POSNET™
Un Producto de First Data

Manual de Sistemas Propios

Especificaciones Funcionales y Técnicas

VERSION 07- 2013

INDICE Y TABLA DE CONTENIDOS

MANUAL DE SISTEMAS PROPIOS

PROLOGO

Este manual tiene como objetivo brindar a los proveedores de sistemas y/o equipamiento la posibilidad de automatizar el manejo de tarjetas de crédito/débito, compra, privadas y/o lealtad, a través de sus sistemas de caja/servidor. A partir de la correspondiente homologación provisoria del sistema, los comercios a ser habilitados para operar, deberán cumplir con un único e importante requisito, el mismo es el promedio de transacciones con tarjetas por comercio o por local si correspondiera, el cual ha sido fijado en un mínimo aproximado requerido de 600 operaciones al mes con cada emisor, no obstante esta cifra, el comercio deberá tratar este punto en particular con cada emisor con el que opere o desee operar.

Con respecto a los vínculos de conexión con los Administradores/Procesadores, los mismos estarán a cargo de cada comercio en cuanto a su contratación, mantenimiento y cualquier otro costo involucrado en los mismos.

Los Administradores/Procesadores fijarán un costo por acceso a la red de comunicaciones (puertas para cada comercio, puntos de venta habilitados, etc), el mismo será fijado por cada Administrador/Procesador en particular.

La plataforma sobre la que se instale el Sistema Propio debe contar con un Sistema Operativo que se encuentre soportado por el fabricante y/o el distribuidor del mismo.

El desarrollo de este sistema implica la aceptación tácita de cada Comercio/Proveedor a mantener el aplicativo actualizado, con las modificaciones y/o desarrollos para la habilitación de nuevas funciones y/o productos que surjan dentro del marco del Acuerdo Tecnológico de la Industria, el no cumplimiento de las mismas habilitará a los Administradores/Procesadores a tomar las medidas que consideren apropiadas.

Este manual ha sido generado dentro del marco del Acuerdo Tecnológico de la Industria, al cual han arribado los principales emisores de tarjetas de crédito a nivel nacional e internacional.

Las definiciones vertidas en el mismo son para aplicación en los sistemas denominados FACE TO FACE, donde hay presencia del socio y su plástico (tarjeta) en un comercio real.

Cualquier otra aplicación que el comercio necesite darle al sistema, por poseer una operatoria diferente a lo standard, deberá ser elevada en forma fehaciente a POSNET y a los administradores de tarjetas, a efectos de que se realice una evaluación de la misma.
Esta referencia es a priori para sistemas de e-commerce, de venta a distancia, sistemas automatizados (selfservice), operatorias donde no se generan tickets de respaldo de las operaciones, sistemas que operen a través de vínculos IP en alguno de sus componentes, etc.

El capítulo H e I de Emisores y Maestro, respectivamente, se encuentran en el manual "Emisores POSNET".

INTRODUCCION

El objetivo de esta carpeta es facilitar a aquellos establecimientos interesados en automatizar la autorización y presentación de cupones de los sistemas de Tarjetas, la interpretación de las pautas operativas a tener en cuenta para efectuar presentaciones mediante transmisiones ON-LINE.

Las características generales de operación son las siguientes:

- ✓ Si el emisor lo permite, los establecimientos contarán con un archivo de boletín protectivo que periódicamente les será provisto.
- ✓ Ante cada operación de venta a resolver en forma OFF-LINE, se deberá consultar dicho boletín a efectos de establecer la aptitud de la tarjeta, en caso de que exista una imposibilidad de conexión con el Administrador/Procesador.
- ✓ Los datos de la tarjeta se obtendrán de la banda magnética y eventualmente se podrán ingresar por teclado. En este último caso será necesario dejar evidencia de que físicamente la tarjeta se encontraba en el lugar de la operación. Por lo tanto, los datos en relieve de la misma deberán quedar estampados en el ticket (de manera similar al cupón manual).
- ✓ Cuando el importe de la operación, a resolver en forma OFF-LINE, supere el límite de venta del establecimiento, se deberá solicitar autorización telefónica e ingresar el correspondiente código recibido.
- ✓ Todos los tickets emitidos por operaciones Off-Line, con o sin lectura de banda magnética, deberán dejar el espacio necesario para dejar evidencia de la presencia física de la tarjeta, estampando los datos del relieve de la misma en el ticket (de manera similar al cupón manual). Esto se realiza hoy día para las operaciones realizadas con ingreso manual del número de tarjeta.
- ✓ Por cada operación se deberá emitir un ticket en dos ejemplares. El original firmado por el socio quedará archivado en el establecimiento por el término dispuesto por cada emisor y el duplicado será entregado al socio.
- ✓ Esta modalidad de operación deja sin efecto el armado de lotes de documentación a ser entregados en la Entidad Pagadora, ya que la presentación ante el Emisor se efectúa a través de líneas de comunicación directas con cada Administrador/Procesador.

Es importante dejar en claro que la operatoria deberá ser siempre ON-LINE, las aclaraciones realizadas en los párrafos precedentes es válida únicamente para los procedimientos de contingencia y por excepción, por fallas del vínculo de comunicaciones y con la expresa autorización de los emisores con los cuales opere.

ADHESION DE ESTABLECIMIENTOS

Los establecimientos que deseen acogerse a esta operatoria deberán manifestar su intención a la Gerencia Comercial del Emisor quien los contactará con el área correspondiente de cada Administradora, a efectos de definir las condiciones particulares de operación.

En todos los casos se efectuarán pruebas de transmisión y de presentación y los establecimientos podrán comenzar a operar sólo si los resultados de dichas pruebas son satisfactorios, dichas pruebas consisten en verificación de mensajes, consistencia de información transmitida, tiempos de comunicación, diseños de impresión de comprobantes y la auditoría de los sistemas.

Una vez finalizadas las mismas, se entregará al comercio una nota de homologación del sistema, cada emisor emitirá un ***"Anexo al Reglamento de Comerciantes de Aplicación exclusiva para operaciones de Draft Capture"*** por cada número de comercio con el que efectúen presentaciones a través de este medio y solicitará su firma al responsable del Establecimiento.
A su vez, las características particulares de operación quedarán establecidas en una carta compromiso que a tal efecto emitirá el Emisor.
Cualquier cambio que se efectúe deberá ser comunicado al Departamento de Operaciones del Emisor por lo menos con dos semanas de anticipación a hacerse efectivo el mismo.

PROCEDIMIENTOS DE AUTORIZACION

a) Lectura de banda magnética para extraer el número de cuenta. Se deberá leer el Track II y el Track I para extraer el apellido y nombre del socio, y además para los emisores que lo soliciten el envío del mismo.

b) Realizar el Control de cuatro últimos dígitos, control de Skimming para quienes lo soliciten.

c) Solicitar el ingreso del Código de Seguridad (si corresponde a la tarjeta), según lo requerido por el emisor.

d) Validación de la tarjeta según el rango ISO (BIN). Serán procesadas solo aquellas tarjetas cuyos rangos ISO se encuentren definidos en el archivo de tarjetas. **Ver CAPITULO H.**

e) Validación del **dígito verificador** del número de cuenta de la tarjeta (si estuviese definido por parámetros) y de la **longitud** del mismo.

f) Validación fecha de vencimiento de la tarjeta (AAMM). Se realizará con los datos contenidos en el Track II, rechazando toda tarjeta con fecha menor a la fecha real actual del sistema. No todos los emisores requieren control de fecha de expiración.

g) Si el ingreso del número de cuenta se realiza en forma manual por teclado se debe solicitar, para los emisores que así lo requieran, el Código de Seguridad de la tarjeta. El mismo posee una longitud de tres a cuatro dígitos, y no debe ser mostrado por visor. El mensaje a mostrar por visor para su ingreso deberá ser: **INGRESE CODIGO DE SEGURIDAD.** Algunos emisores requieren el ingreso del Código de Seguridad también cuando el ingreso del número de tarjeta es por lectura de banda magnética

h) Si la operación es **ON-LINE** continuar en el punto **j)**, caso contrario continuar en el i**)**.

i) Si el emisor lo habilita a operar en forma Off-Line, a toda operación OFF-LINE se le deberán realizar los siguientes controles:

- Validación del número de cuenta (tarjeta) del socio contra las bases de negativas (si las posee). Es decir, que se deberá verificar la existencia de la tarjeta en el archivo de negativas, de figurar se rechazará la operación.
- Validación de importe total de compras de una misma tarjeta, por lote, comparándolo con el límite de venta del establecimiento. En caso de que el importe total supere el límite de venta del establecimiento, deberá solicitar y colocar en el sistema y en el ticket el código de Autorización del emisor correspondiente.

  Control de Uso

  Verificación del "importe de la operación" contra el "límite de venta" del Comercio. En el caso de que el "importe de la operación" supere el Límite de Venta del Comercio, se deberá solicitar autorización telefónica, ingresando el código de autorización correspondiente. **Se deberá considerar para el "importe de la operación" las operaciones realizadas con anterioridad, para esa tarjeta, dentro del mismo lote.**

  El control de uso deberá realizarse dentro de un mismo lote de operaciones, únicamente se tomarán las operaciones generadas dentro del lote abierto.

j) Ingreso de cantidad de cuotas, si corresponde.

k) Selección del Plan de Pagos, si corresponde para dicha tarjeta.

Parámetros a definir en el sistema

- ***Número de lote****:*
  Numérico de 3 posiciones comenzando con 001 e incrementando de 1 en 1 por cada "Cierre de Lote". El último será el 999, el siguiente a éste deberá ser 001.

- ***Número de ticket:***
  Numérico de 4 posiciones comenzando con 0001 e incrementando de 1 en 1 por cada operación aprobada. El último será 9999, el siguiente a éste deberá ser 0001.

- ***Tabla de prefijos ISO por Entidad.*** *(Parametrizable)*

- ***Límites de venta del Comercio por Entidad.***

- ***Tabla de relación:***
  - Nro. Comercio Entidad 1
  - Nro. Comercio Entidad 2
  - Nro. Comercio Entidad N.

- ***Número Serie de Terminal y Nro. de comercio del Emisor***
  Estos números son administrados y entregados por cada Emisor a los Comercios.
  Tener en cuenta que determinados Administradores asignan números de serie de terminal por código de comercio ($ y U$S), **esto significa que cada caja tendrá asignado dos números de terminal, uno para operaciones en moneda local y otro para operaciones en dólares,** manteniendo lotes separados por moneda.

- ***Manejo del Número de Terminal en sistemas distribuidos (Caja-Servidor)***
  En un sistema distribuido de caja-servidor, el número de terminal deberá ser definido por caja y no por servidor. Esta definición surge debido a que el concentrador podrá enviar de esta manera múltiples mensajes hacia el Host, ya que cada operación corresponderá a una única terminal, aprovechándose a full el vínculo
  o IP, enviando los mensajes de requerimiento ISO a medida que son generados por las cajas. Si mantuviéramos un número de terminal por servidor, los mensajes generados para un mismo emisor deberían ir a cola de espera transmitiendo uno a uno a medida que las respuestas fueran recibidas.
  Esto ayudará también a realizar un mejor seguimiento y una puntual detección de problemas en caso de producirse reclamos por operaciones.

- ***Manejo de comunicaciones en sistemas con conexión centralizada de sus sucursales***
  En sistemas que poseen sus sucursales centralizadas a través de casa central o de otra sucursal, se deberá tener especial cuidado en la manera de manejar el vínculo X.25 o IP. El mismo deberá permitir la apertura de varios canales virtuales (si es necesario), con la inteligencia necesaria de balancear el tráfico a través de los mismos. En el momento de solicitar la homologación de este tipo de sistemas, se verá con el personal de comunicaciones las necesidades en base al tipo de comercio.

OPERACIONES

El comercio será **responsable** del contenido de la información transmitida a los emisores.

Las presentaciones deberán efectuarse mediante transmisiones On-line a través de la funcionalidad denominada Cierres de Lote (conciliación de totales). La mayoría de los emisores aceptan presentaciones diarias trabajando bajo esta modalidad.

El plazo máximo para efectuar la presentación mediante transmisiones on-line será hasta las 23:50 horas del mismo día al establecido para la presentación. Pasado dicho horario, las operaciones serán tomadas con la fecha de presentación del día siguiente.

Si bien se hace mención a los plazos horarios máximos de presentación, las transmisiones podrán ser en cualquier horario y además se podrá realizar más de una presentación (Cierre de Lote) diaria.

Operaciones disponibles

- Compra

Debe permitir la selección del tipo de moneda, el ingreso de cantidad de cuotas, selección del plan correspondiente (si el emisor lo requiere) y el importe (generalmente lo toma del subtotal que calcula el POS). Por default el tipo de moneda deberá ser pesos y la cantidad de cuotas 01.
El ticket emitido deberá ser firmado por el socio.

- Devoluciones

Puede ser realizada por una suma parcial o total de la operación original (Compra), siempre debe ser generada en presencia del tarjeta habiente.
Debe permitir la selección del tipo de moneda, el ingreso de cantidad de cuotas, el importe (generalmente lo toma del subtotal que calcula el POS), el número de ticket y la fecha de la operación original. Por default el tipo de moneda deberá ser pesos y la cantidad de cuotas 01. Esta operación debe ser realizada cuando la operación original haya sido presentada en un lote ya cerrado.
El ticket emitido deberá ser firmado por el responsable del comercio y entregado al socio.

- Anulaciones

Deberá ser realizada por el total de la operación original, verificando la existencia de la misma dentro del lote de operaciones abierto. Siempre debe ser realizada en presencia del tarjeta habiente.
Podrán ser anuladas tanto operaciones de **Compra** como de **Devolución**, permitiendo ingresar el número de tarjeta y el número de ticket a anular.
El ticket emitido deberá ser firmado por el responsable del comercio y entregado al socio.

- Pre-Autorización

  Esta operación estará únicamente permitida a aquellos comercios que por su tipo de operatoria la requieran. Funcionalmente opera de la misma forma que una Compra, con la diferencia de que esta operación no genera un Cargo (Cupón) de Captura, solo realiza la inmovilización del monto por la cual fue solicitada.
  Esta operación no requiere la generación de un ticket de respaldo.

- Cierre de Lote

  Esta operación generará la presentación electrónica de las operaciones efectuadas dentro del último lote abierto para cada Administrador/Procesador. Es aconsejable realizar un Cierre de Lote al menos una vez por día.

Todas las operaciones se realizarán leyendo la banda magnética de la tarjeta del socio, tomando el número de cuenta del track II y opcionalmente se podrá extraer el apellido y nombre del socio si se cuenta con lectura del track I. En caso de tratarse de ingresos manuales, hay emisores que requieren el ingreso de un código de seguridad que puede ser de tres o cuatro dígitos, el cual debe ser ingresado (sin mostrarlo por visor) al sistema e informado en el mensaje de requerimiento al Computador Central.

CAPITULO A - TICKETS SOLICITADOS POR LOS EMISORES

Por lo general los tickets originales por operaciones de contado deberán archivarse en el establecimiento durante 1 año, mientras que los correspondientes a operaciones en cuotas se deberán archivar por el término de 2 años. Este punto debe ser acordado con cada emisor con el que opere.

En caso que el Emisor solicite tickets correspondientes a reclamos efectuados por los socios, los mismos deberán remitirse al Departamento correspondiente a cada Emisor. Los mismos deberán remitirse en un plazo no mayor a 2 (dos) días corridos desde la fecha de notificación del pedido. El método u operatoria de envío de esta información deberá ser acordada con cada Emisor.

Tickets

Todas las operaciones emitirán tickets en original y copia. El original firmado por el socio (No Débito) será archivado por el Comercio y la copia se le entregará al socio.

Todos los tickets emitidos por operaciones Off-Line, con o sin lectura de banda magnética, deberán dejar el espacio necesario para dejar evidencia de la presencia física de la tarjeta, estampando los datos del relieve de la misma en el ticket (de manera similar al cupón manual).

Tickets que deberán ser generados por el sistema.

Datos incluidos en los tickets

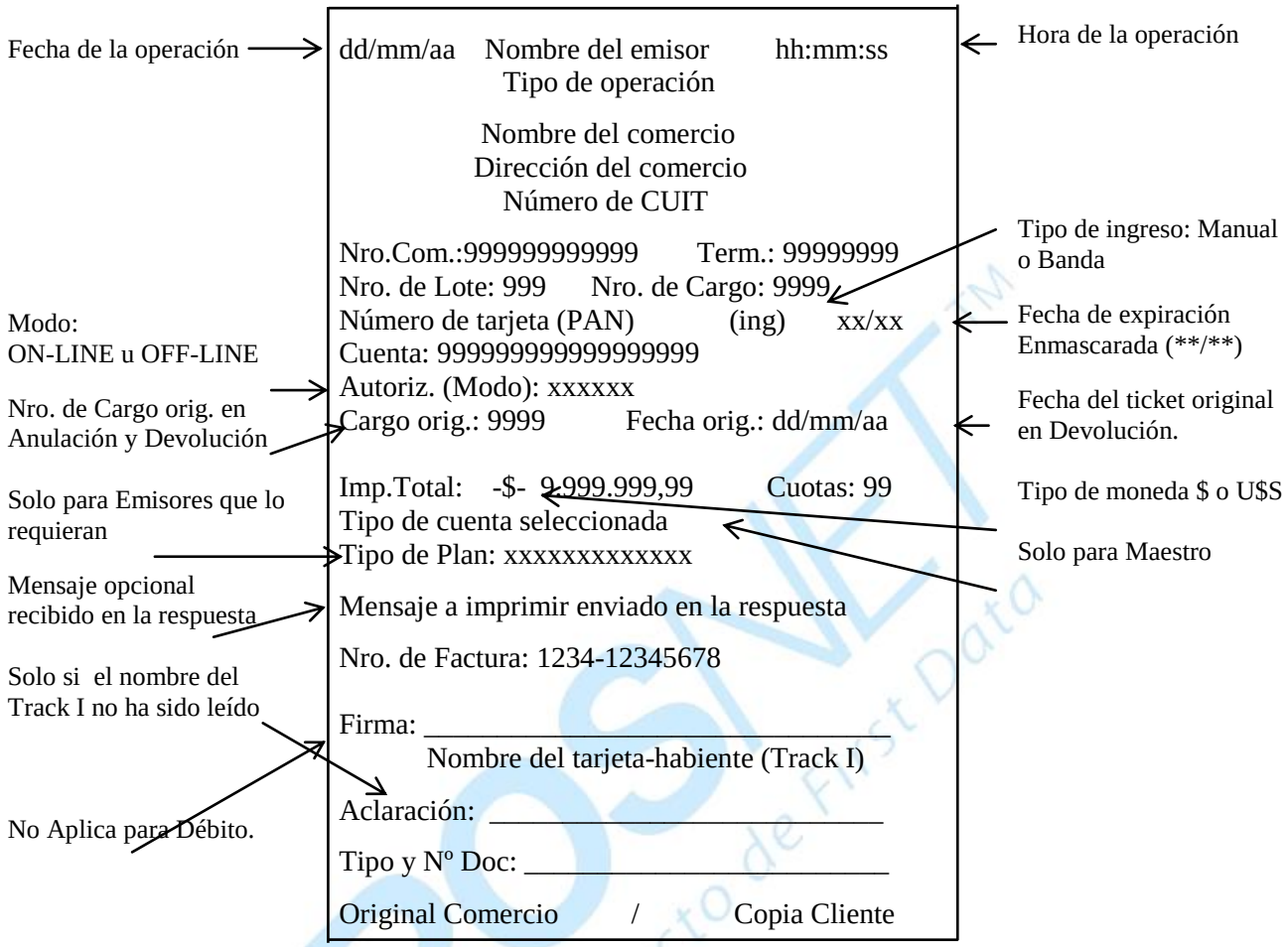
Emisión de tickets:

Ante cada operación, el establecimiento deberá emitir un ticket en original y copia el cual deberá contener como mínimo los siguientes datos:

- Fecha y hora de emisión
- Nombre del Emisor de la Tarjeta
- Tipo de operación (Compra-Anulación-Devolución)
- Nombre del establecimiento
- Domicilio del Establecimiento
- Número de establecimiento asignado por el Emisor (Código de Comercio).
- Número de cargo (cupón).
- Nro. LOTE
- Nro. de Terminal asignado por el Comité de tarjetas, dentro del Acuerdo Tecnológico de la Industria.
- Número de Tarjeta con la que se efectúa la operación.(enmascarado si lo requiere el emisor)
- Modo de ingreso del número de tarjeta (por lector o manual).
- Fecha de vencimiento de la Tarjeta de Crédito (enmascarada).
- Modo de operación (OFF ú ON-line).
- Código de Autorización otorgado por Emisor (en caso de corresponder).
- Importe de la operación.
- Moneda de la operación.
- Cantidad de cuotas.
- Plan de Pago (en caso de corresponder)
- Nro. de cargo original (en Anulaciones y Devoluciones).
- Fecha de la operación original (en Devoluciones).
- Tipo de cuenta seleccionada (Solo Maestro)
- Mensaje opcional recibido en la respuesta a una autorización.
- Firma del Socio o de personal autorizado del comercio en caso de Anulaciones o Devoluciones (Excepto para Maestro que no lo requiere).
- Aclaración del nombre del firmante (Excepto para Maestro que no lo requiere).
- Tipo y Número de Documento (para los emisores que lo soliciten).
- Espacio para el estampado del relieve de la tarjeta. Obligatorio para todas las operaciones Off-Line (sin excepción) y para todas las operaciones On-Line con ingreso manual del número de tarjeta.

El Ticket original, deberá quedar en poder del establecimiento.
El duplicado del Ticket será entregado al socio.

Diseño de tickets



Descripción de Campos

Nombre del Emisor Nombre de la tarjeta con que se realiza la operación.

Tipo de operación Operación realizada:
COMPRA - ANULACION DE COMPRA
DEVOLUCION - ANULACION DE DEVOLUCION.

Modo Modo de operación: ON-LINE u OFF-LINE.

(ing) Es requerimiento que el tipo de ingreso de la tarjeta sea discriminado en el ticket. Puede ser un (*) si es ingreso manual, y por banda se deja en blanco.

CAPITULO B - ESPECIFICACIONES GENERALES

Protocolos

El protocolo de datos a implementar es la norma internacional estándar ISO 8583.

El protocolo de comunicaciones recomendado es IP sobre Frame Relay o X.25. Conviene que el mismo sea a través de alguna red pública nacional de datos, ya que cada Administrador/Procesador con el que opere será una dirección de CALL X.25 o IP distinta (Caller ID).

En caso de inconvenientes con la conexión, el sistema deberá mostrar y/o capturar el código de error recibido de la red de comunicaciones, a fin de efectuar el reclamo correspondiente.

Manejo de variables dentro del sistema

Dentro de un mismo sistema coexistirán varios Procesadores/Emisores con los que se operará. Los mismos podrán operar en forma unitaria, o varios emisores concentrados en un mismo procesador. Es importante tener en cuenta que existen variables que se manejarán a nivel Host y otras a nivel emisor, a saber:

Nivel Host
- Dirección de CALL X.25 o IP
- NII
- Número de terminal
- Código de Comercio de Cierre (solo para procesadores)
- Número de trace del sistema (incrementa de a uno por cada transacción, excepto con los reversos)(único por terminal).
- Número de lote (único por terminal).
- Número de ticket/cupón (incrementa unicamente por operaciones aprobadas) (único por terminal).

Nivel Emisor (tarjeta)
- Host asociado (en caso de estar operando con un procesador)
- Código/s de Comercio **(*)**
- Planes de pago
- Cantidad máxima de cuotas permitidas
- Tipo de moneda habilitada

Nivel de reconocimiento
- Emisor asociado
- Rangos de reconocimiento (bines)

(*) El código de comercio asignado por cada emisor, puede variar por tipo de moneda o por cantidad de cuotas.

Por ejemplo:

01 cuota	Código aaaaaaa
02 a 03 cuotas	Código bbbbbb
.....	
10 a 12 cuotas	Código eeeeee

Envío de operaciones capturadas por el comercio

El comercio realizará **"Cierres de Lote"** por Administrador/Emisor todas las veces que lo considere necesario. Cada "Cierre de Lote" generará un registro con los totales de las operaciones realizadas por el Comercio para ese lote, con las tarjetas de crédito y/o débito que opere por cada Administrador/Emisor.

El Cierre de Lote consiste en el envío de un registro de totales de operaciones. Se debe tener especial atención en el "Cierre de Lote", ya que existen Administradores/Procesadores que operan con más de un emisor, por lo que esta operación involucrará los totales de todos los Emisores con los que el mismo opere, sin discriminar totales por cada uno en la transmisión.

Batch Upload

En caso de existir diferencias entre los totales enviados por el sistema del comercio y los totales que el sistema del Administrador/Procesador haya contabilizado, se requerirá a la terminal el re-envío de todas las operaciones (ON-LINE y OFF-LINE), este proceso se denomina Batch Upload. Al finalizar el envío de las transacciones de Batch Upload, la terminal deberá enviar nuevamente un registro de Cierre de Lote

El Cierre de Lote debe ser generado por cada terminal. En caso de no recibir respuesta al mismo, se deberá reintentar el mismo por lo menos un total de 5 (cinco) veces. No hay motivo para que la respuesta no sea recibida.

En caso de que el Cierre de Lote de una o varias terminales no haya sido realizado, debe tenerse en cuenta que antes de comenzar un nuevo día o lote de operaciones, se deberá realizar el Cierre de Lote automáticamente. Esto permitirá que todas las terminales continúen con el mismo número de lote.

IMPORTANTE: El Host de Posnet no requiere el envío del Batch Upload, éste totaliza únicamente lo capturado al momento del cierre.

Modalidad de transmisión de Mensajes

La operatoria deberá ser FULL ON-LINE, excepto ante un eventual estado de fuera de servicio de la línea de comunicación primaria, en este caso se procederá a utilizar un vínculo secundario de backup, en caso de no funcionar o no poseer este último, se procederá a autorizar localmente contra el archivo de negativos y el límite de comercio, realizando **el control de uso** (operaciones OFF-LINE) si el emisor lo ha habilitado.

Manejo de operaciones OFF-LINE

Cada operación OFF-LINE realizada deberá ser transmitida al computador central cuando se haya recuperado el vínculo de comunicaciones. El funcionamiento ideal es que todas las operaciones que se hayan realizado OFF-LINE se transmitan todas juntas al Host al momento que el vínculo de comunicaciones vuelva a estar operativo.

Si al realizar el Cierre de Lote, hay pendientes de transmisión operaciones OFF-LINE, se deberán transmitir una a una las mismas previas a la transmición del Cierre de Lote.

Reversos

Existen mensajes de reversos por terminal para operaciones en vuelo que no hayan recibido respuesta o que las mismas por problemas de línea o del server no hayan recibido respuesta. **El mensaje de reverso reestablece el límite del tarjeta-habiente e informa al Administrador/Procesador que la operación anterior, para determinada terminal, no ha sido completada**. Todo reverso debe ser informado con el número de trace de la operación original a reversar; el siguiente mensaje sí debe incrementar el número de trace en uno.

Debe tenerse en cuenta que los REVERSOS pueden ser de operaciones ON-LINE como así también de operaciones OFF-LINE.

Ejemplo:

Lote 001	Compra rechazada	tkt 0001	trace 0001
	Compra sin respuesta	tkt 0001	trace 0002
	Reverso	tkt 0001	trace 0002
	Compra aprobada	tkt 0001	trace 0003
	Cierre de Lote con diferencia		trace 0004
	Batch Upload Compra	tkt 0001	trace 0005
	Cierre de Lote		trace 0006
Lote 002	Compra aprobada	tkt 0002	trace 0007
	Anulación tkt 0002	tkt 0003	trace 0008
	Compra OFF-LINE sin resp.	tkt 0004	trace 0009
	Reverso	tkt 0004	trace 0009
	Compra OFF-LINE	tkt 0004	trace 0010
	Cierre de Lote sin diferencia		trace 0011

Timeouts

***De respuesta a un requerimiento de autorización*: 25 segundos.**
En caso de producirse un timeout, y de acuerdo a las normas de cada emisor, el sistema deberá generar la autorización en forma OFF-LINE, realizando los controles descriptos en el punto 3 (Procedimientos de Autorización).

IMPORTANTE: El próximo mensaje a transmitir deberá ser el reverso de la última transacción que salió por timeout.
***De respuesta a un Cierre de Lote*: 30 segundos**

Campos a verificar para la evaluación de mensajes de respuesta

Todo mensaje de respuesta debe ser verificado a través del control de 3 (tres) campos prioritarios. Los mismos son: ***Tipo de Mensaje - Número de Trace - Número de Terminal.***

Si en la respuesta alguno de estos 3 (tres) campos no coincidiera con los datos enviados en el requerimiento, el mensaje debe ser deshechado, continuando la secuencia de espera por el mensaje de respuesta correcto. La probabilidad de que ésto suceda es mínima, pero sí puede darse en el supuesto caso que el computador central responda fuera de los tiempos máximos establecidos, o de que el Timeout parametrizado sea menor al fijado en este manual.

Control de Skimming

Esta funcionalidad tiene por finalidad ingresar el código de seguridad o comparar los últimos cuatro dígitos del número de tarjeta leído por banda contra los últimos cuatro dígitos embozados (impresos) en el plástico, según lo solicitado por cada emisor.

Ingreso del código de seguridad

- Este ingreso se deberá solicitar cuando el número de tarjeta sea leído por el lector de banda o ingresado manualmente.
- Las operaciones involucradas serán COMPRAS ON-LINE y DEVOLUCIONES ON-LINE exclusivamente.
- El código de seguridad ingresado no deberá ser mostrado por visor.

Ingreso de cuatro últimos dígitos

- Este control se deberá solicitar únicamente cuando el número de tarjeta sea leído por el lector de banda.
- Las operaciones involucradas serán AUTORIZACIONES, COMPRAS, ANULACIONES y DEVOLUCIONES, tanto ON-LINE como OFF-LINE.
- Los cuatro últimos dígitos ingresados no deberán ser mostrados por visor.

Definición funcional

- Pasar la tarjeta desde el estado de reposo.
- Si la lectura fue buena, se deberá solicitar el ingreso de los últimos cuatro dígitos del número de tarjeta embozado en relieve en el frente del plástico, durante su ingreso, los mismos no deberán ser mostrados por visor, sino que deberán ser enmascarados con asteriscos ("*****").
- El sistema deberá comparar los cuatro dígitos ingresados contra los cuatro últimos dígitos leídos por lector, en caso de que los mismos sean iguales, se deberá continuar la operatoria normalmente.
- En caso de no concordar, se deberá volver a solicitar el ingreso de los cuatro últimos dígitos, para realizar una segunda verificación. Si la nueva comparación resulta nuevamente diferente, se deberá mostrar un mensaje por display y finalizar la operación.
- Ante dicho mensaje el comercio deberá comunicarse con el Emisor correspondiente, informando de dicho inconveniente.

Definición de mensajes

- Solicitud de primer ingreso de los cuatro últimos dígitos del embozado

COMPRA Nombre Tarjeta **DEVOL. Nombre Tarjeta**
ING 4 ULT DIG. XXXX **ING 4 ULT DIG. XXXX**

- Solicitud de segundo ingreso de los cuatro últimos dígitos del embozado, por diferencia en el primer ingreso. La terminal generará un beep y volverá a solicitar lo mismo.

COMPRA Nombre Tarjeta **DEVOL. Nombre Tarjeta**
REING ULT DIG XXXX **REING ULT DIG XXXX**

- Mensaje a mostrar por visor si el segundo ingreso también resulta con diferencia. Este mensaje quedará en display hasta tanto el operador no presione la tecla **CLEAR.**

LLAMAR CODIGO 10
9999 9999 9999 XXXX **Es el número de tarjeta leído por banda. Excepto los cuatro últimos dígitos que son reemplazados por XXXX (ocultados).**

Se deberá llamar al Centro de Autorizaciones del emisor correspondiente e informar del mensaje que la terminal le está mostrando.
Si la operación es rechazada por el centro de autorizaciones, se cancelará la misma.
Si la operación es confirmada por el centro de autorizaciones, se recibirá el código de autorización respectivo, el que se deberá tipear para que conste en el posterior envío de la transacción. Por lo tanto esta transacción deberá ingresar por tipeo de número de tarjeta, con la referencia del número de autorización recibido y enviada a procesar como si hubiera sido procesada fuera de línea (mensaje Off-Line).

Código de Seguridad (CVC)

En toda operación ONLINE realizada con tarjetas de Crédito MasterCard y Lider, sea con ingreso manual del número de tarjeta o con **lectura de la Banda Magnética**, se deberá solicitar siempre el ingreso del Código de Seguridad (**CVC)**. El ingreso del mismo no debe reflejarse en la pantalla del sistema. Si el sistema muestra por pantalla los datos que se están ingresando, el Código de Seguridad (**CVC)** debe aparecer con *******. El dato debe enviarse en el campo **ISO 55** del mensaje de requerimiento, tal como se hace para las operaciones con ingreso manual del número de tarjeta.

Definiciones

- Se agrega al actual Control de Skimming, ingreso de los 4 (cuatro) últimos dígitos, cuando existe lectura de banda magnética.
- Unicamente debe solicitarse para operaciones On-Line de Compra y Devolución.
- Habilitada actualmente para los productos Mastercard y Lider únicamente.
- Transmisión del mismo en el campo ISO 55, de la misma forma que para las operaciones con ingreso manual del número de tarjeta.

Transmisión TRACK I

En todo ingreso por banda magnética se debe enviar, en el campo **ISO 45** del mensaje de requerimiento, el **Track I** en forma completa. Es decir que se deberán transmitir los **Track I** y **Track II** en todas las transacciones con lectura de Banda.

En el caso que la banda este dañada y el sistema haya leído el **Track II** pero NO haya podido leer el **Track I,** se deberá enviar en el campo **ISO 46** del mensaje de requerimiento, un byte con el valor **"1"** (uno).

En el caso que NO se haya podido leer el **Track II** pero si se leyó el **Track I**, la operación no debe realizarse, y se debe proceder como en la actualidad (reingreso de la tarjeta con lectura de banda o ingreso manual de la tarjeta).

Definiciones

- Requerido para todas las operaciones On-Line de Autorización, Compra, Anulación y Devolución y en operaciones Off-Line de Compra, Anulación y Devolución.
- Las normas de seguridad establecidas por la industria, aplican también para el manejo del **Track I** y del Código de Seguridad (**CVC)**.
- Habilitada actualmente para los productos Mastercard, Lider, Maestro, Cabal y tarjetas regionales (ver especificaciones puntuales).
- El **Track I** debe ser transmitido en el campo ISO 45.
- En el caso de falla en la lectura del **Track I**, se debe enviar el **Track II** (campo ISO 35) y el valor "**1**" en el campo ISO 46.

Impresión en el ticket

En todas las operaciones On-Line u Off-Line de Compra, Anulación y Devolución se deberá agregar al pie del ticket la leyenda.

"Tipo y Nº Doc.: .....".

Maestro ver especificaciones puntuales.

Enmascaramiento de número de Tarjeta

Todo ticket emitido deberá imprimir el número de tarjeta enmascarando con el carácter "*" o "#" los primeros doce dígitos de la misma, a solicitud de cada emisor.

Ejemplo:

Número de tarjeta => 5995 6612 3456 7890 12

Imprimir

**** **** **** 7890 12 o #### #### #### 7890 12

Esta definición deberá ser implementada en primera instancia únicamente para los productos MAESTRO Y MASTERCARD.

Enmascaramiento de la fecha de vencimiento

Todo ticket emitido deberá imprimir la fecha de vencimiento, enmascarando la misma con el carácter "*" o "#".

Ejemplo:

Fecha de vencimiento => 05/12

Imprimir

/ o ##/##

Esta definición deberá ser implementada únicamente para los productos MAESTRO, MASTERCARD, LIDER Y CABAL.

Es importante el desarrollo de estas modificaciones como un atributo adicional por emisor, a efectos de poder ser habilitado a solicitud de las marcas que así lo requieran.

Definiciones para Enmascaramiento de Tarjeta y Envío de Número de Cuenta

Descripción de la Operatoria

Las modificaciones a implementar en la operatoria de transacciones de Tarjetas de Crédito y Débito en los puntos de venta son a efecto de recibir, desde el Host, el Número de Cuenta del TarjetaHabiente e imprimirlo en el comprobante de la operación.

A su vez se deberá enmascarar, en el ticket, el Número de Tarjeta del usuario, esta definición es complementaria a la enviada con anterioridad.

Definiciones de la modificación

- ✓ El POS, desde el momento que está capacitado para recibir el Número de Cuenta, debe enviar en todos los mensajes de Crédito y Débito (salvo cierres de lote, Off Line y con excepciones en reversos) la marca de Número de Cuenta (Campo Iso 59). Con ésta marca el Host sabrá que puede enviar, al POS, el Número de Cuenta para las tarjetas que así lo definan.

- ✓ Siempre que el Número de Cuenta se reciba, en un mensaje de respuesta del Host, se deberá imprimir en el ticket comprobante de la operación.

- ✓ Cuando, en el Número de Cuenta, se reciba al menos un asterisco ("*") se deberá imprimir el Número de Tarjeta en forma Completa y se deberá imprimir el campo Número de Cuenta tal como se lo recibió desde el Host.

- ✓ El Número de Tarjeta se deberá enmascarar en todas las operaciones, se haya recibido el Número de Cuenta o NO, salvo que ocurra el caso del punto anterior.

- ✓ Se debe tener en cuenta que el Emisor puede definir enmascarar o NO el Número de Tarjeta en operaciones del tipo Off-Line.

- ✓ Se debe considerar que, tanto, la cantidad de dígitos y la posición inicial de enmascaramiento será definido por cada Emisor.

CAPITULO C – ESPECIFICACION DE MENSAJES

Diseño de registros para operaciones

Especificaciones

DESCRIPCION DE FORMATOS Y ATRIBUTOS			NOTAS	
B	Binario		**X**	Campo transmitido
n	Dígitos numéricos		**O**	Campo Opcional
Ns	Caracteres numéricos y especiales			
An	Caracteres alfanuméricos		**C1**	Campo mandatorio si el ingreso del número de la tarjeta fue manual.
Ans	Caracteres alfanuméricos y especiales		**C2**	Campo mandatorio si el ingreso del número de la tarjeta fue por banda, para los emisores que lo requieran.
AAMMDD	Año, mes y día		**C4**	Campo mandatorio si se especifica en el requerimiento.
HHMMSS	Hora, minutos y segundos		**C5**	Campo mandatorio si es requerido por el emisor.
VAR	Campo de longitud variable		**C6**	Campo mandatorio si fue especificada en transacción original.
LL,LLL	Longitud del campo variable		**C7**	Código de procesamiento de la operación original NNNNNX X=0 último mensaje X=1 hay mas mensajes
..37 **3**	Campo de longitud variable de hasta 37 caracteres Campo de longitud fija de 3 caracteres		**C8**	Código de procesamiento de la transacción original
..76	Campo de longitud variable de hasta 76 caracteres		**C9**	Si el ingreso del número de tarjeta se realiza por lectura de banda, y la lectura solo arroja el Track II y no el Track I, entonces en este campo se debe enviar el valor "1". Si el Track I es leído correctamente, este campo no debe ser enviado.

ON-LINE (Compra, Anulación, Devolución)

				COMPRA		DEVOLUCION		ANULACION	
		Formato	Atributo	REQ.	RTA.	REQ.	RTA.	REQ.	RTA.
	TPDU		n..10	X	X	X	X	X	X
	TIPO DE MENSAJE			0200	0210	0200	0210	0200	0210
	MAPA DE BIT		B64	X	X	X	X	X	X
2	NUMERO DE CUENTA / TARJETA	LLVAR	n..20	C1	C4	C1	C4	C1	C4
3	CODIGO DE PROCESAMIENTO		N6	000000	000000	200000	200000	020000 220000	020000 220000
4	IMPORTE DE LA TRANSACCION		n12	X	O	X	O	X	O
7	FECHA Y HORA DE TRANSMISION	MMDDHH MMSS	n10	X	O	X	O	X	O
11	NUMERO DE TRACE DEL SISTEMA		n6	X	X	X	X	X	X
12	HORA LOCAL DE LA TRANSACCION	HHMMSS	n6	X		X		X	
13	FECHA LOCAL DE LA TRANSACCION	MMDD	n4	X		X		X	
14	FECHA DE EXPIRACION	AAMM	n4	C1		C1		C1	
22	MODO DE INGRESO EN LA POS		n3	X		X		X	
24	IDENTIF INTERNACIONAL DE LA RED		n3	X	X	X	X	X	X
25	CODIGO DE CONDICION DE LA POS		n2	00		00		00	
34	NUMERO DE CUENTA	LLVAR	ans..28		O		O		O
35	DATOS DEL TRACK II	LLVAR	n..37	C2		C2		C2	
37	RETRIEVAL REFERENCE NUMBER		an12		X		X	X	X
38	CODIGO DE AUTORIZACION		an6		O		O		O
39	CODIGO DE RESPUESTA		an2		X		X		X
41	IDENTIFICACION DE LA TERMINAL		ans8	X	X	X	X	X	X
42	CODIGO DE IDENTIF.DEL COMERCIO		ans15	X	O	X	O	X	O
45	DATOS DEL TRACK I (Mastercad y Lider)	LLVAR	ans..76	C2		C2		C2	
46	TRACK I NO LEIDO	LLLVAR	ans..999	C9		C9		C9	
48	CUOTAS / DATOS ORIGINALES	LLLVAR	ans..999	X	O	X	O	X	O
49	CODIGO DE MONEDA		an3	X	O	X	O	X	O
55	CODIGO DE SEGURIDAD DE LA TARJETA	LLLVAR	ans..999	C5		C5			
59	INFORMACION ADICIONAL	LLLVAR	ans..999	X		X		X	
60	VERSION DE SOFT. DE APLICACION	LLLVAR	ans..999	X		X		X	
62	NUMERO DE TICKET	LLLVAR	ans..999	X		X		X	
63	MENSAJE DEL HOST-MOSTRAR –IMPRIMIR	LLLVAR	ans..999		O		O		O

Descripción de Campos Especiales

CAMPO 48. (CUOTAS / DATOS ORIGINALES)

CAMPOS	ATRIBUTO	LONGITUD	TRANSACCION		DESCRIPCION
PAGOS Plan	an..1	1	TODAS	0..9	Plan
Cuotas	an..2	2		00..99	Cantidad de cuotas
TICKET ORIGINAL	an..4	4	DEVOLUCION	0001..9999	Número de ticket Original
FECHA ORIGINAL	an..6	6	DEVOLUCION	DDMMAA	Fecha de la transacción original

CAMPO 59. (INFORMACION ADICIONAL / PREPARADO PARA NUMERO DE CUENTA)

CAMPOS	ATRIBUTO	LONGITUD	TRANSACCION		DESCRIPCION
Tipo de Producto	an..3	3	TODAS	002	Indica el tipo de producto que se informará
Cantidad de SubCampos	an..4	4	TODAS	0001	Indica la cantidad de SubCampos que posee el producto.
Longitud de SubCampo	an..3	3	TODAS	001	Informa la longitud que tendrá el SubCampo.
ID del SubCampo	an..3	3	TODAS	009	Informa el Nombre del SubCampo.
Valor del SubCampo	an..1	1	TODAS	1	Significa "Preparado para recibir ISO 34"

OFF-LINE (Compra, Anulación, Devolución)

				COMPRA		DEVOLUCION		ANULACION	
		Formato	Atributo	REQ.	RTA.	REQ.	RTA.	REQ.	RTA.
	TPDU		n..10	X	X	X	X	X	X
	TIPO DE MENSAJE			0220	0230	0220	0230	0220	0230
	MAPA DE BIT		b64	X	X	X	X	X	X
2	NUMERO DE CUENTA/ TARJETA	LLVAR	n..20	C1	C4(O)	C1	C4(O)	C1	C4(O)
3	CODIGO DE PROCESAMIENTO		n6	000000	000000	200000	200000	020000 220000	020000 220000
4	IMPORTE DE LA TRANSACCION		n12	X	O	X	O	X	O
7	FECHA Y HORA DE TRANSMISION	MMDDHH MMSS	n10	X	O	X	O	X	O
11	NUMERO DE TRACE DEL SISTEMA		n6	X	X	X	X	X	X
12	HORA LOCAL DE LA TRANSACCION	HHMMSS	n6	X		X		X	
13	FECHA LOCAL DE LA TRANSACCION	MMDD	n4	X		X		X	
14	FECHA DE EXPIRACION	AAMM	n4	C1		C1		C1	
17	FECHA DE CAPTURA	MMDD	n4	X		X		X	
22	MODO DE INGRESO EN LA POS		n3	X		X		X	
24	IDENTIF INTERNACIONAL DE LA RED		n3	X	X	X	X	X	X
25	CODIGO DE CONDICION DE LA POS		n2	00		00		00	
35	DATOS DEL TRACK II	LLVAR	n..37	C2		C2		C2	
37	RETRIEVAL REFERENCE NUMBER		an12		X		X	X	X
38	CODIGO DE AUTORIZACION		an6	O	O	O	O	O	O
39	CODIGO DE RESPUESTA		an2		X		X		X
41	IDENTIFICACION DE LA TERMINAL		ans8	X	X	X	X	X	X
42	CODIGO DE IDENTIF.DEL COMERCIO		ans15	X	O	X	O	X	O
45	DATOS DEL TRACK I	LLVAR	n..76	C2		C2		C2	
46	TRACK I NO LEIDO	LLLVAR	ans..999	C9		C9		C9	
48	CUOTAS / DATOS ORIGINALES	LLLVAR	ans..999	X	O	X	O	X	O
49	CODIGO DE MONEDA		an3	X	O	X	O	X	O
55	CODIGO DE SEGURIDAD DE LA TARJETA	LLLVAR	ans..999						
60	VERSION DE SOFT. DE APLICACION	LLLVAR	ans..999	X		X		X	
62	NUMERO DE TICKET	LLLVAR	ans..999	X		X		X	

Descripción de Campos Especiales

CAMPO 48. (CUOTAS / DATOS ORIGINALES)

CAMPOS	ATRIBUTO	LONGITUD	TRANSACCION		DESCRIPCION
PAGOS Plan	an..1	1	TODAS	0..9	Plan
Cuotas	an..2	2		00..99	Cantidad de cuotas
TICKET ORIGINAL	an..4	4	DEVOLUCION	0001..9999	Número de ticket Original
FECHA ORIGINAL	an..6	6	DEVOLUCION	DDMMAA	Fecha de la transacción original

ON-LINE (Batch UpLoad, Reverso, Cierre de Lote)

				BATCH UPLOAD		REVERSO		CIERRE DE LOTE	
		Formato	Atributo	REQ.	RTA.	REQ.	RTA.	REQ.	RTA.
	TPDU		n..10	X	X	X	X	X	X
	TIPO DE MENSAJE			0320	0330	0400	0410	0500	0510
	MAPA DE BIT		B64	X	X	X	X	X	X
2	NUMERO DE CUENTA / TARJETA	LLVAR	n..20	C6	C4 (O)	C6	C4 (O)		
3	CODIGO DE PROCESAMIENTO		N6	C7	C7	C8	C8	920000 960000	920000 960000
4	IMPORTE DE LA TRANSACCION		N12	X	O	X	O		
7	FECHA Y HORA DE TRANSMISION	MMDDHH MMSS	N10	X	O	X	O	X	O
11	NUMERO DE TRACE DEL SISTEMA		N6	X	X	X	X	X	X
12	HORA LOCAL DE LA TRANSACCION	HHMMSS	N6	X		X			
13	FECHA LOCAL DE LA TRANSACCION	MMDD	N4	X		X			
14	FECHA DE EXPIRACION	AAMM	N4	C6		C6			
15	FECHA DE CIERRE	MMDD	N4					X	O
17	FECHA DE CAPTURA	MMDD	N4	X		C6			
22	MODO DE INGRESO EN LA POS		n3	X		C6			
24	IDENTIF INTERNACIONAL DE LA RED		n3	X	X	X	X	X	X
25	CODIGO DE CONDICION DE LA POS		n2	00		00			
34	NUMERO DE CUENTA	LLVAR	ans..28		O		O		
35	DATOS DEL TRACK II	LLVAR	n..37	C6		C6			
37	RETRIEVAL REFERENCE NUMBER		an12	X	X	C6	X		X
38	CODIGO DE AUTORIZACION		an6	X	O	C6	O		O
39	CODIGO DE RESPUESTA		an2		X		X		X
41	IDENTIFICACION DE LA TERMINAL		ans8	X	X	X	X	X	X
42	CODIGO DE IDENTIF.DEL COMERCIO		ans15	X	O	X	O	X	O
45	DATOS DEL TRACK I	LLVAR	n..76	C6		C6			
46	TRACK I NO LEIDO	LLLVAR	ans..999	C6		C6			
48	CUOTAS / DATOS ORIGINALES	LLLVAR	ans..999	X	O	X	O		
49	CODIGO DE MONEDA		an3	X	O	X	O		
52	PIN/WORKING KEY		b64			C6			O
55	CODIGO DE SEGURIDAD DE LA TARJETA	LLLVAR	ans..999						
59	INFORMACION ADICIONAL	LLLVAR	ans..999	X		X			
60	VERSION DE SOFT. DE APLICACION	LLLVAR	ans..999	X		X		X	
62	NUMERO DE TICKET	LLLVAR	ans..999	X		X			
63	INFORM.DE OPERACION ORIGINAL	LLLVAR	ans..999	X				X	
63	MENSAJE DEL HOST MOSTRAR-IMPRIMIR	LLLVAR	ans..40						O

CAMPO 63. del BATCH UPLOAD (INFORMACION DE OPERACION ORIGINAL)

CAMPOS	ATRIBUTO	LONGITUD	DATOS	DESCRIPCION
TRANSACCION ORIGINAL	an..4	4	0200 / 0220	Tipo de mensaje original
NUMERO DE TRACE DEL SISTEMA ORIG.	an..6	6	000001..999999	Número de Trace de la operación original

CAMPO 63. del CIERRE (INFORMACION DE OPERACION ORIGINAL)

CAMPOS	ATRIBUTO	LONGITUD	DATOS	DESCRIPCION
NUMERO DE BATCH	an..3	3	001..999	Número del Batch
CONTADOR DE COMPRAS	an..4	4	0001..9999	Cantidad de Compras on/off Line Netas
MONTO DE COMPRAS	an..12	12	$$$$$$$$$$CC	Monto total de Compras Neto
CONTADOR DE DEV.	an..4	4	0001..9999	Cantidad de Devoluciones Netas
MONTO DE DEV.	an..12	12	$$$$$$$$$$CC	Monto de Devoluciones Neto
CONTADOR DE ANUL.	an..4	4	0001..9999	Cantidad de Anulaciones
MONTO DE ANULACIONES	an..12	12	$$$$$$$$$$CC	Monto de Anulaciones

ON-LINE (Echo Test)

				ECHO TEST	
		Formato	Atributo	REQ.	RTA.
	TPDU		n..10	X	X
	TIPO DE MENSAJE			0800	0810
	MAPA DE BIT		b64	X	X
2	NUMERO DE CUENTA / TARJETA	LLVAR	n..20		
3	CODIGO DE PROCESAMIENTO		n6	990000	990000
4	IMPORTE DE LA TRANSACCION		n12		
7	FECHA Y HORA DE TRANSMISION	MMDDHH MMSS	n10	X	
11	NUMERO DE TRACE DEL SISTEMA		n6		
12	HORA LOCAL DE LA TRANSACCION	HHMMSS	n6		X
13	FECHA LOCAL DE LA TRANSACCION	MMDD	n4		X
14	FECHA DE EXPIRACION	AAMM	n4		
15	FECHA DE CIERRE	MMDD	n4		
17	FECHA DE CAPTURA	MMDD	n4		
22	MODO DE INGRESO EN LA POS		n3		
24	IDENTIF INTERNACIONAL DE LA RED		n3	X	X
25	CODIGO DE CONDICION DE LA POS		n2		
35	DATOS DEL TRACK II	LLVAR	n..37		
37	RETRIEVAL REFERENCE NUMBER		an12		
38	CODIGO DE AUTORIZACION		an6		
39	CODIGO DE RESPUESTA		an2		
41	IDENTIFICACION DE LA TERMINAL		ans8	X	X
42	CODIGO DE IDENTIF.DEL COMERCIO		ans15		
48	CUOTAS / DATOS ORIGINALES	LLLVAR	ans..999		
49	CODIGO DE MONEDA		an3		
60	VERSION DE SOFT. DE APLICACION	LLLVAR	ans..999	O	
62	NUMERO DE TICKET	LLLVAR	ans..999		
63	INFORM.DE OPERACION ORIGINAL	LLLVAR	ans..999		
63	MENSAJE DEL HOST –MOSTRAR-IMPRIMIR	LLLVAR	ans..40		

El mensaje de ECHO TEST es utilizado para constatar que el vínculo de conexión esté activo y para verificar que el número de terminal con el cual se está operando esté habilitado en el sistema del Computador Central al cual se está comunicando.

Descripción de datos

TPDU (Transport protocol data unit)

Es la dirección de destino y origen para ruteo de mensajes. Este campo de 5 (cinco) bytes se divide de la siguiente forma.

- ID del mensaje	1 byte	Fijo '60'
- Dirección de destino (HOST)	2 bytes	Posnet '0003'
- Dirección de origen (Sistema)	2 bytes	Fijo '0000'

En la respuesta el Computador Central invierte los campos dirección de destino con dirección de origen. Algunos Emisores pueden obviar este campo.

CAMPO 02 y 35

Los campos que informan el número de tarjeta viajan en BCD. Al ser campos LLVAR, la longitud que antecede a los datos corresponde al número de tarjeta real (ingresado por teclado o leído de la banda) y no a la longitud de los datos comprimidos en BCD.

CAMPO 11

El número de trace del sistema es generado e incrementado por el sistema propio, el único mensaje que no incrementa el trace number es el reverso (mensaje 0400). El reverso mantiene el mismo número de trace que el último mensaje enviado (0200 ó 0220), el cual debe ser reversado (Debe incrementarse por teminal y no por sistema).

CAMPO 22

El modo de ingreso en el POS indica si el número de tarjeta fue leido de la banda magnética, a través del teclado del POS o fue un ingreso realizado por página Web.

Valores posibles	INGRESO MANUAL	012	
	LECTOR DE BANDA	022	Para terminales sin PinPad.
	E-COMMERCE	810	

CAMPO 24

El NII para Posnet producción será '003'.
El NII para Posnet homologaciones será '009'.

CAMPO 38

Si el código de autorización contiene menos de 6 caracteres se deberá completar con ceros a la izquierda.

CAMPO 48

El tipo de plan seleccionado se informa en el primer dígito del campo 48. El mismo puede ser un carácter alfanumérico, es decir del 0 al 9 o de la A a la Z.

Ejemplo en hexa campo 48.

0003 41 **30 34**	*0003* 31 **30 32**
long. Plan A 4 cuotas	long. Plan 1 2 cuotas

CAMPO 49

Los valores posibles del campo código de moneda son:

Pesos 032 / Dólares 840

CAMPO 60

En este campo se informará la empresa que ha desarrollado el sistema (2 dígitos), el mismo será asignado por el Administrador/Emisor.

CAMPO 63

En dicho campo se informa el Mensaje Promocional, si el mismo en informado en el bitmap. En este campo se envía el mensaje a visualizar/imprimir.
Para mayor información ver la sección:
"Capitulo H - Mensajes y Leyendas especiales en POS".

Mensajería por TCP

Tener en cuenta que al estar sobre una línea TCP delante del mensaje viajan dos bytes binarios que indican la cantidad de bytes que provienen del mensaje. Esto no forma parte de la capa de mensaje a nivel aplicación.
O sea, la estructura del mensaje debe ser levemente modificada, se trata del HEADER, éste debe de contener en los dos primeros byte´s del mensaje, la longitud del mensaje (en formato big-endian).

Formato de los Datos para transmisión

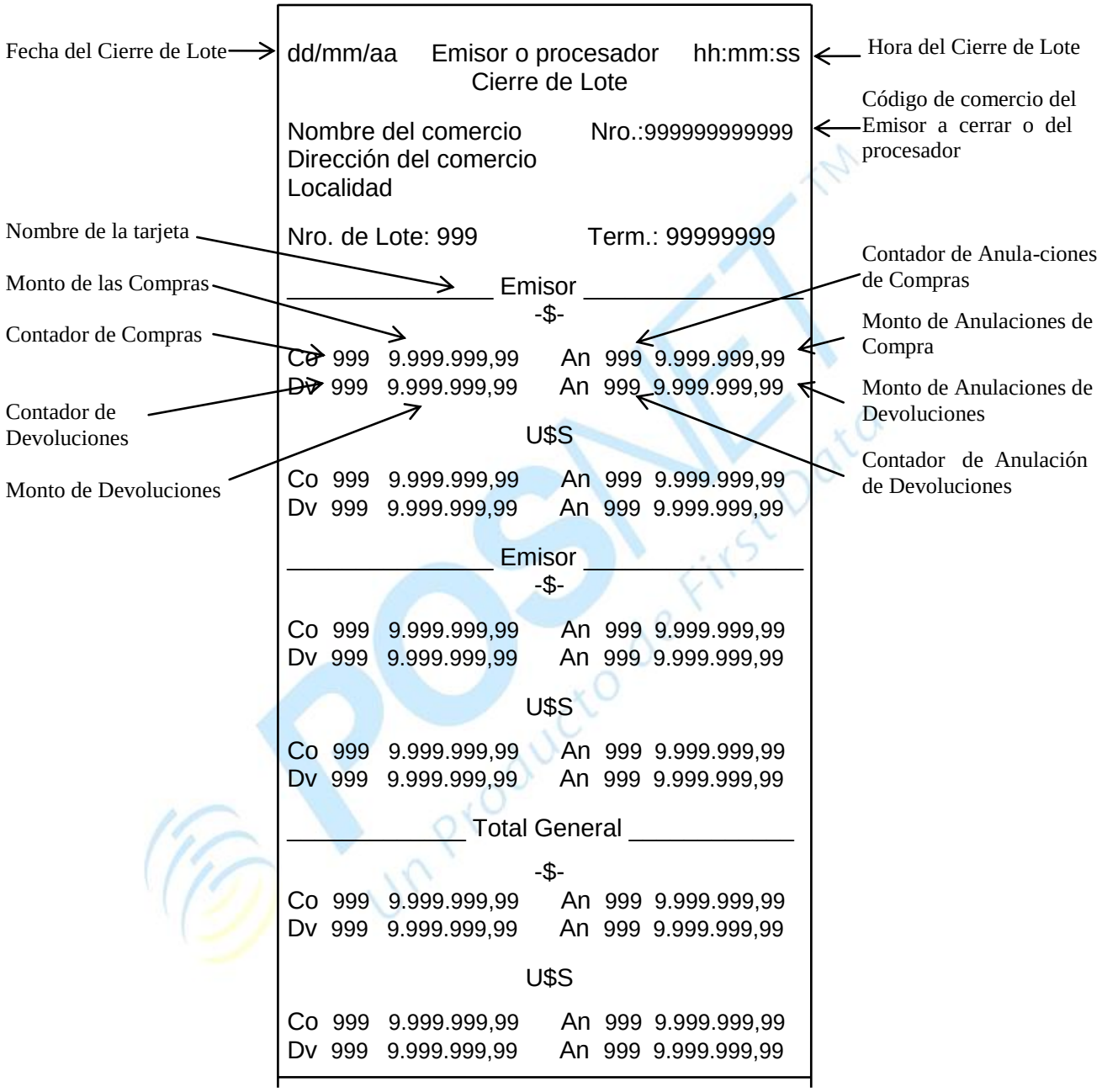
Los campos dentro de los mensajes se transmiten en BCD, excepto los campos 34, 37, 38, 39, 41, 42, 45, 46, 48, 49, 55, 59, 60, 62 y 63, los cuales se transmiten en ASCII, estos últimos son campos de longitud variable, los datos viajan en ASCII, pero la longitud que los precede viaja en BCD.

Códigos de respuesta ISO 8583

Cdgo	Descripción	Observaciones
00	APROBADA (authno)	Operación aprobada, emitir cupón (cargo o ticket).
01	PEDIR AUTORIZACION	Solicitar autorización telefónica, en caso de ser aprobada, cargar el código obtenido y dejar la operación en OFFLINE.
02	PEDIR AUTORIZACION	Idem punto anterior.
03	COMERCIO INVALIDO	Verificar parámetros del sistema, código de comercio mal cargado
04	CAPTURAR TARJETA	Denegada, capturar la tarjeta.
05	DENEGADA	Denegada.
07	RETENGA Y LLAME	Denegada, llamar al Centro de Autorizaciones.
11	APROBADA	Operación aprobada, emitir cupón (cargo o ticket).
12	TRANSAC. INVALIDA	Verificar el sistema, transacción no reconocida en el sistema.
13	MONTO INVALIDO	Verificar el sistema, error en el formato del campo importe.
14	TARJETA INVALIDA	Denegada, tarjeta no corresponde.
25	NO EXISTE ORIGINAL	Denegada, registro no encontrado en el archivo de transacciones.
30	ERROR EN FORMATO	Verificar el sistema, error en el formato del mensaje.
38	EXCEDE ING.DE PIN	Denegada, excede cantidad de reintentos de PIN permitidos.
43	RETENER TARJETA	Denegada, retener tarjeta.
45	NO OPERA EN CUOTAS	Denegada, tarjeta inhibida para operar en cuotas.
46	TARJETA NO VIGENTE	Denegada, tarjeta no está vigente aún.
47	PIN REQUERIDO	Denegada, tarjeta requiere ingreso de PIN.
48	EXCEDE MAX. CUOTAS	Denegada, excede cantidad máxima de cuotas permitida.
49	ERROR FECHA VENCIM.	Verificar el sistema, error en formato de fecha de expiración (vto)
50	ENTREGA SUPERA LIMIT	Denegada, el monto de ENTREGA ingresado está fuera de los límites permitidos.Verifique el monto ingresado.
51	FONDOS INSUFICIENTES	Denegada, no posee fondos suficientes.
53	CUENTA INEXISTENTE	Denegada, no existe cuenta asociada.
54	TARJETA VENCIDA	Denegada, tarjeta expirada.
55	PIN INCORRECTO	Denegada, código de identificación personal es incorrecto.
56	TARJ. NO HABILITADA	Denegada, emisor no habilitado en el sistema.
57	TRANS. NO PERMITIDA	Verificar el sistema, transacción no permitida a dicha tarjeta.
58	SERVICIO INVALIDO	Verificar el sistema, transacción no permitida a dicha terminal.
61	EXCEDE LIMITE	Denegada, excede límite remanente de la tarjeta.
65	EXCEDE LIM. TARJETA	Denegada, excede límite remanente de la tarjeta.
76	LLAMAR AL EMISOR	Solicitar autorización telefónica, en caso de ser aprobada, cargar el código obtenido y dejar la operación en OFFLINE.
77	ERROR PLAN/CUOTAS	Denegada, cantidad de cuotas inválida para el plan seleccionado.
85	APROBADA	Operación aprobada, emitir cupón (cargo o ticket).
89	TERMINAL INVALIDA	Denegada, número de terminal no habilitado por el Emisor.
91	EMISOR FUERA LINEA	Solicitar autorización telefónica, en caso de ser aprobada, cargar el código obtenido y dejar la operación en OFFLINE.
94	NRO. SEC. DUPLICAD	Denegada. Error en mensaje. Envíe nuevamente la transacción incrementando en uno el system trace de la misma.
95	RE-TRANSMITIENDO	Diferencias en la conciliación del cierre, envíe Batch Upload.
96	ERROR EN SISTEMA	Mal funcionamiento del sistema. Solicitar autorización telefónica.
xx	RECHAZADA (codnum)	Denegada, cualquier otro código no contemplado en tabla.

CAPITULO D - REPORTE DE CIERRE DE LOTE

Como ejemplo anexamos un ticket emitido al Cierre de Lote.



Nombre del Emisor Nombre de la tarjeta de la cual se realizó el Cierre, o del Host procesador contra el cual se realiza el Cierre de Lote.

Total General Es la suma de las Tarjetas que cierran contra un mismo procesador.

Este es sólo un ejemplo de información mínima a generar al realizar los Cierres de Lotes de las cajas.

CAPITULO E – DIGITO VERIFICADOR

Fórmula de cálculo de dígito verificador módulo 10 de tarjetas de crédito

La misma corresponde al módulo "10" de la Norma ISO 2894-2974 (E), cuyo algoritmo de cálculo es el siguiente:

Ejemplo:

Número de tarjeta completo: 5399 0456 7891 0517

a)

	5	3	9	9	0	4	5	6	7	8	9	1	0	5	1
x	2		2		2		2		2		2		2		2

b) 10 18 0 10 14 18 0 2

c) 10 + 3 + 18 + 9 + 0 + 4 + 10 + 6 + 14 + 8 + 18 + 1 + 0 + 5 + 2

d) 1 + 0+3 + 1+ 8 + 9 + 0 + 4 + 1+0 + 6 +1+4 + 8 + 1+8 + 1 + 0 + 5 + 2 = 63

e) 70 - 63 = 7 Dígito verificador es 7

1. Considerar los primeros dígitos del número de tarjeta contando de derecha a izquierda (fila a), habiendo eliminado el útimo dígito (verificador).
En forma alternada a partir del primer dígito de la derecha multiplicar por dos cada dígito. El producto obtenido figura en la fila b.

2. Considerar los valores de b. y aquellos valores que no fueron multiplicados por dos, respetando el orden del número de tarjeta (tal como figura en la fila c.)

3. Descomponer en dígitos individuales los valores de la fila c. mayores a 9.
De esta manera se obtiene la fila d. Sumar los dígitos de d.

4. Restar el valor obtenido en la fila d. (en el ejemplo "63") del número más próximo terminado en "0" mayor a dicho valor (múltiplo de 10) (en el ejemplo "70") para obtener el dígito verificador (e).
Si el total obtenido en la fila d. es un número terminado en cero (30, 40, etc.) el dígito verificador es cero.

CAPITULO F - DISPOSITIVOS

Especificaciones básicas del Hardware necesario

Generalidades

- ➔ Equipo Server de comunicaciones, el que recibirá los requerimientos de las terminales y actuará como manejador (Conversor, si es necesario / Switch) de las comunicaciones hacia el/los Host/s.
- ➔ Protocolo de comunicaciones X.25 o IP sobre Frame Relay
- ➔ Protocolo de datos ISO 8583
- ➔ Velocidad de transmisión: hasta 64 kbps
- ➔ Línea de comunicación Sincrónica

Lector de banda magnética

- ➔ Deberá leer Track I y Track II, deberá estar incluido en el dispositivo POS o P.C.
- ➔ El mismo deberá poseer seguridad para la transmisión de los datos de la lectura de la banda desde el lector al sistema.
- ➔ El mismo deberá como mínimo poseer una conexión vía un port serie al hardware al cual está conectado, no deberá ser una conexión Keyboard Wedge (emulador de teclado).

Dispositivo Pin Pad

- ➔ Deberá ser un dispositivo hardware Anti Tamper.
- ➔ Deberá cumplir con el estándar DES y 3 DES (según modalidad requerida).
- ➔ Deberá actuar como encriptor del Pin ingresado en el teclado del mismo, para luego enviar el PIN BLOCK generado al sistema.

CAPITULO G – ESTRUCTURA DE BANDA MAGNETICA

Estructura de la información contenida en la banda magnética

| TRACK 1 | TRACK 2 . |

% | b | PAN | ^ | NOMBRE | ^ | AAMM | S.C. | D. D. | ?| ; | PAN | = | AAMM | S.C. | D.D. |?|

Track I Longitud máxima de 77 (no incluye caracteres de comienzo, fin ni CRC)

%	:	Caracter de comienzo del track 1
b	:	Caracter de control
PAN	:	N° de la tarjeta de crédito / débito
^	:	Caracter de separación
NOMBRE	:	Nombre del usuario de la tarjeta de crédito/débito
AAMM	:	Fecha de vencimiento de la tarjeta de crédito/débito
S. C.	:	Service Code - Campo de 3 dígitos de verificación opcional ***Verificación obligatoria para CABAL***
D. D.	:	Datos discrecionales
?	:	caracter de fin de Track I

Track II Longitud máxima de 37 (no incluye caracteres de comienzo, fin ni CRC)

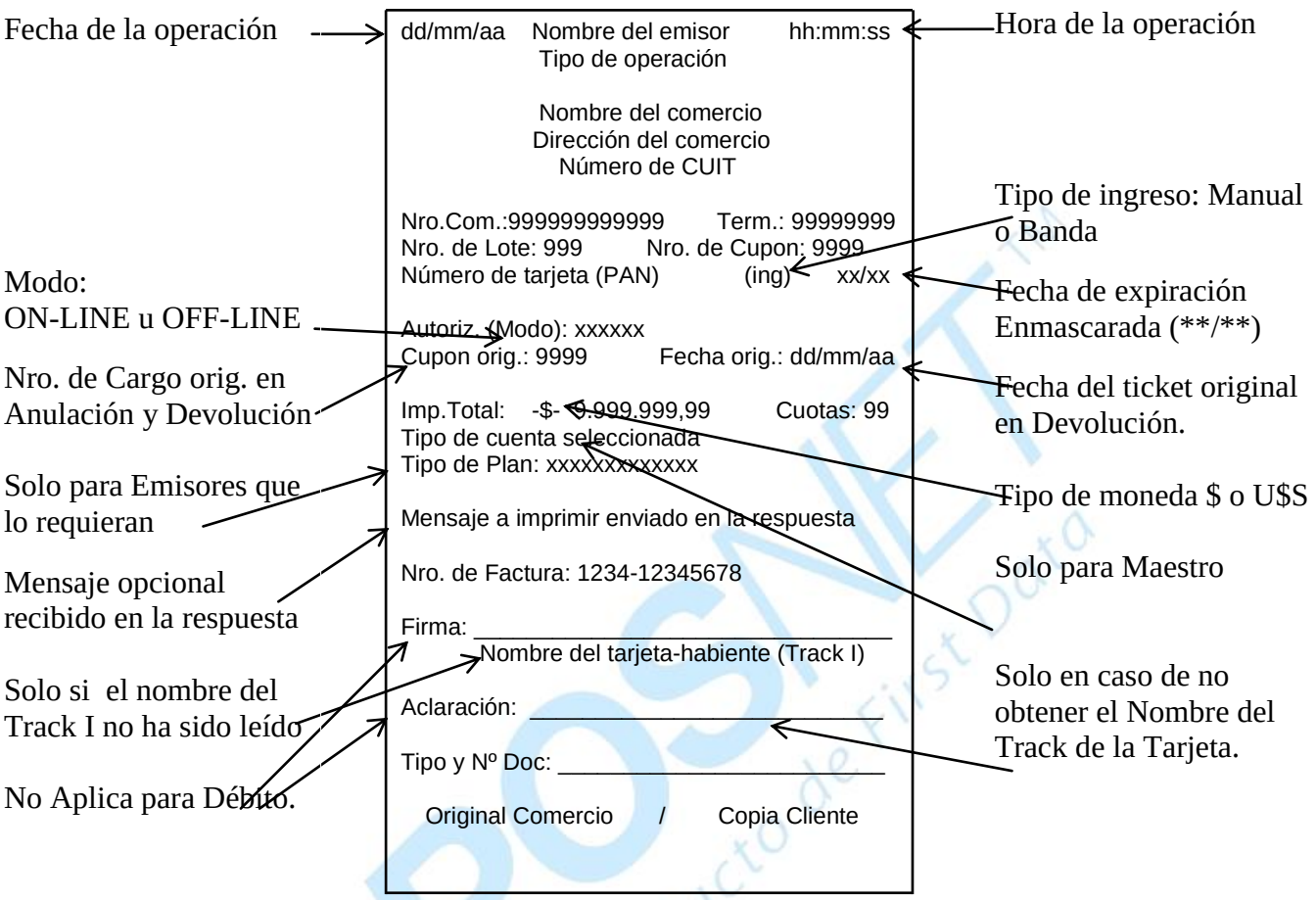
;	:	Caracter de comienzo del track 2
PAN	:	N° de la tarjeta de crédito / débito
=	:	Caracter de separación
AAMM	:	Fecha de vencimiento de la tarjeta de crédito/débito
S. C.	:	Service Code - Campo de 3 dígitos de verificación opcional ***Verificación obligatoria para CABAL***
D. D.	:	Datos discrecionales
?	:	Caracter de fin de track

Diseño de Track 2 de la banda magnética

NOMBRE DELCAMPO	START POSN	YNT FMT	INT LEN	EXT LEN	REP LEN	DEC POS	OCR COUNT	REPORT UPDATE	BLANK AFTER	DATE TIME	CUM FIEL	VALID ATION	ALIAS NAME
STSENT	1	C	1	1	1	0	1	R/U	YES				START SENTINEL C "5E"
ACCNUMB	2	C	16	16	16	0	1	R/U	YES				PRYMARIY ACCOUNT NUMBER
FLDSEP	18	C	1	1	1	0	1	R/U	YES				SAPARATOR C "7E"
EXPDATE	19	C	4	4	4	0	1	R/U	YES				EXPIRATION DATE (AAMM)
CARDTYPE	23	C	3	3	3	0	1	R/U	YES				CARD TYPE (101)
LMTCLASS	26	C	2	2	2	0	1	R/U	YES				CREDIT LIMIT CLASS
FILLER	28	C	10	10	10	0	1	R/U	YES				ZEROS
CONSTANT	38	C	1	1	1	0	1	R/U	YES				X "F8"
ENDSENT	39	C	1	1	1	0	1	R/U	YES				END SENTINEL X "6F"
LNGCHK	40	C	1	1	1	0	1	R/U	YES				LONGITUDINAL REDUNDANCY CHECK

Diseño de Tickets Maestro

(Es obligatorio cumplir con la información mostrada en el presente ejemplo)



Descripción de Campos

Nombre del Emisor	Nombre de la tarjeta con que se realiza la operación.
Tipo de operación	Operación realizada: COMPRA - ANULACION DE COMPRA DEVOLUCION - ANULACION DE DEVOLUCION.
Tipo de Tarjeta	DEBITO
Modo	Modo de operación: ON-LINE (por definición de producto).
(ing)	Es requerimiento que el tipo de ingreso de la tarjeta sea discriminado en el ticket. Ingreso manual no permitido.
Tipo de Cuenta	Cuenta seleccionada desde donde se debitará el importe de la operación al socio. Caja de Ahorros en pesos, Cuenta Corriente en pesos, Caja de Ahorros en dólares o Cuenta Corriente en dólares.

Diseño de registros para operaciones

Especificaciones

DESCRIP. DE FORMATOS Y ATRIBUTOS		NOTAS

b	Binario		**X**	Campo transmitido obligatorio.
n	Dígitos numéricos		**O**	Campo Opcional
Ns	Caracteres numéricos y especiales			
an	Caracteres alfanuméricos		**C1**	Campo mandatorio si el ingreso del número de la tarjeta fue manual.
ans	Caracteres alfanuméricos y especiales		**C2**	Campo mandatorio si el ingreso del número de la tarjeta fue por banda.
AAMMDD	Año, mes y día		**C3**	Campo que si viene informado en la respuesta es la ueva Clave de Trabajo (Working Key)
HHMMSS	Hora, minutos y segundos		**C4**	Campo donde se devuelve informado siempre el número de tarjeta.
VAR	Campo de longitud variable		**C5**	Campo donde se devuelve informado el monto del Saldo.
LL,LLL	Longitud del campo variable		**C6**	Campo mandatorio si fue especificada en transacción original.
..37 **3**	Campo de longitud variable de hasta 37 caracteres Campo de longitud fija de 3 caracteres		**C7**	Código de procesamiento de la operación original NNNNNX. X=0 último mensaje X=1 hay más mensajes
T	Dentro del código de procesamiento se indica la cuenta seleccionada por el tarjeta-habiente Tipo de cuenta seleccionada : 1 - Caja de Ahorros $ 2 - Cuenta Corriente $ 8 - Caja de Ahorros U$S 9 - Cuenta Corriente U$S		**C9**	Si el ingreso del número de tarjeta se realiza por lectura de banda, y la lectura solo arroja el Track II y no el Track I, entonces en este campo se debe enviar el valor "1". Si el Track I es leído correctamente, este campo no debe ser enviado.

ON-LINE (Compra, Anulación)

				COMPRA		ANUALCION	
		Formato	Atributo	REQ.	RTA.	REQ.	RTA.
	TPDU		n..10	X	X	X	X
	TIPO DE MENSAJE			0200	0210	0200	0210
	MAPA DE BIT		b64	X	X	X	X
2	NUMERO DE CUENTA / TARJETA	LLVAR	n..20	C1	C4 (O)	C1	C4 (O)
3	CODIGO DE PROCESAMIENTO		n6	00T000	00T000	02T000 22T000	02T000 22T000
4	IMPORTE DE LA TRANSACCION		n12	X	O	X	O
7	FECHA Y HORA DE TRANSMISION	MMDDHH MMSS	n10	X	X	O	O
11	NUMERO DE TRACE DEL SISTEMA		n6	X	X	X	X
12	HORA LOCAL DE LA TRANSACCION	HHMMSS	n6	X		X	
13	FECHA LOCAL DE LA TRANSACCION	MMDD	n4	X		X	
14	FECHA DE EXPIRACION	AAMM	n4	C1		C1	
22	MODO DE INGRESO EN LA POS		n3	X		X	
24	IDENTIF INTERNACIONAL DE LA RED		n3	X	X	X	X
25	CODIGO DE CONDICION DE LA POS		n2	00		00	
34	NUMERO DE CUENTA	LLVAR	ans..28		O		O
35	DATOS DEL TRACK II	LLVAR	n..37	C2		C2	
37	RETRIEVAL REFERENCE NUMBER		an12		X	X	X
38	CODIGO DE AUTORIZACION		an6		O		O
39	CODIGO DE RESPUESTA		an2		X		X
41	IDENTIFICACION DE LA TERMINAL		ans8	X	X	X	X
42	CODIGO DE IDENTIF.DEL COMERCIO		ans15	X	O	X	O
45	DATOS DEL TRACK I	LLVAR	n..76	C6		C6	
46	TRACK I NO LEIDO	LLLVAR	ans..999	C6		C6	
48	CUOTAS / DATOS ORIGINALES	LLLVAR	ans..999	X	O	X	O
49	CODIGO DE MONEDA		an3	X	O	X	O
52	PIN / WORKING KEY		b64	X	C3	X	C3
59	INFORMACION ADICIONAL	LLLVAR	ans..999	X		X	
60	VERSION DE SOFT. DE APLICACION	LLLVAR	ans..999	X		X	
62	NUMERO DE TICKET	LLLVAR	ans..999	X		X	

Descripción de Campos Especiales

CAMPO 48. (CUOTAS / DATOS ORIGINALES)

CAMPOS	ATRIBUTO	LONGITUD	TRANSACCION		DESCRIPCION
PAGOS Plan Cuotas	an..1 an..2	1 2	TODAS	0..9 00..99	Plan (siempre 0) Cuotas (siempre 01)
TICKET ORIGINAL	an..4	4	DEVOLUCION	0001..9999	Número de ticket Original
FECHA ORIGINAL	an..6	6	DEVOLUCION	DDMMAA	Fecha de la transacción original

Para operaciones de compra y anulación con Maestro actualmente no se utilizan los datos de Plan y Cuotas, fijo en 001.

CAMPO 59. (INFORMACION ADICIONAL / PREPARADO PARA NUMERO DE CUENTA)

CAMPOS	ATRIBUTO	LONGITUD	TRANSACCION		DESCRIPCION
Tipo de Producto	an..3	3	TODAS	002	Indica el tipo de producto que se informará
Cantidad de SubCampos	an..4	4	TODAS	0001	Indica la cantidad de SubCampos que posee el producto.
Longitud de SubCampo	an..3	3	TODAS	001	Informa la longitud que tendrá el SubCampo.
ID del SubCampo	an..3	3	TODAS	009	Informa el Nombre del SubCampo.
Valor del SubCampo	an..1	1	TODAS	1	Significa "Preparado para recibir ISO 34"

ON-LINE (Devolución)

				DEVOLUCION	
		Formato	Atributo	REQ.	RTA.
	TPDU		n..10	X	X
	TIPO DE MENSAJE			0200	0210
	MAPA DE BIT		b64	X	X
2	NUMERO DE CUENTA/ TARJETA	LLVAR	n..20	C1	C4 (O)
3	CODIGO DE PROCESAMIENTO		n6	20T000	20T000
4	IMPORTE DE LA TRANSACCION		n12	X	O
7	FECHA Y HORA DE TRANSMISION	MMDDHHMMSS	n10	X	O
11	NUMERO DE TRACE DEL SISTEMA		n6	X	X
12	HORA LOCAL DE LA TRANSACCION	HHMMSS	n6	X	
13	FECHA LOCAL DE LA TRANSACCION	MMDD	n4	X	
14	FECHA DE EXPIRACION	AAMM	n4	C1	
22	MODO DE INGRESO EN LA POS		n3	X	
24	IDENTIF INTERNACIONAL DE LA RED		n3	X	X
25	CODIGO DE CONDICION DE LA POS		n2	00	
34	NUMERO DE CUENTA	LLVAR	ans..28		O
35	DATOS DEL TRACK II	LLVAR	n..37	C2	
37	RETRIEVAL REFERENCE NUMBER		an12		X
38	CODIGO DE AUTORIZACION		an6		O
39	CODIGO DE RESPUESTA		an2		X
41	IDENTIFICACION DE LA TERMINAL		ans8	X	X
42	CODIGO DE IDENTIF.DEL COMERCIO		ans15	X	O
45	DATOS DEL TRACK I	LLVAR	n..76	C6	
46	TRACK I NO LEIDO	LLLVAR	ans..999	C6	
48	CUOTAS / DATOS ORIGINALES	LLLVAR	ans..999	X	O
49	CODIGO DE MONEDA		an3	X	O
52	PIN / WORKING KEY		b64	X	C3
59	INFORMACION ADICIONAL	LLLVAR	ans..999	X	
60	VERSION DE SOFT. DE APLICACION	LLLVAR	ans..999	X	
62	NUMERO DE TICKET	LLLVAR	ans..999	X	

Especificación de campos

CAMPO 22

El modo de ingreso en el POS indica si el número de tarjeta fue leído de la banda magnética o a través del teclado del POS para operaciones de débito en terminales que poseen conectado un PIN PAD.

Valores posibles INGRESO MANUAL011
LECTOR DE BANDA 021

CAMPO 48 (Cuotas / Datos originales)

Idem página compra y anulación.

CAMPO 52

En los mensajes de requerimiento en este campo se informa la clave encriptada.
En los mensajes de respuesta se informa la nueva clave de trabajo (working key). Puede ser informada en los mensajes de respuesta 0110, 0210 o 0510.

CAMPO 59 (INFORMACION ADICIONAL / PREPARADO PARA NUMERO DE CUENTA)

CAMPOS	ATRIBUTO	LONGITUD	TRANSACCION		DESCRIPCION
Tipo de Producto	an..3	3	TODAS	002	Indica el tipo de producto que se informará
Cantidad de SubCampos	an..4	4	TODAS	0001	Indica la cantidad de SubCampos que posee el producto.
Longitud de SubCampo	an..3	3	TODAS	001	Informa la longitud que tendrá el SubCampo.
ID del SubCampo	an..3	3	TODAS	009	Informa el Nombre del SubCampo.
Valor del SubCampo	an..1	1	TODAS	1	Significa "Preparado para recibir ISO 34"

ON-LINE (Batch UpLoad, Reversos)

				BATCH UPLOAD		REVERSO	
		Formato	Atributo	REQ.	RTA.	REQ.	RTA.
	TPDU		n..10	X	X	X	X
	TIPO DE MENSAJE			0320	0330	0400	0410
	MAPA DE BIT		b64	X	X	X	X
2	NUMERO DE CUENTA / TARJETA	LLVAR	n..20	C6	C4 (O)	C6	C4 (O)
3	CODIGO DE PROCESAMIENTO		n6	C7	C7	C6	C6
4	IMPORTE DE LA TRANSACCION		n12	X	O	X	O
7	FECHA Y HORA DE TRANSMISION	MMDDHH MMSS	n10	X	O	X	O
11	NUMERO DE TRACE DEL SISTEMA		n6	X	X	X	X
12	HORA LOCAL DE LA TRANSACCION	HHMMSS	n6	X		X	
13	FECHA LOCAL DE LA TRANSACCION	MMDD	n4	X		X	
14	FECHA DE EXPIRACION	AAMM	n4	C6		C6	
15	FECHA DE CIERRE	MMDD	n4				
17	FECHA DE CAPTURA	MMDD	n4	X			
22	MODO DE INGRESO EN LA POS		n3	X		X	
24	IDENTIF INTERNACIONAL DE LA RED		n3	X	X	X	X
25	CODIGO DE CONDICION DE LA POS		n2	00		00	
34	NUMERO DE CUENTA	LLVAR	ans.. 28		O		O
35	DATOS DEL TRACK II	LLVAR	n..37	C6		C6	
37	RETRIEVAL REFERENCE NUMBER		an12	X	X	C6	X
38	CODIGO DE AUTORIZACION		an6	X	O	C6	O
39	CODIGO DE RESPUESTA		an2		X		X
41	IDENTIFICACION DE LA TERMINAL		ans8	X	X	X	X
42	CODIGO DE IDENTIF.DEL COMERCIO		ans15	X	O	X	O
48	CUOTAS / DATOS ORIGINALES	LLLVAR	ans..999	X	O	X	O
49	CODIGO DE MONEDA		an3	X	O	X	O
52	PIN/WORKING KEY		b64				
59	INFORMACION ADICIONAL	LLLVAR	ans..999	X	X	X	
60	VERSION DE SOFT. DE APLICACION	LLLVAR	ans..999	X		X	
62	NUMERO DE TICKET	LLLVAR	ans..999	X		X	
63	INFORM.DE OPERACION ORIGINAL	LLLVAR	ans..999	X			

El mensaje de Cierre de Lote (0500) es el mismo que para tarjetas de Crédito, se suman los totales de Crédito y los de Débito en los Cierres, tanto las Compras, las Anulaciones y las Devoluciones.

En los mensajes de respuesta 0510 puede ser enviada una nueva Working Key.

CAPITULO H – MENSAJES Y LEYENDAS ESPECIALES EN POS

CAMPO 63

Los mensajes promocionales se dividen en dos grupos, 40 Caracteres y 200 caracteres.
Para ambos, el emisor puede enviar mensajes a la tarjeta habiente, al comercio o bien a ambos.
Las distintas opciones que pueden darse son:

40 Caracteres:

- Está formateado como para mostrar dos líneas en un display de 2 x 18 o 20 caracteres.
- Si el primer carácter es un punto decimal ".", el texto se debe imprimir en el ticket de la operación y se debe mostrar en el visor de la terminal
- Si el mensaje no tiene ningún carácter especial se debe mostrar solo por visor.
- El mensaje se debe mostrar en cualquier tipo de transacción (tanto aprobada como rechazada) antes de mostrar la respuesta del Host.
- Diners envía este campo de 36 caracteres.

200 Caracteres:

- Si el primer carácter es una coma ",", el texto se debe imprimir únicamente en el ticket de la operación (independientemente si fue aprobada o rechazada, salvo código de rechazo 98)

- Si el primer carácter es un punto y coma ";", el texto se debe imprimir únicamente en el ticket del comercio (independientemente si fue aprobada o rechazada, salvo código de rechazo 98).

- Si el primer carácter son dos puntos ":", el texto se debe imprimir únicamente en el ticket del cliente (independientemente si fue aprobada o rechazada, salvo código de rechazo 98).

✓ Si el código de respuesta es 98, el mensaje recibido informa el error / rechazo del requerimiento.
✓ Se indica el salto de renglón con el carácter "|" (alt + 124).
✓ Se indica el final de texto con el carácter especial "^" (alt + 94).
✓ Si este campo no se informa la terminal muestra el mensaje asociado al código de respuesta (campo 39).

En caso de necesitar soporte técnico para la correcta interpretación de este documento, o bien para efectuar pruebas de los sistemas, contactarse con: implementaciones@posnet.com.ar

CAPITULO J - SEGURIDAD

1. Políticas y estándares de seguridad informática, y procedimientos administración de seguridad		
BEST PRACTICE	**PROCEDIMIENTO**	**REQUERIMIENTOS**
1.1 Políticas de seguridad informática		
• Existen políticas de seguridad informática que sustentan la operatoria de "Sistemas Propios", incluyendo, como mínimo: - Niveles de confidencialidad de los datos, tanto de la empresa como de los clientes. - Integridad de los datos. - Control de acceso físico y lógico. - Acciones a emprender ante violaciones a las políticas / normas. - Utilización de recursos informáticos (por ejemplo módems, correo electrónico etc.) - Las políticas se encuentran actualizadas y aprobadas por la Gerencia y son conocidas por quienes corresponde.	✓ Verificación de la existencia de políticas de seguridad informática. ✓ Revisión de las políticas existentes, sus fechas de actualización y su aprobación de la Gerencia. ✓ Verificación del conocimiento de dichas políticas por parte del personal relacionado con la operación/administración de la aplicación de "Sistemas Propios". ✓ Verificar que el personal que administra los sistemas operativos, bases de datos, software de pago y dispositivos de comunicación relacionados con el entorno de "Sistemas Propios", ha firmado algún compromiso de confidencialidad o las políticas de seguridad relacionadas con la información sensible.	• Políticas de seguridad informática existentes. • Políticas referidas al acceso, almacenamiento, y utilización de los datos de los clientes y de los medios de pago utilizados.
1.2 Estándares de configuración de seguridad lógica		
• Existen estándares que determinan los aspectos principales de configuración de los componentes del esquema de seguridad lógica de "Sistema Propios", incluyendo: - Configuración de seguridad de el/los sistemas operativos - Configuración de seguridad en el Software de pago - Configuración de seguridad en la base de datos que almacenará los datos críticos del tarjetahabiente. - Configuración de los dispositivos de comunicaciones	✓ Verificación de la existencia de estándares de seguridad lógica. ✓ Revisión de los estándares existentes, sus fechas de actualización y su aprobación de la Gerencia.	• Estándares de configuración de seguridad lógica (Ej. identificación, autenticación, registros de eventos, permisos, accesos restringidos, etc.) de los siguientes elementos: - Controladores de dominio. - Sistemas operativos - Base de datos - Software de pago - Dispositivos de Comunicaciones.

- Los estándares se encuentran actualizados y aprobados por la Gerencia y son conocidos por quienes deben aplicarlos.		
1.3 Procedimientos de administración de seguridad lógica		
• Existen procedimientos escritos para la ejecución de las actividades relacionadas con la administración de seguridad lógica, que definen claramente los responsables de su ejecución y control, incluyendo: - Administración de usuarios y claves en el sistema operativo, base de datos, dispositivos de comunicación y el software de pago - Procedimiento y documentación para mantener la configuración de los dispositivos de comunicación. - Forma de administración de dispositivos de comunicación. - Administración/revisión de logs de auditoría en servidores y dispositivos de comunicación. - Procedimientos de prueba e implementación de cambios/nuevas versiones/fixes del software de base (Ejemplos: Sistema operativo, base de datos, adm. del dispositivo de comunicación y el software de pago). - Procedimiento de backup/ restore. • Los procedimientos se encuentran actualizados y aprobados por la Gerencia y son conocidos por quienes deben ejecutarlos.	✓ Verificación de la existencia de procedimientos de administración de seguridad lógica ✓ Revisión de los procedimientos existentes, sus fechas de actualización y aprobación de la Gerencia. ✓ Verificar el cumplimiento de los procedimientos, mediante el seguimiento de los siguientes procesos: - Último cambio de la clave del usuario de máximo privilegio (root, supervisor o administrador) en los servers, en los filtros de red y en la base de datos. - Configuración de los dispositivos de comunicación - Instalación de la última versión en los sistemas operativos.	• Procedimientos de administración de seguridad existentes.
1.4 Administración de la seguridad		
• Debe existir una adecuada segregación de funciones sobre la administración técnica de los sistemas críticos y la seguridad informática.	✓ Verificar la existencia de un responsable por la definición y seguimiento de la seguridad. ✓ Verificar la existencia de una adecuada segregación de funciones sobre la administración técnica de los sistemas críticos (Sistema operativo, base de datos, adm. de dispositivos de	• Descripción de la misión y función del personal responsable por la definición y seguimiento de la seguridad

	comunicación y el software de pago) y la seguridad informática.	
1.5 Auditoría interna y/o externa		
• El entorno informático de la aplicación de "Sistemas Propios" es auditado periódicamente a fin de detectar debilidades de seguridad y mejorar procedimientos de administración.	✓ Chequeo de la existencia de auditoría interna y/o externa. ✓ Análisis de periodicidad de las revisiones y alcance de las mismas.	• Informes de auditoría y/o revisiones de seguridad, por ejemplo, diagnósticos de seguridad, penetration testing, etc., emitidos por organizaciones independientes de los últimos 3 años.

2. Seguridad física de la plataforma		
BEST PRACTICE	**PROCEDIMIENTO**	**REQUERIMIENTOS**
2.1 Control de acceso		
• El centro de cómputos o sector de equipos donde se encuentra instalado el hardware relacionado con la aplicación de venta (incluyendo servers, database servers, dispositivos de comunicación, terminales de captura, etc.), todos relacionados con el Sistema Propio, debe contar con un mecanismo de control de acceso que lo permite sólo a personal autorizado. • Se debe llevar un registro de los ingresos/egresos de personal a dicho sector.	✓ Chequeo de puntos de acceso y comunicación con el exterior (ventanas, pasillos, salidas de emergencia, etc.). ✓ Revisión del método de ingreso al centro de cómputos o sector de equipos, en condiciones normales y por excepción. ✓ Chequeo de los mecanismos de control de acceso, tales como tarjetas magnéticas, cerraduras con clave, etc. ✓ Verificar el cumplimiento del procedimiento de control de acceso, mediante los registros de ingresos/egresos (sistema de control, reportes de circulación de personal) y su autorización respectiva.	• Visita al Centro de Cómputos o Sector de Equipos. • Procedimientos de Control de acceso al centro de cómputos o Sector de Equipos.

3. Seguridad lógica de la plataforma

BEST PRACTICE	PROCEDIMIENTO	REQUERIMIENTOS
3.1 Identificación de usuarios		
• Los usuarios genéricos, tienen un propósito definido (por ejemplo, transferencia de archivos), presentan una justificación técnica u operativa, y se encuentra documentado la lista del personal que utilizan estos usuarios. • Sólo poseen user-id para acceder a los servers y aplicativos las personas correspondientes, en función de sus tareas. • El usuario *guest* (invitado) o a *anónimo* (anonymous) no se encuentra habilitado para ingresar en la red • Existen reglas para la asignación de nombres de usuario. • Existen perfiles definidos para los distintos puestos funcionales de los usuarios (ej. Cajeros; supervisores; etc.)	✓ Chequeo de la asignación y distribución de usuarios. ✓ Análisis de razonabilidad de los usuarios definidos en los equipos críticos, en función del cargo, sector y tareas de la persona responsable respectiva. ✓ Revisión de los usuarios genéricos y los usuarios que por defecto vienen instalados en los sistemas operativos y dispositivos de comunicación. ✓ Revisión de los distintos perfiles de sistemas existentes.	• Lista de user-id, nombre del usuario responsable, descripción, grupo, ¿es de máximo privilegio o user administrador?, ¿Es user personalizado o genérico? Estado del usuario (activo o bloqueado) y último acceso; en cada server, aplicación y dispositivo de comunicación relacionado con el entorno de "Sistemas Propios". • Lista de grupos, descripción o perfil e indicar si es un grupo administrador (Ejemplo: adm de usuarios, backup, adm. de impresión, etc.); en cada server, aplicación y dispositivo de comunicación relacionado con el entorno de "Sistemas Propios". • Detalle del cargo, sector y breve descripción de tareas de cada persona responsable de una cuenta indicada en el requerimiento anterior.
3.2 Autenticación de usuarios		
• Todos los usuarios acceden a los equipos mediante un user-id y password otorgada por los Administradores de seguridad. • La definición de parámetros de seguridad de las passwords (longitud mínima y máxima, período de rotación, etc.) es adecuada. • Los usuarios son bloqueados ante reiterados intentos fallidos de acceso. • Los usuarios se autentican en los equipos críticos y en forma remota, para actividades de administración, mediante herramientas que permiten establecer una conexión robusta en seguridad (Ej. VPN, SSH, etc.).	✓ Verificación de los parámetros de autenticación y autorización. - Longitud mínima/máxima - Duración mínima/máxima - Password history - Bloqueo de cuentas ✓ Verificación de la restricción de acceso sobre los archivos o bases o tablas, que almacenan los usuarios y claves. ✓ Verificación de que las claves se resguardan de manera encriptada.	Requerimientos (a modo de ejemplo) sobre las plataformas Windows NT y UNIX : • Servidores Windows NT – *Account Policies* de los servidores pertenecientes al dominio correspondiente a la aplicación de comercio. • Servidores UNIX Archivos: – /etc/passwd – /etc/shadow – /etc/group – /etc/inetd.cfg

	✓ Chequeo de los servicios, procesos daemon o procesos background habilitados ✓ Verificar que no se encuentren configurados ni activos los servicios FTP, Telnet y R* (rcp, rsh, rlogin) ✓ Verificar la existencia de herramientas "seguras" para acceder en forma remota a los equipos: Dispositivo de comunicación, adm. server, sistemas operativos, server del software de pago y la base de datos; para actividades de administración.	– /etc/hosts.equiv – rhosts del home de algunos usuarios • Bases de Datos Parámetros de autenticación y autorización en cada manejador de bases de datos de clientes • Accesos remotos Lista de herramientas utilizadas para acceder remotamente a los equipos críticos para fines de administración técnica.
3.3 Usuarios sensitivos		
• La cantidad de usuarios con un perfil *alto* de seguridad es reducida y se mantiene una adecuada separación de funciones. • Existen procedimientos de control estrictos sobre la actividad de estos usuarios.	✓ Revisión de usuarios y grupos Administradores (la lista de usuarios y grupos se obtienen del punto 3.1). ✓ Verificar la existencia de registros de actividad y controles aplicados sobre el último acceso de los usuarios de máximo privilegio en los servers críticos: sistemas operativos, dispositivos de comunicación, application servers – incluye al software de pago y database servers.	• Procedimiento de control de la actividad de los usuarios administradores.
3.4 Permisos de acceso a archivos/tablas sensibles		
• El acceso a los archivos/tablas que contienen información sensitiva (por ejemplo, datos financieros de los clientes, datos de la tarjeta de un tarjetahabiente, etc.), se encuentra restringido a personal autorizado. • El acceso a los programas y datos relacionados con el software de pago, se encuentra restringido a personal autorizado. • El acceso a las claves privadas (relacionados con el certificado del Comercio), se encuentra restringido a personal autorizado. • Utilización de los niveles de	✓ Verificación de los usuarios con acceso (read, write, execute, query, report, update, add, delete, etc.) a los archivos/tablas en los que residen datos sensitivos de clientes del entorno "Sistemas Propios" . ✓ Verificación de los usuarios con acceso al software de pago ✓ Verificación de los usuarios con acceso a las claves privadas de los dispositivos de comunicación relacionados con la operatoria de "Sistemas Propios".	• Detalle de tablas de la base de datos y/o archivos de datos en los que se almacena información sensitiva de los clientes (datos que se incluyen en una tarjeta de crédito). • Detalle de usuarios con acceso a estos archivos/tablas y tipos de acceso permitidos • Detalle de usuarios con acceso al software de pago y tipos de acceso permitidos. • Detalle de usuarios con acceso a las claves privadas de los dispositivos de comunicación.

seguridad que ofrece el sistema operativo, por ejemplo, particiones NTFS en Windows NT.	Revisión de las estructuras lógicas (tipo de file systems, permisos de los directorios, permisos sobre las tablas, etc.) que soportan los datos sensibles, en cada caso.	
	3.5 Registros de auditoría	
• La auditoría de eventos de seguridad se encuentra habilitada en todos los sistemas. • Los logs de auditoría, ya sea impresos o en medios magnéticos, se conservan adecuadamente.	✓ Revisión de los eventos de seguridad registrados en los servidores y equipos pertenecientes al entorno "Sistemas Propios" (sistemas operativos, dispositivos de comunicación, software de pago, bases de datos y filtros de red). ✓ Parametrización de las opciones de auditoría de los objetos críticos, definidos en el punto 3.4. ✓ Verificar la registración de logs y el monitoreo de los eventos de seguridad sobre los componentes informáticos, considerados en el punto 3.4.	• Eventos de seguridad que se registran en los servidores y equipos pertenecientes al entorno "Sistemas Propios" (sistemas operativos, dispositivos de comunicación, software de pago, bases de datos y filtros de red). Requerimientos (a modo de ejemplo) sobre las plataformas Windows NT y UNIX : • Windows NT: – Audit policies del dominio. • UNIX: – Archivo /user/adm/lastlog de servidores UNIX – Registros del *sulog* – .sh_history de cada $HOME_DIRECTORY – Sistema Aplicativo: Log de accesos, eliminación de archivos/ Bases de datos, ABM de los parámetros de configuración. • Detalle de los eventos de auditoría activados para los objetos críticos definidos en el punto 3.4. • Lista de eventos que registra el Sistema Aplicativo • Procedimiento de mantenimiento y monitoreo de los logs generados.
	3.6 Actualización del software de base	
• El software de base se encuentra actualizado con las últimas versiones de patches, fixes, correcciones, etc. • Existen procedimientos de pruebas de las nuevas versiones de software de base instaladas.	✓ Chequeo de la versión, *Service Pack* o hot fix instalada. ✓ En el caso de Windows NT, verificación de la instalación de los fixes liberados con posterioridad al último service pack implementado. ✓ Evaluar el grado de cumplimiento del	• Detalle de la última versión, service packs o hot fix, implementado en los principales servers correspondientes al entorno "Sistemas Propios" (sistemas operativos, application servers – incluye al software de pago, database servers y filtros de red). • Documentación de los *hotfixes*

	Procedimiento de pasajes a producción, sobre la última actualización del sistema operativo que soporta al software de pago, base de datos y filtros de red.	implementados desde la aplicación del último service pack.
3.7 Prevención y detección de virus, troyanos u otro código malicioso		
• Los equipos cuentan con productos antivirus actualizados para prevenir y detectar virus. • El entorno de sistemas del comercio que procesa los software aplicativos, cuenta con productos actualizados para prevenir y detectar troyanos, backdoors y otros códigos maliciosos de uso frecuente.	✓ Chequeo de productos antivirus, detector de troyanos, detector de backdoors u otro código malicioso instalado.	• Detalle de los productos antivirus, detector de troyanos, detector de backdoors u otro código malicioso, instalado en los servidores correspondientes a la aplicación de "Sistemas Propios". • Procedimiento, responsables y métodos de actualización de los productos indicados. • Procedimiento ante la detección de un virus, troyano u otro código malicioso.
3.8 Software instalado en los equipos		
• Los equipos que soportan la aplicación de "Sistemas Propios" se utilizan específicamente para este fin, y no se comparte su uso con otras aplicaciones. • El software de base que se ejecuta en los equipos es el mínimo y necesario requerido por la aplicación de "Sistemas Propios". • No se dispone en los equipos dedicados a las aplicaciones del comercio de herramientas tales como, compiladores, linkeadores, software de comunicaciones, etc.	✓ Revisión del software instalado en los servidores y equipos pertenecientes al entorno "Sistemas Propios" (sistemas operativos, dispositivos de comunicación, software de pago, bases de datos y filtros de red). ✓ Análisis de razonabilidad y necesidad del software identificado. ✓ Selección de una muestra de software de base.	• Detalle del software instalado en los servidores y equipos pertenecientes al entorno "Sistemas Propios" (sistemas operativos, dispositivos de comunicación, software de pago, bases de datos y filtros de red).

3.9 Back-ups

• Las copias de resguardo de la información crítica (Ver 5.1) se efectúan diariamente y se conservan en lugares seguros y con acceso restringido por un período máximo de 60 días. • Los datos de los clientes tarjetahabientes considerados confidenciales (ver 5.1), se deben resguardar de manera encriptada. • Se utiliza Dual Control para administrar claves de encripción. • Para proteger las claves de encripción y soportar las funciones de encripción y desencripción, se utiliza un dispositivo hardware de seguridad, con tamper-resistant. • La eliminación o destrucción de los datos, medios de backups y componentes informáticos, que contienen información confidencial de los tarjetahabientes, se efectúan bajo adecuados controles.	✓ Revisión física de los lugares de conservación de las copias de resguardo. ✓ Verificar que los datos confidenciales se resguardan con **herramientas estándares de encriptación.** Son considerados estándares de encriptación a la fecha, los siguientes productos: – RSA con claves de 1024 bits o más – 3DES con claves de 112 o 168 bits – RC2 / RC4 con claves de 128 bits – IDEA con claves de 128 bits – Rijndael con claves de 128 o 256 bits.) ✓ Verificar los controles y niveles de restricción, sobre la administración de una clave de encriptación. ✓ Verificar la existencia de documentación de control relacionado con la actividad de eliminación o destrucción de datos del tarjetahabiente. ✓ Verificar que los backups que contienen datos críticos, se resguardan por un período máximo de 60 días.	• Procedimiento de Backups/ Restore • Acceso físico al sector donde se conservan las copias de resguardo. • Detalle del personal con acceso a las copias de resguardo. • Procedimientos de control para la eliminación de datos, medios de backups y componentes informáticos, que contienen información confidencial de los tarjetahabientes.

4. Seguridad lógica de la red y del filtro de red

BEST PRACTICE	PROCEDIMIENTO	REQUERIMIENTOS
4.1 Existencia de un dispositivo de filtro de red		
• El comercio posee un dispositivo que actúa como filtro que protege a la red interna de los accesos provenientes de redes externas y autoriza determinados servicios de red (ejemplo, TCP/IP) sobre los equipos críticos en el proceso de pago.	✓ Revisión de la topología de red (diagrama de red). ✓ Análisis de los distintos servidores y su función. ✓ Análisis de accesos (ejemplo, servicios TCP/IP) permitidos entre los servidores críticos con los demás servidores, redes internas y otras redes externas al Comercio.	• Diagrama de la red dedicada a la aplicación de "Sistemas Propios" • Reunión con Administrador de Red para una revisión general del diagrama de la red.
4.2 Segmentación de red		
• La red en la cual está *montada* la aplicación de venta se encuentra aislada de otras redes LANs o WANs de la Empresa.	✓ Revisión de los segmentos de red.	• Diagrama de la red dedicada a la aplicación del comercio • Descripción de la función de cada uno de los componentes de la red dedicada a la aplicación del comercio . • Reunión con el Administrador de Red para una revisión general del diagrama de red.
4.3 Administración del dispositivo de filtro de red		
• El número de usuarios con capacidad de realizar tareas de administración del dispositivo de filtro de red es restringido. • Las únicas cuentas de usuario definidas en el dispositivo de filtro de red son las del Administrador y de quien realiza los backups.	✓ Revisión de usuarios con capacidad de realizar tareas de administración del dispositivo de filtro de red. ✓ Revisión de las cuentas de usuario definidas en cada dispositivo de filtro de red.	• Detalle de usuarios con acceso al dispositivo de filtro de red para propósitos de administración. • Detalle de cuentas de usuario definidas en el/los computadores que componen el dispositivo de filtro de red
4.4 Configuración del dispositivo de filtro de red		
• El IP forwarding se encuentra inhabilitado. • El enrutamiento por origen (source routing) no está habilitado en el dispositivo de filtro de red.	✓ Chequeo del estado de IP Forwarding. ✓ Chequeo del estado del Source Routing.	• Listados de parametrización del dispositivo de filtro de red. • Listado con el detalle de reglas de acceso y filtrado establecidas.

• Los puertos (ports) habilitados en el dispositivo de filtro de red, sobre los cuales se puede establecer una conexión, son los adecuados. • Las reglas de acceso definidas en el dispositivo de filtro de red protegen, a la red interna de accesos maliciosos provenientes de redes o conexiones externas al Comercio. Todos los servicios deberían estar negados al menos que estén expresamente permitidos. • Los protocolos habilitados para el tráfico de paquetes son los necesarios y adecuados para la ejecución de las aplicaciones.	✓ Verificación del estado de los puertos 47, 137, 138. 139, y 102x., entre otros. Los mismos deberían estar inhabilitados si no son necesarios para una aplicación propietaria. ✓ Revisión de las tablas de ruteo y acceso. ✓ Revisión de los protocolos activos en función de las necesidades de las aplicaciones.	• Listado con las tablas de ruteo del dispositivo de filtro de red.
4.5 Log de auditoría del dispositivo de filtro de red		
• La auditoría de eventos que ocurren en el dispositivo de filtro de red, tales como intentos de comunicación, cierres del sistema, transferencias de archivos, etc. Debe estar habilitada.	✓ Revisión de la parametrización de las opciones de auditoría del dispositivo de filtro de red.	• Listado con el detalle de la parametrización del dispositivo de filtro de red relacionada con la generación de pistas de auditoría.

5. Seguridad de la Aplicación de Venta "Sistemas Propios"

BEST PRACTICE	PROCEDIMIENTO	REQUERIMIENTOS
5.1 Almacenamiento de datos de tarjeta y personales		
• Toda información contenida en la tarjeta o claves de identificación asociadas, no deben quedar almacenadas en ningún medio, sistematizado o no. • Para la operación con Tarjeta de Débito, no se almacena el Pin Block (información considerada crítica) en las transacciones. • También se considera información crítica al archivo de los "tickets" firmado por los clientes • Solo puede almacenarse en forma encriptada, bajo algoritmos estándares y best practices sobre las claves de encripción, definidos en 3.9 y por un lapso no mayor a los 60 días, los siguientes datos: - Fecha de Operación - Fecha de transmisión de la transacción - Hora de la operación - Hora de transmisión de la transacción - Tipo de operación (autorización, compra, anulación de compra, devolución, anulación de devolución, reversión de operación, cierre de lote) - Modo de operación (On-Line u Off-Line) - Tipo de ingreso del nro. de tarjeta (con lectura de banda, ingreso manual - Número de tarjeta - Fecha de expiración de la tarjeta - Identificación del nro. de terminal en que se procesó la transacción - Código del comercio asociado a la transacción - Importe de la transacción - Tipo de moneda - Cantidad de cuotas - Tipo de plan (en caso de corresponder) - Identificación del número de lote	✓ Identificación de archivos/tablas (temporales/definitivos) con información crítica de la tarjeta de crédito (según la best practice), y el tiempo durante el cual es almacenada la formación. ✓ Verificar los datos almacenados en los archivos/bases de datos de la lista obtenida, validando que no se almacenen datos críticos. Por ejemplo el Código de seguridad, Pin Block y otros campos grabados en la banda magnética. ✓ Verificar los archivos de Logs en los equipos (servers o dispositivos de comunicación) que participan del flujo de información entre el comercio y los **Procesadores**. Ej. Log en el Router. ✓ Análisis de razonabilidad de la información mantenida. ✓ Verificar que los datos críticos permitidos de almacenar (descriptos en la best practice) se resguardan con herramientas estándares de encriptación, por un período máximo de 60 días. ✓ Chequeo del mantenimiento y acceso a claves de encripción.	• Descripción detallada del esquema de funcionamiento previsto de la aplicación en el entorno "Sistemas Propios" y su interacción con los Procesadores. • Detalle de la información almacenada referida a clientes, forma de almacenamiento y tiempo de vida. • Detalle de tablas de la base de datos y/o archivos en los que se almacena información sensitiva de los clientes . • Mecanismos de encriptado de la información almacenada y utilización de claves.

- Identificación del número de comprobante de la transacción que se emite - Código de la autorización - "Trace" del sistema (número secuencial que identifica unívocamente a cada transacción para cada terminal específica) - "Retrieval Reference Number" número secuencial que identifica unívocamente a cada transacción dentro del sistema de autorizaciones de cada emisor - "Retrieval Reference Number" original, en caso de tratarse de anulaciones - Identificación del número de comprobante de la transacción original, en caso de tratarse de devoluciones - Fecha del comprobante de la transacción original, en caso de tratarse de devoluciones. • La información se almacena únicamente con el objetivo de completar las transacciones realizadas por los clientes. • El cliente es notificado en los casos en que se almacena información personal o financiera.	✓ Verificar que la base de datos que resguarda información de los tarjetahabientes, se encuentra instalado en un segmento de red distinto al que contiene otras aplicaciones propias del comercio o conexiones a redes LAN o WAN, con altos niveles de restricción de acceso al nivel usuario y servicios TCP/IP.	
5.2 Depuración en archivos / Bases de Datos		
• La depuración de información crítica contenida en archivos/Bases de Datos, se efectúa al nivel físico y lógico. Los mismos son reemplazados con datos nulos, para evitar su recuperación.	✓ Analizar el proceso de depuración de archivos / Base de Datos con información crítica. ✓ Verificación del mecanismo de depuración sobre una muestra de archivos/Bases de Datos que resguardan información crítica.	• Reunión con el personal técnico, designado por el comercio, para relevar esta actividad.
5.3 Control de acceso a la aplicación		
• El acceso a las funciones de administración de la aplicación se encuentra restringido mediante	✓ Revisión del mecanismo de acceso a las opciones de administración de la	• Detalle de los mecanismos de acceso a la aplicación de ventas.

perfiles de usuario.	aplicación del comercio.	
5.4 Información impresa		
• El acceso a la información crítica impresa de los clientes se encuentra restringido. • La salida impresa de los procesos de la aplicación de comercio con información confidencial de los clientes es destruida luego de su utilización o conservada de manera segura.	✓ Chequeo del tipo de información impresa. ✓ Análisis del tratamiento y resguardo de la salida impresa con información confidencial.	• Detalle del tipo de información impresa. • Procedimiento de circulación de información impresa confidencial.
5.5 Cambio de versiones		
• El pasaje a producción de nuevas versiones de la aplicación de comercio se realiza de manera adecuada para no afectar la disponibilidad del comercio ni la seguridad de las transacciones. • Se mantiene un adecuado control de los cambios de versión.	✓ Revisión del procedimiento de cambio de versiones y puesta en *"Producción"*. ✓ Verificar la existencia de procedimientos para permitir y controlar cambios de emergencia, sobre los programas relacionados con "Sistemas Propios". ✓ Analizar la documentación necesaria, que permitan afirmar que los cambios en el Software de pago, han sido previamente autorizados.	• Detalle del esquema de pasaje a Producción de nuevas versiones de la aplicación.

6. Monitoreo de red y administración de eventos		
BEST PRACTICE	**PROCEDIMIENTO**	**REQUERIMIENTOS**
6.1 Monitoreo de red y configuración de alarmas		
• Se cuenta con herramientas de detección, análisis y scanners, para detectar configuraciones que generen vulnerabilidades, o actividades sospechosas tanto en la red como en los servidores. • Estas herramientas tienen configuradas alarmas para la notificación de eventos relacionados con la seguridad, tales como repetidos intentos de acceso denegados.	✓ Revisión del software que permite detectar vulnerabilidades en la red. ✓ Revisión del software de monitoreo de red en uso.	• Detalle del software que permite detectar vulnerabilidades en la red. • Detalle del software de monitoreo de red en uso. • Detalle de las principales alarmas establecidas.
6.2 Procedimientos de respuesta ante ataques		
• Los eventos detectados como actividades sospechosas se analizan y reportan a los niveles adecuados. • Existen herramientas de detección de intrusos (Intrussion Detection Systems).	✓ Análisis de los mecanismos de notificación y reporte. ✓ Analizar la documentación necesaria, que permita afirmar que se efectúan seguimientos sobre los incidentes de seguridad más relevantes.	• Detalle de las herramientas de detección de intrusos en uso. • Procedimiento ante incidentes de seguridad.

7. Mecanismos de criptografía en la transmisión de datos		
BEST PRACTICE	**PROCEDIMIENTO**	**REQUERIMIENTOS**
7.1 Transmisión de datos de clientes		
• Los datos que proporciona el cliente al momento de realizar la compra en el comercio (lectura de banda magnética, nombre, número de tarjeta de crédito, etc.) se transmiten encriptados, entre los equipos, utilizando herramientas o algoritmos estándares de seguridad, por ejemplo, *VPN, SSL 128 bits, SSH, 3DES, etc*.	✓ Verificación de los protocolos de transmisión empleados por la aplicación de ventas.	• Detalle del mecanismo de encripción empleado, protocolos y versiones. • Longitud de las claves de encripción empleadas. • Autoridad certificante emisora de los certificados digitales. • Fechas de validez de los certificados vigentes.
7.2 Transmisión de datos de clientes entre el comercio y terceras partes		
• Existen mecanismos que aseguran: - Autenticación de las partes. - Privacidad: la información transmitida sólo puede ser accedida por el legítimo destinatario. - Integridad: las alteraciones a la información transmitida pueden ser detectadas. - No repudio: el emisor de información no puede negar haberla enviado.	✓ Relevamiento del esquema de transmisión de datos previsto entre el comercio y terceras partes. ✓ Verificación de los protocolos de transmisión que aseguren autenticación, confidencialidad e integridad, entre el Comercio y terceras partes que intervienen en el proceso del comercio.	• Esquema de transmisión de datos previsto entre el comercio y terceras partes.

8. Control de Operatividad del Aplicativo "Sistemas Propios".

Tipos de aplicaciones en el entorno de Sistemas Propios:

A) Sistema desarrollado para comercios, donde los compradores y vendedores son reales. (Ejemplo: Supermercados, Shopping, Tiendas)

B) Sistema desarrollado para comercios, donde los compradores son virtuales y los vendedores reales. (Ejemplo: Venta telefónica)

C) Sistema desarrollado para comercios, donde los compradores son reales y los vendedores son terminales de venta autoasistida. (Ejemplo: surtidores de combustible)

BEST PRACTICE	PROCEDIMIENTO	REQUERIMIENTOS
8.1 Control de Skimming		
• Para Sistemas del tipo A En todas las operaciones realizadas con lectura de Banda Magnética se solicita y valida el ingreso manual de los últimos 4 dígitos del número de la tarjeta, y en ningún caso se muestra por pantalla los 4 dígitos ingresados, según: Capítulo B – Especificaciones Generales, del "Manual de Especificaciones Técnicas y Funcionales Para el Desarrollo de Sistemas Propios On-line Bajo Protocolo ISO 8583".	✓ Verificar que al efectuarse una transacción por medio de la lectura de la banda magnética de la tarjeta de crédito, se solicita el ingreso de los últimos 4 dígitos de la tarjeta. ✓ Verificar que los cuatro dígitos ingresados se validan contra los últimos cuatro dígitos del número de tarjeta. ✓ Verificar que, en caso de diferencia entre los datos, pida nuevamente el ingreso de los 4 dígitos. ✓ Verificar que, en caso de diferencia entre los datos, muestre por pantalla el mensaje "Error código 10 y el numero de tarjeta leído en la banda. ✓ Verificar en el sistema aplicativo, si este control es parametrizable por emisor y por tipo de operación (con o sin lectura de banda). Verificar, para el caso de las tarjetas de crédito MasterCard, que se enmascare el ingreso de los 4 últimos dígitos con "*".	• Reunión con el personal designado por el comercio, para relevar el procedimiento que controla el skimming. • Configuración / Parámetros del Sistema Aplicativo que se relacionan con esta actividad.

8.2 Proceso "Cierre de Lote"

• Para Sistemas del tipo A, B y C El proceso de "cierre de lote" está íntegramente automatizado. Es decir, al momento de hacer el arqueo de caja o cierre de operaciones del día, el sistema solicita ejecutar el cierre de lote y de no efectuarse manualmente antes de cerrar el sistema, éste lo realiza en forma automática o luego de la apertura del día siguiente no se podrá operar hasta haber efectuado el cierre del día anterior, según se adapte mejor a los usos del comercio. Se registra en el log del sistema, cada operación de cierre de lote, identificando si el mismo fue automático o manual, registrando en cada intento de cierre el número de terminal y el resultado recibido del mismo.	✓ Relevar el procedimiento de cierre de lote, considerando los siguientes aspectos: – Cómo es realizado: en forma manual o automática, – Desde donde es ejecutado, – Horario en el cual es ejecutado, – Procedimiento si no hay conexión on-line, – Archivos generados. – Procedimiento si no hay operaciones pendientes. – Procedimiento ante cierre de lote rechazado. ✓ Verificar que los archivos generados a partir del cierre de lote, no contienen datos críticos (Ver 5.1) e indican que la operación de cierre de lote es automática. Verificar que el archivo de log, relacionado con cada intento de cierre de lote, debe indicar por lo menos: número de terminal, horario de cierre y el resultado recibido del mismo (Ejemplo: Cierre O.K., Cierre con Batch Up Load, No hay respuesta del Host, No hay conexión con el Host, No tiene operaciones a Cerrar).	• Reunión con el personal designado por el comercio, para relevar esta actividad. • Lista de archivos generados a partir del cierre de lote. • Configuración / Parámetros del Sistema Aplicativo que se relacionan con esta actividad.

8.3 Código de Seguridad		
• Para Sistemas del tipo A y B El sistema debe solicitar el código de seguridad, que figura al dorso de la tarjeta (está impreso, sin relieve), en el panel de firma. Este control se efectúa para todo tipo de transacción. En ningún caso se muestra por pantalla el código de seguridad ingresado. El código de seguridad, no debe ser resguardado en ningún archivo o bases de datos del sistema.	✓ Verificar que el Sistema Aplicativo requiere el código de seguridad (3 dígitos para MasterCard, Visa y Diners; 4 dígitos para AMEX) al efectuarse toda operación. ✓ Verificar en el sistema aplicativo, si este control es parametrizable por emisor. ✓ Verificar que no se exhiben por pantalla, el código de seguridad ingresados, ocultando los mismos con "*".	• Configuración / Parámetros del Sistema Aplicativo que se relaciona con esta actividad.
8.4 Fecha de vencimiento		
• Para Sistemas del tipo A, B y C El Sistema Aplicativo siempre valida la fecha de vencimiento de la tarjeta, antes de enviar la solicitud de aprobación a los Procesadores. Excepto para productos de débito como Maestro y Visa Electrón	✓ Verificar que el Sistema Aplicativo requiere y valida la fecha de vencimiento, en modo de operación on-line y off-line (previo a solicitar una autorización telefónica), para transacciones mediante el ingreso manual del número de la tarjeta o por medio de la lectura de la banda magnética. Excepto para productos de débito como Maestro y Visa Electrón, donde no se debe controlar su vencimiento, permitiéndose la aceptación de la misma aún estando vencida. ✓ Verificar en el sistema aplicativo, si este control es parametrizable por emisor.	• Configuración / Parámetros del Sistema Aplicativo que se relacionan con esta actividad.

8.5 Operatoria Off-line, para Tarjetas de Créditos

- Para Sistemas del tipo A y B (esta operatoria NO DEBE ser permitido para Sistemas de tipo C)

• Modalidad Off-line Solo operan bajo la modalidad off-line, los comercios autorizados, los cuales deberán tener definido su límite otorgado para contingencia. La operatoria normal fuera de línea implica solicitar la autorización telefónicamente e ingresar dicho código en el sistema propio para ser enviado al momento de restablecerse el vínculo.	✓ En el caso de operar el comercio bajo la modalidad off-line, verificar su autorización y límite otorgado para contingencia. ✓ Verificar en el sistema aplicativo, si este control es parametrizable por emisor. ✓ Para sistemas de tipo C, verificar que no se encuentre habilitado la operatoria Off-line.	• Configuración / Parámetros del Sistema Aplicativo que se relacionan con esta actividad.
• Control de topes, en una operatoria Off-line - El Sistema Aplicativo permite parametrizar la cantidad máxima de transacciones que pueden efectuarse en un mismo día, y para un mismo número de tarjeta. - El Sistema Aplicativo controla que la sumatoria de importes de las transacciones efectuadas por el mismo tarjetahabiente no supera el límite otorgado para "contingencia" a ese Comercio (este límite está asociado a la autorización para operar en modo off-line).	✓ Analizar el procedimiento de control de topes de cupones para operaciones off-line. ✓ Verificar que existen parámetros en el Sistema Aplicativo que aseguren la cantidad máxima de transacciones que permitirá efectuar el sistema al operar en modo off-line, en un mismo día y para un mismo número de tarjeta. ✓ Relevar el límite establecido para el Comercio ✓ Verificar que el Sistema Aplicativo permite controlar que la sumatoria de importes de las transacciones efectuadas por el mismo tarjetahabiente no supera el límite otorgado para "contingencia" a ese Comercio. Verificar si este control es parametrizable.	• Configuración / Parámetros del Sistema Aplicativo que se relacionan con esta actividad.
• "Boletín protectivo" en una operatoria Off-line - El Sistema Aplicativo valida que el	✓ Verificar que el Comercio esté habilitado, por los emisores para esta operatoria.	• Configuración / Parámetros del Sistema Aplicativo que se relacionan con esta actividad.

"Boletín Protectivo" contenga información, y que ella se encuentre actualizada a la fecha. - El proceso de actualización diario del boletín, es automático. - El Sistema Aplicativo sólo permite transacciones que se encuentren por debajo del límite otorgado para "contingencia", previa validación obligatoria contra el "Boletín Protectivo".	✓ Relevar en qué casos se efectúa el control contra boletín protectivo para operaciones off-line. ✓ Verificar que el boletín protectivo contiene información y se encuentra actualizado. ✓ Verificar que el método de actualización del boletín protectivo es automático. ✓ Verificar que el Sistema Aplicativo sólo permite transacciones que se encuentren por debajo del límite otorgado para "contingencia", previa validación obligatoria contra el "Boletín Protectivo". ✓ Verificar que su habilitación, sea parametrizable por emisor.	
• Operatoria y transacciones Off-line - El Sistema Aplicativo no permite el pasaje "forzado" a modo "off-line". - El envío de transacciones generadas "off-line" se efectúa en forma automática e inmediata, luego de restablecida la comunicación con los respectivos Procesadores. En caso de haberse solicitado código de autorización telefónicamente, este proceso puede dilatarse según el volumen de operaciones recibidas para no generar mayores tiempos de respuesta.	✓ Relevar y verificar si el sistema permite realizar el pasaje manual a modo off-line, mediante un parámetro, una opción de menú o mediante otro procedimiento diferente. ✓ Relevar el procedimiento de envío de transacciones off-line una vez restablecido el vínculo con los Procesadores. ✓ Verificar donde se almacenen las transacciones off-line, hasta tanto sean enviadas a los Procesadores. ✓ Relevar y verificar si es parametrizable el procedimiento de envío de las transacciones off-line.	• Configuración / Parámetros del Sistema Aplicativo que se relacionan con esta actividad.
Operatoria Off-line, para Tarjetas de Débito		
• Para Sistemas del tipo A, B y C	✓ Verificar que no se permite la operatoria Off-line y/o	• Configuración / Parámetros del Sistema Aplicativo que

- No se permite la operatoria Off-line y/o Manual con la Tarjeta de Débito. - En el caso de Visa Electrón, los comercios tienen la posibilidad de tomar diariamente la Tabla con Bines Electrón, para ser usado en el control de los casos de ingreso manual y/o Off-line	Manual con Tarjetas de Débito. ✓ En el caso de Visa Electrón, relevar y verificar si el sistema permite realizar el control en modo off-line, de la Tabla de Bines Electrón para identificarlos.	se relacionan con esta actividad.
8.6 Transacciones de anulaciones o devoluciones		
• Para Sistemas del tipo A y B El Sistema Aplicativo, contempla el procesamiento de transacciones en concepto de anulaciones o devoluciones, realizadas con las respectivas tarjetas, controlando que exista y no supere el valor de la transacción original que pretende anular o sobre la que realiza la devolución	✓ Relevar si el Sistema Aplicativo efectúa operaciones de: – "devolución" por el monto total o parcial de una operación de compra efectuada fuera del lote. Verificar que su inhabilitación, sea parametrizable por emisor. – "anulación" por el monto total de una operación de compra efectuada dentro del lote actual. Verificar que su inhabilitación, sea parametrizable por emisor. ✓ Relevar el procedimiento relacionado con las operaciones de anulación y devolución. Observar los datos requeridos, importe por el cual permite efectuar la anulación y la devolución (monto total o parcial) de la transacción original. ✓ Verificar en los archivos (log de transacciones) la existencia de las transacciones antes	• Configuración / Parámetros del Sistema Aplicativo que se relacionan con esta actividad

	mencionadas con sus respectivos códigos.	
8.7 Informes de gestión		
• Para Sistemas del tipo A, B y C El Comercio cuenta con reportes acerca de la cantidad de operaciones realizada "off line" versus las "on line", como así también las que se realizan con ingreso manual versus las ingresadas por banda. Estos reportes analizados por franjas horarias y por cajero, ofrecen resultados muy positivos en el control del fraude. La salida de esta información debe controlarse habitualmente por personal jerárquico de cada empresa, analizando el motivo de los casos más llamativos y resolviendo en concordancia.	✓ Relevar si existe un módulo que permita generar reportes, analizados por franjas horarias y por cajero, con información sobre: - cantidad de operaciones efectuadas "off line" versus las realizadas "on line", - cantidad de operaciones efectuadas mediante el ingreso manual versus las ingresadas por lectura de la banda. - Verificar que estos reportes incluyan sólo totales y no información crítica (Ver 5.1) ✓ Evaluar el nivel de implantación del Procedimiento de ejecución, control y seguimiento de incidentes, sobre los Informes de gestión.	• Procedimiento de ejecución, control y seguimiento de incidentes, sobre los Informes de gestión. • Lista y copia de una muestra, de los diversos Informes de gestión.
8.8 Impresión de Tickets, sólo para Tarjetas MasterCard y Visa		
• Para Sistemas de Tipo A y C. Los tickets emitidos para operaciones On-line u Off-line, contienen: - La leyenda Tipo y N° Doc.:..... - La fecha de vencimiento de la tarjeta, enmascarado con el carácter "*" - Nombres y apellidos del Tarjetahabiente. - Modo de Operación (On Line u Off Line) - Modo de ingreso del número de tarjeta (lectura o tipeo)	✓ Verificar si el sistema imprime la leyenda solicitada y enmascara la fecha de vencimiento, según se indica en la best practice. ✓ Verificar que se imprime correctamente el modo de ingreso de la operación y del número de tarjeta ✓ Verificar si este control	• Configuración / Parámetros del Sistema Aplicativo que se relacionan con esta actividad • Copia de diversas muestras, de tickets impresos.

	es parametrizable por emisor, en el sistema aplicativo	
• Para Sistemas de Tipo A Los tickets emitidos en toda operación off-line o sin lectura de banda, dejan el espacio necesario para evidenciar presencia física de la tarjeta	✓ Verificar que el ticket deja un espacio para "imprimir" los datos del relieve de la tarjeta, según: Capítulo A – Tickets solicitados por los Emisores, del "Manual de Especificaciones Técnicas y Funcionales Para el Desarrollo de Sistemas Propios On-line Bajo Protocolo ISO 8583".	• Copia de tickets impresos, de todas las operatorias permitidas para el Comercio.
• Para Sistemas de Tipo A, B y C Los Sistemas Aplicativos están adecuados a las especificaciones del Mensaje Promocional. - Si el mensaje es recibido en la respuesta debe ser mostrado por pantalla. - Para mayor detalle ver sección ***"Capitulo H - Mensajes y Leyendas especiales en POS"***.	✓ Verificar que el Sistema Aplicativo esta en condiciones de recibir y procesar el mensaje enviado en el Campo ISO 63, según: Capítulo C – Especificación de Mensajes, del "Manual de Especificaciones Técnicas y Funcionales Para el Desarrollo de Sistemas Propios On-line Bajo Protocolo ISO 8583". ✓ Verificar que el Sistema Aplicativo, muestre por pantalla los caracteres recibidos en la respuesta. ✓ Verificar que el Sistema Aplicativo, muestre por pantalla e imprima en el ticket los 40/200 caracteres recibidos en la respuesta.	• Copia de tickets impresos, de todas las operatorias permitidas para el Comercio.

8.9 Ingreso de las operaciones, sólo para Tarjetas MasterCard y Visa		
• Para Sistemas de Tipo C El sistema aplicativo, acepta únicamente ingreso de operaciones On Line con Lectura de Banda.	✓ Verificar la best practice. ✓ Verificar si este control es parametrizable por emisor, en el sistema aplicativo	• Configuración / Parámetros del Sistema Aplicativo que se relacionan con esta actividad.
8.10 Visualización de la información contenida en una tarjeta		
• Para Sistemas de Tipo A,B y C (modalidades On y Off-Line) Durante todo proceso de captura de datos (lectura de banda, manual, etc.): - Sólo se podrá visualizar la información referida a: - N° de tarjeta - Fecha de Vencimiento - Nombre del tarjetahabiente Finalizado el proceso de captura, el sistema aplicativo, y en todo momento, sólo permite visualizar por pantalla, exclusivamente y como máximo, la información correspondiente a: - Los cuatro últimos dígitos del Número de tarjeta - Nombre del tarjetahabiente	✓ Verificar que el Sistema Aplicativo permite únicamente la exhibición de, a lo sumo, los datos mencionados.	• Configuración / Parámetros del Sistema Aplicativo que se relacionan con esta actividad

1. Políticas y estándares de seguridad informática y procedimientos de admin de seguridad	OPTIMO	ADECUADO	REGULAR	DEFICIENTE	PESO	Matriz de Riesgo / ALCANCE
1.1 Políticas de seguridad informática	Existe un Manual de Políticas de seguridad informática, actualizadas y aprobadas por la Gerencia, conocidas por el personal de la empresa y abarca los siguientes riesgos del entorno de pago: Confidencialidad de los datos, Integridad de los datos, Control de acceso físico, Control de acceso lógico, Utilización de recursos informáticos y Cambio de sistemas.	Existen comunicados formales, actualizados y aprobados por la Gerencia, enviados a todo el personal de la empresa y abarcan parcialmente los riesgos del entorno de pago indicados en el nivel optimo.	Existen comunicados no formales, enviados a todo el personal de la empresa, que abarcan total o parcialmente los riesgos del entorno de pago indicados en el nivel optimo.	No existen políticas de seguridad informática que abarquen total o parcialmente los riesgos del entorno de pago indicados en el nivel optimo.	5	
1.2 Estándares de configuración de seguridad lógica	Existe un Manual de Estándares de seguridad informática, actualizado y aprobado por la Gerencia, conocido por el personal que lo implanta y abarca los siguientes componentes de seguridad lógica del entorno de pago: Sistemas Operativos, Software de Pago, Base de Datos que almacena información crítica del tarjetahabiente, dispositivos de comunicación y Filtros de red.	Existen estándares, envíados a todo el personal que lo implanta, actualizados y aprobados por la Gerencia, a través de comunicados formales y abarcan parcialmente los componentes de seguridad lógica del entorno de pago indicados en el nivel optimo.	Existen estándares, envíados a todo el personal que los implanta, a través de comunicados no formales y abarcan total o parcialmente los componentes de seguridad lógica del entorno de pago indicados en el nivel optimo.	No existen estándares de seguridad informática que abarquen total o parcialmente los componentes de seguridad lógica del entorno de pago indicados en el nivel optimo.	3	
1.3 Procedimientos de administración de seguridad lógica	Existe un Manual de Procedimientos de seguridad informática, actualizadas y aprobadas por la Gerencia, conocidas por el personal que lo implanta y abarca las siguientes actividades de administración y control (sobre los componentes de seguridad lógica del entorno de pago definidos en el item anterior): Administración de usuarios y claves, Administración del Filtro de red y reglas de acceso, Revisión de Logs de auditoría, Cambio de sistemas y Backup/Restore.	Existen procedimientos, envíados a todo el personal que lo implanta, actualizados y aprobados por la Gerencia, a través de comunicados formales y abarcan parcialmente las actividades de administración y control indicados en el nivel optimo.	Existen procedimientos, envíados a todo el personal que lo implanta, a través de comunicados no formales y abarcan total o parcialmente las actividades de administración y control indicados en el nivel optimo.	No existen procedimientos de seguridad informática que abarquen total o parcialmente las actividades de administración y control indicados en el nivel optimo.	5	
1.4 Administración de la seguridad	Existe en la organización una adecuada segregación de funciones administrativas de los sistemas críticos y la seguridad informática. Existen procedimientos para ejecutar controles por oposición.	Existe en la organización una adecuada segregación de funciones administrativas de los sistemas críticos y la seguridad informática. Existen procedimientos informales para ejecutar controles por oposición.	Existe en la organización una adecuada segregación de funciones administrativas de los sistemas críticos y la seguridad informática. No existe documentación de procedimientos para ejecutar controles por oposición.	No existe en la organización una adecuada segregación de funciones administrativas de los sistemas críticos y la seguridad informática. No existe documentación de procedimientos para ejecutar controles por oposición.	2	
1.5 Auditoría interna y/o externa	El entorno informático de la aplicación de "Sistemas Propios" es auditado periódicamente a fin de detectar debilidades de seguridad y mejorar procedimientos de administración. Se efectúan en forma periódica controles a través de test de penetración.	El entorno informático de la aplicación de "Sistemas Propios" es auditado periódicamente a fin de detectar debilidades de seguridad y mejorar procedimientos de administración. No se efectúan en forma periódica controles a través de test de penetración.	El entorno informático de la aplicación de "Sistemas Propios" es auditado parcialmente. No se efectúan en forma periódica controles a través de test de penetración.	El entorno informático de la aplicación de "Sistemas Propios" no es auditado ni se efectúan test de penetración.	4	
	Calificacion % de riesgo del punto 1					A

2 Seguridad física de la plataforma	OPTIMO	ADECUADO	REGULAR	DEFICIENTE		
2.1 Control de Acceso	El centro de cómputos o sector de equipos cuenta con todos sus accesos controlados por mecanismos de seguridad, con control de acceso y registro de ingresos y egresos de personal autorizado. Existe procedimiento formal que describe los controles de acceso y el monitoreo de los mismos.	El centro de cómputos o sector de equipos cuenta con todos sus accesos controlados por mecanismos de seguridad con control de acceso y registro de ingresos y egresos de personal autorizado. Existen documentos no formales que describen los controles de acceso.	El centro de cómputos o sector de equipos cuenta con todos sus accesos controlados por mecanismos de seguridad, con control de acceso de personal autorizado. No existe documentación que describe los controles de acceso.	El centro de cómputos o sector de equipos no cuenta con accesos controlados.	**1**	**SO WS, SO F, SO SP, SO SA, BD, SWS, SP, SF**
	Calificacion % de riesgo del punto 2					**B**

3 Seguridad lógica de la plataforma	OPTIMO	ADECUADO	REGULAR	DEFICIENTE		
3.1 Identificación de usuarios	Existen procedimientos formales para la asignación de accesos en función de sus tareas a través de perfiles de seguridad y existen estándares para la asignación del nombre de cuenta del usuario.	Existen procedimientos formales para la asignación de accesos en función de sus tareas a través de perfiles de seguridad y no existen estándares para la asignación del nombre de cuenta del usuario.	Existen procedimientos no formales para la asignación de accesos en función de sus tareas a través de perfiles de seguridad y existen estándares para la asignación del nombre de cuenta del usuario.	No existe documentación para la asignación de accesos en función de sus tareas a través de perfiles de seguridad ni estándares para la asignación del nombre de cuenta del usuario.	**5**	**SO WS, SO F, SO SP, SO SA, BD, SWS, SP, SF**
3.3 Usuarios sensitivos	Existen procedimientos formales de control sobre los usuarios sensitivos. Los usuarios sensitivos existentes son mínimos y presentan formalmente una justificación técnica u operativa que lo respalda.	Existen procedimientos formales de control sobre los usuarios sensitivos. Existen usuarios sensitivos que no presentan formalmente una justificación técnica u operativa que lo respalde.	Existen procedimientos no formales de control sobre los usuarios sensitivos. Existen usuarios sensitivos que no presentan formalmente una justificación técnica u operativa que lo respalde.	No existe documentación acerca del control sobre los usuarios sensitivos.	**4**	
	Calificacion % de riesgo del punto 3. Identificación					**C**
3.2 Autenticación de usuarios (Tipo de autenticación)	Todos los usuarios acceden mediante dispositivos biometricos o algun componente "two-factor"	Todos los usuarios acceden mediante User ID y password	Existen usuarios no privilegiados, sin token de acceso (biometrico, User Id y password, etc.)	Existen usuarios privilegiados sin token de acceso	**5**	**SO WS, SO F, SO SP, SO SA, BD, SWS, SP, SF**
3.2 Autenticación de usuarios (Parámetros de configuración)	Todos los usuarios tienen la siguiente configuración sobre sus passwords: long mínima (8 o más), duración mínima (45 o menos), history (12 o más), bloqueos (después del tercer intento fallido)	Todos los usuarios están configurados de acuerdo a los estándares de la empresa, sin embargo, los valores definidos no coinciden con la configuración calificada como óptimo.	Existen usuarios no privilegiados, que no cumplen con la configuración calificada como óptimo.	Existen usuarios privilegiados que no cumplen con la configuración calificada como óptimo.	**4**	
3.2 Autenticación de usuarios (Resguardo de parámetros de configuración)	Todos los archivos o bases que almacenan los parámetros de autenticación y el token de acceso (User Id y password, certificado, datos biométricos, etc.), sólo pueden ser accedidos por el personal autorizado y se registra cada actividad	Todos los archivos o bases que almacenan los parámetros de autenticación y el token de acceso, sólo pueden ser accedidos por el personal autorizado, pero no se registra esta actividad	Existen archivos o bases que almacenan los parámetros de autenticación y el token de acceso, pueden ser accedidos por personal no autorizado	Todos los archivos o bases que almacenan los parámetros de autenticación y el token de acceso, pueden ser accedidos por personal no autorizado	**4**	
3.2 Autenticación de usuarios (Encriptación)	Todos los archivos o bases que almacenan los parámetros de autenticación y el token de acceso (User Id y password, certificado, datos biométricos, etc.), se encuentran encriptados por las herramientas indicadas en las MP	Todos los archivos o bases que almacenan los parámetros de autenticación y el token de acceso, se encuentran encriptados por las herramientas distintas a las indicadas en las MP	Existen archivos o bases que almacenan los parámetros de autenticación o el token de acceso, que se encuentran en clear text	Todos los archivos o bases que almacenan los parámetros de autenticación y el token de acceso, se encuentran en clear text	**5**	
3.2 Autenticación de usuarios (Servicios TCP/IP)	No se encuentran activos los servicios FTP, Telnet y R* (rcp, rsh, rlogin). Cada servicio es reemplazado por su equivalente con agregados de confidencialidad, autenticación e integridad (como SSH, VPN, etc.)	Se encuentran activos los servicios FTP, Telnet y R*, para acceder sólo de manera local (red interna), mediante usuarios no privilegiados	Se encuentran activos los servicios FTP, Telnet y R*, para acceder sólo de manera local, mediante algún usuario privilegiado	Se encuentran activos los servicios FTP, Telnet o R*, para acceder de manera local y remota, mediante cualquier usuario	**5**	

3.2 Autenticación de usuarios (Procedimientos)	Existen procedimientos formales o estándares de seguridad, acerca de la administración de los parámetros y mecanismos de autenticación, implantados en su totalidad	Existen procedimientos formales o estándares de seguridad, acerca de la administración de los parámetros y mecanismos de autenticación, implantados parcialmente	Existen procedimientos no formales, acerca de la administración de los parámetros y mecanismos de autenticación	No existe ningúna documentación acerca de la administración de los parámetros y mecanismos de autenticación	**3**	
	Calificacion % de riesgo del punto 3. Autenticación					**D**
3.4 Permisos de acceso a archivos/tablas sensibles	El acceso a los archivos/tablas que contienen información sensible de los clientes, programas/datos relacionados con el software de pago y las claves privadas, se encuentra restringido al personal autorizado. La información sensible es soportada por la estructura de mayor nivel de seguridad que ofrece el sistema.	El acceso a los archivos/tablas que contienen información sensible de los clientes, programas/datos relacionados con el software de pago y las claves privadas, se encuentra restringido al personal autorizado. La información sensible no es soportada por la estructura de mayor nivel de seguridad que ofrece el sistema.	El acceso a los archivos/tablas que contienen información sensible de los clientes, programas/datos relacionados con el software de pago y las claves privadas, se encuentra restringido al personal autorizado. El sistema no cuenta con una estructura de datos con niveles de seguridad.	El acceso a los archivos/tablas que contienen información sensible del cliente o programas/datos relacionados con el software de pago, no se encuentra restringido.	**1**	**SO WS, SO F, SO SP, SO SA, BD, SWS, SP, SF**
	Calificacion % de riesgo del punto 3. Autorización					**E**
3.5 Registros de auditoría	La auditoría de eventos de seguridad del sistema sobre los recursos críticos, se encuentra habilitada. Los registros auditables se resguardan en un medio inalterable de manera adecuada. Existe un procedimiento de control y monitoreo de eventos.	La auditoría de eventos de seguridad del sistema sobre los recursos críticos, se encuentra habilitada. Los registros auditables se resguardan en un medio inalterable de manera adecuada. Existe un procedimiento no formal de control y monitoreo de eventos.	La auditoría de eventos de seguridad del sistema sobre los recursos críticos, se encuentra habilitada. Los registros auditables no se resguardan.	La auditoría de eventos de seguridad del sistema no se encuentra habilitada.	**1**	**SO WS, SO F, SO SP, SO SA, BD, SWS, SP, SF**
	Calificacion % de riesgo del punto 3. Registro de auditoría					**F**
3.6 Actualización del software de base	El software de base se encuentra actualizado con las últimas versiones de patches, fixes, correcciones, etc. Existen procedimientos de pruebas de las nuevas versiones de software de base instaladas y de control de los pasajes de desarrollo a producción	El software de base se encuentra actualizado con las últimas versiones de patches, fixes, correcciones, etc. Existen procedimientos no formales de pruebas de las nuevas versiones de software de base instaladas y de control de los pasajes de desarrollo a producción	El software de base se encuentra actualizado con las últimas versiones de patches, fixes, correcciones, etc. No existe documentación ni procedimientos no formales de pruebas de las nuevas versiones de software de base instaladas y de control de los pasajes de desarrollo a producción	El software de base no se encuentra actualizado con las últimas versiones de patches, fixes, correcciones, etc.	**3**	**SO WS, SO F, SO SP, SO SA, BD, SWS, SF**
3.8 Software instalado en los equipos	Los equipos que soportan la aplicación de "Sistemas Propios" se utilizan específicamente para este fin y no se comparte su uso con otras aplicaciones. El software de base que se ejecuta en los equipos es el mínimo y necesario requerido por la aplicación y en los mismos no se dispone de herramientas de software que comprometa a las aplicaciones instaladas.	Los equipos que soportan la aplicación de "Sistemas Propios" se utilizan específicamente para este fin y no se comparte su uso con otras aplicaciones. El software de base que se ejecuta en los equipos no está optimizado para ser el mínimo y necesario requerido por la aplicación y en los mismos no se dispone de herramientas de software que comprometa a las aplicaciones instaladas.	Los equipos que soportan la aplicación de "Sistemas Propios" se utilizan específicamente para este fin y no se comparte su uso con otras aplicaciones. El software de base que se ejecuta en los equipos no está optimizado para ser el mínimo y necesario requerido por la aplicación y en los mismos se dispone de herramientas de software que comprometa a las aplicaciones instaladas.	Los equipos que soportan la aplicación de "Sistemas Propios" no se utilizan específicamente para este fin y se comparte su uso con otras aplicaciones.	**5**	**SO WS, SO SP, SO SA, BD**
	Calificacion % de riesgo del punto 3. Cambio de software					**G**
3.7 Prevención y detección de virus, troyanos u otro código malicioso	Los equipos o el acceso al entorno de pago, cuentan con productos actualizados para prevenir y detectar virus, troyanos, backdoors, ataques de DoS y otros códigos maliciosos de uso frecuente.	Los equipos o el acceso al entorno de pago, cuentan con productos actualizados para prevenir y detectar virus, troyanos, backdoors y ataques de DoS.	Los equipos o el acceso al entorno de pago, cuentan con productos actualizados para prevenir y detectar virus.	Los equipos o el acceso al entorno de pago, no cuentan con productos para prevenir y detectar virus.	**1**	**SO WS, SO F, SO SP, SO SA, BD, SWS, SP, SF**
	Calificacion % de riesgo del punto 3. Integridad					**H**

3.9 Back-ups	Las copias de resguardo de la información de cliente se conservan en lugares seguros y con acceso restringido, los datos sensibles de los tarjetahabientes se resguardan con herramientas estándares de encriptación. Existe un procedimiento de control acerca de la eliminación de soportes de la información.	Las copias de resguardo de la información de cliente se conservan en lugares seguros y con acceso restringido, los datos sensibles de los tarjetahabientes se resguardan con herramientas no estándares de encriptación. Existe un procedimiento de control acerca de la eliminación de soportes de la información.	Las copias de resguardo de la información de cliente se conservan en lugares seguros y con acceso restringido, los datos sensibles de los tarjetahabientes se resguardan con herramientas no estándares de encriptación. No existe un procedimiento de control acerca de la eliminación de soportes de la información.	Las copias de resguardo de la información de cliente no se conservan en lugares seguros o los datos sensibles de los tarjetahabientes no se encriptan.	**1**	**SO WS, SO SP, SO SA, BD, SWS, SP**
	Calificacion % de riesgo del punto 3. Confidencialidad					**I**

4 Seguridad lógica de la red y del Filtro de Red	OPTIMO	ADECUADO	REGULAR	DEFICIENTE		
4.1 Existencia de un dispositivo de filtro de red	El comercio cuenta con un dispositivo que actúa como filtro de red para proteger la red interna de accesos provenientes de una red externa y tiene habilitados sólo los servicios/ports de TCP/IP necesarios para el funcionamiento del mismo. Los equipos que soportan el software de pago y las bases de datos tienen habilitados sólo los servicios/ports de TCP/IP necesarios para soportar el entorno de pago.	El comercio cuenta con un dispositivo que actúa como filtro de red para proteger la red interna de accesos provenientes de una red externa y tiene habilitados algunos servicios/ports de TCP/IP innecesarios para el funcionamiento del mismo. Los equipos que soportan el software de pago y las bases de datos tienen habilitados sólo los servicios/ports de TCP/IP necesarios para soportar el entorno de pago.	El comercio cuenta con un dispositivo que actúa como filtro de red para proteger la red interna de accesos provenientes de una red externa y tiene habilitados algunos servicios/ports de TCP/IP innecesarios para el funcionamiento del mismo. Los equipos que soportan el software de pago y las bases de datos tienen habilitados algunos servicios/ports de TCP/IP innecesarios para soportar el entorno de pago.	El comercio no cuenta con un dispositivo que actúa como filtro de red.	**5**	
4.2 Segmentación de la red	El entorno cuenta con dispositivos de filtro de red que aísla a la red donde reside la aplicación de venta del resto de las redes instaladas y solo tiene habilitados los servicios para posibilitar que los usuarios responsables accedan a la administración de la red de entorno de "Sistemas Propios".	El entorno cuenta con dispositivos de filtro que aísla a la red donde reside la aplicación de venta del resto de las redes instaladas y controla las direcciones IP y los servicios que se encuentran habilitadas para acceder a la red del entorno de "Sistemas Propios".	El entorno cuenta con dispositivos de filtro que aísla a la red donde reside la aplicación de venta del resto de las redes instaladas y existen excesivas direcciones de IP y servicios habilitados	El entorno no cuenta con dispositivos de filtro que separe las redes instaladas	**4**	
4.3 Administración del dispositivo de filtro de red	El dispositivo de filtro de red cuenta con usuarios suficientes y necesarios para las actividades de administración y backup, cuyo control de acceso el del tipo "two-factor".	El dispositivo de filtro de red cuenta con usuarios suficientes y necesarios para las actividades de administración y backup, cuyo control de acceso es del tipo User-Id y password.	El dispositivo de filtro de red cuenta con usuarios innecesarios para las actividades de administración o backup, cuyo control de acceso es del tipo User-Id y password.	El dispositivo de filtro de red cuenta con usuarios para actividades distintas al de administración y backup.	**4**	
4.4 Configuración del dispositivo de filtro de red	Las reglas de acceso definidas en el dispositivo de filtro de red protegen a la red interna de accesos malicios provenientes de redes externas y existe un procedimiento formal de mantenimiento. El IP forwarding se encuentra inhabilitado. El enrutamiento por origen no está habilitado en el filtro de red.	Las reglas de acceso definidas en el dispositivo de filtro de red protegen a la red interna de accesos malicios provenientes de redes externas y existe un procedimiento no formal de mantenimiento. El IP forwarding se encuentra inhabilitado. El enrutamiento por origen no está habilitado en el filtro de red.	Las reglas de acceso definidas en el dispositivo de filtro de red protegen total o parcialmente a la red interna de accesos malicios provenientes de redes externas y no existe un procedimiento de mantenimiento. El IP forwarding se encuentra inhabilitado. El enrutamiento por origen no está habilitado en el filtro de red.	Las reglas de acceso definidas en el dispositivo de filtro de red no protegen a la red interna de accesos malicios provenientes de redes externas.	**5**	
4.5 Log de auditoría del dispositivo de filtro de red	La auditoría de eventos del dispositivo de filtro de red está habilitada y existe un procedimiento formal para su control.	La auditoría de eventos del dispositivo de filtro de red está habilitada y existe un procedimiento informal para su control.	La auditoría de eventos del dispositivo de filtro de red está habilitada y no existe documentación sobre su control.	La auditoría de eventos del dispositivo de filtro de red no está habilitada.	**3**	
	Calificacion % de riesgo del punto 4					**J**

5 Seguridad de la Aplicación de Venta "Sistemas Propios"	OPTIMO	ADECUADO	REGULAR	DEFICIENTE		
5.1 Almacenamiento del número de tarjeta y datos personales	Todos los datos sensibles de los clientes se guardan utilizando herramientas estándares de encriptación por un tiempo máximo de 60 días.	Todos los datos sensibles de los clientes se guardan utilizando herramientas distintas a los estándares de encriptación por un tiempo máximo de 60 días	Algunos datos sensibles de los clientes no se encriptan y se guardan por un tiempo máximo de 60 días	Todos los datos sensibles de los clientes se guardan en Texto claro.	**5**	**SO SP, SO SA, BD, SP**
5.2 Depuración en archivos / Bases de Datos	La depuración de información crítica contenida en archivos/Bases de Datos, se efectua al nivel físico y lógico. Los mismos son reemplazados con datos nulos, para evitar su recuperación.	La depuración de información crítica contenida en archivos/Bases de Datos, se efectua al nivel físico y lógico.Sin efectuar reemplazo con datos nulos, que eviten su recuperación.	La depuración de información crítica contenida en archivos/Bases de Datos, se efectua al nivel lógico.	No se depura la información crítica contenida en archivos/Bases de Datos.	**5**	
5.3 Control de acceso a la aplicación	El acceso a las funciones de administración de la aplicación se encuentra restringido mediante perfiles de usuario	El acceso a las funciones de administración de la aplicación se encuentra restringido a usuarios sin perfil definido	El acceso a las funciones de administración de la aplicación se encuentra restringido mediante un solo usuario genérico.	No existe control de acceso a las funciones de administración de la aplicación.	**5**	
5.4 Información Impresa	Todos los impresos que contienen datos sensibles de los clientes se guardan en un área restringida con control de acceso que no permita su exposición.	Todos los impresos que contienen datos sensibles de los clientes se guardan en un área restringida.	Algunos impresos que contiene datos sensibles de los clientes se guardan en un área reservada.	Todos los impresos que contienen datos sensibles de los clientes no se guardan en lugares con acceso restringido.	**4**	
5.5 Cambio de versiones	Existen procedimientos formales que permitan controlar y habilitar una nueva versión de la aplicación de "Sistemas Propios" sin afectar la disponibilidad del mismo, con control histórico de versiones y reinstalaciones de versiones anteriores en caso de emergencias.	Existen procedimientos formales parcializados que permitan controlar y habilitar una nueva versión de la aplicación de "Sistemas Propios" sin afectar la disponibilidad del mismo, con control histórico de versiones , de reinstalaciones de versiones anteriores en caso de emergencias.	Existen procedimientos informales que permiten controlar y habilitar una nueva versión de la aplicación de "Sistemas Propios".	No existe documentación ni procedimientos informales que permitan controlar y habilitar una nueva versión de la aplicación de "Sistemas Propios".	**3**	**SP**
	Calificacion % de riesgo del punto 5					**K**

6 Monitoreo de red y administración de eventos	OPTIMO	ADECUADO	REGULAR	DEFICIENTE		
6.1 Monitoreo de red y configuración de alarmas	Cuentan con herramientas de detección , análisis y scanner, para detectar configuraciones que generen vulnerabilidades o actividades sospechosas tanto en la red como en los servidores	Cuentan con herramientas parciales de detección , análisis y scanner para detectar configuraciones que generen vulnerabilidades o actividades sospechosas tanto en la red como en los servidores	Generan análisis y scanner parciales en forma manual para detectar configuraciones que generen vulnerabilidades o actividades sospechosas.	No cuentan con herramientas ni procedimientos de monitoreo y generación de alarmas.	**5**	
6.2 Procedimiento de respuestas ante ataques	Cuenta con procedimientos formales de análisis, detección de ataques y respuestas previstas a los mismos	Cuenta con procedimientos formales e informales en forma parcial, de análisis, detección de ataques y respuestas previstas a los mismos	Cuentan con procedimientos informales de análisis de detección de ataques	No cuentan con documentación para el tratamiento de ataques	**3**	
	Calificacion % de riesgo del punto 6					**L**

7 Mecanismos de criptografía en la transmisión de datos	OPTIMO	ADECUADO	REGULAR	DEFICIENTE		
7.1 Transmisión de datos de clientes	Los datos sensibles de los clientes se transmiten entre los equipos utilizando VPN, o SSL (128 bits), etc , que permite la identificación y autenticación del equipo conectado.	Los datos sensibles de los clientes se transmiten entre los equipos utilizando SSL (menor que 128 bits), que permite la identificación y autenticación del equipo conectado.	Los datos sensibles de los clientes se transmiten entre equipos encriptados y no permiten identificar o autenticar el equipo conectado.	Los datos sensibles de los clientes se transmiten entre equipos en texto plano.	**5**	
7.2 Transmisión de datos de clientes entre el Comercio y terceras partes	Los canales de comunicación entre el comercio y terceras partes cuentan con mecanismos de autenticación de las partes intervinientes, privacidad, confidencialidad, integridad y No repudio de los datos transmitidos.	Los canales de comunicación entre el comercio y terceras partes cuentan con mecanismos de autenticación de las partes intervinientes, confidencialidad y No repudio de los datos transmitidos.	Los canales de comunicación entre el comercio y terceras partes cuentan con mecanismos de autenticación de las partes intervinientes y confidencialidad.	Los canales de comunicación entre el comercio y terceras partes no cuentan con mecanismos de autenticación de las partes intervinientes o confidencialidad.	**5**	
	Calificacion % de riesgo del punto 7					**M**
8 Control de Operatividad del Aplicativo "Sistemas Propios".	OPTIMO			DEFICIENTE		
8.1 Control de Skimming	Cumple la best practice			Cumple parcialmente o no cumple la best practice	**5**	
	Calificacion % de riesgo del punto 8.1					**N**
8.2 Proceso "Cierre de Lote"	Cumple la best practice			Cumple parcialmente o no cumple la best practice	**5**	
	Calificacion % de riesgo del punto 8.2					**O**
8.3 Código de Seguridad	Cumple la best practice			Cumple parcialmente o no cumple la best practice	**5**	
	Calificacion % de riesgo del punto 8.3					**P**
8.4 Fecha de vencimiento	Cumple la best practice			Cumple parcialmente o no cumple la best practice	**5**	
	Calificacion % de riesgo del punto 8.4					**Q**
8.5 Operatoria Off-Line	Cumple la best practice			Cumple parcialmente o no cumple la best practice	**5**	
	Calificacion % de riesgo del punto 8.5					**R**
8.6 Transacciones de anulaciones o devoluciones	Cumple la best practice			Cumple parcialmente o no cumple la best practice	**5**	
	Calificacion % de riesgo del punto 8.6					**S**
8.7 Informes de gestión, 8.8 Impresión de Tickets y 8.9 Ingreso de las operaciones	Cumple la best practice			Cumple parcialmente o no cumple la best practice	**5**	
	Calificacion % de riesgo del punto 8.7					**T**
8.10 Visualización de la información contenida en la tarjeta	Cumple la best practice			Cumple parcialmente o no cumple la best practice	**5**	

Calificacion % de riesgo del punto 8.10		U

Valor de la Calificación

Optimo	**0**
Adecuado	**1**
Regular	**2**
Deficiente	**3**

Componentes Informáticos Incluidos en esta Revisión

Componente Informático	Abreviatura
SO del Equipo Input de datos críticos	SO WS
SO del Filtro de Red	SO F
SO del server de pago	SO SP
SO del Server de aplicación	SO SA
BD del Server de aplicación	BD
Sistema Input de datos de la tarjeta	SWS
Sistema de pago	SP
Sistema del Filtro de Red	SF

A los efectos de una correcta interpretación del resultado del trabajo realizado, se requiere de la Consultora la confección de un Informe detallado que contenga como mínimo lo siguiente:

ALCANCE

- Describir la lista del personal entrevistado durante el desarrollo del Plan de Revisión.
- Describir la lista de los equipos informáticos y dispositivos de comunicación, alcanzados por el Plan de Revisión, indicando, de ser posible, los componentes informáticos revisados, como: marca y modelo del hardware, sistema operativo, bases de datos, software de base, sistemas aplicativos, herramientas de seguridad, etc.
- Describir el "Sistema Propio", indicando: nombre del software, proveedor o área de la empresa responsable del mantenimiento del sistema, lenguaje de programación, base de datos o tipos de archivos que utiliza para el resguardo de la información confidencial, sistema operativo que lo soporta, marca y modelo del equipo donde se procesa este sistema.
- Representar mediante un diagrama topológico, el entorno de pago del "Sistema Propio", indicando todos los equipos informáticos y dispositivos de comunicación, incluidos en dicho entorno y relacionados con la operatoria de tarjetas de débito y/o crédito. Asimismo, este diagrama deberá describir los lugares físicos (razón social, dirección y teléfonos) donde están instalados estos equipos informáticos o dispositivos de comunicación.

RESULTADO DEL PLAN DE REVISION

- **Observaciones**

Describir en detalle las vulnerabilidades detectadas de acuerdo al procedimiento indicado en el Plan de Revisión de Seguridad Informática.

Las vulnerabilidades deberán describirse por cada tarea de verificación o análisis o relevamiento que se indica en el Plan descripto precedentemente.

- **Impacto**

  Describir los posibles riesgos derivados de las observaciones detalladas, a los efectos que el Cliente conozca los probables hechos y perjuicios a los que podría enfrentarse de no corregir dichas observaciones.

- **Recomendaciones**

  Describir las recomendaciones de la Consultora para corregir cada observación.

- **Informe del cliente**

El Cliente describirá en nota adjunta, una manifestación sobre el resultado del Plan de Revisión donde podrá hacer constar las mejoras a realizar y los tiempos previstos para eliminar las principales observaciones.

METRICA DEL PLAN DE REVISION

Analizar y resolver, la calificación porcentual de riesgo de cada ítem, que se indica en las métricas asociadas al Plan de Revisión.

Control de Cambios

Versión	Fecha	Responsable	Descripción
1.0	09/05/11	Implementaciones	✓Documento Simplificado modulo base.
1.1	02/10/12	Damian Ahlin	✓Corrección y verificación del Campo63
1.2	02/11/12	Roberto Mazzieri	✓ Agregado -Mensaje Promocional_Cap. H
1.3	12/04/13	Roberto Mazzieri	✓ Agregado –Mensajeria por TCP
1.4	05/07/13	Roberto Mazzieri	✓ Se agrega el envío del campo 59 para reversos de maestro.