío de la transacción hacia Banorte, ésta es la única llamada que requieren hacer para completar el proceso de leer la tarjeta, formar la transacción, enviarla a Banorte, recibir la respuesta y procesarla. La aplicación no recibirá el control hasta que se tenga respuesta del banco, o bien, haya expirado el tiempo máximo especificado para la transacción. En caso de recibir respuesta del banco, los parámetros de salida indicarán el resultado de la transacción; de lo contrario ocurrirá una excepción.

El método a ejecutar es ***processTransaction*** sobre el objeto PIN Pad; previamente deberá haberse ejecutado el método ***startTransaction***, ya que de lo contrario no se recibirá la respuesta esperada del dispositivo.

Este método espera dos parámetros, cada uno de ellos de tipo **java.util.Map**. El primer mapa define los parámetros de entrada, los cuales proveerán información para que la transacción pueda procesarse; el segundo mapa deberá pasarse sin información, y será llenado por la API con el resultado de la transacción.

Los parámetros de entrada requeridos para este método se muestran en la tabla de la sección **Parámetros de entrada** del proceso de transacción. A continuación se muestra un ejemplo:

```
//Se crean las tablas para los parámetros de la transacción
HashMap parametrosEntrada = new HashMap(20);
HashMap parametrosSalida = new HashMap(20);

//Parámetros de entrada de la transacción
parametrosEntrada.put("MERCHANT_ID", "7395007");
parametrosEntrada.put("USER", "a7395007");
parametrosEntrada.put("PASSWORD", "a7395007*********");
parametrosEntrada.put("CMD_TRANS", "AUTH");
parametrosEntrada.put("TERMINAL_ID", "327779587");      parametrosEntrada.put("AMOUNT",
"0.01");
parametrosEntrada.put("CONTROL_NUMBER", "VENTA0001");
parametrosEntrada.put("MODE", "PRD");
parametrosEntrada.put("RESPONSE_LANGUAGE", "EN");
parametrosEntrada.put("BANORTE_URL", "https://via.pagosbanorte.com/InterredesSeguro");

//Se realiza el proceso de la transacción
try {
pinpad.processTransaction(parametrosEntrada, parametrosSalida);
```

```
} catch (BanorteException e) {
System.out.println("Falla al procesar la transacción: " + e.getMessage());
}

String declinadaOffline = (String) parametrosSalida.get("CHIP_DECLINED");

//Validamos si la transacción fue declina Offline
if (declinadaOffline.equals("1")) {
pinpad.displayText("Declinada Offline");
} else {

//Si no fue declinada Offline se revisa el resultado
String codigoBanorte = (String) parametrosSalida.get("PAYW_RESULT");

//Verificar si la transacción fue aprobada
if (codigoBanorte.equals("A")) {
String codigoAut = (String) parametrosSalida.get("AUTH_CODE");
System.out.println("Transacción aprobada con código: " + codigoAut);
pinpad.displayText("Aprobada: " + codigoAut);
} else {
System.out.println("Transacción declinada");
pinpad.displayText("Declinada");
}
}
```

A diferencia de utilizar el método Leer y Enviar, en el método Procesar Transacción al enviar el parámetro **PAGO_MOVIL** con valor de "1", únicamente se procesarán transacciones con tarjetas Pago Móvil. El desarrollador deberá realizar alguna forma para que el usuario final de la aplicación de punto de venta haga una selección del método de pago: tarjeta o Pago Móvil.

Proceso de transacciones por módulos (Leer, Enviar y Notificar)

Lectura de tarjeta

Para aquellos usuarios que únicamente deseen utilizar la API para lectura de tarjetas y envíen la transacción a Banorte por un medio alterno, ésta llamada será la necesaria para obtener la información sobre tarjeta leída. A partir de los datos de salida devueltos por esta llamada, la aplicación será responsable de formar el mensaje hacia Banorte, dependiendo del medio que utilice para tal fin, y una vez obtenido el resultado, independientemente de si fue aprobada, declinada o sin respuesta. Para transacciones de chip deberá ejecutar una llamada al método ***notifyResult***, el cual se explica a continuación.

Para pedir al PIN Pad que se prepare para leer una tarjeta, la aplicación del cliente deberá ejecutar la llamada al método ***readCard***. Este método tiene dos versiones, la primera espera dos argumentos: un mapa de parámetros de entrada y otro de parámetros de salida. La segunda versión espera como único argumento un mapa de parámetros de salida.

La primera versión del método (con parámetros de entrada y de salida) debe usarse siempre que la lectura de tarjeta sea con el fin de procesar alguna transacción que eventualmente pudiera ser con tarjeta de chip, para que se hagan las inicializaciones necesarias en el lector correspondiente. La aplicación del cliente debe especificar como mínimo el monto de la transacción que se ejecutará. Recuérdese que si la transacción es de chip, la aplicación del cliente debe notificar el resultado posteriormente con una llamada al método ***notifyResult***.

Obsérvese que si se usa esta versión del método, entonces como mínimo deberá de pasarse el monto de la transacción en el mapa de parámetros de entrada; de lo contrario el método lanzará una excepción.

La segunda versión del método (sin parámetros de entrada) puede usarse cuando la aplicación del cliente trabaje con tarjetas propias de banda magnética y no hay la posibilidad de que se presenten transacciones de chip.

En ambas versiones, el mapa de parámetros de salida se deberá proporcionar inicialmente vacío; el método internamente llenará el mapa con información para la aplicación acerca de las características de la lectura realizada.

Como en otros métodos, el tipo de los mapas de parámetros será **java.util.Map**, y tanto el nombre del parámetro como su valor serán de tipo **java.lang.String**.

En el momento de la ejecución de este método, el PIN Pad desplegará un mensaje en su pantalla invitando al cliente a insertar o deslizar su tarjeta. En el caso de tarjeta de chip, ésta no deberá retirarse del PIN Pad hasta que la aplicación haya completado la llamada a ***notifyResult***.

Los posibles parámetros de entrada que pueden ser enviados en este método, se muestran en la tabla de **Parámetros de entrada** del método leer tarjeta en el **Apéndice A**.

```
//Se crean los HashMaps para los parámetros de la lectura de la tarjeta HashMap leerEntrada
= new HashMap(20);
HashMap leerSalida = new HashMap(20);

//Se crean los HashMaps para los parámetros para enviar la transacción
HashMap parametrosEntrada = new HashMap(20);
HashMap parametrosSalida = new HashMap(20);

//Ingresamos los parámetros de entrada para la lectura de la tarjeta
String amount = "1";
String PagoMovil = "0";
leerEntrada.put("AMOUNT", amount);
leerEntrada.put("PAGO_MOVIL", PagoMovil);

//Se solicita la lectura de la tarjeta
try{
pinpad.readCard(leerEntrada, leerSalida);
}catch(BanorteException e){
System.out.println("Error al leer la tarjeta" + e.getMessage());
```

```
}

//Recuperamos datos de la Lectura de la Tarjeta
String Track1 = (String) leerSalida.get("TRACK1");
String Track2 = (String) leerSalida.get("TRACK2");

//Determinar el Tipo de Entrada (Banda/Chip/Contactless)
String PosEntryMode = (String) leerSalida.get("MODO_ENTRADA");
String declinadaChip = "";
String EmvTags = "";

//Revisamos si es de Chip para así poder obtener los EMVTAGS
if (PosEntryMode.equals("CHIP") || (PosEntryMode.equals("CONTACTLESSCHIP")){
EmvTags = (String) leerSalida.get("EMV_TAGS");
parametrosEntrada.put("EMV_TAGS", EmvTags);
declinadaChip = (String)leerSalida.get("CHIP_DECLINED");
}

//Primeramente validamos si no fue un Declinado Offline, validando el valor de la variable de
retorno DECLINADA_CHIP
if (declinadaChip.equals("1"){

//Aquí termina la transacción
System.out.println("La transacción fue declinada offline");
pinpad.desplegarTexto("Declinada Offline");
}else{

//Se envía transacción a Banorte mediante el método readCard
}
```

NOTA: Al enviar el parámetro **PAGO_MOVIL** con valor de "1" en el método ***readCard*** (***leerTarjeta***) el PIN Pad permitirá los 3 métodos de lectura de tarjeta: banda, chip y manual (Pago Móvil). Si se envía con valor de "0" únicamente permitirá la lectura de banda y, de chip y de Contactless.

Envío de Transacción

Para aquellos usuarios que por su arquitectura no estén en condiciones de enviar directamente la transacción a Banorte desde su punto de venta por medio de la llamada a ***processTransaction***, pero que puedan hacerlo desde otro punto y no requieran de utilizar ningún componente de software adicional, la API provee una clase denominada ***ConectorBanorte***, el cual posee un único método de tipo estático ***sendTransaction***, que tiene la capacidad de enviar una transacción hacia Banorte a partir de un mapa de parámetros de entrada y entregar información sobre el resultado en un mapa de parámetros de salida inicialmente vacío.

Como siempre, los mapas de parámetros tanto de entrada como de salida, deberán ser objetos que implementen la interfaz **java.util.Map**, y tanto los nombres como los valores de cada parámetro serán objetos de tipo **java.lang.String**.

Es importante enfatizar, que este método no tiene relación alguna con el manejo de la transacción a nivel PIN Pad, sino que constituye una vía de comunicación directa a Banorte para aquellos usuarios que por sus características puedan encontrarlo de utilidad. La aplicación del cliente deberá usar las otras llamadas de la API (particularmente ***readCard*** y ***notifyResult***) en los equipos que tengan conectado el PIN Pad para hacerse cargo de la manipulación de éste.

También es importante señalar que, debido a que la comunicación se hace directamente con el procesador central de pagos de Banorte, es necesario especificar el idioma en que se manejarán los parámetros. Los dos idiomas soportados por Payworks son español e inglés.

La aplicación del cliente deberá ser responsable de asegurarse de poner la totalidad de parámetros necesarios en el mapa de entrada. Por ejemplo, si utiliza el método ***readCard*** para procesar las lecturas de tarjetas de clientes y una de ellas resultare ser de chip, deberá asegurarse de incluir los parámetros **EMV_TAG** y **ENTRY_MODE** que la llamada a ***readCard*** le haya regresado en el mapa de parámetros de entrada que se pase al método ***sendTransaction***.

Al igual que en el caso del método ***processTransaction*** invocado sobre el objeto PIN Pad, el método ***sendTransaction*** invocado estáticamente sobre la clase ***ConectorBanorte*** requieren visibilidad hacia Banorte desde el equipo en donde se hace la ejecución.

Obsérvese que la gran diferencia entre el método ***processTransaction*** invocado sobre el objeto PIN Pad y el método ***sendTransaction*** invocado estáticamente sobre la clase ***ConectorBanorte***, es que el primero incluye el manejo de la lectura de la tarjeta en el PIN Pad y la notificación del resultado de la transacción, mientras que el segundo es exclusivamente para hacer llegar una transacción hacia el procesador central de pagos de Banorte y se asume que la aplicación del cliente se está haciendo cargo aparte del manejo del PIN Pad por medio de las llamadas a ***readCard*** y ***notifyResult***.

Un ejemplo de invocación de este método sería el siguiente:

```
//Llenamos la tabla para enviar la transacción
parametrosEntrada.put("MERCHANT_ID", "7395007");
parametrosEntrada.put("USER", "a7395007");
parametrosEntrada.put("PASSWORD", "a7395007*********");
parametrosEntrada.put("CMD_TRANS", "AUTH");
parametrosEntrada.put("TERMINAL_ID", "327779587");
parametrosEntrada.put("CONTROL_NUMBER", "TRANSACCIONPRO249");
parametrosEntrada.put("MODE", "PRD");
parametrosEntrada.put("AMOUNT", amount);
parametrosEntrada.put("TRACK2", Track2);
parametrosEntrada.put("ENTRY_MODE", PosEntryMode);
parametrosEntrada.put("RESPONSE_LANGUAGE", "EN");
parametrosEntrada.put("BANORTE_URL", "https://via.pagosbanorte.com/InterredesSeguro");
```

```
//Validamos si el Track1 está presente
if Track1 != "" {
    parametrosEntrada.put("TRACK1", EmvTags);
}

//Método Enviar Transacción
try{
ConectorBanorte.sendTransaction(parametrosEntrada,parametrosSalida);
}catch(BanorteException e){
System.out.println("Error al enviar la operación a Banorte: " +
e.getMessage());
}
```

Al enviar la transacción hacia Payworks, el parámetro **PAGO_MOVIL** deberá ir en "1" para transacciones realizadas de forma manual (Pago Móvil). Si el método de entrada es diferente a **MANUAL** el parámetro **PAGO_MOVIL** no deberá ser enviado o enviado con valor de "0".

Respecto a transacciones con American Express, la aplicación del comercio debe solicitar el CVV2 antes de enviar la transacción cuando en la transacción la lectura sea por banda magnética, debido a que éste es un parámetro de entrada del método y se envía en la transacción.

Notificación de resultado

La ejecución de este método es requerida para aquellos usuarios que se hagan cargo del envío de la transacción, cuando ésta sea de chip.

El método ***readCard*** retorna a la aplicación del cliente información en los parámetros de salida acerca del tipo de lectura obtenida (chip, banda, contactlesschip o contactlessbanda~~o banda forzada~~). En el caso de chip, la aplicación deberá ejecutar una llamada a este método una vez que tenga el resultado de la transacción. La llamada deberá hacerse, independientemente si la transacción fue aprobada o declinada, e inclusive si no hubo respuesta.

En caso de que el banco emisor de la tarjeta haya decidido enviar información de autenticación al chip de la tarjeta, ésta será recibida por la aplicación del cliente al momento de recibir respuesta de la transacción enviada a Banorte y deberá pasarse como parámetro de entrada al método ***notifyResult***.

Finalmente, sólo para el caso de transacciones aprobadas, deberá también proporcionarse como parámetro de entrada el código de autorización recibido. Para mayor detalle revisar los parámetros de notificación de resultado.

Un ejemplo para invocar este método se describe a continuación:

```
// Validamos si la tarjeta es CHIP
if (PosEntryMode.equals("CHIP")){

//Se crean los HashMaps para los parámetros de Notificar Resultado
```

```
HashMap parametrosNotifyEntrada = new HashMap(20);
HashMap parametrosNotifySalida = new HashMap(20);

//Obtenemos datos de salida del procesamiento de la transacción
String resultadoPayw = (String) parametrosSalida.get("PAYW_RESULT");
String codigoAut = (String)parametrosSalida.get("AUTH_CODE");
String datosEMV = (String)parametrosSalida.get("EMV_DATA");

//Validamos si hubo respuesta de la transacción
if(resultadoPayw != null){

//Validamos si existe información en DATOS_EMV
if (datosEMV != null){
parametrosNotifyEntrada.put("EMV_DATA", datosEMV);
}

if (resultadoPayw.equals("A")){
parametrosNotifyEntrada.put("RESULT", "APPROVED");
parametrosNotifyEntrada.put("AUTH_CODE", codigoAut);
}else
if (resultadoPayw.equals("D")){
parametrosNotifyEntrada.put("RESULT", "DECLINED");
}else{
parametrosNotifyEntrada.put("RESULT", "NO_RESPONSE");
}
 }
} else{
parametrosNotifyEntrada.put("RESULT", "NO_RESPONSE");
}

//Método notificar resultado
try {
pinpad.notifyResult(parametrosNotifyEntrada, parametrosNotifySalida);
}
catch (BanorteException e) {
System.out.println("Error al notificar el resultado:" +e.getMessage());
}

//Obtenemos el resultado de notificar la transacción
String resultadoEMV = (String) parametrosNotifySalida.get("EMV_RESULT");

//Validamos resultadoEMV
if (resultadoEMV != null){

if (resultadoEMV.equals("D") && resultadoPayw.equals("A")){
pinpad.displayText("DECLINADA EMV");

//Se genera el reverso por Declinado EMV
//Se crean los hashMaps para el reverso
HashMap reversaEntrada = new HashMap(20);
```

```
HashMap reversaSalida = new HashMap(20);

//Se obtiene la referencia de la transacción anterior
String reference = (String) parametrosSalida.get("REFERENCE");

//Se llena la table con los parámetros del reverso
reversaEntrada.put("MERCHANT_ID", "7395007");
reversaEntrada.put("USER", "a7395007");
reversaEntrada.put("PASSWORD", "a7395007********");
reversaEntrada.put("CMD_TRANS", "REVERSAL");
reversaEntrada.put("TERMINAL_ID", "327779587");
reversaEntrada.put("REFERENCE", reference);
reversaEntrada.put("MODE", "PRD");
reversaEntrada.put("RESPONSE_LANGUAGE", "EN");
reversaEntrada.put("BANORTE_URL", "https://via.pagosbanorte.com/InterredesSeguro");

//Como fue un declinado EMV se envía el parámetro CAUSE con valor fijo 17
reversaEntrada.put("CAUSE", "17");

//Método Enviar Transacción para enviar el reverso
try{
ConectorBanorte.sendTransaction(parametrosEntrada,parametrosSalida);
}catch(BanorteException e){
System.out.println("Error al enviar la operación a Banorte: " +
e.getMessage());
}
}else if (resultadoEMV.equals("A") && resultadoPayw.equals("A")){
pinpad.displayText("APROBADA");
}else{
pinpad.displayText("DECLINADA");
}
}
}
}else{

//Si la transacción fue realizada con banda magnética
String resultado = (String)parametrosSalida.get("PAYW_RESULT");

//Únicamente se valida el resultado de Payworks
if (resultado.equals("A")){
String codAut = (String) parametrosSalida.get("AUTH_CODE");
pinpad.displayText("APROBADA: " + codAut);
}else{
pinpad.displayText("DECLINADA");
}
}
```

Finalizar transacción

Una vez completada una transacción, la aplicación deberá ejecutar el método ***endTransaction*** para indicar este evento al dispositivo. Obsérvese que la ejecución de este método, junto con el de inicio de transacción deberá hacerse **POR CADA TRANSACCION** realizada con el dispositivo. Este método no requiere parámetros.

Ejemplo:

```
try {
pinpad.endTransaction();
} catch(BanorteException e) {
System.out.println("Falla al terminar la transacción: " +
e.getMessage());
}
```

Despliegue de texto

El método ***displayText*** es útil y puede ser empleado por la aplicación del cliente para personalizar los mensajes que aparecen en la pantalla del PIN Pad.

Recibe como parámetro único un objeto de tipo **java.lang.String** que contiene el texto que se desea desplegar. Se recomienda no utilizar acentos ni caracteres especiales, ya que no es seguro que éstos sean soportados por todas las versiones de firmware en los dispositivos.

Ejemplo:

Se desea desplegar en pantalla el mensaje "APROBADA: xxxxxx", donde xxxxxx es el código de autorización recibido de la transacción, o bien DECLINADA en caso de rechazo.

```
if (codigoBanorte.equals("A")){
String codigoAut = (String)parametrosSalida.get("AUTH_CODE");
pinpad.displayText("Aprobada: " + codigoAut);
}else {
pinpad.displayText(" DECLINADO ");
}
```

Liberación de dispositivo

El método ***releaseDevice*** debe ejecutarse al terminar la operación del PIN Pad, para asegurarse de liberar el puerto serial y los recursos asignados por el sistema operativo. Este método no requiere parámetros.

Ejemplo:

```
try {
pinpad.releaseDevice();
} catch(BanorteException e) {
```

```
System.out.println("Falla al liberar dispositivo: " + e.getMessage());
}
```

Obtención de versión de la API

El método ***getVersion*** es un método utilitario suministrado para que la aplicación del cliente pueda verificar con qué versión la API se encuentra trabajando y así llevar un control efectivo en caso de que posteriormente sean liberadas versiones adicionales con nuevas capacidades. Este es un método estático que deberá ser invocado sobre la clase API, incluida dentro del mismo paquete **com.banorte.pinpad**.

El método deberá ser invocado con un objeto de tipo **java.util.Map** inicialmente vacío; que el método retornará lleno con información sobre su versión. La tabla **Obtención de versión** muestra los nombres de dichos parámetros, a fin de que la aplicación del usuario pueda reconocerlos.

Ejemplo:

```
//Se crea el HashMap para obtener la versión
HashMap parametrosSalida = new HashMap();

try {
API.getVersion(parametrosSalida);
String version = parametrosSalida.get("VERSION");
System.out.println("Versión de API: " + version);
} catch(BanorteException e) {
System.out.println("Incapaz de obtener versión de API: " +
e.getMessage());
}
```

Excepciones

Los métodos de la API en general pueden lanzar una excepción si ocurrió un problema durante la ejecución del método. La clase que representa esta excepción se llama ***BanorteException*** y está dentro del mismo paquete **com.banorte.pinpad** que se incluye dentro del archivo .JAR entregado al cliente.

La clase ***BanorteException*** deriva directamente de **java.lang.Exception**, y por tanto, el mensaje de error representado por la excepción puede obtenerse, como con cualquier excepción Java, por medio del método ***getMessage()***. Sin embargo, para comodidad del usuario, se incluye un método adicional, denominado ***getCodigo()***, el cual provee un código de error que la aplicación del cliente puede analizar para determinar exactamente la causa del error reportado y tomar la acción correspondiente. En el apéndice especial se encuentran documentados los posibles códigos de error y sus textos asociados. También se proporciona una breve ayuda sobre cuáles podrían ser las causas y posibles soluciones.

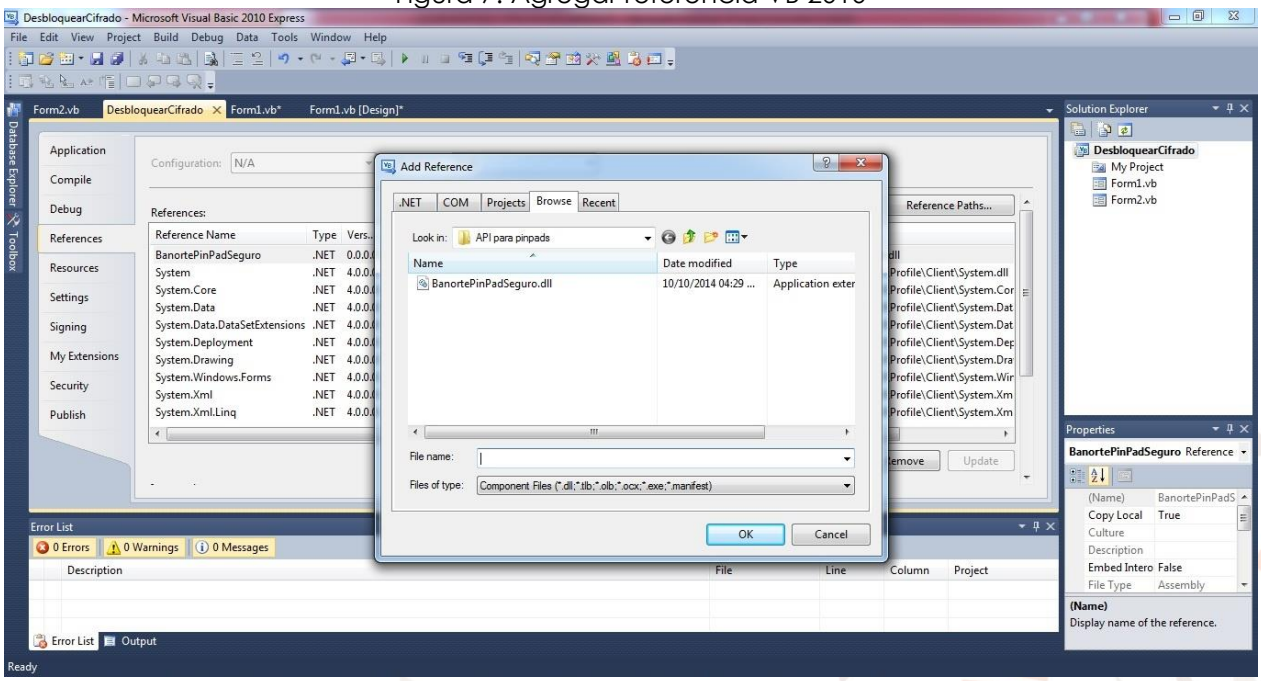
Integración con aplicaciones .NET

Para los usuarios que utilizan .NET que desean integrar con la API Banorte, será necesario realizar lo siguiente~~: para preparar el ambiente de ejecución adecuado:~~

~~Ejecutar el archivo de instalación que es proporcionado por el Laboratorio de Payworks de Banorte. Después de realizar la instalación el archivo estará disponible en la dirección C:\Program Files\Grupo Financiero Banorte\API para pinpads. En este directorio podrá encontrar el archivo DLL bajo el nombre **BanortePinPadSeguro.dll**.~~

Tendremos que generar una referencia a **BanortePinPadSeguro.dll**, esto dando botón derecho al proyecto y Agregar referencia (Ver Figura 7):

Figura 7. Agregar referencia VB 2010



La DLL diseñada y detallada en esta sección muestra cada uno de los métodos a usar y sus respectivos ejemplos para una mayor comprensión. La mayoría de los métodos ofrecidos por las clases pueden eventualmente lanzar la excepción ***BanorteException*** en caso de un problema; la aplicación del cliente deberá considerar esta situación para poder atrapar posibles excepciones y en su caso tomar la acción correspondiente. La totalidad de clases e interfaces se encuentran dentro de **Banorte.PinPad**.

> **NOTA:** Debido a que el archivo **BanortePinpadSeguro.dll** fue compilado utilizando el .NET Framework 4, es necesario que el desarrollo de la aplicación de punto de venta sea realizado en Visual Studio 2010 o mayor.

Interfaz PIN Pad

La API para .NET contiene una interfaz que define ciertos métodos que todo dispositivo PIN Pad provisto por Banorte deberá proporcionar. Dentro del mismo paquete existirá una clase por cada diferente tipo de dispositivo soportado por Banorte.

Aún cuando la creación del objeto PIN Pad se haga sobre una versión en particular de dispositivo, se recomienda al diseñador de la aplicación del cliente tratar de usar la interfaz como sigue:

```
'DECLARA UN OBJETO PINPAD
Dim pinpad As New Banorte.PinPad.Vx820Segura("EN")
```

De esta forma, la aplicación del cliente puede dinámicamente instanciar el PIN Pad a utilizar (probablemente con base a un archivo de configuración), y el código que haga uso de los servicios del PIN Pad será independiente del dispositivo específico.

Creación de objeto PIN Pad

Para comenzar a utilizar el PIN Pad, será necesario instanciar un objeto de tipo PIN Pad usando algunas de las clases concretas disponibles en la dll. Como parámetro opcional, el usuario puede especificar una cadena de caracteres que indique el idioma deseado. En este caso los idiomas disponibles son español (ES) e inglés (EN). Recuérdese que los textos de los parámetros de entrada y salida, así como los textos de los mensajes de error reportados por las excepciones varían en función del idioma seleccionado.

```
'DECLARA UN OBJETO PINPAD EN EL IDIOMA INGLÉS
Dim pinpad As New Banorte.PinPad.Vx820Segura("EN")

'DECLARA UN OBJETO PINPAD EN EL IDIOMA ESPAÑOL
Dim pinpad As New Banorte.PinPad.Vx820Segura("ES")
```

Este paso deberá hacerse una vez por cada PIN Pad conectada físicamente al equipo de punto de venta; la referencia devuelta será utilizada más adelante para solicitar servicios al objeto creado.

Inicialización de dispositivo

Una vez creado el objeto PIN Pad, el paso siguiente consiste en inicializar el dispositivo. Recuérdese que el PIN Pad se conecta por medio de un puerto serial, físico o virtual, por lo que será necesario definir los parámetros de configuración de dicho puerto. El PIN Pad cuenta con la siguiente configuración:

Tabla 7. Configuración de PIN Pad

Parámetro	Valor
Velocidad	19200 bps

Paridad	Ninguna
Bits de datos	8
Bits de paro	1

Para inicializar el dispositivo, deberá ejecutarse una llamada al método ***prepareDevice***, pasando como parámetro de entrada un objeto de tipo **Hashtable**. Este objeto deberá tener una entrada por cada combinación (parámetro, valor) que se requiera. Tanto el nombre del parámetro como el valor deberán ser de tipo **String**. La tabla con los parámetros necesarios se presenta en la subsección Parámetros de Inicialización.

```
'CREAR TABLA DE PARÁMETROS DE CONFIGURACIÓN DEL DISPOSITIVO
Dim config As New Hashtable()
config.Add("PORT", "COM1")
config.Add("BAUD_RATE", "19200")
config.Add("PARITY", "N")
config.Add("STOP_BITS", "1")
config.Add("DATA_BITS", "8")
Try
pinpad.prepareDevice(config)
Catch ex As Exception
MsgBox("Falla al iniciar la transacción: " + ex.Message)
End Try
```

La llamada anterior deberá hacerse solamente una sola vez durante el tiempo de vida de la aplicación.

Inicio de transacción

Por cada transacción que se desee ejecutar, será necesario antes hacer una llamada al método ***startTransaction*** del objeto PIN Pad. Esto se requiere para preparar el hardware del dispositivo para una nueva operación. Este método no requiere parámetros.

```
Try
pinpad.startTransaction()
Catch ex As Exception
MsgBox("Falla al iniciar la transacción: " + ex.Message)
End Try
```

Obtener la información del PIN Pad

Esta función realiza la petición al dispositivo para que provea la información contenida en el dispositivo. La llamada ***getInformation*** retorna el número de serie del dispositivo y la versión de la aplicación financiera instalada en el mismo. Esta llamada se realiza antes de aplicar una carga de llave de cifrado o de una actualización de la llave. A continuación se muestra el procedimiento:

```
'CREAMOS EL HASHTABLE PARA OBTENER LA INFORMACIÓN
Dim salidaInformacion As New Hashtable()
Dim numeroSerie As String

'OBTENEMOS LA INFORMACIÓN DEL DISPOSITIVO
Try
Pinpad.getInformation(salidaInformacion)
numeroSerie = salidaInformacion.Item("SERIAL_NUMBER")
Catch ex As Exception
    MsgBox("Falla al obtener la información del pinpad: " + ex.Message)
End Try
```

Carga de llaves

Carga de llaves con modo de operación Process Transaction

Esta función será utilizada exclusivamente por comercios en el que su punto de venta tiene acceso directo a Banorte mediante la Internet. Mediante la llamada ***updateMasterKey*** se realizará la carga de la llave de encriptación en el dispositivo. A continuación se muestra un ejemplo:

```
'CREAMO EL HASTABLE PARA LA CARGA DE LA LLAVE
Dim entradaCarga As New Hashtable()

'LLENAMOS EL HASHTABLE
entradaCarga.Add("USER", "a7395007")
entradaCarga.Add("PASSWORD", "a7395007********")
entradaCarga.Add("MERCHANT_ID", "7395007")
entradaCarga.Add("CONTROL_NUMBER", "CARGA0001")
entradaCarga.Add("RESPONSE_LANGUAGE", "EN")
entradaCarga.Add("SERIAL_NUMBER", numeroSerie)
entradaCarga.Add("BANORTE_URL", "https://via.pagosbanorte.com/InterredesSeguro")

'REALIZAMOS LA CARGA DE LA LLAVE
Try
Pinpad.updateMasterKey(entradaCargar)
Catch ex As Exception
    MsgBox("Falla al cargar la llave en el pinpad: " + ex.Message)
End Try
```

Si la seguridad de la información del dispositivo estuviera comprometida puede solicitarse la regeneración de una llave de encriptación y volver a ejecutar la llamada ***updateMasterKey***.

Carga de llave con modo de operación Leer, Enviar y Notificar Transaccion

Para los usuarios que desde su punto de venta no cuenten con acceso directo a Banorte será necesario realizar los siguientes pasos:

Obtención del selector

Es necesario solicitar el selector del dispositivo para obtener de Banorte la llave que el dispositivo especifico requiere. Mediante la llamada ***getSelector*** se obtienes este dato. Por ejemplo:

```
'SE CREA EL HASHTABLE PARA LA OBTENCIÓN DEL SELECTOR
Dim salidaSelector As New Hashtable()
Dim selector As String

'SE SOLICITA EL SELECTOR
Try
Pinpad.getSelector(salidaSelector)
selector = salidaSelector("SELECTOR")
Catch ex As Exception
    MsgBox("Falla al obtener el selector: " + ex.Message)
End Try
```

Solicitud de la llave de encriptación

Como el punto de venta no tiene acceso directo a Banorte, la solicitud de la llave de encriptación se puede realizar utilizando la clase ***ConectorBanorte***, la cual contiene un único método estático llamado ***sendTransaction***. Este método utiliza dos **hashtables**, uno de parámetros de entrada y otro de parámetros de salida. Este método no realiza una conexión con el PIN Pad, sino que envía una transacción o un comando hacia Banorte, por lo tanto puede ser utilizado en una ubicación diferente al punto de venta, por ejemplo un servidor. A continuación se presenta un ejemplo:

```
'SE CREAN LOS HASHTABLES PARA SOLICITAR LA LLAVE
Dim entradaEnviar As New Hashtable()
Dim salidaEnviar As New Hashtable()

entradaEnviar.Add("CMD_TRANS", "GET_KEY")
entradaEnviar.Add("USER", "a7395007")
entradaEnviar.Add("PASSWORD", "a7395007********")
entradaEnviar.Add("MERCHANT_ID", "7395007")
entradaEnviar.Add("CONTROL_NUMBER", "CARGALLAVE0001")
entradaEnviar.Add("SELECTOR", selector)
entradaEnviar.Add("RESPONSE_LANGUAGE", "EN")
entradaEnviar.Add("BANORTE_URL", "https://via.pagosbanorte.com/InterredesSeguro")

'SE ENVÍA EL COMANDO A BANORTE PARA LA SOLICITUD DE LA LLAVE
Try
Banorte.ConectorBanorte.sendTransaction(entradaEnviar, salidaEnviar)
Catch ex As Exception
    MsgBox("Falla al enviar la transacción: " + ex.Message)
End Try

Dim resultadoPayw, paywCode As String
```

```
resultadoPayw = salidaEnviar.Item("PAYW_RESULT")
paywCode = salidaEnviar.Item("PAYW_CODE")
```

Carga de llave de encriptación

Ya que se tiene la llave de encriptación se procede a cargar la llave en el dispositivo. Para realizar la carga en el dispositivo se realizan los siguientes pasos:

```
'SE VALIDA QUE SE HAYA OBTENIDO CORRECTAMENTE LA LLAVE
If resultadoPayw <> "A" Then
Dim entradaCancelar As New Hashtable()
entradaCancelar.Add("SERIAL_NUMBER", numeroSerie)

Try
pinpad.cancelLoadKey(entradaCancelar)
    Catch ex As Exception
MsgBox("Falla al cancelar la carga de llave: " + ex.Message)
End Try
Else
Dim entradaCarga As New Hashtable()
Dim llaveMaestra As String
llaveMaestra = salidaEnviar.Item("TEXT")

entradaCarga.Add("SERIAL_NUMBER", numeroSerie)
entradaCarga.Add("MASTER_KEY", llaveMaestra)

Try
pinpad.loadMasterKey(entradaCarga)
Catch ex As Exception
MsgBox("Falla al realizar la carga de llave: " + ex.Message)
End Try
End If
```

Si el comercio cree que la llave de encriptación del dispositivo está comprometida deberá solicitar a su ejecutivo que genere una nueva llave de encriptación. Después, el comercio realizará nuevamente los pasos para la carga de la llave, desde la obtención del selector hasta la carga de la llave.

Procesamiento de transacciones

Proceso Autónomo de transacción

Para aquellos usuarios que prefieran dejar a cargo de la API el envío de la transacción hacia Banorte, ésta es la única llamada que requieren hacer para completar el proceso de leer la tarjeta, formar la transacción, enviarla a Banorte, recibir la respuesta y procesarla. La aplicación no recibirá el control hasta que se tenga respuesta del banco, o bien, haya expirado el tiempo

máximo especificado para la transacción. En caso de recibir respuesta del banco, los parámetros de salida indicarán el resultado de la transacción; de lo contrario ocurrirá una excepción.

El método a ejecutar es ***processTransaction*** sobre el objeto PIN Pad; previamente deberá haberse ejecutado el método ***startTransaction***, ya que de lo contrario no se recibirá la respuesta esperada del dispositivo.

Este método espera dos parámetros, cada uno de ellos de tipo **Hashmap**. El primer mapa define los parámetros de entrada, los cuales proveerán información para que la transacción pueda procesarse; el segundo mapa deberá pasarse sin información, y será llenado por la API con el resultado de la transacción.

Los parámetros de entrada requeridos para este método se muestran en la tabla de la sección Parámetros para formar la transacción.

Ejemplo:

```
'CREAMOS LOS HASHTABLE DE PARAMETROS PARA LA TRANSACCION
Dim parametrosEntrada As New Hashtable()
Dim parametrosSalida As New Hashtable()

'PARAMETROS DE ENTRADA PARA LA TRANSACCION
parametrosEntrada.Add("MERCHANT_ID", "7395007")
parametrosEntrada.Add("USER", "a7395007")
parametrosEntrada.Add("PASSWORD", "a7395007*********")
parametrosEntrada.Add("CMD_TRANS", "AUTH")
parametrosEntrada.Add("TERMINAL_ID", "327782962")
parametrosEntrada.Add("CONTROL_NUMBER", "TRANSACCION01")
parametrosEntrada.Add("MODE", "PRD")
parametrosEntrada.Add("AMOUNT", "10.00")
parametrosEntrada.Add("RESPONSE_LANGUAGE", "EN")
parametrosEntrada.Add("BANORTE_URL",
"https://via.pagosbanorte.com/InterredesSeguro")

'METODO PROCESAR TRANSACCION
Try
pinpad.processTransaction(parametrosEntrada, parametrosSalida)
Dim codigoBanorte, codigoAut, declinadaOffline As String

'OBTENEMOS LOS DATOS PARA IDENTIFICAR EL RESULTADO
codigoBanorte = parametrosSalida.Item("PAYW_RESULT")
declinadaOffline = parametrosSalida.Item("CHIP_DECLINED")

'REVISAMOS SI FUE UN DECLINADO OFFLINE
If declinadaOffline = "1" Then
Console.WriteLine("Declinada Offline")
Else
If codigoBanorte = "A" Then
codigoAut = parametrosSalida.Item("AUTH_CODE")
```

```
Console.WriteLine("Transacción aprobada: " + codigoAut)
Else
Console.WriteLine("Transacción declinada")
End If
End If
Catch ex As Exception
Console.WriteLine("Falla al procesar transacción: " + ex.Message)
End Try
```

En el método Procesar Transacción al enviar el parámetro **PAGO_MOVIL** con valor de "1", únicamente se procesarán transacciones con tarjetas Pago Móvil. El desarrollador deberá realizar alguna forma para que el usuario final de la aplicación de punto de venta haga una selección del método de pago: tarjeta o Pago Móvil.

Proceso de transacciones por módulos (Leer, Enviar y Notificar)

Lectura de tarjeta

Para aquellos usuarios que únicamente deseen utilizar la API para lectura de tarjetas y envíen la transacción a Banorte por un medio alterno, ésta llamada será la necesaria para obtener la información sobre tarjeta leída. A partir de los datos de salida devueltos por esta llamada, la aplicación será responsable de formar el mensaje hacia Banorte dependiendo del medio que utilice para tal fin, y una vez obtenido el resultado, independientemente de si fue aprobada, declinada o sin respuesta. Para transacciones de chip deberá ejecutar una llamada al método ***notifyResult***, el cual se explica más adelante.

Para pedir al PIN Pad que se prepare para leer una tarjeta, la aplicación del cliente deberá ejecutar la llamada al método ***readCard***. Este método tiene dos versiones. La primera espera dos argumentos: un **hashtable** de parámetros de entrada y otro de parámetros de salida. La segunda versión espera como único argumento un **hashtable** de parámetros de salida.

La primera versión del método (con parámetros de entrada y de salida) debe usarse siempre que la lectura de tarjeta sea con el fin de procesar alguna transacción que eventualmente pudiera ser con tarjeta de chip, para que se hagan las inicializaciones necesarias en el lector correspondiente. La aplicación del cliente debe especificar como mínimo el monto de la transacción que se ejecutará. Recuérdese que si la transacción es de chip, la aplicación del cliente debe notificar el resultado posteriormente con una llamada al método ***notifyResult***.

Obsérvese que si se usa esta versión del método entonces como mínimo deberá de pasarse el monto de la transacción en el **hashtable** de parámetros de entrada; de lo contrario el método lanzará una excepción.

La segunda versión del método (sin parámetros de entrada) puede usarse cuando la aplicación del cliente trabaje con tarjetas propias de banda magnética y no haya la posibilidad de que se presenten transacciones de chip.

En ambas versiones, el **hashtable** de parámetros de salida se deberá proporcionar inicialmente vacío; el método internamente llenará el **hashtable** con información para la aplicación acerca de las características de la lectura realizada.

En el momento de la ejecución de este método, el PIN Pad desplegará un mensaje en su pantalla invitando al cliente a insertar o deslizar su tarjeta. En el caso de tarjeta de chip, ésta no deberá retirarse del PIN Pad hasta que la aplicación haya completado la llamada a ***notifyResult***.

Los posibles parámetros de entrada que se pueden pasar a este método se documentan en el Apéndice A en la sección de **Parámetros de entrada**.

Ejemplo:

```
'CREAMOS LOS HASHTABLES PARA LA LECTURA DE LA TARJETA
Dim lecturaEntrada As New Hashtable()
Dim lecturaSalida As New Hashtable()

'CREAMOS LOS HASHTABLES PARA LOS PARAMETROS PARA ENVIAR LA TRANSACCION
Dim parametrosEntrada As New Hashtable()
Dim parametrosSalida As New Hashtable()

'INGRESAMOS COMO PARAMETRO DE ENTRADA EL MONTO DE LA TRANSACCION
lecturaEntrada.Add("AMOUNT", "10.00")
lecturaEntrada.Add("PAGO_MOVIL", "0")

'METODO DE LEER TARJETA
Try
pinpad.readCard(lecturaEntrada, lecturaSalida)
Catch ex As Exception
MsgBox("Falla al Leer la Tarjeta: " + ex.Message)
End Try
'OBTENEMOS LOS DATOS DE LA LECTURA DE LA TARJETA
Dim track2, track1, posEntryMode, tagsEMV As String

tagsEMV = lecturaSalida.Item("EMV_TAGS")
track1 = lecturaSalida.Item("TRACK1")
track2 = lecturaSalida.Item("TRACK2")
posEntryMode = lecturaSalida.Item("ENTRY_MODE")

'SI LA TARJETA ES CHIP ENVIAMOS LOS TAGS EMV
If PosEntryMode = "CHIP" or  PosEntryMode = "CONTACTLESSCHIP" Then
parametrosEntrada.Add("EMV_TAGS ", tagsEMV)
End If

'OBTENEMOS EL VALOR DE CHIP_DECLINED Y VER SI FUE UN DECLINADO OFFLINE
Dim declinadoOffline As String
declinadoOffline = lecturaSalida.Item("CHIP_DECLINED")

'VALIDAMOS UN DECLINADO OFFLINE
```

```
If declinadoOffline = "1" Then

'AQUI TERMINA LA OPERACION
Console.WriteLine("DECLINADO OFFLINE")
Else

'MÉTODO ENVIAR TRANSACCIÓN
End If
```

NOTA: Al enviar el parámetro **PAGO_MOVIL** con valor de "1" en el método ***readCard*** (***leerTarjeta***) el PIN Pad permitirá únicamente la lectura de una tarjeta en forma manual para PagoMóvil. Si se envía con valor de "0" únicamente permitirá la lectura de banda, y de chip y Contactleschip.

Envío de transacción

Para aquellos usuarios que por su arquitectura no estén en condiciones de enviar directamente la transacción a Banorte desde su punto de venta por medio de la llamada a ***processTransaction***, pero que puedan hacerlo desde otro punto y no requieran de utilizar ningún componente de software adicional, la API provee una clase denominada ***ConectorBanorte***, el cual posee un único método de tipo estático ***sendTransaction***, que tiene la capacidad de enviar una transacción hacia Banorte a partir de un **hashtable** de parámetros de entrada y entregar información sobre el resultado en un **hashtable** de parámetros de salida inicialmente vacío.

Es importante enfatizar, que este método no tiene relación alguna con el manejo de la transacción a nivel PIN Pad, sino que constituye una vía de comunicación directa a Banorte para aquellos usuarios que por sus características puedan encontrarlo de utilidad. La aplicación del cliente deberá usar las otras llamadas de la API (particularmente ***readCard*** y ***notifyResult***) en los equipos que tengan conectado el PIN Pad para hacerse cargo de la manipulación de éste.

También es importante señalar que, debido a que la comunicación se hace directamente con el procesador central de pagos de Banorte, los parámetros de entrada deberán especificarse en su versión en inglés, y los retornados en la salida igualmente se entregarán en su versión en inglés.

La aplicación del cliente deberá ser responsable de asegurarse de poner la totalidad de parámetros necesarios en el **hashtable** de entrada. Por ejemplo, si utiliza el método readCard para procesar las lecturas de tarjetas de clientes y una de ellas resultare ser de chip, deberá asegurarse de incluir los parámetros **EMV_TAGS** y **MODO_ENTRADA** que la llamada a readCard le haya regresado en el **hashtable** de parámetros de entrada que se pase al método ***sendTransaction***.

Al igual que en el caso del método ***processTransaction*** invocado sobre el objeto PIN Pad, el método ***sendTransaction*** invocado estáticamente sobre la clase ***ConectorBanorte*** requieren visibilidad hacia Banorte desde el equipo en donde se hace la ejecución.

Obsérvese que la gran diferencia entre el método ***processTransaction*** invocado sobre el objeto PIN Pad y el método ***enviarTransaccion*** invocado estáticamente sobre la clase ***ConectorBanorte***, es que el primero INCLUYE el manejo de la lectura de la tarjeta en el PIN Pad y la notificación del resultado de la transacción, mientras que el segundo es exclusivamente para hacer llegar una transacción hacia el procesador central de pagos de Banorte y se asume que la aplicación del cliente se está haciendo cargo aparte del manejo del PIN Pad por medio de las llamadas a ***readCard*** y ***notifyResult***. Ejemplo:

```
'LLENAMOS LOS PARAMETROS DEL HASHTABLE
parametrosEntrada.Add("CMD_TRANS", "AUTH")
parametrosEntrada.Add("MODE", "PRD")
parametrosEntrada.Add("MERCHANT_ID", "7395007")
parametrosEntrada.Add("USER", "a7395007")
parametrosEntrada.Add("PASSWORD", " a7395007")
parametrosEntrada.Add("TERMINAL_ID", "327782962")
parametrosEntrada.Add("CONTROL_NUMBER", "VENTA201410150001")
parametrosEntrada.Add("TRACK2", track2)
parametrosEntrada.Add("RESPONSE_LANGUAGE", "EN")
parametrosEntrada.Add("BANORTE_URL", "https://via.pagosbanorte.com/InterredesSeguro")
parametrosEntrada.Add("AMOUNT", "10.00")
parametrosEntrada.Add("ENTRY_MODE", posEntryMode)

If posEntryMode = "CHIP" or  posEntryMode = "CONTACTLESSCHIP"  Then
parametrosEntrada.Add("EMV_TAGS", tagsEMV)
ElseIf track1 <> "" Then
parametrosEntrada.Add("TRACK1", track1)
    End If
End If

'TOMAMOS DATOS DEL HASHTABLE Y LA ENVIA A PROCESAR A BANORTE
Try
Banorte.ConectorBanorte.sendTransaction(parametrosEntrada,
parametrosSalida)
Catch ex As Exception
MsgBox("Falla al procesar la transacción: " + ex.Message)
End Try
```

Notificación de resultado

La ejecución de este método es requerida para aquellos usuarios que se hagan cargo del envío de la transacción, cuando ésta sea de chip.

El método ***readCard*** retorna a la aplicación del cliente información en los parámetros de salida acerca del tipo de lectura obtenida (chip, banda o banda forzada). En el caso de chip, la aplicación deberá ejecutar una llamada a este método una vez que tenga el resultado de la transacción. La llamada deberá hacerse independientemente, si la transacción fue aprobada o declinada, e inclusive si no hubo respuesta.

En caso de que el banco emisor de la tarjeta haya decidido enviar información de autenticación al chip de la tarjeta, ésta será recibida por la aplicación del cliente al momento de recibir respuesta de la transacción enviada a Banorte y deberá pasarse como parámetro de entrada al método ***notifyResult***.

Finalmente, sólo para el caso de transacciones aprobadas, deberá también proporcionarse como parámetro de entrada, el código de autorización recibido a los parámetros de entrada que deben pasarse al método ***notifyResult***.

En el ejemplo de código mostrado en esta sección, se indica la lógica completa para una aplicación que se hace cargo de la transacción; el fragmento correspondiente a la llamada a ***notifyResult*** se pone aquí para comodidad del lector.

```
Dim codigoBanorte, codigoAut As String
codigoBanorte = parametrosSalida("PAYW_RESULT")
codigoAut = parametrosSalida("AUTH_CODE")

'REVISAREMOS SI LA TRANSACCION FUE CHIP O BANDA
If posEntryMode = "CHIP" Then

    'CREAMOS EL HASHTABLE PARA NOTIFICAR EL RESULTADO
    Dim parametrosEntradaNotificacion As New Hashtable()
    Dim parametrosSalidaNotificacion As New Hashtable()

'NOTIFICAMOS EL RESULTADO DEBIDO A QUE ES CHIP
If codigoBanorte <> "" Then
Dim datosEMV As String
datosEMV = parametrosSalida("EMV_DATA")

If datosEMV <> "" Then
parametrosEntradaNotificacion.Add("EMV_DATA", datosEMV)
End If

If codigoBanorte = "A" Then
parametrosEntradaNotificacion.Add("RESULT", "APPROVED")
parametrosEntradaNotificacion.Add("AUTH_CODE", codigoAut)
ElseIf condigoBanorte = "D"
parametrosEntradaNotificacion.Add("RESULT", "DECLINED")
Else
    parametrosEntradaNotificacion.Add("RESULT", "NO_RESPONSE")
End If
Else
parametrosEntradaNotificacion.Add("RESULT", "NO_RESPONSE")
End If

'METODO NOTIFICAR RESULTADO
Try
pinpad.notifyResult(parametrosEntradaNotificacion,
parametrosSalidaNotificacion)
```

```
Catch ex As Exception
MsgBox("Falla al notificar el resultado: " + ex.Message)
End Try

Dim EMVResultado As String
EMVResultado = parametrosSalidaNotificacion("EMV_RESULT")

If EMVResultado = "A" And codigoBanorte = "A" Then
Console.WriteLine("APROBADA")
ElseIf EMVResultado = "D" And codigoBanorte = "A" Then
Console.WriteLine("DECLINADA EMV")
Console.WriteLine("***** AQUI SE ENVIA LA REVERSA *****")

'GENERAMOS LOS HASTABLE PARA EL REVERSO DE LA TRANSACCIÓN ANTERIOR
Dim entradaReversa As New Hashtable()
Dim salidaReversa As New Hashtable()
Dim referencia As String
referencia = parametrosSalida.Item("REFERENCE")

'LLENAMOS LOS PARAMETROS DEL HASHTABLE
entradaReversa.Add("CMD_TRANS", "REVERSAL")
entradaReversa.Add("MODE", "PRD")
entradaReversa.Add("MERCHANT_ID", "7395007")
entradaReversa.Add("USER", "a7395007")
entradaReversa.Add("PASSWORD", " a7395007")
entradaReversa.Add("TERMINAL_ID", "327782962")
entradaReversa.Add("REFERENCE", referencia)
entradaReversa.Add("RESPONSE_LANGUAGE", "EN")
entradaReversa.Add("BANORTE_URL", "https://via.pagosbanorte.com/InterredesSeguro")

'EN TODAS LAS REVERSAS CUANDO EL EMV_RESULT ES IGUAL A "D" SE DEBE ENVIAR EL
PARÁMETRO "CAUSA" CON VALOR FIJO DE "17"
entradaReversa.Add("CAUSA", "17")

'TOMAMOS LOS DATOS DEL HASHTABLE Y SE ENVIA EL REVERSO A BANORTE
Try
Banorte.ConectorBanorte.sendTransaction(entradaReversa,
salidaReversa)
Catch ex As Exception
MsgBox("Falla al procesar el reverso: " + ex.Message)
End Try
Else
Console.WriteLine("DECLINADA")
End If
Else

'SOLO REPORTAMOS EL RESULTADO DEBIDO A QUE ES BANDA
If codigoBanorte = "A" Then
Console.WriteLine("APROBADA: " + codigoAut)
Else
```

```
Console.WriteLine("DECLINADA")
End If
End If
```

Finalizar transacción

Una vez completada una transacción, la aplicación deberá ejecutar este método para indicar este evento al dispositivo. Obsérvese que la ejecución de este método, junto con el de inicio de transacción deberá hacerse **POR CADA TRANSACCION** realizada con el dispositivo. Este método no requiere parámetros.

```
Try
pinpad.endTransaction()
Catch ex As Exception
MsgBox("Falla: " + ex.Message)
End Try
```

Despliegue de Texto

El método ***displayText*** es un método utilitario que puede ser empleado por la aplicación del cliente para personalizar los mensajes que aparecen en la pantalla del PIN Pad. Recibe como parámetro único un objeto de tipo **String** que contiene el texto que se desea desplegar. Se recomienda no utilizar acentos ni caracteres especiales, ya que no es seguro que éstos sean soportados por todas las versiones de firmware en los dispositivos.

Este llamado se puede operar como en el siguiente ejemplo:

```
If (CodigoBanorte = "A") Then
pinpad.displayText("Aprobada: " + CodigoAut)
Else
pinpad.displayText("Declinada")
End If
```

Liberación de dispositivo

El método ***releaseDevice*** debe ejecutarse al terminar la operación del PIN Pad, para asegurarse de liberar el puerto serial y los recursos asignados por el sistema operativo. Este método no requiere parámetros.

Ejemplo:

```
Try
pinpad.releaseDevice()
Catch ex As Exception
Console.WriteLine("Error al liberar dispositivo: " + ex.Message)
End Try
```

Obtención de versión de la API

El método ***getVersion*** es un método utilitario suministrado para que la aplicación del cliente pueda verificar con qué versión de la API se encuentra trabajando y así llevar un control efectivo en caso de que posteriormente sean liberadas versiones adicionales con nuevas capacidades.

El método deberá ser invocado con un objeto de tipo **Hashtable** inicialmente vacío; que el método retornará lleno con información sobre su versión. A continuación se muestra los nombres de dichos parámetros, a fin de que la aplicación del usuario pueda reconocerlos.

Ejemplo:

```
Dim salidaVersion As New Hashtable()
Dim version As String

Try
API.getVersion(salidaVersion)
version = salidaVersion.Item("VERSION")
Console.WriteLine("Versión de API: "+ version)
Catch ex As Exception
Console.WriteLine("Falla al obtener la versión: " + ex.Message)
End Try
```

Excepciones

Los métodos de la API en general pueden lanzar una excepción si ocurrió un problema durante la ejecución del método. La clase que representa esta excepción se llama ***BanorteException*** y se encuentra de igual manera dentro de ***BanortePinPad.dll*** (**Banorte.BanorteException**).

Para comodidad del usuario, se incluye un método adicional, denominado **getCodigo()**, el cual provee un código de error que la aplicación del cliente puede analizar para determinar exactamente la causa del error reportado y tomar la acción correspondiente. En el apéndice B se encuentran documentados los posibles códigos de error y sus textos asociados. También se proporciona una breve ayuda sobre cuáles podrían ser las causas y posibles soluciones.

Otros lenguajes

Banorte cuenta también con Dll y ejemplos para los siguientes leguajes de programación:

- NET ~~Java~~
- Delphi 7
- Delphi XE.
- ~~Java~~ ~~NET~~
- ~~Delphi 7~~
- ~~Delphi XE.~~

Si se desea información sobre el desarrollo de alguno de estos lenguajes contactar al Laboratorio de Payworks para solicitar más información.

APÉNDICE A: Tablas de parámetros

La mayoría de las llamadas de la API de PIN Pad provisto por Banorte trabajan utilizando mapas de parámetros de entrada y/o de salida. El contenido de este apéndice detalla los posibles valores de parámetros por llamada. Obsérvese que aunque la estructura de datos utilizada para contener tales parámetros es dependiente del lenguaje de programación utilizado, la semántica de los parámetros es la misma. En el capítulo Funciones de la API el usuario encontrará la información técnica específica sobre diferentes lenguajes de programación soportados por la versión actual de la API.

NOTA: Se recomienda **no utilizar** acentos ni caracteres especiales en las variables que se envíen al motor de pagos para una mejor interpretación de la información. Ya que los caracteres especiales son eliminados del mensaje para evitar problemas en el procesamiento y compensación de transacción.

Por ejemplo: Comillas (“), coma (,), diagonales (/,\), ampersand (&),porciento (%), pesos($), símbolos admiración (!, ¡), barra vertical (|), símbolos de interrogación (?,¿), comilla simple (‘), asterisco (*), guion medio(-), guion bajo(_), almohadilla o numeral (#) y paréntesis (()).

Obtención de versión

Parámetros de salida

Tabla 8. Parámetros de salida en obtener versión.

Parámetro		Comentario
Español	Inglés	
VERSION	**VERSION**	Contiene información sobre la versión de la API. Deberá ser una cadena de la forma x.yy.zz, donde ‘x’ corresponde a la versión, ‘yy’ a la subversión, y ‘zz’ a la construcción.

Inicialización de dispositivo (inicializarDispositivo/prepareDevice)

Parámetros de entrada

Tabla 9. Parámetros de entrada en inicialización de dispositivo.

Parámetro	Comentario	¿Requerido?

Español	Inglés		
PUERTO	**PORT**	El nombre del puerto que se vaya a utilizar con el PIN Pad. Ejemplo: COM3	Sí
VELOCIDAD	**BAUD_RATE**	La velocidad a utilizar en el puerto. Puede ser cualquier número entero positivo entre 9600 y 115200. Se recomienda usar valores estándar: 9600, 14400, 19200, etc.	Sí
PARIDAD	**PARITY**	Paridad a usar en la comunicación con el puerto serial. Valores posibles: N (Sin paridad), E (paridad par), O (paridad impar).	Sí
BITS_DATOS	**DATA_BITS**	Número de bits de datos usados en la comunicación con el puerto serial. Valores posibles: 7, 8.	Sí
BITS_PARO	**STOP_BITS**	No. de bits de paro usados en la comunicación con el puerto serial. Valores posibles: 1, 2.	Sí

Obtención de la información (obtenerInformacion/getInformation)

Parámetros de salida

Tabla 10. Parámetros de salida en la obtención de la información.

Parámetro		Comentario
Español	Inglés	
NUMERO_SERIE	**SERIAL_NUMBER**	Número de serie del dispositivo.
VERSION_APLICACION	**APPLICATION_VERSION**	Versión de la aplicación financiera instalada en el dispositivo.
IND_OPERATIVO	**OPERATIVE_FLAG**	Indica si el dispositivo ya cuenta con una clave de encriptación para operar. Valores posibles: • **"0".** El dispositivo no tiene llave cargada. • **"1".** El dispositivo tiene llave cargada.

Obtención del selector (obtenerSelector/getSelector)

Parámetros de salida

Tabla 11. Parámetros de salida en la obtención del selector.

Parámetro		Comentario
Español	Inglés	
SELECTOR	**SELECTOR**	Selector proporcionado por el dispositivo necesario para solicitar la llave de encriptación a Banorte cuando no se tiene conexión directa a Banorte desde el punto de venta.

Carga de llave con Modo de Operación Procesar Transaccion (actualizarLlaveMaestra/ loadMasterKey)

Parámetros de entrada

Tabla 12. Parámetros de entrada para la carga de llaves cuando existe conexión directa a Banorte.

Parámetro		Comentario	¿Requerido?
Español	Inglés		
ID_AFILIACION	**MERCHANT_ID**	El número de afiliación con el que se ejecuta el comando.	Sí
USUARIO	**USER**	Usuario con el que se ejecuta el comando	Sí
CLAVE_USR	**PASSWORD**	Clave con la que se ejecuta el comando.	Sí
NUMERO_SERIE	**SERIAL_NUMBER**	Número de serie del dispositivo al que se le va a hacer la carga de llaves.	Sí
IDIOMA_RESPUESTA	**RESPONSE_LANGUAGE**	A(2) Especifica el idioma en que se devolverán las variables de salida. Valores posibles: ES – Español, EN – Inglés	Sí
URL_BANORTE	**BANORTE_URL**	Enlace de pagos Banorte a donde se realizará la solicitud de la transacción. Liga de Payworks Seguro: https://via.pagosbanorte.com/InterredesSeguro	Sí

Carga de llave Modo de Operación Leer, Enviar y Notificar Transacción (cargarLlaveMaestra/ loadMasterKey)

Parámetros de entrada

Tabla 13. Parámetros de entrada para la carga de llaves cuando no existe conexión directa a Banorte.

Parámetro		Comentario	¿Requerido?
Español	Inglés		
NUMERO_SERIE	**SERIAL_NUMBER**	Número de serie del dispositivo al que se le va a hacer la carga de llaves.	Sí
LLAVE_MAESTRA	**MASTER_KEY**	Llave de encriptación proporcionada por Banorte para el dispositivo en específico.	Sí

Cancelación de carga de llave (cancelarCargaLlave/cancelLoadKey)

Parámetros de entrada

Tabla 14. Parámetros de entrada para la cancelación de la carga de llave.

Parámetro		Comentario	¿Requerido?
Español	Inglés		
NUMERO_SERIE	**SERIAL_NUMBER**	Número de serie del dispositivo al que se le va a cancelar la carga de llaves.	Sí

Procesamiento de transacciones

Modo de Operación Procesar Transacción (procesarTransaccion/processTransaction)

Parámetros de entrada

Tabla 15. Parámetros de entrada en proceso de transacción.

Parámetro		Comentario	¿Requerido?
Español	Inglés		
ID_AFILIACION	**MERCHANT_ID**	El número de afiliación con la que se ejecuta la transacción.	Sí, requerida siempre para cualquier transacción o comando.
USUARIO	**USER**	Usuario con el que se ejecuta la transacción.	Sí, requerida siempre para cualquier transacción o comando.
CLAVE_USR	**PASSWORD**	Contraseña del usuario con el que se ejecuta la transacción.	Sí, requerida siempre para cualquier transacción o comando
ID_TERMINAL	**TERMINAL_ID**	El identificador de punto de venta o terminal sobre la que se ejecuta la transacción	Sí, requerida para todas las transacciones (no para los comandos). El Identificador especificado deberá existir en la base de datos de Payworks, lo cual se hará normalmente al registrar una afiliación.
CMD_TRANS	**CMD_TRANS**	Indica la transacción o comando que se desea realizar. Posibles valores: • VENTA / AUTH	Sí

		• CASHBACK • VENTA_FORZADA / FORCED_AUTH • PREAUTORIZACION / PREAUTH • REAUTORIZACION / REAUTH • POSTAUTORIZACION / POSTAUTH • DEVOLUCION / REFUND • ~~CANCELACION / VOID~~ • REVERSA / REVERSAL • CIERRE_AFILIACION / MCHNT_SETTLEMENT • CIERRE_LOTE / GROUP_SETTLEMENT • VERIFICACION / VERIFY • SUSPENSION / LOCK • REACTIVACION / UNLOCK	
MONTO	**AMOUNT**	Especifica el monto de la transacción. Ejemplo: 147.50	Sí, excepto para comandos, y REVERSA.
MONTO_CASHBACK	**CASHBACK_AMOUNT**	Especifica el monto de cashback. Ejemplo: 150.00	Únicamente para transacciones CASHBACK
PAGO_MOVIL	**PAGO_MOVIL**	N(1) Permite que se abra el teclado para recibir una tarjeta de forma manual ÚNICAMENTE para tarjetas Pago Móvil. • 0 = No abre el teclado. • 1 = Abre el teclado.	Únicamente cuando se desea abrir el teclado para recibir transacciones Pago Móvil.
MODO	**MODE**	Indica el modo en que se ejecutará la transacción. Valores posibles: • Modo Producción: PRD • Modo de prueba autorizando siempre: AUT • Modo de prueba declinando siempre: DEC • Modo de prueba con autorización aleatoria: RND	Sí
REFERENCIA	**REFERENCE**	Especifica el no. de referencia entregada por Payworks para una transacción previamente procesada sobre la que esta nueva transacción o comando desea operar.	Requerida para las siguientes transacciones: REAUTORIZACION POSTAUTORIZACION DEVOLUCION. ~~CANCELACION y~~Y para la REVERSA o VERIFICACION. Si no se cuenta con este parámetro se debe

			enviar el NUMERO_CONTROL Y para los siguientes comandos: SUSPENSION REACTIVACION
LOTE	**GROUP**	AN (1..30) Identificador asignado por el comercio, sirve para agrupar un conjunto de preautorizaciones.	Opcional para una PREAUTORIZACION. Obligatorio para un CIERRE_LOTE.
CODIGO_AUT	**AUTH_CODE**	Número de autorización.	Solamente para la venta forzada
NUMERO_CONTROL	**CONTROL_NUMBER**	Referencia única para la transacción controlada por el cliente.	Requerida para cada transacción, y la VERIFICACION. Si se usa, la combinación del número de afiliación con este número de control deberá ser única por transacción.
REF_CLIENTE1	**CUSTOMER_REF1**	AN(1..30) Dato para uso exclusivo del cliente.	Opcional para cualquier transacción.
REF_CLIENTE2	**CUSTOMER_REF2**	AN(1..30) Dato para uso exclusivo del cliente.	Opcional para cualquier transacción.
REF_CLIENTE3	**CUSTOMER_REF3**	AN(1..30) Dato para uso exclusivo del cliente.	Opcional para cualquier transacción.
REF_CLIENTE4	**CUSTOMER_REF4**	AN(1..30) Dato para uso exclusivo del cliente.	Opcional para cualquier transacción.
REF_CLIENTE5	**CUSTOMER_REF5**	AN(1..30) Dato para uso exclusivo del cliente.	Opcional para cualquier transacción. En este parámetro se envía el identificador de las alianzas, integradores y agregadores.
URL_BANORTE	**BANROTE_URL**	Enlace de Pagos Banorte a donde se realizará la solicitud de la transacción. Liga de Payworks Seguro: **https://via.pagosbanorte.com/InterredesSeguro**	Sí.
TIEMPO_MAX	**TRANS_TIMEOUT**	Indica el tiempo máximo en segundos que se esperará por respuesta de la transacción	No (por defecto 120 segundos).
DIFERIMIENTO_INICIAL	**INITIAL_DEFERMENT**	N(2)	Requerida únicamente para las siguientes

		Indica el No. de meses a los que se difiere el pago (compre hoy y pague después). Si no hay diferimiento inicial, el valor reportado deberá ser 00.	transacciones: VENTA para indicar que incluyen promoción. Si está presente, las siguientes variables también deben estarlo: NUMERO_PAGOS TIPO_PLAN
NUMERO_PAGOS	**PAYMENTS_NUMBER**	N(2) Indica el no. de meses en los que se diluye el pago. Si sólo hay diferimiento inicial, el valor reportado deberá ser 00.	Requerida únicamente para las siguientes transacciones: VENTA para indicar que incluyen promoción. Si está presente, las siguientes variables también deben estarlo: DIFERIMIENTO_INICIAL TIPO_PLAN
TIPO_PLAN	**PLAN_TYPE**	N(2) Indica el tipo de plan de la promoción sobre la que se hace la transacción. Valores posibles: Si hay diferimiento inicial: 07 Si hay no. de pagos: 03 - sin intereses 05 - con intereses	Requerida únicamente para las siguientes transacciones: VENTA para indicar que incluyen promoción. Si está presente, las siguientes variables también deben estarlo: DIFERIMIENTO_INICIAL NUMERO_PAGOS
IDIOMA_RESPUESTA	**RESPONSE_LANGUAGE**	A(2) Especifica el idioma en que se devolverán las variables de salida. Valores posibles: ES – Español, EN – Inglés	Sí
QPS	**QPS**	N(1) Variable enviada para transacciones QPS (Quick Payment Service). Valores posibles: • 1 – Transacción QPS • 0 – Transacción normal	Sólo para transacciones donde no se requiera la firma autógrafa del tarjetahabiente.

Parámetros de salida

Tabla 16. Parámetros de salida en proceso de transacción

Parámetro		Comentario
Español	Inglés	

ID_AFILIACION	**MERCHANT_ID**	El número de afiliación sobre la que se ejecuta la transacción.
NUMERO_CONTROL	**CONTROL_NUMBER**	AN(1..30) Referencia única para la transacción controlada por el cliente. Entregada para todas las transacciones, sin importar si fueron aprobadas o no. Devuelta tal como el cliente la envía.
REFERENCIA	**REFERENCE**	Especifica el número de referencia entregada por Payworks para una transacción previamente procesada sobre la que esta nueva transacción o comando desea operar.
FECHA_REQ_CTE	**CUST_REQ_DATE**	AN(21) Fecha y hora en que la transacción/comando fue recibida del cliente en horario Payworks. Formato: AAAAMMDD HH:MM:SS.sss Entregada para todas las transacciones y comandos.
FECHA_REQ_AUT	**AUTH_REQ_DATE**	AN(21) Fecha y hora en que la transacción fue enviada al autorizador en horario Payworks Formato: AAAAMMDD HH:MM:SS.sss Entregada para todas las transacciones que se enviaron al autorizador.
FECHA_RSP_AUT	**AUTH_RSP_DATE**	AN(21) Fecha y hora en que la transacción/comando fue respondida por el autorizador en horario Payworks. Formato: AAAAMMDD HH:MM:SS.sss Entregada para todas las transacciones para las que se recibió respuesta del autorizador.
FECHA_RSP_CTE	**CUST_RSP_DATE**	AN(21) Fecha y hora en que la transacción/comando fue respondida al cliente. Formato: AAAAMMDD HH:MM:SS.sss Entregada para todas las transacciones y comandos.
RESULTADO_PAYW	**PAYW_RESULT**	A(1) Indica el resultado que Payworks reporta del proceso de la transacción o comando. Valores posibles: • A - Aprobada • D - Declinada • R - Rechazada • T - Sin respuesta del autorizador. Entregada para todas las transacciones y comandos.
RESULTADO_AUT	**AUTH_RESULT**	AN(1..10) Código enviado por el autorizador en la respuesta a una transacción. Entregada para todas las transacciones para las que se recibió respuesta del autorizador.
CODIGO_PAYW	**PAYW_CODE**	AN(8)

		Indica la razón por la que una transacción o comando es rechazado por Payworks. Entregada únicamente para transacciones o comandos que son rechazados por Payworks.
CODIGO_AUT	**AUTH_CODE**	AN(1..10) Código de autorización entregado por el autorizador para una transacción aprobada. Entregada opcionalmente para transacciones aprobadas por el Payworks (modo pruebas).
TEXTO	**TEXT**	AN(1..200) Texto adicional que proporciona mayor explicación sobre el resultado de la transacción. Opcionalmente entregada para una transacción o comando.
TARJETAHABIENTE	**CARD_HOLDER**	AN(1..50) Nombre del tarjetahabiente. Opcionalmente entregada por el autorizador para una transacción aprobada.
BANCO_EMISOR	**ISSUING_BANK**	AN(1..20) Nombre del banco emisor de la tarjeta. Opcionalmente entregada por el autorizador para una transacción aprobada.
MARCA_TARJETA	**CARD_BRAND**	AN(1..20) Marca de la tarjeta. Opcionalmente entregada por el autorizador para una transacción aprobada.
TIPO_TARJETA	**CARD_TYPE**	AN(1..20) Indica si la tarjeta es de débito o crédito. Opcionalmente entregada por el autorizador para una transacción aprobada.
NUMERO_TARJETA	**CARD_NUMBER**	N (16) Número de tarjeta.
FECHA_EXP	**CARD_EXP**	Fecha de expiración de la tarjeta con la que se realiza la transacción. El formato es AAMM. Si la transacción es manual (Pago Móvil) la fecha de expiración es retornada en el formato MMAA.
MODO_ENTRADA	**ENTRY_MODE**	Indica el modo en el que se procesó la tarjeta. Los valores posibles son los siguientes: • BANDA/MAGSTRIPE • CHIP • MANUAL (Pago Móvil) • CONTACTLESSCHIP • CONTACTLESSBANDA
DATOS_EMV	**EMV_DATA**	AN(1..200) Texto adicional que proporciona mayor explicación sobre el resultado de la transacción. Opcionalmente entregada por el autorizador para una transacción aprobada con tarjeta de chip.
ARQC	**ARQC**	Devuelto únicamente en transacciones con CHIP. No es necesario enviarlo hacia

		Banorte.
TVR	**TVR**	Terminal Verification Results (Tag 95). Devuelto únicamente en transacciones con CHIP para imprimir en el ticket. No es necesario enviarlo hacia Banorte.
TSI	**TSI**	Transactions Status Informations (Tag 9B). Devuelto únicamente en transacciones con CHIP para imprimir en el ticket. No es necesario enviarlo hacia Banorte.
AID	**AID**	Application ID (Tag 4F). Devuelto únicamente en transacciones con CHIP para imprimir en el ticket. No es necesario enviarlo hacia Banorte.
APN	**APN**	Application Preferred Name (Tag 9F12). Devuelto únicamente en transacciones con CHIP para imprimir en el ticket. No es necesario enviarlo hacia Banorte.
AL	**AL**	Application Label (Tag 50). Devuelto únicamente en transacciones con CHIP para imprimir en el ticket. No es necesario enviarlo hacia Banorte.
RESULTADO_EMV	**EMV_RESULT**	Resultado procesamiento EMV. Valores posibles: • A: Aprobado • D: Declinado.
DECLINADA_CHIP	**CHIP_DECLINED**	Si el valor es igual a 1, indica que por reglas de prevención de fraudes aplicadas en la validación del chip se declina de forma Offline la transacción. Esta transacción no deberá ser enviada a procesar a Banorte. Valores posibles: • 1: Declinada Offline Si la transacción fue exitosa no se retornará el parámetro.
TAGS_EMV	**EMV_TAGS**	Únicamente se retorna cuando es declinado Offline, estos datos se utilizan para imprimir algunos de los EMV Tags en el ticket. Ver Ejemplos Voucher.
TARJETA_REFERIDA	**REFERRED_CARD**	N (4) Últimos 4 dígitos de la tarjeta implicada en una transacción Referenciada. Entregada únicamente para las siguientes transacciones: ~~CANCELACION,~~ DEVOLUCIÓN, POSTAUTORIZACIÓN,

		REAUTORIZACIÓN, REVERSA.
CAPTURA_NIP	**PIN_ENTRY**	N (1) Indica si al momento de la transacción se ingresó un PIN para la validación del tarjetahabiente. Valores posibles: • 1 = Se ingresó PIN • 0 = No se ingresó PIN

Modo de Operación Leer, Enviar y Notificar Transacción

Lectura de tarjeta (leerTarjeta/readCard)

Parámetros de entrada

Tabla 17. Parámetros de entrada en lectura de tarjeta.

Parámetro		Comentario	¿Requerido?
Español	**Inglés**		
MONTO	**AMOUNT**	Especifica el importe de la transacción. Puede ser un número entero o con dos decimales. Ejemplo: 147.50	Sí
PAGO_MOVIL	**PAGO_MOVIL**	N (1) Indicador que permite abrir el teclado para ingresar manualmente una tarjeta Pago Móvil. • 0 = no abre teclado. • 1 = abre teclado.	No, únicamente si se desea abrir el teclado.
TIEMPO_MAX	**TRANS_TIMEOUT**	Indica el tiempo máximo en segundos que se esperará por respuesta de la transacción.	No (por defecto 120 segundos)

Parámetros de salida

Tabla 18. Parámetros de salida en lectura de tarjeta.

Parámetro		Comentario
Español	**Inglés**	
TARJETAHABIENTE	**CARD_HOLDER**	Nombre del tarjetahabiente. Alfanumérico de longitud variable. Retornado únicamente para aquellas tarjetas que sean reconocidas como bancarias.
NUMERO_TARJETA	**CARD_NUMBER**	Número de tarjeta leída (16 dígitos). Retornado únicamente para aquellas tarjetas que sean reconocidas como bancarias.
FECHA_EXP	**CARD_EXP**	Fecha de expiración de la tarjeta leída en formato AAMM. Retornado únicamente para aquellas tarjetas que sean reconocidas como bancarias. Si la transacción es manual (Pago Móvil) la fecha de expiración es retornada en el formato MMAA.

CODIGO_SEGURIDAD	**SECURITY_CODE**	CVV2/CVC2/4DBC retornado únicamente en tarjetas Pago Móvil y tarjetas American Express/JCB cuando el modo de entrada es banda magnética.
MODO_ENTRADA	**ENTRY_MODE**	Indica el modo en el que se procesó la tarjeta. Los valores posibles son los siguientes: • BANDA/MAGSTRIPE • CHIP • MANUAL (Pago Móvil) • CONTACTLESSCHIP • CONTACTLESSBANDA
TRACK1	**TRACK1**	Track 1 de la tarjeta con la que se realiza la transacción.
TRACK2	**TRACK2**	Track 2 de la tarjeta con la que se realiza la transacción.
TAGS_EMV	**EMV_TAGS**	Devuelto únicamente para lectura de tarjetas de chip. Es una secuencia de dígitos hexadecimales de longitud variable. La aplicación del cliente está obligada a enviar este dato a Banorte por el medio alterno que utilice.
ARQC	**ARQC**	Devuelto únicamente en transacciones con CHIP. No es necesario enviarlo hacia Banorte.
DECLINADA_CHIP	**CHIP_DECLINED**	Si el valor es igual a 1, indica que por reglas de prevención de fraudes aplicadas en la validación del chip se declina de forma Offline la transacción. Esta transacción no deberá ser enviada a procesar a Banorte. Valores posibles: • 1: Declinada Offline Si la validación del chip de la tarjeta fue exitosa no se retornará el parámetro.
AID	**AID**	Application ID (Tag 4F). Devuelto únicamente en transacciones con CHIP para imprimir en el ticket. No es necesario enviarlo hacia Banorte.
APN	**APN**	Application Preferred Name (Tag 9F12). Devuelto únicamente en transacciones con CHIP para imprimir en el ticket. No es necesario enviarlo hacia Banorte.
AL	**AL**	Application Label (Tag 50). Devuelto únicamente en transacciones con CHIP para imprimir en el ticket. No es necesario enviarlo hacia Banorte.
CAPTURA_NIP	**PIN_ENTRY**	N (1) Indica si al momento de la transacción se ingresó un PIN para la validación del tarjetahabiente. Valores posibles: • 1 = Se ingresó PIN • 0 = No se ingresó PIN

Envío de transacciones (enviarTransaccion/sendTransaction)

Parámetros de entrada

Tabla 19. Parámetros de entrada en envío de transacciones.

Parámetro		Comentario	¿Requerido?
Español	Inglés		
ID_AFILIACION	**MERCHANT_ID**	El número de afiliación con la que se ejecuta la transacción.	Sí, requerida siempre para cualquier transacción o comando.
USUARIO	**USER**	Usuario con el que se ejecuta la transacción.	Sí, requerida siempre para cualquier transacción o comando.
CLAVE_USR	**PASSWORD**	Contraseña del usuario con el que se ejecuta la transacción.	Sí, requerida siempre para cualquier transacción o comando.
ID_TERMINAL	**TERMINAL_ID**	El identificador de punto de venta o terminal sobre la que se ejecuta la transacción.	Requerida para todas las transacciones (no para los comandos). El identificador especificado deberá existir en la base de datos de Payworks, lo cual se hará normalmente al registrar una afiliación.
CMD_TRANS	**CMD_TRANS**	Indica la transacción o comando que se desea realizar. Posibles valores: • VENTA / AUTH • CASHBACK • VENTA_FORZADA / FORCED_AUTH • PREAUTORIZACION / PREAUTH • REAUTORIZACION / REAUTH • POSTAUTORIZACION / POSTAUTH • DEVOLUCION / REFUND • ~~CANCELACION / VOID~~ • REVERSA / REVERSAL • CIERRE_AFILIACION / MCHNT_SETTLEMENT • CIERRE_LOTE / GROUP_SETTLEMENT • VERIFICACION / VERIFY • SUSPENSION / LOCK • REACTIVACION / UNLOCK • OBTENER_LLAVE / GET_KEY	Sí
MONTO	**AMOUNT**	Especifica el monto de la transacción. Ejemplo: 147.50	Sí, excepto para comandos, y REVERSA

MONTO_CASHBACK	**CASHBACK_AMOUNT**	Especifica el monto de cashback. Ejemplo: 150.00	Únicamente para transacciones CASHBACK
PAGO_MOVIL	**PAGO_MOVIL**	N(1) Permite que se abra el teclado para recibir una tarjeta de forma manual ÚNICAMENTE para tarjetas Pago Móvil. • 0 = Indica que la transacción no es Pago Móvil. • 1 = Indica que la transacción es Pago Móvil.	Únicamente cuando se desea abrir el teclado para recibir transacciones Pago Móvil.
MODO_ENTRADA	**ENTRY_MODE**	Indica el modo en el que se procesó la tarjeta. Los valores posibles son los siguientes: • BANDA/MAGSTRIPE • CHIP • MANUAL (Pago Móvil) • CONTACTLESSCHIP	Sí
MODO	**MODE**	Indica el modo en que se ejecutará la transacción. Valores posibles: • Modo Producción: PRD • Modo de prueba autorizando siempre: AUT • Modo de prueba declinando siempre: DEC • Modo de prueba con autorización aleatoria: RND	Sí
REFERENCIA	**REFERENCE**	Especifica el no. de referencia entregada por Payworks para una transacción previamente procesada sobre la que esta nueva transacción o comando desea operar.	Requerida para las siguientes transacciones: REAUTORIZACION POSTAUTORIZACION DEVOLUCION ~~CANCELACION~~ Y para los siguientes comandos: SUSPENSION REACTIVACION Obligatorio al enviar REVERSA o VERIFICACION. Si no se cuenta con este parámetro se deberá enviar el NUMERO_CONTROL
LOTE	**GROUP**	AN (1..30)	Opcional para una PREAUTORIZACION.

		Identificador asignado por el comercio, sirve para agrupar un conjunto de preautorizaciones.	Obligatorio para un CIERRE_LOTE.
CODIGO_AUT	**AUTH_CODE**	Número de autorización.	Solamente para la venta forzada.
NUMERO_CONTROL	**CONTROL_NUMBER**	Referencia única para la transacción controlada por el cliente.	Opcional para cualquier transacción, y para el comando VERIFICACION. Si se usa, la combinación del número de afiliación con este número de control deberá ser única por transacción.
IDIOMA_RESPUESTA	**RESPONSE_LANGUAGE**	A(2) Especifica el idioma en que se devolverán las variables de salida. Valores posibles: ES – Español, EN – Inglés	Sí
REF_CLIENTE1	**CUSTOMER_REF1**	AN(1..30) Dato para uso exclusivo del cliente.	Opcional para cualquier transacción.
REF_CLIENTE2	**CUSTOMER_REF2**	AN(1..30) Dato para uso exclusivo del cliente.	Opcional para cualquier transacción.
REF_CLIENTE3	**CUSTOMER_REF3**	AN(1..30) Dato para uso exclusivo del cliente.	Opcional para cualquier transacción.
REF_CLIENTE4	**CUSTOMER_REF4**	AN(1..30) Dato para uso exclusivo del cliente.	Opcional para cualquier transacción.
REF_CLIENTE5	**CUSTOMER_REF5**	AN(1..30) Dato para uso exclusivo del cliente.	Opcional para cualquier transacción. En este parámetro se envía el identificador de las alianzas, integradores y agregadores.
URL_BANORTE	**BANORTE_URL**	Enlace de Pagos Banorte a donde se realizará la solicitud de la transacción. Liga de Payworks Seguro: **https://via.pagosbanorte.com/InterredesSeguro**	Sí.
TRACK1	**TRACK1**	Track 1 de la tarjeta con la que se realiza la transacción.	Sólo si está presente. Excepto para transacciones manuales.
TRACK2	**TRACK2**	Track 2 de la tarjeta con la que se realiza la transacción.	Sí, excepto para transacciones manuales.

NUMERO_TARJETA	**CARD_NUMBER**	Número de tarjeta leída (16 dígitos).	Únicamente para transacciones con tarjeta Pago Móvil
FECHA_EXP	**CARD_EXP**	N(4) Fecha de expiración de la tarjeta leída en formato AAMM.	Únicamente para transacciones con tarjeta Pago Móvil
CODIGO_SEGURIDAD	**SECURITY_CODE**	N(3..4) CVV2/CVC2/4DBC de la tarjeta	Únicamente para transacciones de American Express, JCB y manuales (Pago Móvil).
TAGS_EMV	**EMV_TAGS**	Secuencia de dígitos hexadecimales retornada por el lector de tarjetas cuando ésta es de chip. Deberá enviarse tal como se reciba a Banorte.	Únicamente para ventas y preautorizaciones con tarjetas de chip.
DIFERIMIENTO_INICIAL	**INITIAL_DEFERMENT**	N(2) Indica el No. de meses a los que se difiere el pago (compre hoy y pague después). Si no hay diferimiento inicial, el valor reportado deberá ser 00.	Requerida únicamente para las siguientes transacciones: VENTA para indicar que incluyen promoción. Si está presente, las siguientes variables también deben estarlo: NUMERO_PAGOS TIPO_PLAN
NUMERO_PAGOS	**PAYMENTS_NUMBER**	N(2) Indica el no. de meses en los que se diluye el pago. Si sólo hay diferimiento inicial, el valor reportado deberá ser 00.	Requerida únicamente para las siguientes transacciones: VENTA para indicar que incluyen promoción. Si está presente, las siguientes variables también deben estarlo: DIFERIMIENTO_INICIAL TIPO_PLAN
TIPO_PLAN	**PLAN_TYPE**	N(2) Indica el tipo de plan de la promoción sobre la que se hace la transacción. Valores posibles: Si hay diferimiento inicial: 07 Si hay no. de pagos:	Requerida únicamente para las siguientes transacciones: VENTA para indicar que incluyen promoción.

		03 - sin intereses 05 - con intereses	Si está presente, las siguientes variables también deben estarlo: DIFERIMIENTO_INICIAL NUMERO_PAGOS
QPS	**QPS**	N(1) Variable enviada para transacciones QPS (Quick Payment Service). Valores posibles: • 1 – Transacción QPS • 0 – Transacción normal	Solo para transacciones donde no se requiera la firma autógrafa del tarjetahabiente.
CAUSA	**CAUSE**	Variable que se envía únicamente para generar ~~cancelaciones~~ las reversas por Declinado EMV, cuando se envíe esta variable Payworks reconocerá que la transacción ha fallado por autenticación de chip en el dispositivo y generará correctamente el mensaje de reversa esperado hacia el emisor. Valor fijo que se debe enviar es **"17".**	Solamente para transacciones en donde se debe generar una REVERSA por falla en autenticación de Chip (Declinado EMV).

Parámetros de salida

Tabla 20. Parámetros de salida en envío de transacciones.

Parámetro		Comentario
Español	**Inglés**	
NUMERO_CONTROL	**CONTROL_NUMBER**	AN(1..30) Referencia única para la transacción controlada por el cliente. Entregada para todas las transacciones, sin importar si fueron aprobadas o no. Devuelta tal como el cliente la envía.
REFERENCIA	**REFERENCE**	Especifica el número de referencia entregada por Payworks para una transacción previamente procesada sobre la que esta nueva transacción o comando desea operar.
FECHA_REQ_CTE	**CUST_REQ_DATE**	AN(21) Fecha y hora en que la transacción/comando fue recibida del cliente en horario Payworks. Formato: AAAAMMDD HH:MM:SS.sss Entregada para todas las transacciones y comandos.
FECHA_REQ_AUT	**AUTH_REQ_DATE**	AN(21) Fecha y hora en que la transacción fue enviada al autorizador en horario Payworks Formato: AAAAMMDD HH:MM:SS.sss Entregada para todas las transacciones que se enviaron al autorizador.
FECHA_RSP_AUT	**AUTH_RSP_DATE**	AN(21)

		Fecha y hora en que la transacción/comando fue respondida por el autorizador en horario Payworks. Formato: AAAAMMDD HH:MM:SS.sss Entregada para todas las transacciones para las que se recibió respuesta del autorizador.
FECHA_RSP_CTE	**CUST_RSP_DATE**	AN(21) Fecha y hora en que la transacción/comando fue respondida al cliente. Formato: AAAAMMDD HH:MM:SS.sss Entregada para todas las transacciones y comandos.
RESULTADO_PAYW	**PAYW_RESULT**	A(1) Indica el resultado que Payworks reporta del proceso de la transacción o comando. Valores posibles: • A - Aprobada • D - Declinada • R - Rechazada • T - Sin respuesta del autorizador. Entregada para todas las transacciones y comandos.
RESULTADO_AUT	**AUTH_RESULT**	AN(1..10) Código enviado por el autorizador en la respuesta a una transacción. Entregada para todas las transacciones para las que se recibió respuesta del autorizador.
CODIGO_PAYW	**PAYW_CODE**	AN(8) Indica la razón por la que una transacción o comando es rechazado por Payworks. Entregada únicamente para transacciones o comandos que son rechazados por Payworks.
CODIGO_AUT	**AUTH_CODE**	AN(1..10) Código de autorización entregado por el autorizador para una transacción aprobada. Entregada opcionalmente para transacciones aprobadas por el Payworks (modo pruebas).
TEXTO	**TEXT**	AN(1..200) Texto adicional que proporciona mayor explicación sobre el resultado de la transacción. Opcionalmente entregada para una transacción o comando. Si se solicitó la llave de encriptación a Banorte, se retornará la llave de encriptación que deberá ser inyectada en el dispositivo.
BANCO_EMISOR	**ISSUING_BANK**	AN(1..20) Nombre del banco emisor de la tarjeta. Opcionalmente entregada por el autorizador para una transacción aprobada.
MARCA_TARJETA	**CARD_BRAND**	AN(1..20) Marca de la tarjeta. Opcionalmente entregada por el autorizador para una transacción aprobada.

TIPO_TARJETA	**CARD_TYPE**	AN(1..20) Indica si la tarjeta es de débito o crédito. Opcionalmente entregada por el autorizador para una transacción aprobada.
ID_AFILIACION	**MERCHANT_ID**	El número de afiliación sobre la que se ejecuta la transacción.
DATOS_EMV	**EMV_DATA**	AN(1..200) Texto adicional que proporciona mayor explicación sobre el resultado de la transacción. Opcionalmente entregada por el autorizador para una transacción aprobada con tarjeta de chip.
TARJETA_REFERIDA	**REFERRED_CARD**	N (4) Últimos 4 dígitos de la tarjeta implicada en una transacción Referenciada. Entregada únicamente para las siguientes transacciones: ~~CANCELACION,~~ DEVOLUCIÓN, POSTAUTORIZACIÓN, REAUTORIZACIÓN, REVERSA.

Notificación de resultado (notificarResultado/notifyResult)

Parámetros de entrada

Tabla 21. Parámetros de entrada en notificación de resultado.

Parámetro		Comentario	¿Requerido?
Español	**Inglés**		
RESULTADO	**RESULT**	Indica el resultado de la transacción. Valores posibles: • SIN_RESPUESTA (inglés: NO_RESPONSE) • APROBADA (inglés: APPROVED) • DECLINADA (inglés: DECLINED)	Sí
CODIGO_AUT	**AUTH_CODE**	Especifica el código de autorización recibido para la transacción en caso de que ésta haya sido aprobada. Número de 6 dígitos.	Sólo para transacciones aprobadas
DATOS_EMV	**EMV_DATA**	Script de Retorno del Banco Emisor. Retornada en algunas ocasiones en la función *enviarTransaccion*. Ejemplo: 910A2269D6C87518D4D130307110860E04D A9F580903DBE547581DED2F61 No necesita hacer ningún tipo de transformación o reconocimiento de la información recibida: simplemente deberá incluir la secuencia tal como se	Sólo Cuando haya una información Full EMV de parte del emisor.

	recibió. En caso de no recibirse el parámetro en *enviarTransaccion*, debe entenderse que el emisor no está enviando información Full EMV y por tanto este elemento no se incluirá en el mapa de entrada. No es válido pasar espacios en blanco o cadenas vacías para este caso.

Parámetros de salida

Tabla 22. Parámetros de salida en notificar resultado.

Parámetro		Comentario
Español	Inglés	
TVR	**TVR**	Terminal Verification Results (Tag 95). Devuelto únicamente en transacciones con CHIP para imprimir en el ticket. No es necesario enviarlo hacia Banorte.
TSI	**TSI**	Transactions Status Informations (Tag 9B). Devuelto únicamente en transacciones con CHIP para imprimir en el ticket. No es necesario enviarlo hacia Banorte.
RESULTADO_EMV	**EMV_RESULT**	Resultado procesamiento EMV. Valores posibles: • A: Aprobado • D: Declinado (debe generarse reversa).

APÉNDICE B: Códigos de error, rechazo y respuesta del emisor

Códigos de error

La Tabla 23 presenta la relación completa de posibles códigos de error reportados por los servicios de la API incluyendo el texto asociado, así como posibles causas y soluciones.

Tabla 23. Códigos de error de la API.

Código	Mensaje	Comentarios
ERR001	La lista de parámetros de entrada está vacía.	Se ejecutó una llamada a un servicio del API que requiere obligatoriamente por lo menos un dato en los parámetros de entrada.
ERR002	No se proporcionó el parámetro requerido xxx.	La estructura de parámetros de entrada no contiene un parámetro que es requerido para ese servicio de la API.
ERR003	El parámetro xxx es inválido.	El parámetro proporcionado (indicado en el texto del mensaje) no tiene ninguno de los

		posibles valores esperados por ese servicio de la API.
ERR004	Modelo de PIN Pad indicado no está soportado.	Generado cuando se trata de construir un objeto PIN Pad que no tiene soporte en la versión actual de la API.
ERR005	Operación no permitida debido a que el PIN Pad no ha sido inicializado.	La aplicación del cliente está tratando de ejecutar un servicio sobre el PIN Pad antes de ejecutar la inicialización correspondiente.
ERR006	Operación cancelada; el PIN Pad ya ha sido inicializado.	La aplicación del cliente está tratando de volver a inicializar el PIN Pad cuando ya lo había hecho. Debe ejecutarse antes una llamada a liberar Dispositivo.
ERR007	Falla al intentar inicializar puerto; verifique que exista y esté libre.	Generado cuando el identificador de puerto serial proporcionado no existe o está ocupado por otra aplicación. También puede ocurrir debido a una mala instalación del controlador del PIN Pad.
ERR008	Falla al configurar el puerto; verifique parámetros proporcionados.	Generado cuando alguno o algunos de los parámetros de configuración pasados en la inicialización del dispositivo no están soportados en la plataforma de ejecución. También puede ocurrir si existe algún problema de hardware o de controlador en el puerto serial seleccionado.
ERR009	Falla en transmisión hacia dispositivo; verifique conexiones.	Indica que la API no pudo enviar un paquete de datos hacia el PIN Pad. Esto puede deberse típicamente a: El PIN Pad está desconectado El PIN Pad está inestable El puerto está siendo usado por otra aplicación El controlador no se instaló correctamente La versión de firmware en el PIN Pad no es la adecuada
ERR010	Falla en recepción de dispositivo; verifique conexiones.	Indica que falló la recepción de un paquete de datos desde el PIN Pad hacia el equipo que lo maneja. Esto puede deberse típicamente a: El PIN Pad está desconectado El PIN Pad está inestable El puerto está siendo usado por otra aplicación El controlador no se instaló correctamente La versión de firmware en el PIN Pad no es la adecuada
ERR011	No se recibió respuesta de la PIN Pad en el tiempo máximo permitido.	Generado cuando el máximo tiempo de respuesta para la operación con el PIN Pad se agotó, y éste no ha respondido. Puede deberse a: El PIN Pad está desconectado El PIN Pad está inestable El puerto está siendo usado por otra aplicación

		El controlador no se instaló correctamente La versión de firmware en el PIN Pad no es la adecuada
ERR012	Respuesta inválida de PIN Pad; verifique versión y conexiones.	Se produce cuando el PIN Pad responde a los comandos enviados por la API, pero estas respuestas no están conforme a protocolo. Esto puede deberse a: El puerto está siendo usado por otra aplicación El controlador no se instaló correctamente La versión de firmware en el PIN Pad no es la adecuada
ERR013	Transacción cancelada por el usuario.	Se produce cuando el cliente oprime el botón Cancelar en el teclado del PIN Pad, originando que se aborte la transacción en curso.
ERR014	Transacción abortada por falla en lectura de chip de tarjeta.	Originada cuando el chip de la tarjeta que se inserta no puede ser leído después del número máximo de reintentos y no hay posibilidad de hacer una lectura de banda forzada.
ERR015	Código de autorización no es válido.	Generado por el servicio notifyResult de la API, cuando el código de autorización que se pasa como parámetro de entrada no tiene el formato esperado.
ERR016	Falla al intentar enviar transacción a Banorte. Código interno = xxx. Por Ejemplo: (016, 052)	Se produce al momento de intentar enviar una transacción hacia Banorte, y el envío falla. Típicamente puede provocarse por un problema en el entorno de ejecución: No hay conexión a Internet, o el medio de acceso a Banorte está caído Existe algún tipo de bloqueo en la red del cliente que no permite la salida hacia Banorte Existe algún problema de comunicaciones en el equipo donde se ejecuta la llamada En caso de no encontrar la falla se recomienda tomar nota del código interno reportado en el texto del mensaje para solicitar ayuda a soporte Banorte.
ERR017	Tarjeta ha sido retirada antes de tiempo; transacción abortada.	Se produce cuando el cliente retira su tarjeta de chip antes de que el proceso de notificación del resultado de la transacción se haya llevado a cabo.
ERR018	La transacción ha sido abortada inesperadamente.	Generada por el dispositivo PIN Pad cuando se detecta alguna anomalía inesperada (por ejemplo, una falla en el mecanismo de lectura de chip).
ERR019	No se recibió respuesta del banco; verifique si la transacción fue realmente procesada.	Se produce cuando una transacción se envía a Banorte pero no se recibe respuesta en el tiempo máximo esperado. Se recomienda

		revisar la línea de acceso a Banorte; si se comprueba que todo está bien entonces dirigirse al área de soporte técnico.
ERR020	URL de conexión no es válido.	La dirección proporcionada para enviar la transacción a Banorte no tiene el formato esperado.
ERR021	Incapaz de establecer conexión con Banorte.	El equipo donde está instalada la Dll no tiene acceso a Internet para enviar la transacción.
ERR022	URL no reconocido; verifique valor proporcionado y/o disponibilidad de conexión al banco.	La dirección proporcionada para enviar la transacción a Banorte es válida pero no pudo ser resuelta por ninguno de los servidores DNS. Puede presentarse con clientes que accedan a Banorte a través de Internet y cuyo proveedor ISP tenga algún tipo de problema.
ERR023	Parámetro proporcionado no es del tipo esperado; se requiere un objeto Dictionary.	El dato proporcionado no es correcto.
ERR024	La tarjeta no es válida para realizar transacciones con este dispositivo.	Tarjeta inválida.
ERR025	El emisor de la tarjeta no está soportado actualmente en el dispositivo.	Se está realizando una transacción con una tarjeta que no puede ser leída en el dispositivo.
ERR026	La tarjeta presenta algún daño físico que impide su lectura.	La tarjeta está dañada.
ERR027	La transacción fue declinada fuera de línea por el dispositivo.	La transacción fue declinada fuera de línea.
ERR028		Se produce cuando existe un problema al tratar de recuperar la información del dispositivo.
ERR029		Existe un problema para recuperar el selector proporcionado por el equipo.
ERR030		Los datos internos generados por el dispositivo al ejecutar la función *getSelector* no cumplen con las especificaciones esperadas por la interfaz.
ERR031		Este error puede producirse al ejecutar la función *obtenerSelector* si la verificación de redundancia cíclica efectuada por la API. Al selector leído del dispositivo no es satisfactoria.
ERR032		El número de serie proporcionado no coincide con el número de serie del dispositivo.
ERR033		La llave que se está intentando cargar está siendo rechazada por el dispositivo. Debido a que ha sido modificada o el dispositivo no está esperando una carga de llave.
ERR034		No fue posible obtener una llave de encriptación o el dispositivo todavía no cuenta con una llave registrada en Banorte.

ERR099	Falla inesperada; por favor contacte a Soporte Payworks Banorte.	Se detectó una anomalía interna en el software de la API. Se pide llamar a soporte Banorte y proporcionar información detallada sobre la forma en que logró generarse este error.

Códigos de rechazo

La siguiente tabla muestra los códigos de rechazo enviados por Payworks al enviar una transacción. Estos códigos de rechazo se retornan en el parámetro **CODIGO_PAYW** en español y **PAYW_CODE** en inglés.

Tabla 24. Códigos de rechazo de Payworks.

CODIGO	TEXTO EN INGLES	TEXTO EN ESPAÑOL
PROBLEMAS RELACIONADOS CON SSL		
PAYW-0001	Platform does not support requested SSL algorithm	El algoritmo definido para encriptar en SSL no está soportado en esta plataforma
PAYW-0002	Unexpected error when trying to access local keystore	Falla inesperada al acceder almacén de llaves (keystore)
PAYW-0003	The keystore could not be found at the configured location	El almacén de llaves (keystore)especificado no existe en la ubicación configurada
PAYW-0004	The keystore is not valid or is corrupted	El almacén de llaves (keystore) configurado no es válido o está corrupto
PAYW-0005	Access to keystore is not allowed	El acceso al almacén de llaves (keystore) fue denegado por falta de permisos
PAYW-0006	General failure during SSL handshaking	Falla general de seguridad en manejo de socket SSL
PROBLEMAS RELACIONADOS CON SERVIDOR TCP		
PAYW-0101	Socket server cannot be started	Falla al inicializar servidor de sockets
PROBLEMAS RELACIONADOS CON CLIENTE TCP		
PAYW-0201	Client was unable to create socket to connect to server xxx	Falla al intentar crear socket en cliente hacia servidor xxx
PAYW-0202	Unable to connect to server xxx	Incapaz de establecer conexión con servidor xxx
PAYW-0203	Connection to server xxx has been closed. Trying to reconnect	No se tiene conexión actualmente con el servidor xxx. Se intenta reconexión
PROBLEMAS RELACIONADOS CON MENSAJERIA ISO		
PAYW-1001	Received ISO message does not meet the expected format	El mensaje ISO recibido no tiene el formato esperado
PAYW-1002	Invalid TPU in the received ISO message	El mensaje ISO recibido contiene una TPDU no válida
PAYW-1003	The bitmap in the received ISO message is not valid	El mensaje ISO recibido no tiene un mapa de bits consistente
PAYW-1004	Received ISO message has an invalid suffix	El mensaje ISO recibido tiene un terminador no válido
PAYW-1005	Failure when trying to decode field xxx	Falla al decodificar el campo xxx
PAYW-1006	Failure when trying to encode xxx. Value\: "yyy"	Falla al codificar el campo xxx. Valor\: 'yyy"

PAYW-1007	Field contents in the ISO message exceeds the maximum allowed	El contenido del campo excede el máximo permisible
PAYW-1008	Unexpected type for field xxx in the ISO message	El tipo del campo xxx no es del tipo esperado
PAYW-1009	Charset ISO-8859-1 is not supported in the current execution platform	El juego de caracteres ISO-8859-1 no está soportado en esta plataforma
PAYW-1010	Incomplete field xxx in the ISO message	El campo xxx está incompleto
PAYW-1011	Invalid field xxx in the ISO message	El campo xxx no es válido
PAYW-1012	Variable length for field xxx exceeds value specified in the prefix	La longitud del campo variable xxx excede lo indicado en el prefijo
PAYW-1013	Field xxx has an invalid content	El contenido del campo xxx no es válido
PAYW-1014	POS Entry Mode (field 22) has an invalid value	El modo de entrada (campo 22) no es válido
PAYW-1015	Field xxx is required but was not included in the ISO message	El campo xxx es requerido y no fue incluido en el mensaje ISO
PAYW-1016	Statistical message does not have the expected format	El mensaje de estadísticos recibido no tiene el formato esperado
PAYW-1017	Unable to recognize transaction sent by device	No ha sido posible identificar el tipo de transacción enviada por el dispositivo
PAYW-1018	Information about Q6 promotion is not valid	La información de promoción Q6 es inválida
	PROBLEMAS RELACIONADOS CON INTERFAZ HTTP	
PAYW-2001	Unexpected failure when Processing command/transaction	Falla inesperada al intentar procesar transacción
PAYW-2002	Parameter 'xxx' cannot be provided for a manual transaction	El parámetro 'xxx' no puede incluirse en una transacción manual
PAYW-2003	Parameter 'xxx' cannot be provided for transaction with a swiped/inserted card	El parámetro 'xxx' no puede incluirse en una transacciónconplástico presente
PAYW-2004	Parameter 'xxx' with value 'yyy' can only be provided for a transaction with a chip card	El parámetro 'xxx' con valor 'yyy' sólo es requerido en una transacción de chip
PAYW-2005	Parameter 'xxx' with value 'yyy' cannot be accepted for a manual transaction	El parámetro 'xxx' con valor 'yyy' no es compatible con una transacción manual
PAYW-2006	Parameter 'xxx' with value 'yyy' cannot be accepted for a swiped / inserted card	El parámetro 'xxx' con valor 'yyy' no es compatible con una transacción con plástico presente
PAYW-2007	Promotional transaction requires some missing fields	La información sobre la promoción en la transacción no está completa
PAYW-2008	Parameter 'xxx' with value 'yyy' specifies an expired date	El parámetro 'xxx' con valor 'yyy' corresponde a una fecha expirada
PAYW-2009	Command requires either 'REFERENCE' or 'CONTROL_NUMBER'	El comando requiere 'REFERENCIA' o 'NUMERO_CONTROL'
PAYW-2010	Required parameter 'CMD_TRANS' was not supplied	No se especificó el parámetro requerido 'CMD_TRANS'
PAYW-2011	Requested Command/transaction 'xxx' is not valid or not supported	El comando/transacción 'xxx' no es válido(a) o no está soportado(a)
PAYW-2012	Value 'yyy' supplied for parameter 'xxx' is not valid	El valor 'yyy' suministrado para el parámetro 'xxx' es inválido

PAYW-2013	Value 'yyy' supplied for parameter 'xxx' exceeds maximum allowed length\: zzz	El valor 'yyy' suministrado para el parámetro 'xxx' excede la longitud máxima permitida\: zzz
PAYW-2014	Parameter 'xxx' cannot be null	El parámetro 'xxx' no puede ser nulo
PAYW-2015	No response received for the command / transaction	No hubo respuesta para el comando / transacción
PAYW-2016	Parameters 'XID' y 'CAVV' are required for this type of transaction	Los parámetros 'XID' y 'CAVV' son obligatorios para este tipo de transacción
PAYW-2017	Failure while trying to decypher transaction data	Falla al intentar descifrar campos de transacción
PAYW-2018	The following parameter is required to process the request: ''	El siguiente parámetro es requerido para procesar el requerimiento: ''
PAYW-2019	The key needed to decrypt data from this device has not been loaded or is not available	La llave necesaria para procesar datos cifrados no ha sido cargada para este dispositivo o no está disponible
PAYW-2020	Unable to decrypt data received at the 'INTERREDES' channel	Falla al intentar descifrar requerimiento enviado al canal INTERREDES
PAYW-2021	Parameter '' cannot accept negative values	El parámetro '' no puede aceptar valores negativos
PAYW-2022	Response url not valid	Respuesta url no válida
PAYW-2023	Control number not secure	El número de control no es seguro
PAYW-2024	Response url not valid	Respuesta url no válida
	PROBLEMAS RELACIONADOS CON COMANDOS Y TRANSACCIONES	
PAYW-3001	Unable to execute command/transaction; please retry later	Incapaz de realizar operación. Por favor intente más tarde
PAYW-3002	Invalid Affiliation / User	La afiliación o el usuario proporcionados no existen
PAYW-3003	Invalid User / Password	Usuario o contraseña inválidos
PAYW-3004	Affiliation xxx is currently inactive	La afiliación xxx no se encuentra activa
PAYW-3005	Client xxx is currently inactive	El cliente xxx no se encuentra activo
PAYW-3006	User xxx is currently inactive	El usuario xxx no se encuentra activo
PAYW-3007	User xxx is not allowed to execute commands / transactions	El usuario xxx no tiene el permiso necesario para ejecutar comandos/transacciones
PAYW-3008	Terminal xxx does not exist for this affiliation	La terminal xxx no existe para esta afiliación
PAYW-3009	Terminal xxx is currently inactive	La terminal xxx no se encuentra activa
PAYW-3010	Card brand / terminal do not allow this type of transaction	Transacción no permitida para esta terminal y marca de tarjeta
PAYW-3011	Command xxx is not currently supported	El comando xxx no está soportado actualmente
PAYW-3012	Referred transaction xxx does not exist	La transacción referenciada xxx no existe
PAYW-3013	Referred transaction xxx has been previously cancelled	La transacción referenciada xxx ya había sido cancelada
PAYW-3014	Rejected: The total amount for transaction xxx has been already refunded	Rechazada: El 100% del importe de la transacción referenciada xxx ya ha sido devuelto
PAYW-3015	Rejected: Partial refunds have been already applied to referred transaction xxx	Rechazada: La transacción referenciada xxx ya tiene devoluciones parciales aplicadas

PAYW-3016	Illegal to execute a refund on the referred transaction xxx	La transacción referenciada xxx no permite devoluciones
PAYW-3017	Refund requires the referred transaction xxx to be closed first (still open)	No es posible efectuar una devolución sobre la transacción xxx, la cual no ha sido cerrada
PAYW-3018	Amount requested in the refund xxx exceeds the maximum allowed: yyy	El importe de la devolución por xxx excede el máximo disponible: yyy
PAYW-3019	Not allowed to close a reauthorization; please use the original preauthorization	No se admite el cierre de reautorizaciones; utilice la preautorización original
PAYW-3020	Postauthorizations are only valid for open preauthorizations	Sólo se permiten postautorizaciones para preautorizaciones abiertas
PAYW-3021	Postauthorization's amount of xxx exceeds the maximum allowed: yyy	El monto de la postautorización por xxx excede el máximo disponible: yyy
PAYW-3022	Reauthorizations are only valid for open preauthorizations	Sólo se permiten reautorizaciones para preautorizaciones abiertas
PAYW-3023	Reauthorizations are not allowed for this application type: xxx	El tipo de aplicación xxx no permite reautorizaciones
PAYW-3024	Illegal to execute a cancellation on the referred transaction xxx	La transacción referenciada xxx no permite cancelaciones
PAYW-3025	Cancellation requires the referred transaction xxx to be closed first (still open)	No es posible efectuar una cancelación sobre la transacción xxx, la cual no ha sido cerrada
PAYW-3026	Not allowed to execute cancellations	No se tiene el permiso necesario para ejecutar una cancelación
PAYW-3027	Not allowed to execute a cashback	No se tiene el permiso necesario para ejecutar una transacción de cashback
PAYW-3028	Not allowed to execute a credit	La transacción de crédito directo no está habilitada
PAYW-3029	Not allowed to execute a refund	No se tiene el permiso necesario para ejecutar una transacción de devolución
PAYW-3030	Unrestricted or late refunds are not allowed	Las devoluciones tardías (sin restricción de batch) no están habilitadas
PAYW-3031	Not allowed to execute transactions including promotions	No se tiene el permiso necesario para efectuar una transacción con promoción
PAYW-3032	Not allowed to execute QPS transactions	No se tiene el permiso necesario para ejecutar transacciones QPS
PAYW-3033	Not allowed to execute a forced authorization	No se tiene el permiso necesario para realizar una venta forzada
PAYW-3034	Amount exceeds the maximum allowed for a QPS transaction	El monto indicado en la transacción QPS excede el máximo permisible
PAYW-3035	Affiliation requires a valid terminal number to be supplied	La afiliación requiere que se proporcione una terminal válida
PAYW-3036	Default terminal does not exist in the database	La terminal por defecto no ha sido creada en la base de datos
PAYW-3037	Card type xxx is not currently supported	No hay soporte para las tarjetas de marca xxx
PAYW-3038	Authorizer xxx is not currently supported	No hay soporte para el autorizador xxx
PAYW-3039	Control number xxx has been already used for a previous transaction	El no. de control xxx ya existe para una transacción anterior
PAYW-3040	Transactions with amount zero are not valid	No se permite monto cero en una transacción
PAYW-3041	FALLBACK transactions are not allowed	Las transacciones FALLBACK no están permitidas

PAYW-3042	The 3DSecure eCommerce indicator (ECI) received for this transaction is not allowed	El indicador de 3DSecure (ECI)recibido para esta transacción no está permitido
PAYW-3043	Previous operation required by this transacction could not be executed	La operación previa requerida para ejecutar esta transacción no tuvo éxito
PAYW-3044	Previous operation required by this transacction was declined by authorizer	La operación previa requerida para ejecutar esta transacción fue declinada por el autorizador
PAYW-3045	No response received for previous operation required by this transaction	La operación previa requerida para ejecutar esta transacción no tuvo respuesta
PAYW-3046	The security code is required and was not supplied	El código de seguridad es requerido y no fue proporcionado
PAYW-3047	Transaction entry mode is not allowed for affiliation type: xxx	El modo de entrada de la transacción no es compatible con el tipo de afiliacion: xxx
PAYW-3048	No manual entry mode for transactions is allowed	No se tiene el permiso necesario para ejecutar transacciones digitadas o manuales
PAYW-3049	Referred transaction xxx has been previously reversed	La transacción referenciada xxx ya había sido reversada
PAYW-3050	The referred transaction cannot be reversed	La transacción referenciada no admite reversas
PAYW-3051	Referred transaction xxx had not been approved	La transacción referenciada xxx no había sido aprobada
PAYW-3052	Referred transaction xxx is currently locked	La transacción referenciada xxx se encuentra en estado de suspensión
PAYW-3053	Cashback is only allowed for transactions with card present (CHIP / MAGSTRIPE)	La transacción de cashback sólo está permitida con plástico presente (CHIP / BANDA)
PAYW-3054	No transaction was found for the affiliation / terminal supplied	No se encontró ninguna transacción para la afiliación/terminal suministrados
PAYW-3055	Referred transaction exists, but it was not generated by the supplied terminal	La transacción referenciada existe, pero no fue generada por la terminal proporcionada
PAYW-3056	Referred transaction exists,but it does not belong to the supplied affiliation	La transacción referenciada existe, pero no pertenece a la afiliación proporcionada
PAYW-3057	Settlement for group xxx is already running; cannot be executed concurrently more than once	El cierre del lote xxx ya está en proceso; no puede ejecutarse concurrentemente más de una vez
PAYW-3058	Settlement for this affiliation is already running; cannot be executed concurrently more than once	El cierre masivo para esta afiliación ya está en proceso; no puede ejecutarse concurrentemente más de una vez
PAYW-3059	No transaction mode was sent (if it is an ISO transaction, please make sure that the affiliation is of type TPV)	No se especificó modo de la transacción (si es ISO verifique que la afiliación sea de tipo TPV).
PAYW-3060	The affiliation is of type TPV. It is not valid to provide the MODE parameter	La afiliación es de tipo TPV;no es válido proporcionar el parámetro MODO
PAYW-3061	The affiliation has been configured as aggregator but the format indicator is null	La afiliación ha sido configurada como agregador pero el indicador de formato es nulo
PAYW-3062	The affiliation has been configured as aggregator; missing associated merchant is required (SUB_MERCHANT)	La afiliación es un agregador; se requiere obligatoriamente el nombre del comercio asociado (SUB_AFILIACION)

PAYW-3063	This transaction is not acceptable under mobile payment mode	Esta transacción no es aceptable con pago móvil
PAYW-3064	Not allowed to execute mobile payment transactions	No se tiene el permiso necesario para ejecutar transacciones de pago móvil
PAYW-3065	This card cannot be used in mobile payment transactions	Esta tarjeta no está autorizada para realizar transacciones de pago móvil
PAYW-3066	Mobile payment transactions can only be manually entered	Las transacciones de pago móvil únicamente pueden ser digitadas
PAYW-3067	Plan type xxx is not valid	El valor del tipo de plan suministrado xxx es inválido
PAYW-3068	Promotion is not valid or not supported	La promoción proporcionada es inválida o no está soportada
PAYW-3069	Plan type xxx conflicts with other data in the promotion	El tipo de plan xxx es inconsistente con la promoción proporcionada
PAYW-3070	This transaction cannot be sent in test mode, since the referred transaction was sent in production mode	No se admite esta transacción en modo de prueba, ya que la transacción referenciada fue enviada en modo de producción
PAYW-3071	This transaction cannot be sent in production mode, since the referred transaction was sent in test mode	No se admite esta transacción en modo de producción, ya que la transacción referenciada fue enviada en modo de prueba
PAYW-3072	The requested cashback amount is below the minimum required	El monto a disponer en esta transacción está por debajo del mínimo requerido
PAYW-3073	The requested cashback amount exceeds the maximum allowed	El monto a disponer en esta transacción excede el máximo autorizado
PAYW-3074	The maximum number of cashback transactions allowed per day has been already reached	El número máximo de transacciones cashback que pueden ejecutarse en un día ha sido ya alcanzado
PAYW-3075	Transacion rejected since it would cause the maximum allowed daily cashback disposal to be exceeded	Transacción rechazada ya que se excedería el monto máximo diario autorizado de disposición cashback
PAYW-3076	Reauthorizations on a previous EMV transaction are not acceptable; a new preauthorization is required	No se admiten reautorizaciones de una transacción previa de tipo EMV; se requiere nueva lectura de plástico
PAYW-3077	Amount exceeds maximum limit allowed for a manual transaction	El monto excede el tope máximo permisible para una transacción digitada
PAYW-3078	One or more elements required by the referred transaction are empty	Uno o más elementos requeridos por la transacción referenciada no fueron proporcionados
PAYW-3079	Selector validation for device serial number '' failed	Falla al validar el selector enviado para el pinpad con número de serie ''
PAYW-3080	Unable to cypher master key for device with serial number ''	Falla al intentar cifrar la llave que se enviará al pinpad con número de serie ''
PAYW-3081	No terminal was found having the provided serial number ''	No se encontró una terminal válida para el número de serie proporcionado ''
PAYW-3082	The device with serial number '' has not been assigned a key	El dispositivo con número de serie '' no cuenta con una llave asignada
PAYW-3083	Unable to retrieve exception bins for the requesting customer	Falla al obtener lista de bines de excepción para el cliente solicitante
PAYW-3084	Failure when trying to cipher list of exception bins requested by device with serial number ''	Falla al intentar cifrar lista de bines de excepción que se enviará al dispositivo con número de serie ''

PAYW-3085	Referred transaction '' had not been approved	La transacción referenciada '' no había sido aprobada
PAYW-3086	Transacion rejected. Use chip reader slot	Transacción rechazada, utilice lector chip
PAYW-3087	Referred transaction {0} does not exist	La transaccion referenciada {0} no existe
PAYW-3088	Exceeded the days of the closing time limit	Excedio los dias del tiempo limite de cierre
	PROBLEMAS RELACIONADOS CON AUTORIZADORES	
PAYW-4001	Configuration for connector to authorizer xxx does not include any channel	El conector hacia el autorizador xxx no tiene canales configurados
PAYW-4002	Authorizer xxx is not currently available	El autorizador xxx no está disponible
PAYW-4003	Transaction xxx is not supported for authorizer yyy	La transacción xxx no está soportada para el autorizador yyy
PAYW-4004	Timeout for transaction xxx; response not received within the maximum amount of time	El tiempo máximo de espera para la transacción xxx ha sido excedido
PAYW-4005	Authorizer requires track 1 for this transaction	El track 1 es requerido por el autorizador para esta transacción
PAYW-4006	There is no information in the database about the Specified affiliation/terminal for the authorizer xxx	No hay información en la base de datos sobre afiliación/terminal para enviar hacia el autorizador xxx
PAYW-4007	There is no terminal id for the authorizer xxx	No existe no. de terminal paraenviar hacia el autorizador xxx
PAYW-4008	There is no merchant id for the authorizer xxx	No existe no. de afiliación para enviar hacia el autorizador xxx
PAYW-4009	Invalid type plan ('xxx') for a promotion	El valor para el tipo de plan ('xxx') no es válido
PAYW-4010	Plan type value ('xxx') mismatches other parameters in the promotion	El valor para el tipo de plan ('xxx') no es congruente con el resto de parámetros de la promoción
PAYW-4011	Promotion must include initial deferment and/or payments number	La promoción debe incluir diferimiento inicial y/o número de pagos
PAYW-4012	Supplied EMV information is not valid or incomplete	La información de EMV suministrada no es válida o está incompleta
PAYW-4013	Failure to decode token xxx: Value 'yyy' for subfield zzz is not aceptable according to the specification	Falla al decodificar token xxx: El valor 'yyy' para el subcampo zzz no es aceptable de acuerdo a especificación.
PAYW-4014	Supplied EMV data does not contain element '' and it is required	El elemento '' no está presente en la información EMV suministrada y es requerido
PAYW-4015	Element '' supplied as part of EMV data is invalid	El elemento '' suministrado en la información EMV es inválido
PAYW-4016	Transaction '' is too old and will not be sent to the authorizer	La transacción '' fue recibida hace ya demasiado tiempo y no se enviará al autorizador
PAYW-4017	Inconsistent card number	Número de tarjeta inconsistente
PAYW-4018	Timeout for transaction ''; response not received within the maximum amount of time, it has reversal ''	El tiempo máximo de espera para la transacción '' ha sido excedido, reversa generada ''
	PROBLEMAS RELACIONADOS CON EL CONECTOR PROSA	
PAYW-4501	Falla al decodificar token '': el valor '' para el subcampo '' no es aceptable de acuerdo a especificación	Falla al decodificar token '': el valor '' para el subcampo '' no es aceptable de acuerdo a especificaci\u00f3n

PROBLEMAS RELACIONADOS CON BASE DE DATOS		
PAYW-5000	Failure when trying to execute operation in the database\: ''	Falla al intentar ejecutar la siguiente operación en base de datos\: ''
PAYW-5001	Failure when trying to execute operation in the database: xxx.	Falla al intentar ejecutar la siguiente operación en base de datos: xxx.
PROBLEMAS RELACIONADOS CON REGLAS DE PREVENCION DE FRAUDE		
PAYW-6001	Transaction has been rejected due to application of rule xxx assigned to this affiliation.	Transacción rechazada por aplicación de la regla xxx asignada para esta afiliación.
PAYW-6002	Rule xxx assigned to this affiliation contains errors in its formula.	Transacción rechazada por error en la fórmula definida para la regla xxx asignada para esta afiliación.
PAYW-6003	Failure when executing formula defined for rule xxx assigned to this affiliation.	Transacción rechazada por falla al procesar la fórmula definida para la regla xxx asignada para esta afiliación.
PAYW-6004	Class defined for rule xxx has not been implemented yet.	La clase definida para la regla xxx no ha sido implementada.
PAYW-6005	Unable to create executor for rule xxx.	Falla al instanciar clase definida para la regla xxx
PAYW-6006	Invalid search condition for rule xxx	Condición inválida de búsqueda en regla xxx.
PAYW-6007	The search table used in formula for rule xxx does not exist.	La tala de búsqueda proporcionada en la fórmula para la regla xxx no existe.
PAYW-6008	The Excel file needed by formula defined for rule xxx does not exist.	El archivo Excel requerido por la fórmula definida para la regla xxx no existe.
PAYW-6009	Failure when trying to access the Excel file needed by formula defined for rule xxx.	Falla al intentar accesar el archivo Excel requerido por la fórmula definida para la regla xxx.
PAYW-6010	Failure when querying table needed by rule xxx.	Falla al ejecutar búsqueda en tabla requerida por la regla xxx.
PAYW-6011	Unable to load Excel driver required to execute rule xxx.	Incapaz de cargar driver Excel para ejecutar regla xxx.
PAYW-6012	="excep.regla.comercio" value="	
PROBLEMAS RELACIONADOS CON EL SERVICIO VISA CHECK OUT		
PAYW-6100	Service Temporarily Unavailable	Servicio no disponible
PAYW-6101	Invalid request data; a required field is either missing or invalid	Solicitud invalida, uno de los campos falta o es invalido
PAYW-6102	shipping region is not accepted by the merchant	La región de envió no es aceptada por el comercio.
PAYW-6103	The API key used in the operation is not authorized for the requested action; ensure that the API key corresponds to the call ID.	El API key usado en la operación es invalido, asegúrese de proporcionar el API key correcto para el call ID
PAYW-6104	El nivel de acceso de acceso a los datos (dataLevel) de la solicitud es invalido	El nivel de acceso de acceso a los datos (dataLevel) de la solicitud es invalido
PAYW-6105	x-pay-token header missing or invalid, or API key is missing or invalid	El encabezado x-pay-token falta o es invalido, o el API key falta o es invalido
PAYW-6106	API key is not authorized to request dataLevel=FULL	El API key no está autorizado para la solicitud dataLevel=FULL
PAYW-6107	La cuenta del cliente está bloqueada	Customer's account is locked
PAYW-6108	La cuenta del cliente se encuentra inactiva	Customer's account is closed
PAYW-6109	No se permiten más operaciones en la tarjeta	Further operations on the card are not allowed

PAYW-6110	API key o call ID no encontrados, o la referencia del dato por el API key o call ID son inválidos o no están disponibles	API key or call ID not found, or data referenced by the API key or call ID is invalid or not available
PAYW-6111	El Call ID se encuentra expirado	Expired Call ID
PAYW-6112	La afiliación no tiene el producto visa check out activo	Merchant doesn't have visa check out active
PAYW-6113	La afiliación no está registrada en visa check out	Merchant isn't record in visa check out
PAYW-6114	Transacción no valida	transaction not valid
	PROBLEMAS RELACIONADOS CON EL SERVIDOR DE CORREO	
PAYW-6301	Attached element '' was not found in expected location	El elemento adjunto '' no existe en la ubicación esperada
PAYW-6302	Attached element '' is not really a file	El elemento adjunto '' no es un archivo
PAYW-6303	Attached element '' cannot be read	El elemento adjunto '' no puede ser leído
PAYW-6304	Unable to send mail. Reason: ''	Incapaz de enviar correo. Causa: ''
	PROBLEMAS RELACIONADOS CON REPORTES DE CIERRE	
PAYW-6601	Unable to initialize group capture report. Cause: ''	Falla al inicializar reporte de cierre de lote. Causa: ''
PAYW-6602	Unable to create header in group capture report. Cause: ''	Falla al crear encabezado de reporte de cierre de lote. Causa: ''
PAYW-6603	Unable to add row to group capture report. Cause: ''	Falla al agregar línea al reporte de cierre de lote. Causa: ''
PAYW-6604	Unable to create group capture report file. Name: ''	Falla al tratar de crear archivo de reporte de cierre de lote. Nombre: ''
PAYW-6605	Unable to initialize affiliation capture report. Cause: ''	Falla al inicializar reporte de cierre de afiliación. Causa: ''
PAYW-6606	Unable to create header in affiliation capture report. Cause: ''	Falla al crear encabezado de reporte de cierre de afiliación. Causa: ''
PAYW-6607	Unable to add row to affiliation capture report. Cause: ''	Falla al agregar línea al reporte de cierre de afiliación. Causa: ''
PAYW-6608	Unable to create affiliation capture report file. Name: ''	Falla al tratar de crear archivo de reporte de cierre de afiliación. Nombre: ''
	PROBLEMAS RELACIONADOS CON CYBERSOURCE	
PAYW-6801	Cybersource service is not available for this type of affiliation	El servicio Cybersource no está disponible para este tipo de afiliación
PAYW-6802	The transaction received (Cybersource Id = '') has not been previously verified by Cybersource	La transacción proporcionada (Id Cybersource = '') no ha sido validada previamente por Cybersource
PAYW-6803	The transaction received (Cybersource Id = '') was previously rejected by Cybersource and cannot be processed	La transacción proporcionada (Id Cybersource = '') fue rechazada por Cybersource y no puede ser procesada
PAYW-6804	Unable to connect to BanorteCybersource service to validate the submitted transaction (Cybersource Id = '')	No ha podido establecerse la conexión necesaria con el sistema BanorteCybersource para validar la transacción (Id Cybersource = '')
	PROBLEMAS RELACIONADOS CON AMERICAN EXPRESS	
PAYW-6900	There isn't a fraudulency secure level: high, middle, there isn't verification	No se tiene asignado un nivel de seguridad contra fraude (SIN VALIDACION, MEDIO, ALTO)
PAYW-6901	The fraudulency secure level '' isn't valid	El nivel de seguridad contra fraudes '' no es valido
PAYW-6902	The fields are necessary: ''	Los siguientes datos deben ser proporcionados ''

PAYW-6903	There aren't AAV, phone and email verification	No existen las validaciones AAV, Teléfono y Correo electrónico
PAYW-6904	There isn't a format valid for AAV, phone and email verification	Validaciones AAV, Teléfono y Correo electrónico tiene un formato incorrecto
PAYW-6905	Values CID supplied for parameter Fraud Prevention Services is not valid	El valor CID proporcionado para el parámetro Servicio de Prevención de Fraudes no es valido
PAYW-6906	Values ZIP CODE, STREET ADDRESS, PHONE NUMBER and EMAIL ADDRESS supplied for parameters Fraud Prevention Services are not valid	Los valores CODIGO POSTAL, DIRECCION, NUMERO TELEFONICO y CORREO ELECTRONICO proporcionados para el parámetro Servicio de Prevención de Fraudes no son validos
PAYW-6907	Values ZIP CODE, PHONE NUMBER, EMAIL ADDRESS supplied for parameters Fraud Prevention Services are not valid	Los valores CODIGO POSTAL, NUMERO TELEFONICO y CORREO ELECTRONICO proporcionados para el parámetro Servicio de Prevención de Fraudes no son validos
PAYW-6908	Values ZIP CODE, STREET ADDRESS and PHONE NUMBER supplied for parameters Fraud Prevention Services are not valid	Los valores CODIGO POSTAL, DIRECCION y NUMERO TELEFONICO proporcionados para el parámetro Servicio de Prevención de Fraudes no son validos
PAYW-6909	Values ZIP CODE and PHONE NUMBER supplied for parameters Fraud Prevention Services are not valid	Los valores CODIGO POSTAL y NUMERO TELEFONICO proporcionados para el parámetro Servicio de Prevención de Fraudes no son validos
PAYW-6910	Values ZIP CODE, STREET ADDRESS and EMAIL ADDRESS supplied for parameters Fraud Prevention Services are not valid	Los valores CODIGO POSTAL, DIRECCION y CORREO ELECTRONICO proporcionados para el parámetro Servicio de Prevención de Fraudes no son validos
PAYW-6911	Values ZIP CODE and EMAIL ADDRESS supplied for parameters Fraud Prevention Services are not valid	Los valores CODIGO POSTAL y CORREO ELECTRONICO proporcionados para el parámetro Servicio de Prevención de Fraudes no son validos
PAYW-6912	Values ZIP CODE, STREET ADDRESS supplied for parameters Fraud Prevention Services are not valid	Los valores CODIGO POSTAL y DIRECCION proporcionados para el parámetro Servicio de Prevención de Fraudes no son validos
PAYW-6913	Value ZIP CODE supplied for parameter Fraud Prevention Services is not valid	El valor CODIGO POSTAL proporcionado para el parámetro Servicio de Prevención de Fraudes no es valido
PAYW-6914	Values STREET ADDRESS, PHONE NUMBER and EMAIL ADDRESS supplied for parameters Fraud Prevention Services are not valid	Los valores DIRECCION, NUMERO TELEFONICO y CORREO ELECTRONICO proporcionados para el parámetro Servicio de Prevención de Fraudes no son validos
PAYW-6915	Values PHONE NUMBER and EMAIL ADDRESS supplied for parameters Fraud Prevention Services are not valid	Los valores NUMERO TELEFONICO y CORREO ELECTRONICO proporcionados para el parámetro Servicio de Prevención de Fraudes no son validos
PAYW-6916	Values STREET ADDRESS and PHONE NUMBER supplied for parameters Fraud Prevention Services are not valid	Los valores DIRECCION y NUMERO TELEFONICO proporcionados para el parámetro Servicio de Prevención de Fraudes no son validos
PAYW-6917	Value PHONE NUMBER supplied for parameter Fraud Prevention Services is not valid	El valor NUMERO TELEFONICO proporcionado para el parámetro Servicio de Prevención de Fraudes no es valido
PAYW-6918	Values EMAIL and STREET ADDRESS supplied for parameters Fraud Prevention Services are not valid	Los valores CORREO ELECTRONICO Y DIRECCION proporcionados para el

		parámetro Servicio de Prevención de Fraudes no son validos
PAYW-6919	Value EMAIL ADDRESS supplied for parameter Fraud Prevention Services is not valid	El valor CORREO ELECTRONICO proporcionado para el parámetro Servicio de Prevención de Fraudes no es valido
PAYW-6920	Value STREET ADDRESS supplied for parameter Fraud Prevention Services is not valid	El valor DIRECCION proporcionado para el parámetro Servicio de Prevención de Fraudes no es valido
PAYW-6921	Does not meet the fraud prevention configuration chosen by the Electronic Commerce	No cumple con la configuración de prevención de fraudes elegida por el Comercio Electrónico
PROBLEMAS RELACIONADOS CON OPERACIONES DE CIFRADO O DESCIFRADO		
PAYW-7001	Failure when trying to encrypt a text	Falla al intentar cifrar un texto
PAYW-7002	Failure when trying to decrypt a text	Falla al intentar descifrar un texto
PAYW-7003	Unable to generate a key for a device	Falla al intentar generar llave para dispositivo
PAYW-7004	Unable to decypher key in database for device with id ''	Falla al intentar descifrar llave en base de datos para el dispositivo con id ''
PAYW-7005	Unable to initialize HSM. Message = ''	Incapaz de inicializar HSM. Mensaje = ''
PAYW-7006	Unable to retrieve key from the HSM	Falla al intentar obtener llave del HSM
PAYW-7007	The HSM device is not currently active	El dispositivo HSM no se encuentra operativo
PAYW-7008	Failure when trying to remove a key from the HSM	Falla al eliminar llave del HSM
PAYW-7009	Failure when trying to add a key into the HSM	Falla al agregar llave al HSM
PROBLEMAS RELACIONADOS CON 3D SECURE		
PAYW-7100	The Transaction does not contain valid information.	La transacción no contiene información válida.
PROBLEMAS MISCELANEOS INESPERADOS		
PAYW-9999	Unexpected failure.	Falla inesperada en aplicación.

Códigos de respuesta del autorizador

La Tabla 25 muestra los valores que el autorizador regresa en una transacción. Estos valores aparecen en los parámetros **AUTH_RESULT** en inglés y **RESULTADO_AUT** en español. Estos códigos **NO** son valores retornados por Banorte, son códigos retornados por el autorizador.

Tabla 25. Códigos de respuesta del autorizador.

Código	Descripción
00	Approval
01	Referral / Call issuer
02	Refer to issuer: special condition
03	Invalid merchant
04	Pick up card
05	Decline
06	Error

07	Reserved
08	Approved with positive ID
09	No action taken (unable to back out previous transaction)
11	Approval VIP
12	Invalid transaction
13	Invalid amount
14	Invalid account number
15	No such issuer
30	System malfunction
31	System malfunction
33	Expired card
34	Pick up card: special condition
35	Pick up card: special condition
36	Error
37	Pick up card: special condition
38	Allowable number of PIN entry retries exceeded
39	No savings account
41	Lost card
43	Pick uup card (stolen card)
51	Not sufficient funds
54	Expired card
55	Incorrect PIN
56	Unable to locate record in file or account is missing
57	Transaction not permitted to cardholder
58	Transaction not permitted to cardholder
59	Required authorization code CVV2/CVC2 was not supplied
61	Withdrawal amount exceeds activity limit
62	Restricted card
65	Activity count limit exceeded
68	System malfunction
75	Allowable number of PIN entry retries exceeded
76	Reserved
77	Reserved
78	Reserved
79	Reserved
81	Reserved
82	Security violation
83	Reserved
84	Reserved
85	Reserved
86	Reserved
87	Reserved
88	Reserved
89	Reserved

90	Host not available
91	Host not available
92	Decline/Not reply/No such host/Invalid category
94	No action taken (unable to back out previous transaction)
96	System malfunction
N0	Reserved
N1	Reserved
N2	Reserved
N3	Reserved
N4	Reserved
N5	Reserved
N6	Reserved
N7	Reserved
N8	Reserved
N9	Reserved
O0	Reserved
O1	Reserved
O2	Reserved
O3	Reserved
O4	Reserved
O5	Reserved
O6	Reserved
O7	Reserved
O8	Reserved
O9	Reserved
P0	Reserved
P1	Reserved
P2	Reserved
P3	Reserved
P4	Reserved
P5	Reserved
P6	Reserved
P7	Reserved
P8	Reserved
P9	Reserved
Q0	Reserved
Q1	Reserved
Q2	Reserved
Q3	Reserved
Q4	Reserved
Q5	Reserved
Q6	Reserved
Q7	Reserved
Q8	Reserved

Q9	Reserved
R0	Reserved
R1	Reserved
R2	Reserved
R3	Reserved
R4	Reserved
R5	Reserved
R6	Reserved
R7	Reserved
R8	Reserved
S4	Reserved
S5	Error
S6	Reserved
S7	Reserved
S8	No such record
S9	Reserved
T1	Reserved
T2	Reserved
T3	Reserved
T4	Reserved
T5	Reserved
T6	Reserved
T7	Reserved

APÉNDICE C: Glosario de términos

La Tabla 26 presenta una lista de términos que se consideran relevantes para la comprensión del presente documento.

Tabla 26. Glosario de términos.

Término	Descripción
API	Acrónimo de "Application Program Interface". Designa un componente de software que permite a una aplicación hacer uso de ciertos servicios implementados por un tercero, siguiendo las especificaciones de programación proporcionadas por el propio componente.
Archivo .JAR	Es un archivo comprimido utilizado comúnmente por aplicaciones Java. Internamente contiene la versión compilada de un conjunto de clases que son requeridas por la aplicación que hace uso del archivo.
Biblioteca de ejecución dinámica	Es un componente de software que provee ciertos servicios a una aplicación, y tiene la característica de que no está físicamente ligado al código de la aplicación, sino que se mantiene como una entidad independiente, y es activado por el sistema operativo cuando la aplicación hace uso por primera vez de él. De esta forma, el mismo código puede ser compartido por varias aplicaciones a la vez, en lugar de aparecer físicamente ligado a cada una.

Cashback	Operación realizada con tarjeta de crédito o débito en la que se presenta disposición de efectivo por parte del cliente en el punto de venta.
Chip	Es un componente electrónico integrado a ciertas tarjetas bancarias con la capacidad de almacenar datos y software. Se utiliza como un medio para reducir el nivel de fraude en el uso de tarjetas tanto de crédito como de débito.
Contactless Chip	Tecnologías de identificación por radiofrecuencia incorporadas en tarjetas de crédito o débito, tarjetas inteligentes, teléfonos móviles u otros dispositivos que permiten a los consumidores pagar una transacción acercando el dispositivo a un lector del terminal punto de venta, de tal forma que no es necesario leer la tarjeta de forma física a través de una ranura de lectura.
Clase	Es una estructura utilizada en lenguajes de programación orientada a objetos que define una plantilla con características a partir de la cual se hará la creación de objetos. Define atributos propios y servicios (métodos) que pueden ser utilizados por otros objetos.
Código de autorización	Es un número (típicamente 6 dígitos) que es retornado cuando una transacción de tarjeta bancaria es aprobada por el banco emisor.
Controlador	Es un componente de software de bajo nivel responsable de atender un dispositivo. Producido normalmente por los fabricantes de hardware; su estructura es dependiente por completo del sistema operativo.
Criptograma	Es un mensaje cifrado cuyo significado resulta ininteligible hasta que no es descifrado. Es utilizado por algunos bancos emisores para incrementar el nivel de seguridad en las transacciones con tarjetas de chip.
Declinada	Declinada indica que la transacción viajo hasta el Banco emisor y este fue quien rechazo la transacción.
Declinada EMV	La transacción fue enviada al Banco emisor, esta pudiera estar aprobada pero al momento de notificar al Chip y este realizó validaciones de prevención de fraudes y determinó que debe ser rechazada. En caso de utilizar las funciones Leer/Enviar/Notificar se deberá generar una Reversa (Reversal) de la transacción. Si utiliza la función procesarTransacción, ésta la generará de forma automática.
Declinada Offline	La transacción fue declinada por reglas de validación del CHIP sin ser enviada al Banco emisor.
DLL	Acrónimo del inglés "Dynamic Link Library". Véase **Biblioteca de ejecución dinámica**.
Driver	Véase **Controlador**.
EMV	Acrónimo de "Europay Mastercard Visa". Estándar de interoperabilidad internacional entre tarjetas con chip definido en conjunto por esas empresas para incrementar el nivel de seguridad en las transacciones.
EMVCo	Empresa creada en 1999 por Europay, Mastercard y Visa para regular y administrar la especificación EMV.
Excepción	Evento que tiene la característica de interrumpir el flujo normal de un programa, debido típicamente a un problema encontrado en un punto de ejecución. Disponible en varios lenguajes de programación; en algunos de ellos orientados a objetos estos eventos se modelan como clases que mantienen información específica sobre el error.
ISO	Acrónimo de "International Organization for Standardization". Es un organismo creado en 1947 para promover el desarrollo de normas internacionales de

	fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.
ISO 8583	Estándar definido por ISO que define especificaciones para el intercambio de transacciones de tipo financiero.
JDK	Acrónimo de "Java Developer Kit". Es un conjunto de herramientas normalmente instalado en equipos en donde se hace desarrollo Java.
JRE	Acrónimo de "Java Runtime Environment". Es la implementación de la máquina virtual Java que debe estar presente para poder ejecutar una aplicación desarrollada en dicha plataforma. Es responsable de interpretar los códigos de operación de la máquina virtual Java, convertirlos a código nativo de la plataforma donde se encuentra y ejecutarlos.
Método	En lenguajes de programación orientados a objetos, cada uno de los servicios (funciones) ofrecidos por una clase.
.NET Framework	Símil del JRE de Java pero exclusivo para plataforma Microsoft
PIN/NIP/No. de Identificación Personal	Secuencia de dígitos que se utiliza para autentificar la identidad de un cliente al hacer uso de un dispositivo electrónico bancario.
PIN Pad	Dispositivo con pantalla y teclado numérico integrados, que posee lectores de banda magnética y de chip. Utilizado para aceptar tarjetas de los clientes y enviar información al equipo que lo controla. Para aquellas tarjetas que así lo requieran, permite ingresar y/o cambiar el NIP del cliente.
Punto de venta	Con este término se designa comúnmente tanto al hardware como al software utilizado para registrar la venta de algún bien o servicio.
QPS	Quick Payment Service. Tipo de transacción en la que no es necesaria la firma autógrafa del tarjetahabiente en el comprobante de la transacción.
Tag EMV	Dentro de la especificación EMV, cada uno de los componentes que aportan un elemento de información sobre la transacción. Cada tag tiene un número que lo identifica de manera única y su contenido normalmente es una secuencia de bytes que es interpretado por el receptor del tag.
Track 1	Dentro del estándar de grabación de tarjetas bancarias de banda magnética, se refiere al primero de los tracks que deben estar presentes en la banda magnética. Normalmente tiene un formato predefinido que contiene información sobre el tarjetahabiente, la cuenta, la fecha de expiración, el código de servicio, etc.
Track 2	Dentro del estándar de grabación de tarjetas bancarias de banda magnética, se refiere al segundo de los tracks que deben estar presentes en la banda magnética. Normalmente tiene un formato predefinido que contiene información sobre la cuenta, la fecha de expiración y el código de servicio.
URL	Acrónimo de "Universal Resource Locator". Es una secuencia de caracteres que sigue un formato estándar, y que usa con la finalidad de encontrar recursos en una red (normalmente Internet), tales como documentos, imágenes, aplicaciones, etc.

APÉNDICE D: Validación de PIN Offline

PIN Offline

Actualmente existen en el mercado tarjetas de crédito y/o débito que solicitan al tarjetahabiente insertar el PIN Offline en el dispositivo al momento de realizar una transacción. El dispositivo proporcionado por Banorte está listo para solicitar el PIN Offline en caso de que la tarjeta así lo requiera.

La DLL de Banorte, al momento de realizar la lectura de la tarjeta, retorna un indicador que señala si el PIN Offline de la tarjeta fue correctamente validado. Al ejecutar la llamada a la DLL ***readCard*** (***leerTarjeta***) y la llamada ***processTransaction*** (***procesarTransaccion***), la DLL retorna como parámetro de salida el parámetro **PIN_ENTRY** (**CAPTURA_NIP**). Este parámetro indica si se realizó la validación del PIN Offline de la tarjeta. Si se retorna un '1', indica que la verificación del PIN Offline fue satisfactoria. Si retorna un '0', indica que la verificación del PIN Offline no fue satisfactoria o que no se solicitó un PIN Offline al momento de realizar la transacción.

Si el PIN Offline fue verificado correctamente y la tarjeta no solicita la firma autógrafa del tarjetahabiente se deberá desplegar en el comprobante de compra el mensaje: **AUTORIZADO CON FIRMA ELECTRÓNICA**. Si el PIN Offline fue verificado correctamente y la tarjeta solicita la firma autógrafa del tarjetahabiente, se debe mostrar en el comprobante de compra el mensaje "**PIN VERIFICADO**" y el espacio respectivo para colocar la firma autógrafa de tarjetahabiente.

Firma del tarjetahabiente

El solicitar el PIN Offline en una transacción no indica que no se deberá solicitar la firma autógrafa de tarjetahabiente. La firma autógrafa del tarjetahabiente puede ser solicitada aún y cuando el tarjetahabiente insertó el PIN Offline de forma correcta.

Para saber si la tarjeta requiere que se solicite o no se solicite la firma autógrafa del tarjetahabiente, la aplicación de Punto de Venta del comercio deberá analizar el Cardholder Verification Method (CVM) Results (Tag 9F34). El byte 1 de este tag proporciona la información necesaria para conocer si solicitar o no solicitar la firma autógrafa del tarjetahabiente. Si el byte 1 del tag 9F 34 viene con valores de **03**, **05**, **1E**, **43**, **45** o **5E**, la aplicación de punto de venta del comercio deberá imprimir en el comprobante de venta la línea respectiva para que el tarjetahabiente firme. Para conocer cómo interpretar los Tags EMV ver el **APÉNDICE E** en la sección de **¿Cómo interpretar los tags EMV?**

Si el voucher muestra la línea para la firma del tarjetahabiente y el voucher no está firmado, no será válido para una controversia, por eso se recomienda imprimir la línea para la firma del tarjetahabiente únicamente cuando sea solicitado por la tarjeta. Si la tarjeta solicita el PIN Offline y además requiere que el tarjetahabiente firme el voucher, tanto el mensaje de **PIN VERIFICADO** como la firma autógrafa del tarjetahabiente deben de estar presentes en el voucher.

APÉNDICE E: Generación de vouchers

Información Requerida

El voucher que se entrega al cliente debe contar con al menos la siguiente información:

1. Entidad financiera (Banorte).
2. Número de afiliación.
3. Nombre del comercio (asociado a la afiliación).
4. Dirección y plaza geográfica donde se realiza la operación (asociada a la afiliación).
5. Teléfono (asociado a la afiliación).
6. Fecha y hora de la transacción.
7. Tipo de operación (venta, devolución, etc.).
8. Número de control de la transacción (asignado por el comercio).
9. Terminal ID.
10. Monto de la operación (importe).
11. Monto cashback. (únicamente si se dispuso efectivo).
12. Monto total (suma de todos los importes).
13. Nombre del tarjetahabiente (cuando sea proporcionado).
14. Firma del tarjetahabiente.
15. Últimos 4 dígitos de la tarjeta.
16. Fecha de expiración de la tarjeta.
17. Código de autorización de la transacción si la transacción es aprobada; motivo de rechazo si la transacción es declinada.
18. Referencia de la transacción.
19. Referencia anterior (transacciones referenciadas).
20. En transacciones con AMEX - Chip imprimir ARQC.
21. Meses a los cuales se defirió el pago en caso de aplicar (Pagos diferidos).
22. Tipo de tarjeta (Visa/MasterCard/American Express).
23. Tipo de producto (crédito o débito).
24. Nombre del Banco emisor del plástico (Ejemplo. Banorte, Santander, Banamex, etc).
25. Validación de PIN
26. Modo de entrada (únicamente en transacciones American Express y JCB).

Como parte de la certificación para EMVFull se agrega la siguiente información para ser impresa en los vouchers, para los casos en que hubo lectura de Chip:

1. AID (Application ID Tag 4F)
2. TVR (Terminal Verification Results Tag 95)
3. TSI (Terminal Status Information Tag 9B)

4. Application Preferred Name (Tag 9F12)
5. Application Label (Tag 50) (Sólo cuando el Application Preferred Name no exista)
6. EMVTags Requeridos para caso de Declinada Offline:
    - Tag 9F26 (Application Cryptogram)
    - Tag 9F27 (Cryptogram Information Data)
    - Tag 9F10 (Issuer Application Data)
    - Tag 9F37 (Unpredictable Number)
    - Tag 9F36 (Application Transaction Counter)
    - Tag 95 (Terminal Verification Results)
    - Tag 9A (Transaction Date)
    - Tag 9C (Transaction Type)
    - Tag 9F02 (Amount, Authorized)
    - Tag 5F2A (Transaction Currency Code)
    - Tag 82 (Application Interchange Profile)
    - ~~Tag 5A (PAN - truncado)~~
    - Tag 9F1A (Terminal Country Code)
    - Tag 9F34 (CVM Results)
    - Tag 9F03 (Amount, Other)
    - Tag 5F34 (PAN Sequence Number)

¿Cómo obtener la información?

Método Leer y Enviar

En la Tabla 27 se muestran los valores solicitados y en la columna siguiente se explica la manera donde se puede obtener dicha información, utilizando la DLL con el método Leer y Enviar.

Tabla 27. Obtención de información para voucher en método Leer y Enviar.

Información requerida	¿Cómo obtenerla?
Entidad financiera	Su valor por default es BANORTE.
Número de afiliación	Dato otorgado por Banorte al momento del alta de la afiliación. Para transacciones Visa/MasterCard se debe imprimir el número de afiliación proporcionado por Banorte. Para transacciones American Express/JCB se debe imprimir el número de afiliación proporcionado por American Express.
Terminal ID	Terminal ID con la que se envió la transacción. Este dato es único por dispositivo y se envía en el parámetro ID_TERMINAL en español y TERMINAL_ID en inglés.
Nombre del comercio	El nombre del comercio que va ligado con el número de afiliación.
Dirección y plaza geográfica donde se realiza la operación	Dirección del comercio en dónde se realiza la transacción.
Teléfono	Teléfono del comercio
Fecha y hora de la transacción	Fecha y hora local en que se efectuó la transacción.

Tipo de operación efectuada (venta, devolución, etc.)	Tipo de transacción efectuada.
Número de control	El número de control proporcionado por el comercio para cada operación. Este número de comercio debe ser generado por la aplicación del comercio y debe ser irrepetible para cada transacción.
Monto de la operación	Es el monto enviado al momento de la transacción.
Monto cashback	Monto de disposición de efectivo.
Monto total	Suma total de los importes. Si es cashback es la suma de del importe más la disposición de efectivo.
Nombre del tarjetahabiente	Este valor se obtiene del resultado del envío de la transacción en la variable TARJETAHABIENTE en español y CARD_HOLDER en inglés.
Firma del tarjetahabiente	Es la firma autógrafa del tarjetahabiente.
Últimos 4 dígitos de la tarjeta	Este valor es el número de tarjeta, y se obtiene al momento de realizar la lectura de la tarjeta en la variable NUMERO_TARJETA en español y CARD_NUMBER en inglés. Para transacciones referenciadas donde no se presenta una lectura de tarjeta, se retorna el parámetro TARJETA_REFERIDA en español y REFERED_CARD en inglés con los últimos 4 dígitos de la tarjeta.
Fecha de expiración de la tarjeta	Este valor se obtiene del resultado de la lectura de la tarjeta en la variable FECHA_EXP en español y CARD_EXP en inglés. Este valor debe imprimirse únicamente en las transacciones en la que se realice una lectura de la tarjeta.
Código de autorización de la transacción si la transacción es aprobada; motivo de rechazo si la transacción es declinada.	Este valor se obtiene del resultado del envío de la transacción en la variable CODIGO_AUT en español y AUTH_CODE en inglés.
Referencia	Código retornado en el parámetro REFERENCIA en español y REFERENCE en inglés en cada transacción realizada.
Referencia anterior	Referencia de la transacción anterior. Es el valor enviado en el parámetro REFERENCIA en español y REFERENCE en inglés en una transacción referenciada (devolución, reversa, postautorización, etc.)
En transacciones con AMEX - CHIP imprimir ARQC	Este valor se obtiene en la variable del resultado de la lectura ARQC.
Meses a los cuales se defirió el pago en caso de aplicar (pagos diferidos)	Estos datos se obtienen de las variables de envío para una venta a pagos diferidos
Tipo de tarjeta (VISA O MC)	Este valor se obtiene del resultado del envío de la transacción en la variable MARCA_TARJETA en español y CARD_BRAND en inglés.
Tipo de Producto (débito o crédito)	Este valor se obtiene del resultado del envío de la transacción en la variable TIPO_TARJETA en español y CARD_TYPE en inglés.

Nombre del Banco Emisor del plástico	Este valor se obtiene del resultado del envío de la transacción en la variable BANCO_EMISOR en español e ISSUING_BANK en inglés.
AID	Este dato lo podemos obtener como resultado del procesamiento del método *readCard* en inglés y *leerTarjeta* en español, en la variable AID. Este valor debe imprimirse únicamente en las transacciones en la que se realice una lectura de la tarjeta.
APN	Este dato lo podemos obtener como resultado del procesamiento del método *readCard* en inglés y *leerTarjeta* en español, en la variable APN. Este valor debe imprimirse únicamente en las transacciones en la que se realice una lectura de la tarjeta.
AL	Este dato lo podemos obtener como resultado del procesamiento del método *readCard* en inglés y *leerTarjeta* en español, en la variable AL. Este dato deberá imprimirse en el voucher ÚNICAMENTE cuan el APN no esté presente. Este valor debe imprimirse únicamente en las transacciones en la que se realice una lectura de la tarjeta.
TVR	Este dato lo podemos obtener como resultado del procesamiento del método *nofityResult* en inglés y *notificarResultado* en español, en la variable TRV. Este valor debe imprimirse únicamente en las transacciones en la que se realice una lectura de la tarjeta.
TSI	Este dato lo podemos obtener como resultado del procesamiento del método *nofityResult* en inglés y *notificarResultado* en español, en la variable TSI. Este valor debe imprimirse únicamente en las transacciones en la que se realice una lectura de la tarjeta.
Validación de PIN	Este dato lo obtenemos del parámetro CAPTURA_NIP en español y PIN_ENTRY en inglés. Indica que el PIN Offline solicitado por la tarjeta fue verificado.
Modo de lectura	Este dato lo obtenemos de la respuesta de la lectura de la tarjeta en el parámetro MODO_ENTRADA en español y ENTRY_MODE en inglés. Este dato se deberá imprimir únicamente en los vouchers de transacciones American Express/JCB. Los valores a imprimir son los siguientes: Chip – **(C)** Banda – **(S)** Manual – **(M)**
Tag 9F26 (Application Cryptogram) **Tag 9F27 (Cryptogram Information Data)** **Tag 9F10 (Issuer Application Data)** **Tag 9F37 (Unpredictable Number)** **Tag 9F36 (Application Transaction Counter)** **Tag 95 (Terminal Verification Results)**	Todos estos datos los obtenemos de la variable que se obtiene al momento de la lectura de la tarjeta en la variable: TAGS_EMV/EMV_TAGS

Tag	Longitud	Valor
4F	07	A0000000041010
50	0A	4D415354455243415244
5A	08	5413330000000050

Tag 9A (Transaction Date)	82	02	5800
Tag 9C (Transaction Type)	84	07	A0000000041010
Tag 9F02 (Amount, Authorized)	8A	02	5A31
Tag 5F2A (Transaction Currency Code)	95	05	0080008800
Tag 82 (Application Interchange Profile)	9A	03	121206
~~Tag 5A (PAN - truncated)~~	9B	02	E800
Tag 9F1A (Terminal Country Code)	9C	01	00
Tag 9F34 (CVM Results)	C2	01	00
Tag 9F33 (Terminal Capabilities)	E2	01	00
Tag 9F03 (Amount, Other)	5F20	0E	4D5449503130204D434420393041
Tag 5F34 (PAN Sequence Number)	5F24	03	141231
	5F25	03	40101
	5F28	02	0056
	5F2A	02	0484
	5F30	02	0201
	5F34	01	03
	9F02	06	000000001000
	9F03	06	000000000000
	9F07	02	FF00
	9F09	02	0084
	9F0D	05	FC50A00000
	9F0E	05	0000000000
	9F0F	05	F870A49800
	9F10	12	021085000F040000410300000000000000FF
	9F12	0A	4D617374657243617264
	9F15	02	2701
	9F1A	02	0484
	9F1C	08	3230343639343130
	9F1E	08	3436393431363430
	9F6E	07	04840000303000
	9F21	03	112433
	9F26	08	89C4A39CEB12BD0C
	9F27	01	00
	9F33	03	E0B0C8
	9F34	03	410302
	9F35	01	22
	9F36	02	009A
	9F37	04	9BA32B69
	9F39	01	05
	9F41	04	00000036
	9F53	01	52

Método Procesar Transacción

En la Tabla 28 se muestran los valores solicitados y en la columna siguiente se explica la manera de donde se puede obtener dicha información, utilizando la DLL con el método Procesar Transacción.

Tabla 28. Obtención de información para voucher en método Procesar Transacción

Información requerida	¿Cómo obtenerla?
Entidad financiera	Su valor por default es BANORTE.
Número de afiliación	Dato otorgado por Banorte al momento del alta de la afiliación. Para transacciones Visa/MasterCard se debe

	imprimir el número de afiliación proporcionado por Banorte. Para transacciones American Express/JCB se debe imprimir el número de afiliación proporcionado por American Express.
Terminal ID	Terminal ID con la que se envió la transacción. Este dato es único por dispositivo y se envía en el parámetro ID_TERMINAL en español y TERMINAL_ID en inglés.
Nombre del comercio	El nombre del comercio que va ligado con el número de afiliación.
Dirección y plaza geográfica donde se realiza la operación	Dirección del comercio en dónde se realiza la transacción.
Teléfono	Teléfono del comercio
Fecha y hora de la transacción	Fecha y hora local en que se efectuó la transacción.
Tipo de operación efectuada (venta, devolución, etc.)	Tipo de transacción efectuada.
Número de control	El número de control proporcionado por el comercio para cada operación. Este número de comercio debe ser generado por la aplicación del comercio y debe ser irrepetible para cada transacción.
Monto de la operación	Es el monto enviado al momento de la transacción.
Monto cashback	Monto de disposición de efectivo.
Monto total	Suma total de los importes. Si es cashback es la suma de del importe más la disposición de efectivo.
Nombre del tarjetahabiente	Este valor se obtiene del resultado del proceso de la transacción en la variable TARJETAHABIENTE en español y CARD_HOLDER en inglés.
Firma del tarjetahabiente	Es la firma autógrafa del tarjetahabiente.
Últimos 4 dígitos de la tarjeta	Este valor es el número de tarjeta, y se obtiene al momento de realizar el proceso de la transacción en la variable NUMERO_TARJETA en español y CARD_NUMBER en inglés. Para transacciones referenciadas donde no se presenta una lectura de tarjeta, se retorna el parámetro TARJETA_REFERIDA en español y REFERED_CARD en inglés con los últimos 4 dígitos de la tarjeta.
Fecha de expiración de la tarjeta	Este valor se obtiene del resultado del proceso de la transacción en la variable FECHA_EXP en español y CARD_EXP en inglés. Este valor debe imprimirse únicamente en las transacciones en la que se realice una lectura de la tarjeta.
Código de autorización de la transacción si la transacción es aprobada; motivo de rechazo si la transacción es declinada.	Este valor se obtiene del resultado del proceso de la transacción en la variable CODIGO_AUT en español y AUTH_CODE en inglés.
Referencia	Código retornado en el parámetro REFERENCIA en español y REFERENCE en inglés en cada transacción realizada.
Referencia anterior	Referencia de la transacción anterior. Es el valor enviado en el parámetro REFERENCIA en español y REFERENCE en

	inglés en una transacción referenciada (devolución, reversa, postautorización, etc.)
En transacciones con AMEX - CHIP imprimir ARQC	Este valor se obtiene en la variable del proceso de la transacción ARQC.
Meses a los cuales se defirió el pago en caso de aplicar (pagos diferidos)	Estos datos se obtienen de las variables de envío para una venta a pagos diferidos
Tipo de tarjeta (VISA O MC)	Este valor se obtiene del resultado del proceso de la transacción en la variable MARCA_TARJETA en español y CARD_BRAND en inglés.
Tipo de Producto (débito o crédito)	Este valor se obtiene del resultado del proceso de la transacción en la variable TIPO_TARJETA en español y CARD_TYPE en inglés.
Nombre del Banco Emisor del plástico	Este valor se obtiene del resultado del proceso de la transacción en la variable BANCO_EMISOR en español e ISSUING_BANK en inglés.
AID	Este dato lo podemos obtener como resultado del procesamiento de la transacción en la variable AID. Este valor debe imprimirse únicamente en las transacciones en la que se realice una lectura de la tarjeta.
APN	Este dato lo podemos obtener como resultado del procesamiento de la transacción en la variable APN. Este valor debe imprimirse únicamente en las transacciones en la que se realice una lectura de la tarjeta.
AL	Este dato lo podemos obtener como resultado del procesamiento de la transacción en la variable AL. Este dato deberá imprimirse en el voucher ÚNICAMENTE cuan el APN no esté presente. Este valor debe imprimirse únicamente en las transacciones en la que se realice una lectura de la tarjeta.
TVR	Este dato lo podemos obtener como resultado del procesamiento de la transacción en la variable TRV. Este valor debe imprimirse únicamente en las transacciones en la que se realice una lectura de la tarjeta.
TSI	Este dato lo podemos obtener como resultado del procesamiento de la transacción en la variable TSI. Este valor debe imprimirse únicamente en las transacciones en la que se realice una lectura de la tarjeta.
Validación de PIN	Este dato lo obtenemos del parámetro CAPTURA_NIP en español y PIN_ENTRY en inglés. Indica que el PIN Offline solicitado por la tarjeta fue verificado.
Modo de lectura	Este dato lo obtenemos de la respuesta del proceso de la transacción en el parámetro MODO_ENTRADA en español y ENTRY_MODE en inglés. Este dato se deberá imprimir únicamente en los vouchers de transacciones American Express/JCB. Los valores a imprimir son los siguientes: Chip – **(C)** Banda – **(S)** Manual – **(M)**

Tag 9F26 (Application Cryptogram)
Tag 9F27 (Cryptogram Information Data)
Tag 9F10 (Issuer Application Data)
Tag 9F37 (Unpredictable Number)
Tag 9F36 (Application Transaction Counter)
Tag 95 (Terminal Verification Results)
Tag 9A (Transaction Date)
Tag 9C (Transaction Type)
Tag 9F02 (Amount, Authorized)
Tag 5F2A (Transaction Currency Code)
Tag 82 (Application Interchange Profile)
~~Tag 5A (PAN - truncated)~~
Tag 9F1A (Terminal Country Code)
Tag 9F34 (CVM Results)
Tag 9F33 (Terminal Capabilities)
Tag 9F03 (Amount, Other)
Tag 5F34 (PAN Sequence Number)

Todos estos datos los obtenemos como respuesta al procesar una transacción que ha sido declinada offline en la variable: TAGS_EMV/EMV_TAGS

Tag	Longitud	Valor
4F	07	A0000000041010
50	0A	4D415354455243415244
~~5A~~	~~08~~	~~5413330000000050~~
82	02	5800
84	07	A0000000041010
8A	02	5A31
95	05	0080008800
9A	03	121206
9B	02	E800
9C	01	00
C2	01	00
E2	01	00
5F20	0E	4D5449503130204D434420393041
5F24	03	141231
5F25	03	40101
5F28	02	0056
5F2A	02	0484
5F30	02	0201
5F34	01	03
9F02	06	000000001000
9F03	06	000000000000
9F07	02	FF00
9F09	02	0084
9F0D	05	FC50A00000
9F0E	05	0000000000
9F0F	05	F870A49800
9F10	12	021085000F040000410300000000000000FF
9F12	0A	4D617374657243617264
9F15	02	2701
9F1A	02	0484
9F1C	08	3230343639343130
9F1E	08	3436393431363430
9F6E	07	04840000303000
9F21	03	
9F26	08	112433
9F27	01	89C4A39CEB12BD0C
9F33	03	00
9F34	03	E0B0C8
9F35	01	410302
9F36	02	22
9F37	04	009A
9F39	01	9BA32B69
9F41	04	05
9F53	01	00000036
		52

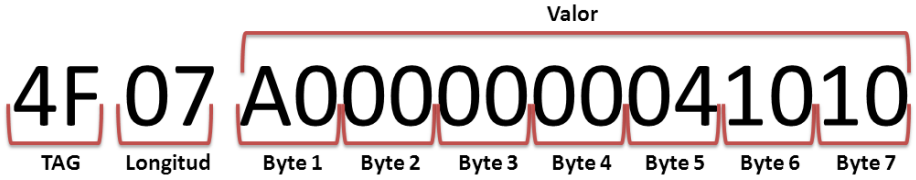
¿Cómo interpretar los tags EMV?

La variable **TAGS_EMV** en español y **EMV_TAGS** contiene toda la información de los EMVTags en una cadena de String. Cada tag, tiene formato **TLV** (Tag, Longitud, Valor).Entonces si yo estoy buscando en la cadena el Tag 4F, lo encontraría así:

TAGS_EMV=**4F07A0000000041010**500A4D415354455243415244 5A0854133300000000528202580 0950500000088009A031212149B02E8009C0100C201005F200E4D5449503130204D4344203930415F24 03141231 5F2A0204845F300202015F3401039F02060000000010009F0306000000000009F10120210850 00F040000410300000000000000FF9F120A4D617374657243617264 9F1A0204849F26085DE6BAC21716 7D069F2701009F34034103029F3602009B9F37047374E976**TAGS_EMV**=E201005F25031609285F280284 005F2A020484820219808407A0000000041010950500000080009A031805249C01009F01009F0206000 0000000019F0306000000000009F0702FF009F090200029F10120110A040032400000000000000000 0000FF9F150227019F16009F1A0204849F1C0839303239373639369F1E0839303239373639369F21009 F260830163A010ADE51EC9F2701809F33030008089F34031F03029F3501229F360200C39F370413BA 2A0E9F3901079F41009F5301059F6E07084000003030009F0D05B4508400009F0E0500000000009F0F 05B4708480005F3401009B02E800C20100**4F07A0000000041010**500A4D415354455243415244 5F2000 5F24031909305F30009F120A4D415354455243415244

Dónde:

Figura 8. Tag 4F en formato TLV



NOTA: La longitud del tag está en hexadecimal y se debe convertir a decimal para representar la longitud en bytes. Si convertimos el 07 a decimal sería 7, por lo tanto serían 7 bytes.

Ahora buscaremos el Tag 50 que se refiere al Application Label, en la cadena aparecería así:

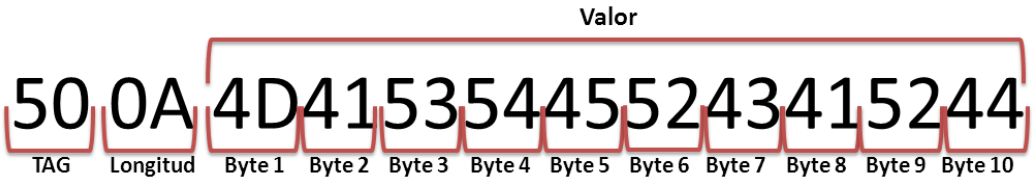
TAGS_EMV=E201005F25031609285F280284005F2A020484820219808407A000000004101095050 0000080009A031805249C01009F01009F0206000000000019F0306000000000009F0702FF009F0902 00029F10120110A040032400000000000000000000000FF9F150227019F16009F1A0204849F1C0839303 239373639369F1E0839303239373639369F21009F260830163A010ADE51EC9F2701809F33030008089 F34031F03029F3501229F360200C39F370413BA2A0E9F3901079F41009F5301059F6E0708400000303 0009F0D05B4508400009F0E0500000000009F0F05B4708480005F3401009B02E800C201004F07A0000 00004101**500A4D41535445524341524**45F20005F24031909305F30009F120A4D415354455243415244

TAGS_EMV=4F07A0000000041010**500A4D41535445524341524**45A0854133300000000528202580 0950500000088009A031212149B02E8009C0100C201005F200E4D5449503130204D4344203930415F24 03141231 5F2A0204845F300202015F3401039F02060000000010009F0306000000000009F10120210850

00F040000410300000000000000FF9F120A4D617374657243617264F1A0204849F26085DE6BAC217167D069F2701009F34034103029F3602009B9F37047374E976

Donde:

Figura 9. Tag 50 en formato TLV



NOTA: La longitud del tag está en hexadecimal y se debe convertir a decimal para representar la longitud en bytes. Si convertimos el 0A a decimal sería 10, por lo tanto serían 10 bytes.

Convertir valores a ASCII

Para impresión de los vouchers hay 2 tags que su valor se debe convertir a valor ASCII, esos 2 tags son el Tag 50 y el Tag 9F12.

Tag	Longitud	Valor en hexadecimal	Valor en ASCII
9F12	0A	4D617374657243617264	MasterCard
50	0A	4D415354455243415244	MASTERCARD

NOTA: El valor de cada Tag puede variar según la tarjeta.

Ejemplos de impresión

Figura 10. Vouchers de venta y devolución con tarjeta de banda Visa/MasterCard

Banorte

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251741VEN1REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA **Tipo:** CRÉDITO
Banco Emisor: BANORTE

Código Autorización: 072521
Referencia: 437615390672

Importe: $100.00

Juan Pérez López

Fecha: Martes 03 de Junio de 2014
Hora: 01:41:31 p.m.

Banorte

Devolución

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251741CAN2REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	

Aprobada

Tipo de tarjeta: **Tipo:**
Banco Emisor:

Código Autorización: 072521
Referencia: 376153906728
Referencia original: 437615390672

Importe: $100.00

Fecha: Martes 03 de Junio de 2014
Hora: 01:41:31 p.m.

Figura 11. Vouchers de preautorización y reautorización con tarjeta de banda Visa/MasterCard

Banorte

Preautorización

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251753PRE1REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA Tipo: CRÉDITO
Banco Emisor: BANORTE

Código Autorización: 072521
Referencia: 437615390672

Importe: $100.00

Juan Pérez López

Fecha: Martes 03 de Junio de 2014
Hora: 01:41:31 p.m.

Banorte

Reautorización

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251758REA2REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	

Aprobada

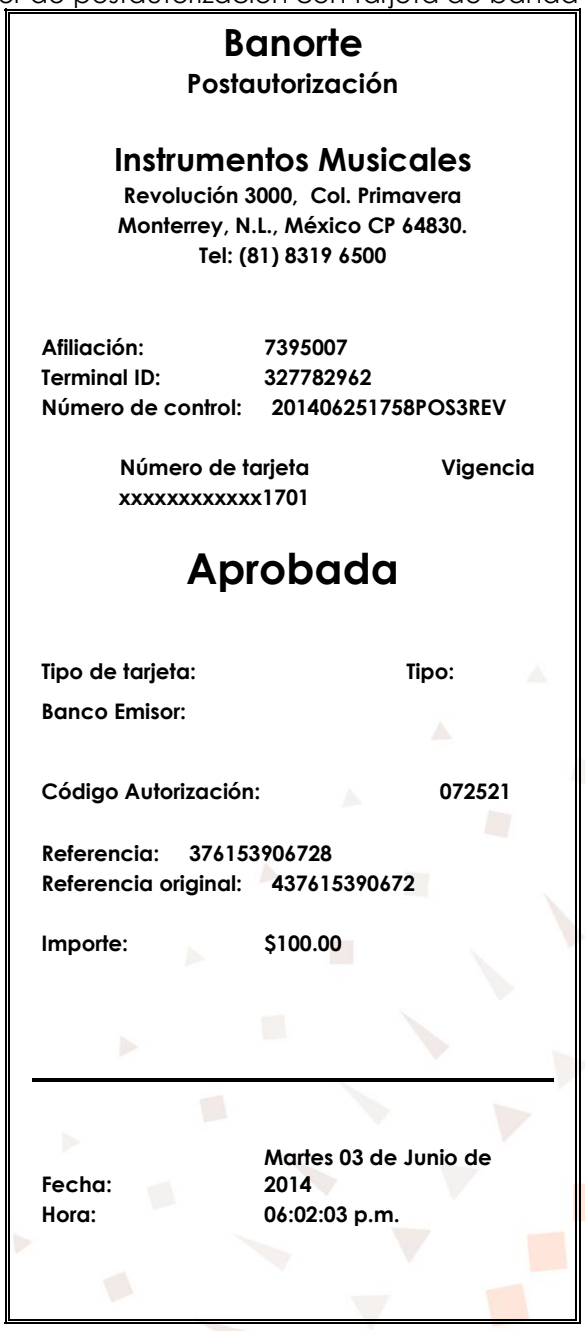
Tipo de tarjeta: Tipo:
Banco Emisor:

Código Autorización: 072521
Referencia: 376153906728
Referencia original: 437615390672

Importe: $100.00

Fecha: Martes 03 de Junio de 2014
Hora: 01:41:31 p.m.

Figura 12. Voucher de postautorización con tarjeta de banda Visa/MasterCard



Banorte
Postautorización

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251758POS3REV

Número de tarjeta **Vigencia**
xxxxxxxxxxxx1701

Aprobada

Tipo de tarjeta: **Tipo:**
Banco Emisor:

Código Autorización: 072521

Referencia: 376153906728
Referencia original: 437615390672

Importe: $100.00

Fecha: Martes 03 de Junio de 2014
Hora: 06:02:03 p.m.

Figura 13. Vouchers de venta QPS y preautorización restaurante con tarjeta de banda Visa/MasterCard

Banorte
Venta

Instrumentos Musicales Revolución 3000,
Col. Primavera Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251823VEN1REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA **Tipo:** CRÉDITO
Banco Emisor: BANORTE

Código Autorización: 072521
Referencia: 437615390672

Importe: $150.00

Autorizado sin firma

Fecha: Miércoles 25 de Junio del 2014
Hora: 06:23:53 p.m.

Banorte
Preautorización

Instrumentos Musicales Revolución 3000,
Col. Primavera Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251835VEN2REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA **Tipo:** DÉBITO
Banco Emisor: BANORTE

Código Autorización: 072468
Referencia: 376153906728

Consumo: $300.00
Propina: $_____.__
Total: $_____.__

Juan Pérez López

Fecha: Miércoles 25 de Junio del 2014
Hora: 06:35:12 p.m.

Figura 14. Vouchers de pagos diferidos y cashback con tarjeta de banda Visa/MasterCard

Banorte

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251823VEN1REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA Tipo: CRÉDITO
Banco Emisor: BANORTE

Código Autorización: 072521
Referencia: 437615390672

3 meses sin intereses

Importe: $3,000.00

Juan Pérez López

Fecha: Miércoles 25 de Junio del 2014
Hora: 06:23:53 p.m.

Banorte

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251835VEN2REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA Tipo: DÉBITO
Banco Emisor: BANORTE

Código Autorización: 072468
Referencia: 376153906728

Importe: $100.00
Cashback: $50.00
Total: $150.00

Juan Pérez López

Fecha: Miércoles 25 de Junio del 2014
Hora: 06:35:12 p.m.

Figura 15. Vouchers de venta y devolución con tarjeta de chip Visa/MasterCard

Banorte

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251741VEN1REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA Tipo: CRÉDITO
Banco Emisor: BANORTE

Código Autorización: 072521
Referencia: 437615390672

Importe: $100.00

Juan Pérez López

Fecha: Martes 03 de Junio de 2014
Hora: 01:41:31 p.m.

AID: A0000000031010
TVR: 0080008800
TSI: E800
APN: VISA ELECTRON

Banorte

Devolución

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251741CAN2REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	

Aprobada

Tipo de tarjeta: Tipo:
Banco Emisor:

Código Autorización: 072521
Referencia: 376153906728
Referencia original: 437615390672

Importe: $100.00

Fecha: Martes 03 de Junio de 2014
Hora: 01:41:31 p.m.

AID:
TVR:
TSI:
APN:

Figura 16. Vouchers de preautorización y reautorización con tarjeta de chip Visa/MasterCard

Banorte

Preautorización

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406261741PRE1REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA Tipo: CRÉDITO
Banco Emisor: BANORTE

Código Autorización: 072521
Referencia: 437615390672

Importe: $100.00

Juan Pérez López

Fecha: Jueves 26 de Junio del 2014
Hora: 01:41:31 p.m.

AID: A0000000031010
TVR: 0080008800
TSI: E800
APN: VISA ELECTRON

Banorte

Reautorización

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406261741REA2REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	

Aprobada

Tipo de tarjeta: Tipo:
Banco Emisor:

Código Autorización: 072521
Referencia: 376153906728
Referencia original: 437615390672

Importe: $100.00

Fecha: Jueves 26 de Junio del 2014
Hora: 02:02:37 p.m.

AID:
TVR:
TSI:
APN:

Figura 17. Voucher de postautorización con tarjeta de chip Visa/MasterCard

Banorte

Postautorización

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406261741POS2REV

Número de tarjeta **Vigencia**
xxxxxxxxxxxx1701

Aprobada

Tipo de tarjeta: **Tipo:**
Banco Emisor:

Código Autorización: 072521
Referencia: 376153906728
Referencia original: 437615390672

Importe: $100.00

Fecha: Jueves 26 de Junio del 2014
Hora: 02:02:37 p.m.

AID:
TVR:
TSI:
APN:

Figura 18. Voucher de venta con validación de PIN y sin solicitud de firma.

Banorte

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251741VEN1REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA **Tipo:** CRÉDITO
Banco Emisor: BANORTE

Código Autorización: 072521
Referencia: 437615390672

Importe: $100.00

AUTORIZADO CON FIRMA ELECTRÓNICA

Juan Pérez López

Fecha: Martes 03 de Junio de 2014
Hora: 01:41:31 p.m.

AID: A0000000031010
TVR: 0080008800
TSI: E800
APN: VISA ELECTRON

Figura 19. Vouchers de venta QPS y preautorización restaurante con tarjeta de chip Visa/MasterCard

Banorte

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201407251741VEN9REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA Tipo: CRÉDITO
Banco Emisor: BANORTE

Código Autorización: 072521
Referencia: 437615390672

Importe: $100.00

Autorizado sin firma

Fecha: Lunes 03 de Junio de 2013
Hora: 01:41:31 p.m.

AID: A0000000031010
TVR: 0080008800
TSI: E800
APN: VISA ELECTRON

Banorte

Preautorización

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201407251741PRE2REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA Tipo: CRÉDITO
Banco Emisor: BANORTE

Código Autorización: 072521
Referencia: 437615390672

Consumo: $400.00
Propina: $_____.__
Total: $_____.__

Juan Pérez López

Fecha: Lunes 03 de Junio de 2013
Hora: 01:41:31 p.m.

AID: A0000000031010
TVR: 0080008800
TSI: E800
APN: VISA ELECTRON

Figura 20. Vouchers de pagos diferidos y cashback con tarjeta de chip Visa/MasterCard

Banorte

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201407251741VEN9REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA Tipo: CRÉDITO
Banco Emisor: BANORTE

Código Autorización: 072521
Referencia: 437615390672

3 meses sin intereses

Importe: $3,000.00

Juan Pérez López

Fecha: Lunes 03 de Junio de 2013
Hora: 01:41:31 p.m.

AID: A0000000031010
TVR: 0080008800
TSI: E800
APN: VISA ELECTRON

Banorte

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201407251741CAS2REV

Número de tarjeta	Vigencia
xxxxxxxxxxxx1701	01/15

Aprobada

Tipo de tarjeta: VISA Tipo: CRÉDITO
Banco Emisor: BANORTE

Código Autorización: 072521
Referencia: 437615390672

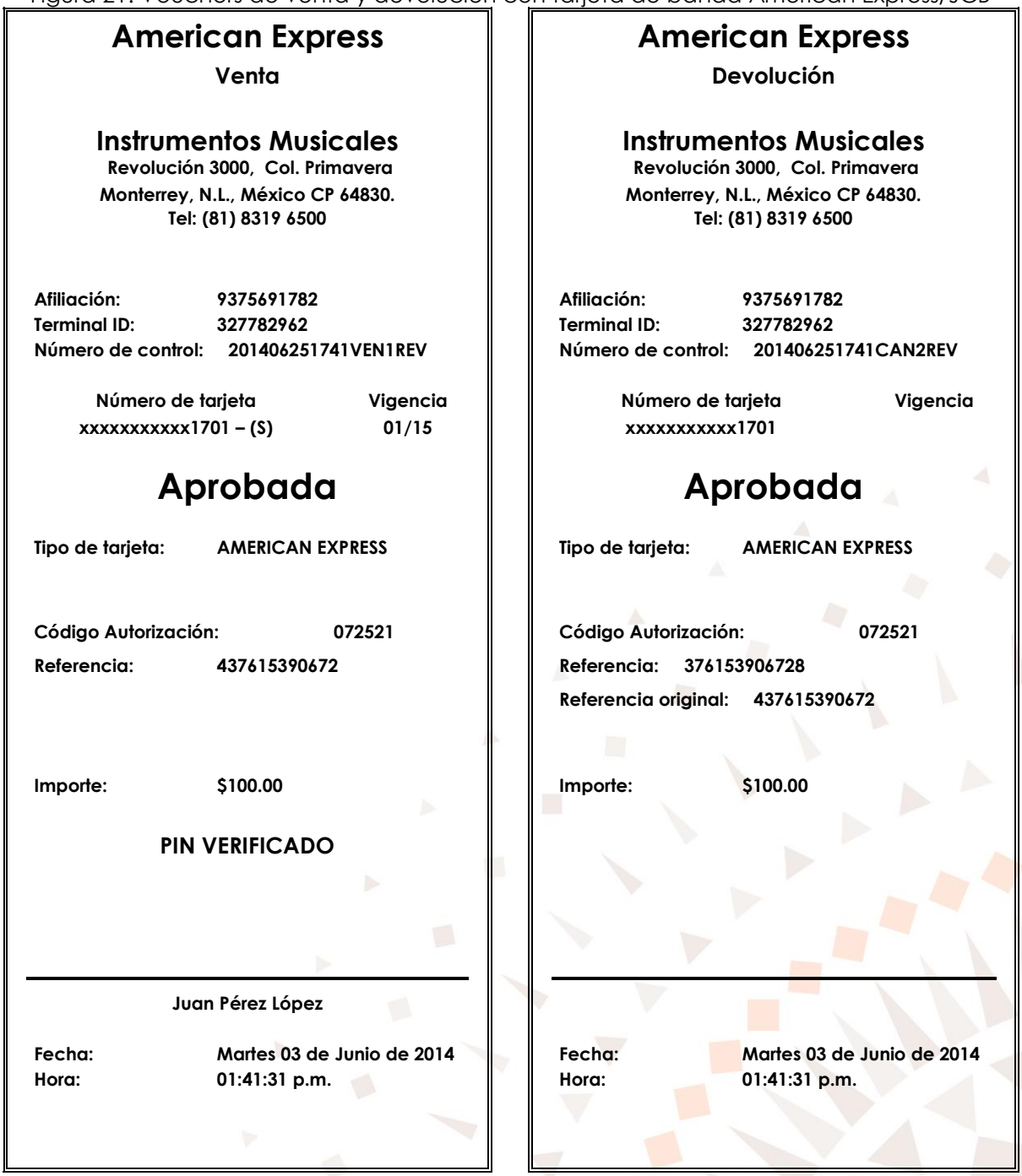
Importe: $200.00
Cashback: $50.00
Total: $250.00

Juan Pérez López

Fecha: Lunes 03 de Junio de 2013
Hora: 01:41:31 p.m.

AID: A0000000031010
TVR: 0080008800
TSI: E800
APN: VISA ELECTRON

Figura 21. Vouchers de venta y devolución con tarjeta de banda American Express/JCB



American Express

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 9375691782
Terminal ID: 327782962
Número de control: 201406251741VEN1REV

Número de tarjeta	Vigencia
xxxxxxxxxxx1701 – (S)	01/15

Aprobada

Tipo de tarjeta: AMERICAN EXPRESS

Código Autorización: 072521
Referencia: 437615390672

Importe: $100.00

PIN VERIFICADO

Juan Pérez López

Fecha: Martes 03 de Junio de 2014
Hora: 01:41:31 p.m.

American Express

Devolución

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 9375691782
Terminal ID: 327782962
Número de control: 201406251741CAN2REV

Número de tarjeta	Vigencia
xxxxxxxxxxx1701	

Aprobada

Tipo de tarjeta: AMERICAN EXPRESS

Código Autorización: 072521
Referencia: 376153906728
Referencia original: 437615390672

Importe: $100.00

Fecha: Martes 03 de Junio de 2014
Hora: 01:41:31 p.m.

Figura 22. Vouchers de preautorización y postautorización con tarjeta de banda American Express/JCB

American Express
Preautorización

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 9375691782
Terminal ID: 327782962
Número de control: 201406251741PRE1REV

Número de tarjeta	Vigencia
xxxxxxxxxxx1701 – (S)	01/15

Aprobada

Tipo de tarjeta: AMERICAN EXPRESS

Código Autorización: 072521
Referencia: 437615390672

Importe: $100.00

PIN VERIFICADO

Juan Pérez López

Fecha: Martes 03 de Junio de 2014
Hora: 01:41:31 p.m.

American Express
Postautorización

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 9375691782
Terminal ID: 327782962
Número de control: 201406251741POS2REV

Número de tarjeta	Vigencia
xxxxxxxxxxx1701	

Aprobada

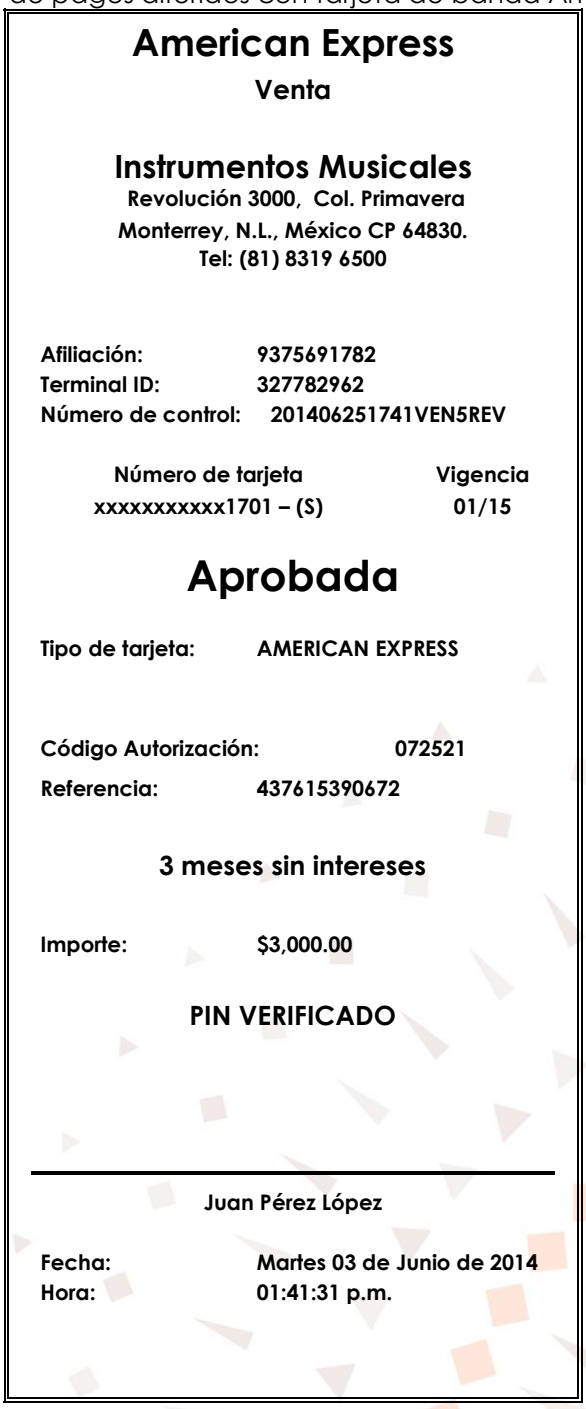
Tipo de tarjeta: AMERICAN EXPRESS

Código Autorización: 072521
Referencia: 376153906728
Referencia original: 437615390672

Importe: $100.00

Fecha: Martes 03 de Junio de 2014
Hora: 01:41:31 p.m.

Figura 23. Vouchers de pagos diferidos con tarjeta de banda American Express/JCB



American Express

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 9375691782
Terminal ID: 327782962
Número de control: 201406251741VEN5REV

Número de tarjeta	Vigencia
xxxxxxxxxxx1701 – (S)	01/15

Aprobada

Tipo de tarjeta: AMERICAN EXPRESS

Código Autorización: 072521
Referencia: 437615390672

3 meses sin intereses

Importe: $3,000.00

PIN VERIFICADO

Juan Pérez López

Fecha: Martes 03 de Junio de 2014
Hora: 01:41:31 p.m.

Figura 24. Vouchers de venta y devolución con tarjeta de chip American Express/JCB

American Express

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 9375691782
Terminal ID: 327782962
Número de control: 201406251741VEN1REV

Número de tarjeta	Vigencia
xxxxxxxxxxx1701 – (C)	01/15

Aprobada

Tipo de tarjeta: AMERICAN EXPRESS

Código Autorización: 072521
Referencia: 437615390672
ARQC: 42C392FF83059411

Importe: $100.00

PIN VERIFICADO

Juan Pérez López

Fecha: Lunes 03 de Junio de 2013
Hora: 01:41:31 p.m.

AID: A000000025010801
TVR: 0000008800
TSI: F800
AL: AMERICAN EXPRESS

American Express

Devolución

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 9375691782
Terminal ID: 327782962
Número de control: 201406251741CAN2REV

Número de tarjeta	Vigencia
xxxxxxxxxxx1701	

Aprobada

Tipo de tarjeta: AMERICAN EXPRESS

Código Autorización: 072521
Referencia: 376153906728
Referencia original: 437615390672
ARQC:

Importe: $100.00

Fecha: Lunes 03 de Junio de 2013
Hora: 01:41:31 p.m.

AID:
TVR:
TSI:
AL:

Figura 25. Vouchers de preautorización y postautorización con tarjeta de chip American Express/JCB

American Express

Preautorización

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 9375691782
Terminal ID: 327782962
Número de control: 201406251741PRE7REV

Número de tarjeta	Vigencia
xxxxxxxxxxx1701 – (C)	01/15

Aprobada

Tipo de tarjeta: AMERICAN EXPRESS

Código Autorización: 072521
Referencia: 437615390672
ARQC: 42C392FF83059411

Importe: $100.00

PIN VERIFICADO

Juan Pérez López

Fecha: Lunes 03 de Junio de 2013
Hora: 01:41:31 p.m.

AID: A000000025010801
TVR: 0000008800
TSI: F800
AL: AMERICAN EXPRESS

American Express

Postautorización

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 9375691782
Terminal ID: 327782962
Número de control: 201406251741POS8REV

Número de tarjeta	Vigencia
xxxxxxxxxxx1701	

Aprobada

Tipo de tarjeta: AMERICAN EXPRESS

Código Autorización: 072521
Referencia: 376153906728
Referencia original: 437615390672
ARQC:

Importe: $100.00

Fecha: Lunes 03 de Junio de 2013
Hora: 01:41:31 p.m.

AID:
TVR:
TSI:
AL:

Figura 26. Vouchers de pagos diferidos con tarjeta de chip American Express/JCB

American Express

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 9375691782
Terminal ID: 327782962
Número de control: 201406251741VEN9REV

Número de tarjeta	Vigencia
xxxxxxxxxxx1701 – (C)	01/15

Aprobada

Tipo de tarjeta: AMERICAN EXPRESS

Código Autorización: 072521
Referencia: 437615390672
ARQC: 42C392FF83059411

3 meses sin intereses

Importe: $3,000.00

PIN VERIFICADO

Juan Pérez López

Fecha: Lunes 03 de Junio de 2013
Hora: 01:41:31 p.m.

AID: A000000025010801
TVR: 0000008800
TSI: F800
AL: AMERICAN EXPRESS

NOTA: Para los voucher impresos en transacciones de American Express se debe imprimir el número de afiliación proporcionado por American Express y no el proporcionado por Banorte.

Figura 27. Vouchers de transacción declinada offline.

Banorte

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación:	7395007
Terminal ID:	327782962
Número de control:	201406251741VEN1REV

Declinada Offline

Fecha:	Lunes 03 de Junio de 2013
Hora:	01:41:31 p.m.

AID:	A0000000031010
APN:	VISA ELECTRON

5A 08 XXXXXXXXXXXX1743
82 02 5C00
95 05 0000008800
9A 03 140603
9C 01 00
5F2A 02 0484
5F34 01 01
9F02 06 000000015000
9F03 06 000000000000
9F10 07 06010A03A02000
9F1A 02 0484
9F26 08 F830C4727E89B958
9F27 01 80
9F33 03 E0B0C8
9F34 03 1E0300
9F36 02 0149
9F37 04 A7221118

Figura 28. Vouchers de transacción declinada offline (segunda opción).

Banorte
Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación:	7395007
Terminal ID:	327782962
Número de control:	201406251741VEN1REV

Declinada Offline

Fecha:	Lunes 03 de Junio de 2013
Hora:	01:41:31 p.m.
AID:	A0000000031010
APN:	VISA ELECTRON

4F 07 A0000000041010
50 0A 4D415354455243415244
5A 08 5413330089020050
82 02 5800
84 07 A0000000041010
8A 02 5A31
95 05 0080008800
9A 03 121206
9B 02 E800
9C 01 00
C2 01 00
E2 01 00
5F20 0E 4D5449503130204D434420393041
5F24 03 141231
5F25 03 040101
5F28 02 0056
5F2A 02 0484
5F30 02 0201
5F34 01 03
9F02 06 000000001000
9F03 06 000000000000
9F07 02 FF00
9F09 02 0084
9F0D 05 FC50A00000
9F0E 05 0000000000
9F0F 05 F870A49800
9F10 12 021085000F040000410300000000000000FF
9F12 0A 4D617374657243617264
9F15 02 2701
9F1A 02 0484
9F1C 08 3230343639343130
9F1E 08 3436393431363430
9F21 03 112433
9F26 08 89C4A39CEB12BD0C
9F27 01 00
9F33 03 E0B0C8
9F34 03 410302
9F35 01 22
9F36 02 009A
9F37 04 9BA32B69
9F39 01 05
9F41 04 00000036
9F53 01 52

Figura 29. Vouchers de transacciones declinadas EMV.

Banorte

Venta

Instrumentos Musicales
Revolución 3000, Col. Primavera
Monterrey, N.L., México CP 64830.
Tel: (81) 8319 6500

Afiliación: 7395007
Terminal ID: 327782962
Número de control: 201406251741VEN1REV

Declinada EMV

Fecha: Lunes 03 de Junio de 2013
Hora: 01:41:31 p.m.

AID: A0000000031010
APN: VISA ELECTRON

5A 08 XXXXXXXXXXXX1743
82 02 5C00
95 05 0000008800
9A 03 140603
9C 01 00
5F2A 02 0484
5F34 01 01
9F02 06 000000015000
9F03 06 000000000000
9F10 07 06010A03A02000
9F1A 02 0484
9F26 08 F830C4727E89B958
9F27 01 80
9F33 03 E0B0C8
9F34 03 1E0300
9F36 02 0149
9F37 04 A7221118

NOTA: Se valida que el recibo de la transacción cuente con las datos mínimos mandatorios (últimos 4 dígitos de la tarjeta, numero de autorización, fecha de la transacción, Firma del tarjeta habiente o la leyenda "Autorizado mediante firma electrónica" cuando se solicita ingreso de PIN, Nombre del comercio, importe y Numero de afiliación), pero no garantiza la protección ante un contra-cargo por: situaciones de entrega (no recibió la mercancía), cargo duplicado, pago por otros medios, mercancía defectuosa, crédito no procesado (devolución no realizada), no es lo descrito, ilegibilidad y servicios no prestados.

APÉNDICE F: EMV Data

Como parámetros de entrada, siempre que haya una información Full EMV de parte del emisor se recibirá la variable respectiva en la salida de Payworks DATOS_EMV (EMV_DATA) la cual tendrá un formato TLV codificado en ASCII. Típicamente esta cadena contendrá uno o más de los siguientes elementos:

Tabla 29. Descripción de datos EMV.

Elemento	Tag	Descripción
ARPC	91	Criptograma de autenticación
Secuencia Script	71	Uno o más scripts que deberán ser ejecutados previos al segundo comando GENERATE AC en el chip.
Secuencia Script	72	Uno o más scripts que deberán ser ejecutados después del segundo comando GENERATE AC en el chip.

El orden en que se reciban los elementos dentro de la variable no está garantizado; sin embargo, el usuario de la función ***notificarResultado*** (***notifyResult***) no necesita hacer ningún tipo de transformación o reconocimiento de la información recibida: simplemente deberá incluir la secuencia tal como se recibió **DATOS_EMV** (**EMV_DATA**), en el mapa de parámetros de entrada suministrado a la función. El nombre de la variable que se pasará en el mapa de entrada para la función será la misma que se haya recibido de Payworks **DATOS_EMV** (**EMV_DATA**). Ejemplo de secuencia que puede recibirse:

910A2269D6C87518D4D13030711086 0E04DA9F580903DBE547581DED2F61

Obsérvese que en el ejemplo se está recibiendo un criptograma ARPC (Tag 91) de longitud 10 bytes, y a continuación un elemento de script (Tag 71) de longitud 16 bytes. En caso de no recibirse la variable de parte de Payworks en la respuesta a la transacción, debe entenderse que el emisor no está enviando información Full EMV y por tanto este elemento **NO SE INCLUIRÁ** en el mapa de entrada para la función ***notificarResultado*** (***notifyResult***). No es válido pasar espacios en blanco o cadenas vacías para este caso.

APÉNDICE G: Diagramas de flujo

Figura 30. Información diagramas de flujo.

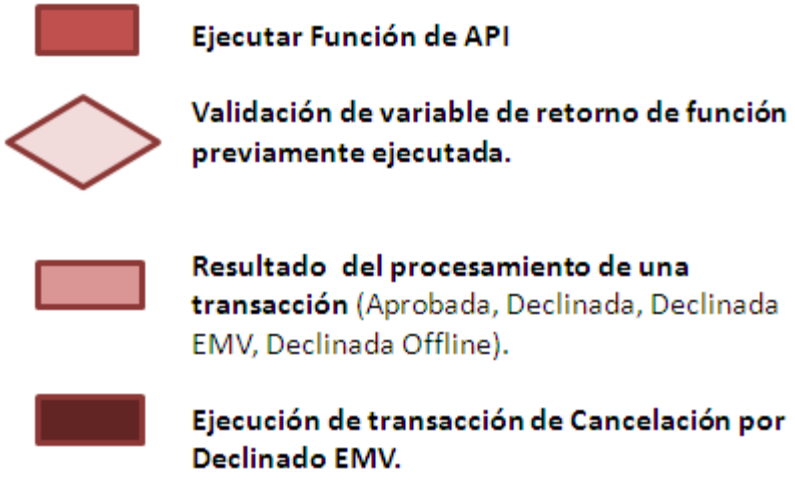
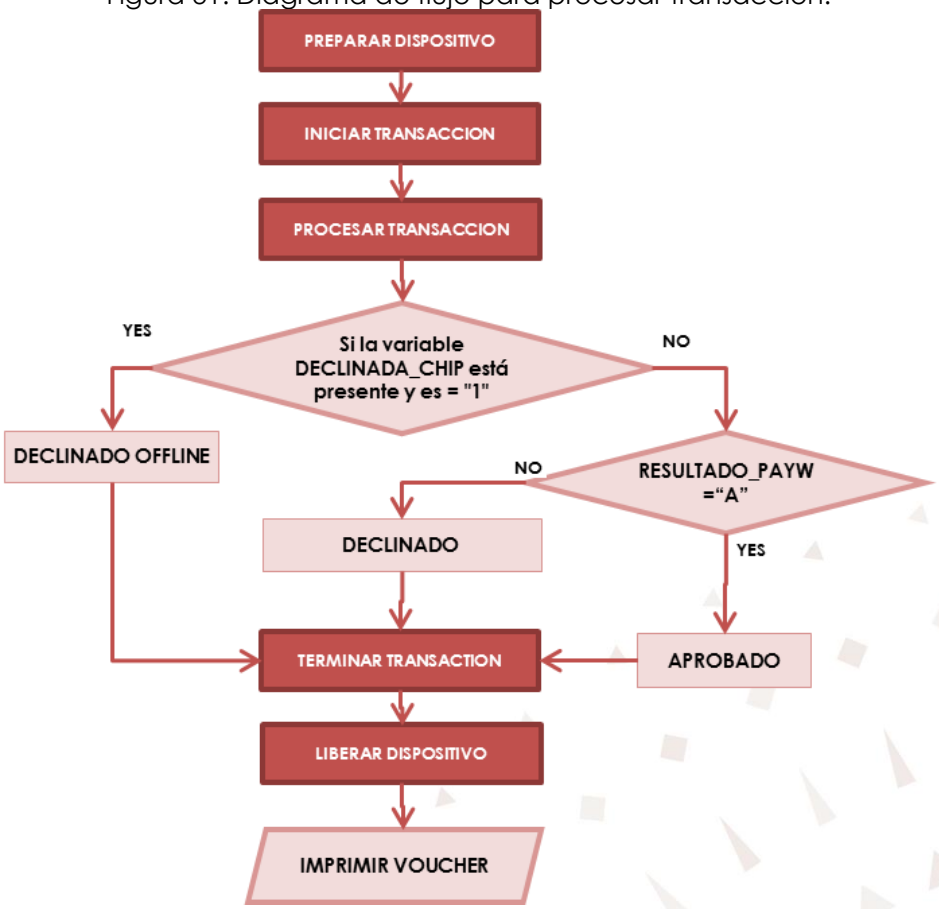


Tabla 30. Descripción de transacciones declinadas.

Tipos de declinación	Descripción
Declinada	Declinada indica que la transacción viajo hasta el Banco emisor y este fue quien rechazo la transacción.
Declinada EMV	La transacción fue enviada al Banco emisor, esta pudiera estar aprobada pero al momento de notificar al Chip y este realizó validaciones de prevención de fraudes y determino que debe ser rechazada. En caso de utilizar la función Leer/Enviar/Notificar se deberá generar una Reversa (**REVERSAL**) de la transacción. Si utiliza la función Transacción, está la generará de forma automática.
Declinada Offline	La transacción fue declinada por reglas de validación del CHIP sin ser enviada al Banco emisor.

Procesar transacción

Figura 31. Diagrama de flujo para procesar transacción.

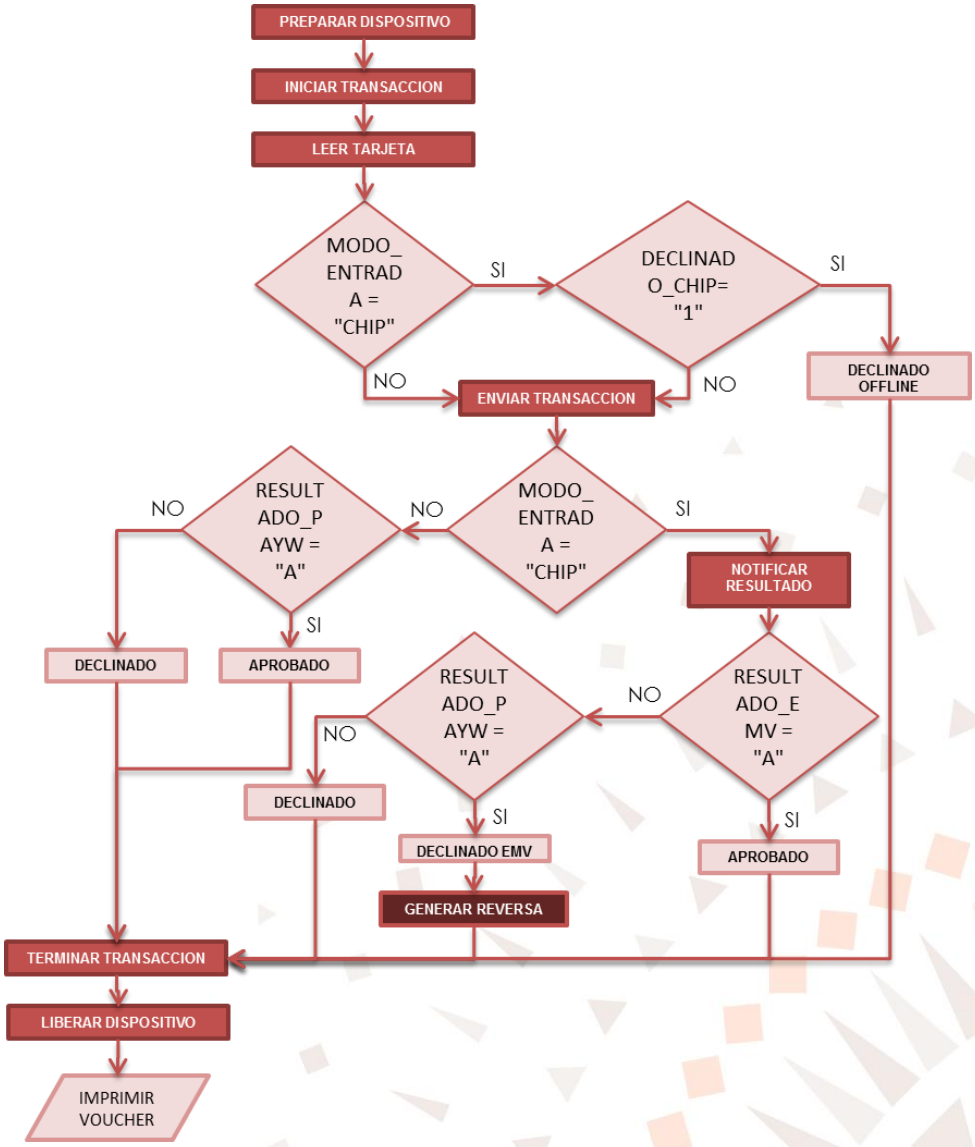


NOTA: En el diagrama se plasma únicamente el nombre de parámetro en español, si utiliza los parámetros en inglés sería el nombre equivalente acorde al manual.

Leer tarjeta/Enviar transacción/Notificar resultado

Si implementó las funciones Leer/Enviar/Notificar Resultado, este es un diagrama de flujo de una transacción.

Figura 32. Diagrama de flujo para Leer/Enviar/Notificar



NOTA: En el diagrama se plasma únicamente el nombre de parámetro en español, si utiliza los parámetros en inglés sería el nombre equivalente acorde al manual.

Verificación de transacciones

Las transacciones pueden ser verificadas mediante la herramienta administrativa web que Banorte provee. La dirección URL de la herramienta es **https://via.banorte.com/PaywPlusComercios/**. Las credenciales para ingresar a esta herramienta son proporcionadas mediante correo electrónico al momento de dar de alta la afiliación. La información de la transacción estará disponible hasta 90 días naturales después de realizada la transacción.

APÉNDICE H: Certificación y liberación a producción

Una vez que el usuario administrador del comercio reciba la contraseña, es necesario que realice el cambio de la misma y que se cree un usuario de solo ejecución para utilizarlo en su implementación. También es altamente recomendable la creación de usuarios independientes para cada persona que requiera consultar reportes. Estas modificaciones las pueden realizar desde el módulo de Usuarios de la Herramienta Administrativa.

Los usuarios requeridos son los siguientes:

- Usuario administrador para la gestión de los usuarios creados
- Usuario de solo ejecución para utilizarlo en la implementación
- Usuario para cada persona que requiera consultar reportes

NOTA: Es responsabilidad del usuario administrador la gestión de los usuarios y el correcto uso de su contraseña.

Antes de la liberación a producción es requerido que se lleve a cabo un proceso de certificación, este proceso verifica que su integración cumpla con los requerimientos necesarios para operar, este proceso es obligatorio para todo comercio que realizó un desarrollo propio o con un tercero para su conexión al motor de pagos de Banorte.

El proceso se compone de distintas fases:

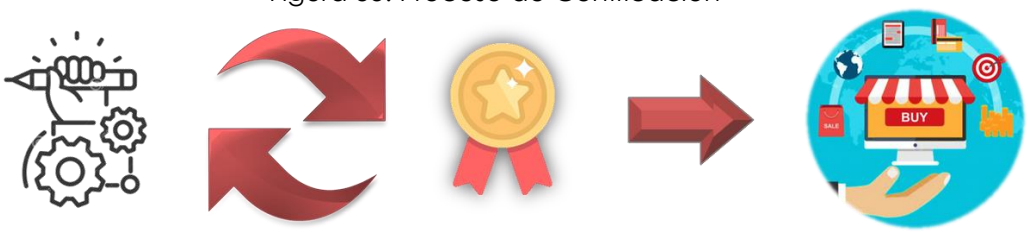
En la primera fase el comercio nos debe solicitar y hacer llegar llenados dos documentos que se les compartirá.

1. **Solicitud de certificación:** Este es un documento en Word en el cual se solicitan datos de la integración (características generales del proyecto, transacciones a usar, etc.).
2. **Matriz de pruebas:** Es un documento en formato Excel en el cual se debe llenar con los datos de las transacciones que se van a certificar (Afiliación, Numero de control, Referencia, Hora, Fecha entre otros datos).

En la segunda fase el Laboratorio Payworks procede a verificar la documentación anterior así como la mensajería transaccional enviada al motor, esta revisión se realiza con cada una de las transacciones que nos describieron en la matriz de certificación. Si las validaciones son correctas, se realizará la entrega de una Carta de Certificación, documento que avala la integración del

comercio cumple con los requisitos mínimos necesarios para operar, y describe las características de la integración del comercio, transacciones que implemento, Notas u Observaciones, entre otros datos. Si las Validaciones no son correctas se solicitará al comercio las adecuaciones necesarias para la corrección.

Figura 33. Proceso de Certificación



El comercio realiza la integración al motor de pagos Payworks.

El comercio realiza la certificación de la integración con Banorte.

Concluida la certificación el comercio puede salir a producción.

NOTA: Si el comercio inicia transacciones productivas antes de finalizar el proceso de certificación, **Banorte no se hará responsable** por:

- Fallas en la integración del comercio.
- Contra cargo generado durante este periodo.
- El Abono de lo operado a modo producción mientras no finalice el proceso de certificación.

APÉNDICE I: Información de contacto

Tabla 31. Soporte técnico Payworks

Teléfonos	Correo
Clave Internacional: +52 Teléfono directo: (81) 8319 7379 Conmutador: (81) 8319 7200 Ext.: 8810-1002# 8810-1007# 8810-1008# 8810-1021# RED Banorte 8810-1002 8810-1007 8810-1008 8810-1021	L.Soporte_Payworks_Interredes@banorte.com
Horario de Atención: Lunes a Viernes de 9:00am a 6:00 pm Horario Central	