PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

FACULTAD DE INGENIERIA

ESCUELA DE SISTEMAS

PROPUESTA DE CUMPLIMIENTO DE LAS EXIGENCIAS DEL ESTÁNDAR ISO 8583 DE 1993 PARA LA MIGRACIÓN DESDE EL ESTÁNDAR ISO 8583 DE 1987 EN LAS INSTITUCIONES FINANCIERAS; Y, REQUERIMIENTOS PARA LA CERTIFICACIÓN PCI DSS DE BANRED, PARA ASEGURAR LA CALIDAD TRANSACCIONAL BANCARIA.

JUAN PABLO BAQUERO JIMENEZ

RODRIGO DAVID MURILLO ZUMARRAGA

"Trabajo previo a la obtención del Título de Ingeniero en Sistemas"

QUITO, 2014

Dedicatoria

Con todo mi cariño y mi amor para las personas que me apoyaron durante todo este trayecto. Doy gracias a Dios por haberme dado fuerza y valor para culminar esta etapa de mi vida.

A mis padres que me han dado su apoyo incondicional, consejos, amor y el ejemplo para seguir mejorando cada día.

Agradezco a mi hermana Sarita y a mi abuelita Mericita que estuvieron conmigo durante este arduo camino dándome una mano cuando la necesitaba.

David Murillo

Este trabajo va dedicado a toda mi familia y amigos que me estuvieron apoyondo en todo este proceso parea poder cumplir una de las tantas metas planteadas a lo largo de mi vida.

Juan Pablo Baquero

Índice

Capítulo I: Requerimientos del Estándar ISO 8583 de 1987

1.1 Introducción

El estándar ISO 8583 creado por la Organización Internacional de Normalización (ISO), se ocupa de regularizar las transacciones electrónicas con mensajes originados en una tarjeta de crédito, enfocándose en los mensajes de intercambio.

El modelo ISO 8583 determina un formato en los mensajes de intercambio de las tarjetas y un flujo de comunicación para los diferentes sistemas con los que se puedan realizar este tipo de transacciones. En la mayor parte de las operaciones efectuadas por un cajero automático, como también en el uso de una tarjeta para cumplir con el pago de un consumo en un local se usa la norma ISO 8583 en algún punto de la cadena de comunicación con la institución financiera a la cual el cajero automático o la tarjeta pertenezca.

Una transacción es un mensaje que contiene información detallada de: el número de cuenta, la terminal, el importe y además un conjunto de datos que pueden ser agregados por los sistemas intervinientes. Una vez emitida la transacción el sistema podrá autorizar o rechazar dicha transacción generando un mensaje de respuesta a la terminal. Las transacciones incluyen operaciones como: depósitos, compras, retiros, reversos, pagos, transferencias entre cuentas.

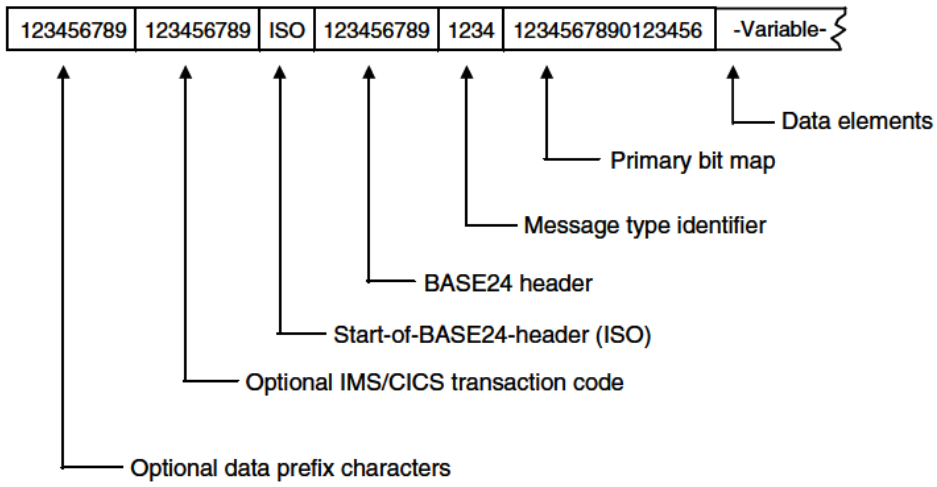
Cada sistema ajusta el estándar 8583 a sus propias necesidades modificando los campos previamente nombrados. La posición de los campos varía de acuerdo a la versión del estándar utilizado.

Los mensajes que se rigen bajo esta norma constan de las siguientes partes: indicador de tipo de mensaje, uno o más bitmaps, indicando que elementos están presentes en el mensaje y los campos del mensaje.

1.2 Partes de la mensajería

Los mensajes están conformados en de los siguientes componentes, algunos de ellos son obligatorios mientras que otros son opcionales y se encuentran estructurados en el siguiente gráfico:

Ilustración 1: Partes de la mensajería



Fuente: BASE24_External_Message, ACI Worldwide, Inc
Elaborado por: ACI Worldwide, Inc

1.2.1 Prefijo de caracteres de datos

El software que manejan diferentes tipos de switch transaccionales, permite a los servidores definir ciertos caracteres al inicio del mensaje que van a recibir de dicho software. Estos caracteres son llamados prefijos, son opcionales y solo están incluidos en el mensaje si son especificados por el centro de procesamiento de datos en el archivo de configuración del servidor. Un servidor puede especificar hasta nueve caracteres que preceden sus mensajes. Estos prefijos son predeterminados.

1.2.2 IMS o CISC códigos de transacción

Para servidores IMS[1] o CISC[2] que usan códigos de transacción diferentes a los usados por el software de un switch transaccional se puede incluir códigos de transacción equivalentes en el mensaje.

1.2.3 Cabecera (ISO)

El software del switch transaccional requiere de la palabra ISO como su indicador de inicio de la cabecera que utiliza el software para los mensajes. Para mensajes enviados siempre están presentes, para mensajes recibidos siempre se requires.

1.2.4 Cabecera de mensaje

La cabecera es requerida para todos los mensajes, tiene que estar inmediatamente después de la cabacera ISO. La cabecera de mensaje tiene nueve posiciones que serán detalladas en la siguiente tabla.

Tabla 1: Posiciones de la cabecera del mensaje

Posición	Longitud	Nombre	Descripción
1-2	2	Indicador de Producto	Indica el producto con el que está asociado el mensaje.
3-4	2	Numero de versión	Indica la versión del software del switch transaccional.
5-7	3	Estado	Indica si existió un problema con la interpretación del mensaje.
8	1	Generador de Códigos	Indica la entidad que introdujo la transacción.
9	1	Código de Respuesta	Indica la entidad que creó la respuesta.

Fuente: BASE24 External Message
Elaborada por: Juan Pablo Baquero, David Murillo

[1] IMS: Sistema multimedia de IP
[2] CICS: Sistema de control de información de clientes

1.2.5 Tipo de mensaje

Es un código de 4 dígitos que identifica la función general del mensaje. Este es necesario en todos los mensajes.

- Mensajes de Autorización
  - ✓ Mensaje de solicitud de autorización (0100): es el que exige la aprobación o la garantía para que la transacción se efectúe.
  - ✓ Mensaje de respuesta de la solicitud de autorización (0110): este tipo de mensaje se espera a cambio del mensaje de solicitud de autorización aprobando o negando el pedido.
  - ✓ Mensaje de aviso de autorización (0120): este mensaje informa de una operación autorizada en nombre del emisor de la tarjeta.
  - ✓ Mensaje de repetición de advertencia (0121): este mensaje es idéntico al mensaje de aviso de autorización, excepto que indica al receptor que se trata de un posible mensaje duplicado. Un mensaje 0121 se utiliza cuando no se recibió el mensaje 0120.
  - ✓ Mensaje de respuesta del aviso de autorización: este mensaje reconoce la recepción de un mensaje 0120 o de un mensaje 0121.
- Mensajes de Transacciones Financieras
  - ✓ Mensaje de solicitud de transacción financiera (0200): este mensaje solicita la aprobación para una transacción, si es aprobada, inmediatamente puede ser ejecutada a la cuenta del cliente para propósitos de facturación o declaración.
  - ✓ Mensaje de respuesta para la solicitud de una transacción financiera (0210): este tipo de mensaje se espera a cambio del mensaje de solicitud de transacción financiera aprobando o negando el pedido.

- ✓ Mensaje de aviso de transacción financiera (0220): este mensaje informa de una operación financiera previamente completada.

- ✓ Mensaje de repetición de advertencia para una transacción financiera (0221): este mensaje es idéntico al mensaje de aviso de autorización para una transacción financiera, excepto que indica al receptor que se trata de un posible mensaje duplicado. Un mensaje 0221 se utiliza cuando no se recibió el mensaje 0220.

- ✓ Mensaje de respuesta del aviso de una transacción financiera (0230): este mensaje reconoce la recepción de un mensaje 0220 o de un mensaje 0221.

- Solicitud de actualización de archivos

  - ✓ Mensaje de solicitud de actualización de archivos (0300): este mensaje contiene instrucciones para investigar, agregar, cambiar, borrar o reemplazar un archivo o un registro.

  - ✓ Mensaje de respuesta de una solicitud de actualización de archivos (0310): este tipo de mensaje se espera a cambio del mensaje de solicitud de actualización de archivos aprobando o negando el pedido.

- Mensaje de advertencia de Reversión

  - ✓ Mensaje de reversión (0420): este mensaje revierte una transacción o autorización anterior.

  - ✓ Mensaje de repetición de advertencia de reversión (0421): este mensaje es idéntico al mensaje 0420, excepto que indica al receptor que se trata de un posible mensaje duplicado. Un mensaje 0421 se utiliza cuando no se recibió el mensaje 0420.

- ✓ Mensaje de respuesta a una reversión (0430): este mensaje reconoce un mensaje 0420 o un 0421.

- Mensaje de Administración de Red

  - ✓ Mensaje de solicitud de administración de red (0800): este mensaje se utiliza para enviar un "echo-test" (prueba), la gestión dinámica de claves, inicio y cierre de sesión de mensajes.

  - ✓ Mensaje de respuesta para la solicitud de una administración de red (0810): este mensaje es en respuesta a un mensaje 0800.

- Mensajes de Impresión

  - ✓ Mensaje de solicitud de impresión (0205): Este mensaje solicita información adicional para una impresión en progreso.

  - ✓ Mensaje de respuesta de impresión (0215): Este tipo de mensaje retorna información en respuesta al mensaje 0205, el cual puede tener el formato del mensaje 0200 (mensaje de solicitud de transacción financiera) o un mensaje de solicitud de impresión (0205).

- Consulta de archivos y actualización de mensajes

  - ✓ Mensaje de solicitud de actualización de mensaje/Consulta de archivos (0300): Este mensaje contiene una consulta o actualización para un registro determinado.

  - ✓ Mensaje de respuesta de actualización de mensaje/Consulta de archivos (0310): Este mensaje retorna información en respuesta a un mensaje 0300 aprobando o negando la solicitud previa.

- ✓ Mensaje de advertencia sobre una consulta/Actualización de archivos (0320): Este mensaje advierte de una actualización previamente completada de un archivo.

- ✓ Mensaje de repetición advertencia sobre una consulta/Actualización de archivos (0321): Este mensaje es similar al mensaje 0320, excepto que indica al receptor que posiblemente es un mensaje duplicado. Un mensaje 0321 se utiliza cuando un mensaje 0320 nunca fue recibido.

- ✓ Mensaje de respuesta a una advertencia sobre una consulta/Actualización de archivos (0330): Este mensaje reconoce la recepción de un mensaje 0320 (Mensaje de advertencia sobre una consulta/Actualización de archivos) o un mensaje 0321 (Mensaje de repetición advertencia sobre una consulta/Actualización de archivos)

- Mensajes de Reversión

  - ✓ Mensaje de solicitud de reversión por parte del emisor de la tarjeta (0402): Este mensaje revierte, parcial o totalmente una autorización o transacción previamente efectuada.

  - ✓ Mensaje de respuesta a solicitud de reversión por parte del emisor de la tarjeta (0412): Este mensaje reconoce la recepción y disposición de un mensaje 0402 (Mensaje de solicitud de reversión por parte del emisor de la tarjeta).

- Mensajes de solicitud de reconciliación

  - ✓ Mensaje de solicitud de reconciliación (0500): Solicita una confirmación de los totales adquirente con el fin de obtener un acuerdo entre las partes.

- ✓ Mensaje de respuesta para solicitud de reconciliación (0510): Este mensaje responde a un mensaje 0500 con el fin de indicar la disposición o una respuesta a ese mensaje.

- ✓ Mensaje de advertencia de reconciliación (0520): Informa de los totales para obtener un acuerdo entre las partes.

- ✓ Mensaje de repetición de advertencia de reconciliación (0521): Este mensaje es similar al mensaje 0520, excepto que indica al receptor que posiblemente es un mensaje duplicado. Un mensaje 0521 se utiliza cuando un mensaje 0520 nunca fue recibido.

- ✓ Mensaje de respuesta a advertencia de reconciliación (0530): Este mensaje reconoce la recepción de un mensaje 0520 (Mensaje de advertencia de reconciliación) o de un mensaje 0521.

- Mensajes de administración

  - ✓ Mensaje de solicitud administrativa (0600): Este mensaje permite iniciar y cerrar sesión en cualquier terminal.

  - ✓ Mensaje de respuesta a solicitud administrativa (0610): Este mensaje sirve en respuesta a un mensaje 0600 para indicar la disposición de la terminal (iniciar o cerrar sesión).

  - ✓ Mensaje de advertencia administrativa (0620): Este mensaje advierte sobre el inicio o cierre de sesión en una terminal.

  - ✓ Mensaje de repetición de advertencia administrativa (0621): Este mensaje es idéntico al mensaje 0620, excepto que indica al receptor que posiblemente es un mensaje duplicado. Un mensaje 0621 se utiliza cuando un mensaje 0620 nunca fue recibido.

- ✓ Mensaje de respuesta a advertencia administrativa (0630): Este mensaje reconoce la recepción de un mensaje 0620 (Mensaje de advertencia administrativa) o de un mensaje 0621 (Mensaje de repetición de advertencia administrativa).

1.2.6 Bit map primario

Es un campo de 16 posiciones requerido en todos los mensajes. Representa 64 bits de datos utilizados para identificar la presencia (denotado por 1) o ausencia (denotado por 0) de los primeros 64 elementos de datos en el mensaje. 64 bits son convertidos en 16 bytes de datos de pantalla utilizando los equivalentes hexadecimales.

1.2.7 Elementos de datos

Los elementos de datos son campos que contienen la información esencial sobre una transacción. En la norma ISO 8583 de 1997 existen 128 campos definidos que se explicaran en la siguiente tabla. Cada uno de estos campos denotan un significado y formato especifico, sin embargo la norma ISO 8583 agrega algunos campos que son fundamentales para determinados sistemas o países. Dichos campos son implementados de acuerdo a las necesidades.

Tabla 2: Campos de datos

N	Nombre	Formato/Longitud	Descripción
P1	Secundary bit map	AN 16	Este bit map secundario define la presencia o la ausencia de elementos de datos desde el 65 hasta el 128
P2	Primary Acount Number	AN 19 N 19	Contiene el número primario de la cuenta de ahorros del portador de la tarjeta involucrado en la transacción o el pedido actualizado que se está procesando.

Tabla 3: Campos de datos

P3	Processing Code	AN 6 N 6	Contiene una serie de dígitos usados para describir el efecto de la transacción en la cuenta del cliente y en las cuentas afectadas.
P4	Transaction Amount	N 12	No es utilizado por la ISO 8583:1987.
P5	Settlement Amount	N 12	No es utilizado por la ISO 8583:1987.
P6	Cardholder Billing Amount	N 12	No es utilizado por la ISO 8583:1987.
P7	Transmission Date and Time	N10 (MMDDhhmmss)	Contiene el tiempo del mensaje en el que este es iniciado por el originador de mensajes. Este tiempo es generado para cada mensaje enviado.
P8	Cardholder Billing Free Amount	N 8	No es utilizado por la ISO 8583:1987
P9	Settlement Conversion Rate	N 8	No es utilizado por la ISO 8583:1987
P10	Cardholder Billing Conversion Rate	N 8	No es utilizado por la ISO 8583:1987

Tabla 4: Campos de datos

P11	Systems Trade Audit Number	N 6	Contiene un número que tiene que ser fijado por un emisor de mensajes y recibido por un receptor de mensajes. Se utiliza para hacer coincidir las respuestas a los mensajes originales y no está destinado a seguir siendo la misma a lo largo de la vida de una transacción.
P12	Local Transaction Time	N 6	Contiene la hora local a la que la transacción comenzó en la ubicación del aceptador de la tarjeta.
P13	Local Transaction Date	N 4	Contiene el día y el mes local en los cuales la transacción empezó.
P14	Expiration Date	N 4	Contiene el día y el año en los cuales la tarjeta expira.
P15	Settlement Date	N 4	Es usado en el software del switch transaccional para mantener la fecha de liquidación de intercambio. Esa fecha es cuando la transacción se liquida por el intercambio, si el intercambio está involucrado en la transacción.
P16	Conversion Date	N 4 (MMDD)	No es utilizado por la ISO 8583:1987
P17	Capture Date	N 4	Contiene el día y el mes en los cuales el software del switch transaccional procesó la transacción.

Tabla 5: Campos de datos

P18	Merchant Type	N 4	Contiene el código del Estándar Industrial de Clasificación[3] del detalle involucrado en la transacción.
P19	Acquiring Institution Country Code	N 3	No es utilizado por la ISO 8583:1987
P20	Country Code Primary Account Number Extended	N 3	No es utilizado por la ISO 8583:1987
P21	Forwarding Institution Country Code	N 3	No es utilizado por la ISO 8583:1987
P22	Point of Service Entry Mode	N 3	Es un campo que contiene dos códigos. El primero es uno de dos dígitos que indica el método por el cual el número de cuenta fue ingresado al sistema. El segundo es uno de un solo dígito que indica la capacidad de entrada disponible en el punto de servicio.

[3] Estándar Industrial de Clasificación: Sistema de las Naciones Unidas para clasificación de datos económicos.

Tabla 6: Campos de datos

P23	Car Sequence Number	N 3	Contiene el numero del miembro en el software del switch transaccional para la tarjeta que inició la transacción.
P24	Network International Identifier	N 3	No es utilizado por la ISO 8583:1987
P25	Point of Service Condition Code	N 2	Contiene un código que identifica la condición bajo la cual la transacción está en el punto de servicio.
P26	Point of Service PIN Capture Code	N 2	No es utilizado por la ISO 8583:1987
P27	Authorization Identification Response	N 1	Contiene la longitud del código de autorización.
P28	Transaction Fee Amount	X + N 8	Contiene la cantidad de un cargo (de pago o incentivo) evaluada en una transacción de cajero automático.
P29	Settlement Fee Amount	X + N 8	No es utilizado por la ISO 8583:1987.
P30	Transaction Processing Fee Amount	X + N 8	No es utilizado por la ISO 8583:1987.

Tabla 7: Campos de datos

P31	Settlement Processing Fee Amount	X + N 8	No es utilizado por la ISO 8583:1987.
P32	Acquiring Institution Identification Code	N..11	Contiene un código que identifica a la entidad adquirente de la operación, o su agente. La entidad adquirente puede ser diferente del que acepta la tarjeta.
P33	Forwarding Institution Identification Code	N..11	Contiene un código que identifica el proveedor del servicio en el software del switch transaccional.
P34	Extended Primary Account Number	AN..28	Contiene un número que identifica la cuenta del cliente o la relación que existe en la transacción o solicitud de actualización que se está procesando.
P35	Track 2 Data	ANS..37	Es la información codificada en la cinta magnética ubicada en la parte de atrás de la tarjeta.
P36	Track 3 Data	ANS..104	Es la información codificada en la cinta magnética ubicada de la parte de atrás de la tarjeta.
P37	Retrieval Reference Number	AN 12	Contiene un número asignado por el iniciador del mensaje para identificar de forma única una transacción. Este número se mantendrá para todos los mensajes en toda la vida de una transacción.

Tabla 8: Campos de datos

P38	Authorization Identification Response	AN 6	Contiene un número de identificación asignado por la respuesta de la institución que autoriza la transacción.
P39	Response Code	AN 2	Contiene un código que indica la disposición de un mensaje.
P40	Service Restriction Code	AN 3	No es utilizado por la ISO 8583:1987.
P41	Card Acceptor Terminal Identification	ANS 16	Contiene un código único que identifica el terminal de la localización del autorizador de la tarjeta.
P42	Card Acceptor Identification Code	ANS 15	Contiene un código utilizado para identificar el titular de la tarjeta en una transacción.
P43	Card Acceptor Name/Location	ANS 40	Contiene el nombre y la locación del titular de la tarjeta
P44	Additional Response Data	ANS 27	Es utilizado para poner información adicional.
P45	Track 1 Data	ANS..76	Es la información codificada en la cinta magnética ubicada de la parte de atrás de la tarjeta.

Tabla 9: Campos de datos

P46	ISO Additional Data	ANS 999	No es utilizado por la ISO 8583:1987.
P47	National Additional Data	ANS 999	No es utilizado por la ISO 8583:1987.
P48	atm Additional Data	ANS 47	Es utilizado para poner información adicional
P49	Transaction Currency Code	N 3	Contiene un código que define la moneda de la ubicación de origen de la transacción.
P50	Settlement Currency Code	N 3	No es utilizado por la ISO 8583:1987.
P51	Cardholder Billing Currency Code	N 3	No es utilizado por la ISO 8583:1987.
P52	Personal Identification Number (PIN) Data	AN 16	Contiene un número asignado a un cliente para identificarlo en el punto del servicio.
P53	Security Related Control Information	N 16	Contiene datos de gestión de claves dinámicas.

Tabla 10: Campos de datos

P54	Additional Amounts	ANS 15	Contiene la cantidad del reembolso en efectivo de los depósitos y adquisiciones cuando se devuelve dinero al cliente.
P55	Through P-56 ISO Reserved	ANS..99	No es utilizado por la ISO 8583:1987.
P56			No es utilizado por la ISO 8583:1987.
P57	National Reserved	ANS..99	No es utilizado por la ISO 8583:1987.
P58	Financial Token	ANS 135	Contiene cantidades y otros campos necesarios para el procesamiento de las transacciones financieras.
P59	CAF Update Token	ANS 17	Contiene los capos requeridos para actualizar el estado de la tarjeta en el CAF[4].
P60	Terminal Data	ANS 15	Lleva la información del terminal requerida para el procesamiento del cajero.
P61	Card Issuer and Authorizer	ANS 16	Contiene información que identifica de forma única una entidad financiera.
P62	Postal Code	ANS 13	Lleva el código postal de la terminal de origen de la transacción.
P63	PIN Offset	ANS 19	Se utiliza para realizar un desplazamiento que soporta la capacidad del software del cajero automático para permitir a los clientes seleccionar sus propios pines.

[4] CAF: Banco de desarrollo de América Latina

Tabla 11: Campos de datos

P64	Primary Message Authentication Code	AN 16	Contiene el código de autorización MAC
S65	Extended Bit Map	No definido	No es utilizado por la ISO 8583:1987
S66	Settlement Code	N 1	No es utilizado por la ISO 8583:1987
S67	Extended Payment Code	N 2	No es utilizado por la ISO 8583:1987
S68	Receiving Institution Country Code	N 3	No es utilizado por la ISO 8583:1987
S69	Settlement Institution Country Code	N 3	No es utilizado por la ISO 8583:1987

Tabla 12: Campos de datos

S70	Network Management Information Code	N 3	Contiene código que se utiliza para administrar el estado de tramitación en línea entre el software del switch y un sistema host. Este código identifica el objetivo de un mensaje de solicitud de administración de red. Los siguientes códigos son los más comunes: 001: Iniciar sesión 002: Cerrar sesión 161: Cambiar contraseña 162: Nueva contraseña 163: Contraseña repetida 164: Verificar contraseña 301: Prueba Este elemento de dato es mandatorio para los mensajes 0800 y 0810
S71	Message Number	N 4	No es utilizado por la ISO 8583:1987
S72	Message Number Last	N 4	No es utilizado por la ISO 8583:1987
S73	Action Date	N 6 (YYMMDD)	Contiene la fecha de pago efectivo de la transacción.
S74	Number Credits	N 10	No es utilizado por la ISO 8583:1987
S75	Reversal Number Credits	N 10	No es utilizado por la ISO 8583:1987
S76	Number Debits	N 10	No es utilizado por la ISO 8583:1987

Tabla 13: Campos de datos

S77	Reversal Number Debits	N 10	No es utilizado por la ISO 8583:1987
S78	Number Transfer	N 10	No es utilizado por la ISO 8583:1987
S79	Reversal Number Transfer	N 10	No es utilizado por la ISO 8583:1987
S80	Number Inquiries	N 10	No es utilizado por la ISO 8583:1987
S81	Number Authorizations	N 10	No es utilizado por la ISO 8583:1987
S82	Processing Fee Amount Credits	N 12	No es utilizado por la ISO 8583:1987
S83	Transaction Fee Amount Credits	N 12	No es utilizado por la ISO 8583:1987
S84	Processing Fee Amount Debits	N 12	No es utilizado por la ISO 8583:1987
S85	Transaction Fee Amount Debits	N 12	No es utilizado por la ISO 8583:1987
S86	Amount Credits	N 16	No es utilizado por la ISO 8583:1987
S87	Reversal Amount Credits	N 16	No es utilizado por la ISO 8583:1987

Tabla 14: Campos de datos

S88	Amount Debits	N 16	No es utilizado por la ISO 8583:1987
S89	Reversal Amount Debits	N 16	No es utilizado por la ISO 8583:1987
S90	Original Data Elements	N 42	Contiene un grupo de 5 sub elementos incluidos en un mensaje de revocación o de ajuste. En el caso de ajuste, los primeros dos dígitos del elemento pueden ser: 02: Ajuste de debito 14: Ajuste de Adelantos en Efectivo 19: Compra con ajuste de devolución de dinero 22: Ajuste de crédito
S91	File Update Code	AN 1	Contiene código que identifica el tipo de archivo que va a ser actualizado. Los siguientes valores pueden ser fijados: 1: Agregar un registro 2: Reemplazar un registro 3: Eliminar un registro 5: Consultar un registro 9: Incrementar un registro Este campo es mandatorio para todos los mensajes de tipo 0300 y 0310
S92	File Security Code	AN 2	No es utilizado por la ISO 8583:1987
S93	Response Indicator	AN 5	No es utilizado por la ISO 8583:1987
S94	Service Indicator	AN 7	No es utilizado por la ISO 8583:1987
S95	Replacement Amounts	AN 42	Contiene el monto de la nueva transaccion.

Tabla 15: Campos de datos

S96	Message Security Code	AN 16	No es utilizado por la ISO 8583:1987
S97	Net Settlement Amount	X+N 16	No es utilizado por la ISO 8583:1987
S98	Payee	ANS 25	Contiene el nombre de la tercera parte beneficiaria en una transacción financiera en el código de procesamiento que indica un pago.
S99	Settlement Institution Identification Code	N ..11	No es utilizado por la ISO 8583:1987
S100	Receiving Institution Identification Code	N ..11	Contiene código que identifica la institución que recibe un mensaje de solicitud.
S101	File Name	ANS 4	Contiene código que identifica el tipo de archivo o la sentencia SQL de la tabla que está siendo actualizada. Este campo es mandatorio para todos los mensajes 0300 y 0310
S102	Account Identification 1	ANS ..28	Contiene una serie de dígitos utilizados para identificar la cuenta de un cliente determinado.
S103	Account Identification 2	ANS ..28	Contiene una serie de dígitos utilizados para identificar la cuenta de un cliente determinado.
S104	Transaction Description	ANS 63	Contiene el nombre y la información de la cuenta para el proveedor. Este campo es condicional para los mensajes 0110, 0120, 0121, 0200, 0210, 0220, 0221, 0420 y 0421.
S105	ISO Reserved	ANS ..999	

Tabla 16: Campos de datos

S106	ISO Reserved	ANS ..999	
S107	ISO Reserved	ANS ..999	
S108	ISO Reserved	ANS ..999	
S109	ISO Reserved	ANS ..999	
S110	ISO Reserved	ANS ..999	
S111	ISO Reserved	ANS ..999	
S112	From host maintenance Enhanced Preauthorized Hold Information	ANS 105	Este campo es utilizado cuando existen más de 9 ocurrencias de pre autorizaciones fijados en mensajes de entrada o salida
S113	Override Token	ANS ..157	Contiene los campos requeridos para sobrescribir una transacción. Es condicional para los mensajes 0210 y 0310.
S114	from host maintenance Automated Hot Card Update Information	ANS ..276	Contiene la información utilizada para dar formato a una tarjeta de mensaje de actualización de estado de (0300) que se envía a una interfaz de intercambio.

Tabla 17: Campos de datos

S114	from host maintenance Application File and Table Information	AN ..429 / ANS ..276	Contiene información para los datos de servicio al cliente o actualizaciones automáticas de tarjetas.
S114	WHFF Inquiry Token— Part 1	ANS ..429	Contiene información acerca de las advertencias o depósitos relacionado con una cuenta o cuentas que participan en la transacción. Este dato es condicional para mensajes 0210, 0300, 0310, 0320, 0321 y 0330
S115	WHFF Inquiry Token— Part 2	ANS 389	Contiene información acerca de las advertencias o depósitos relacionado con una cuenta o cuentas que participan en la transacción. Este dato es condicional para mensajes 0210, 0300, 0310, 0320, 0321 y 0330.
S115	from host maintenance CAF and PBF Base User Information	ANS 153	contiene campos de usuario reservados para futuras mejoras del producto, las futuras mejoras regionales y futuras modificaciones de software a medida que sean realizados en el archivo de autorización titular o archivo saldo positivo.
S116	WHFF Inquiry Token— Part 3	ANS 389	Contiene información acerca de las advertencias o depósitos relacionado con una cuenta o cuentas que participan en la transacción. Este dato es condicional para mensajes 0210, 0300, 0310, 0320, 0321 y 0330
S116	from host maintenance CAF Non– Currency Dispense	ANS 155	Contiene la información requerida para la actualización de un segmento del archivo de autorización del usuario.

Tabla 18: Campos de datos

S117	PBF Update Token	ANS 7	Contiene los campos necesarios para actualizar el estado de su cuenta.
S117	from host maintenance CAF EMV	ANS 32	Contiene la información necesaria para actualizar la Europay, MasterCard y Visa.
S118	from host maintenance CAF and PBF Data	ANS 52 / ANS 71	Contiene la información necesaria para actualizar el segmento preferido de transacciones del archivo de autorización titular.
S118	SPF Update Token	ANS 103	Contiene la información necesaria para añadir o eliminar registros en el SPF[5].
S119	from host maintenance Self-Service Banking Check Information	ANS 67 / ANS 13	Contiene información utilizada para la consulta o actualización del servicio de banca.
S119	WHFF Update Token	ANS 83	Contiene los campos necesarios para agregar o eliminar registros.
S120	Key Management	ANS 9	Contiene los dígitos de control de intercambio de claves. Este dato es condicional para mensajes de administración de red.
S121	Terminal Address-Branch-Region	ANS 36	Contiene la información para el terminal involucrado en la transacción.

[5] SPF: es una protección contra la falsificación de direcciones en el envío de correo electrónico

Tabla 19: Campos de datos

S122	Card Issuer Identification Code	ANS 14	Contiene un valor que identifica la institución que emitió la tarjeta que está involucrado en la transacción. Este valor se utiliza sólo cuando el emisor de la tarjeta es diferente a la institución receptora y el software del switch no tiene conocimiento de la diferencia
S123	Deposit Credit Amount	N 15	Contiene la cantidad que se añade al saldo disponible para el titular de la tarjeta como resultado de una operación de depósito. Este dato es condicional para mensajes 0210, 0220, 0221, 0420 y 0421. Si la transacción es un depósito, es necesario este dato, de lo contrario, no se utiliza.
S124	Depository Type	ANS 4	Contiene código que se utiliza para las transacciones que requieren un depositante. Este dato es condicional en mensajes 0200, 0210, 0220, 0221, 0420 y 0421, y sólo es necesaria si la transacción requiere el uso de un depositante (depósito, el pago adjunto, el mensaje de la institución).
S125	Account Indicator/Statement Print Data	ANS 4 / ANS 375	Contiene un valor que se utiliza en los mensajes de salida para indicar la cuenta o cuentas que participan en una transacción de dos lados (transferencia o pago de). Los valores son los siguientes: 0: Se procesa la cuenta del emisor y del receptor 1: Se procesa la cuenta emisor 2: Se procesa la cuenta del receptor
S126	Additional Data	ANS ..800	Contiene información adicional dentro del mensaje.
S127	User Data	ANS ..200	Contiene información definida por el usuario que el software del switch puede llevar en su mensaje interno, pero no reconoce y no se utilizará para el procesamiento. Este elemento de datos está disponible para todos los mensajes.

Tabla 20: Campos de datos

S128	Secondary Message Authentication Code	AN 16	Contiene código de autenticación para el mensaje, sujeto a las siguientes condiciones: • La autenticación de mensajes se ha configurado mediante el archivo de clave • Este elemento de datos se especifica como condicional en el archivo de mensajes externo. • El mensaje contiene al menos un elemento de datos secundarios

Fuente: Base 24 External Message
Elaborada por: Juan Pablo Baquero, David Murillo
Traducida por: Juan Pablo Baquero, David Murillo

1.3. Ventajas y Desventajas

1.3.1 Ventajas

- Facilidad de mantenimiento: Cuando se aplica la norma ISO 8583 de 1987 a un software se puede medir la facilidad y la eficacia de las transacciones financieras así como también los procesos que estas conllevan.

- Accesibilidad: La norma ISO 8583 de 1987 facilita tanto a los usuarios como a los administradores de una aplicación transaccional poder acceder con comodidad a los datos involucrados en cualquier procedimiento que se efectué.

- Compatibilidad: Se refiere al hecho de garantizar la posibilidad de que la norma ISO 8583 de 1987 sea aplicada en cualquier plataforma o cualquier dispositivo de navegación.

- Flexibilidad: Se refiere a que la norma puede adaptarse a las necesidades de la institución financiera, utilizando las bases esenciales para cumplir con el cometido.

- Interoperabilidad: La norma permite intercambiar y mezclar contenido de múltiples fuentes, se puede utilizar en distintos sistemas con el propósito de plantear una comunicación para el intercambio de información.

- Reusabilidad: El contenido de la norma puede ser agrupado, desagrupado y reutilizado dependiendo de los requerimientos de la institución financiera.

- Gestionabilidad: La norma permite obtener y trazar la información adecuada sobre las transacciones financieras, los procedimientos y datos sobre el usuario.

- Escalabilidad: Las tecnologías que se manejan dentro de la institución financiera tienen la habilidad de configurarse con el fin de aumentar sus funcionalidades basándose en la norma para dar un mejor servicio a los usuarios.

1.3.2 Desventajas

- Cambios de versión: Al existir una nueva versión de la norma en la que los cambios sean drásticos y puedan afectar al sistema de la institución financiera en donde es aplicada no sería factible o el proceso de migración demandaría de esfuerzo desperdiciando asi tiempo y dinero para la organización.

1.4 Usos y Aplicaciones

En cualquiera de los casos que se vaya a utilizar una tarjeta de crédito, de debito, o para realizar un retiro en un cajero automático la información que contiene la transacción que se realiza en este proceso es enviada de un sistema hacia otro. Por ejemplo una compra efectuada en una tienda particular puede ser procesada a través de una terminal, hacia uno o más sistemas conectados mediante una red, con el fin de notificar al banco de la cuenta del cliente de que esta transacción es solicitada. La transacción contiene información sobre el tipo de transacción, el uso de la tarjeta, el comerciante, el monto de la transacción, información de seguridad, entre otros. La respuesta a esta solicitud, autorizando o rechazando la transacción, debe ser retornada por la misma ruta hacia la terminal.

La información entre terminales necesita basarse en un formato estándar para integración, intercambio e interoperabilidad. La ISO 8583 intercambia especificaciones de mensajes adoptadas por un gran segmento de la industria de pagos. Este estándar puede ser extendido a través de los sistemas por donde las transacciones toman su rumbo. La ISO 8583 establece una estructura de mensaje, un formato y contenido, los elementos de datos y sus valores. El estándar puede ser implementado de acuerdo a las necesidades de la institución financiera que lo vaya a utilizar.

Las transacciones originadas a través de una tarjeta de crédito incluyen compras, retiros, depósitos, devoluciones, reversiones, consultas de saldo, pagos y transferencias interbancarias. La ISO 8583 define mensajes determinados de sistema a sistema para intercambios seguros o cualquier otro propósito administrativo.

La ISO 8583 se puede aplicar a diferentes prácticas dependiendo de las necesidades de la institución financiera, a continuación se mencionará algunas de estas.

- ATM y POS: En este caso se efectúa una solicitud entre dos sistemas (ATM/POS y terminal), al momento que la conexión está establecida entre el sistema uno y el sistema dos, el sistema uno manda un mensaje de solicitud para el sistema dos y este envía un mensaje de respuesta. El sistema uno empezara a mandar mas mensajes hasta obtener una respuesta, el sistema dos responderá a todos estos mensajes. Después el sistema uno enviará la solicitud de transacción financiera y el sistema dos responderá autorizando o rechazando dicha solicitud todo esto mediante mensajes basados en la ISO 8583. Si después de un tiempo determinado no existe respuesta se enviara un mensaje de reversión entre estos dos sistemas.

- KIOSK: Mediante estos puntos de acceso público a internet se puede restringir las capacidades del usuario para evitar que se efectúen acciones que cause peligro o daño al sistema.

- Testing funcional de aplicaciones con ISO 8583: La aplicación utiliza el protocolo ISO 8583 con el fin de establecer una comunicación entre terminales el cual se basa en solicitar y responder autorizaciones a transacciones bancarias. En esta aplicación se utiliza un archivo cuyo formato es predeterminado en el estándar, los son enviados y recibidos constan de una lista de campos con un identificador y un valor asociado (cada organización define que campos se utilizaran y cuáles serán sus valores).

  Para enviar y recibir estos mensajes se debe convocar una funcionalidad en un servidor que escucha dichos mensajes por medio de un puerto. Para esta aplicación se desarrolló una herramienta llamada “ISO Test Tool”.

Esta herramienta brinda una interfaz para establecer la comunicación con un servidor y enviar/recibir mensajes mediante el protocolo ISO 8583. Esta herramienta crea y mantiene un historial de transacciones enviadas y recibidas para su posterior análisis.

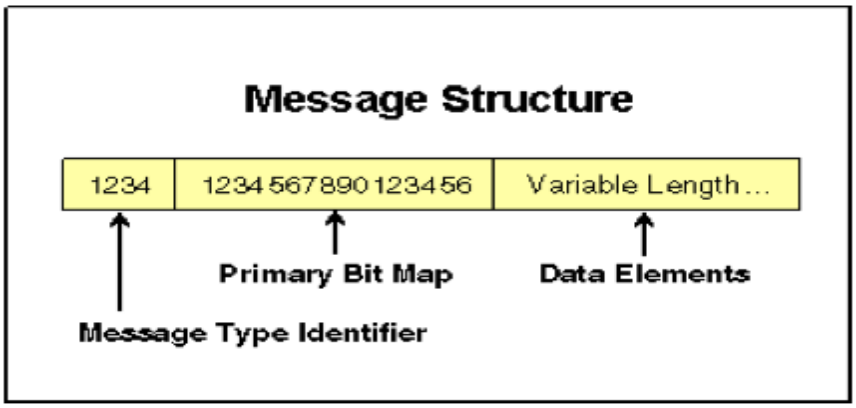
La aplicación permite transformar manualmente los mensajes en un mensaje ISO 8583, de esta manera se puede interpretar el resultado obtenido y compararlo con el resultado esperado para cada una de las pruebas ejecutadas.

Capítulo II: Requerimientos del Estándar ISO 8583 de 1993

2.1 Partes de la mensajería

Los mensajes están conformados en de los siguientes componentes, algunos de ellos son obligatorios mientras que otros son opcionales y se encuentran estructurados en el siguiente gráfico:

Ilustración 2: Partes de la mensajería



Fuente: BASE24_External_Message, ACI Worldwide, Inc
Elaborado por: ACI Worldwide, Inc

2.1.1 Tipo de mensaje

Es un código de 4 dígitos que identifica la función general del mensaje. Este es necesario en todos los mensajes.

- Mensajes de Autorización
  - ✓ Mensaje de solicitud de autorización (1100): Este mensaje exige la aprobación de la transacción.
  - ✓ Mensaje de repetición de autorización (1101): Indica al receptor de un posible mensaje duplicado. Este mensaje se utiliza cuando no se recibió el mensaje 1100.

- ✓ Mensaje de respuesta a la solicitud de autorización (1110): Este mensaje se espera a cambio del mensaje de solicitud de autorización aprobando o negando el pedido.
- ✓ Mensaje de aviso de autorización (1120): Se informa de una operación autorizada por el emisor de la tarjeta.
- ✓ Mensaje de repetición de aviso (1121): Este mensaje se utiliza cuando no se recibió el mensaje 1120 indicando al receptor sobre un posible mensaje duplicado.
- ✓ Mensaje de repuesta al aviso de autorización (1130): Este mensaje reconoce la recepción del mensaje 1120/1121.
- ✓ Mensaje de notificación de autorización (1140): Notifica al emisor sobre la recepción del mensaje.

- Mensajes de Transacciones Financieras
  - ✓ Mensaje de solicitud de transacción financiera (1200): Solicita la aprobación de una transacción con el fin de ser ejecutada en la cuenta del emisor.
  - ✓ Mensaje de repetición de solicitud de transacción financiera (1201): Este mensaje es idéntico al mensaje de solicitud de transacción financiera exceptuando que indica al receptor de un mensaje duplicado.
  - ✓ Mensaje de respuesta para la solicitud de una transacción financiera (1210): Este mensaje aprueba o niega el pedido del mensaje de solicitud de transacción financiera.
  - ✓ Mensaje de aviso de transacción financiera (1220): Este mensaje informa de una operación financiera previamente completada.

- ✓ Mensaje de repetición del aviso de transacción financiera (1221): Este mensaje es exactamente al 1220.
- ✓ Mensaje de respuesta al aviso de la transacción financiera (1230): Indica la recepción exitosa de un mensaje 1220/1221.
- ✓ Mensaje de notificación de la transacción financiera (1240): Notifica al emisor sobre la recepción del mensaje.

- Mensajes de Actualización de Archivos
  - ✓ Mensaje de solicitud de actualización de archivos (1304): Este mensaje contiene instrucciones para realizar operaciones como: consultar, añadir, eliminar o actualizar un archivo o registro.
  - ✓ Mensaje de repetición de solicitud de actualización de archivos (1305): Este mensaje es idéntico al mensaje de actualización de archivos exceptuando que indica al receptor de un mensaje duplicado.
  - ✓ Mensaje de respuesta a la solicitud de actualización de archivos (1314): Este mensaje se espera a cambio del mensaje de solicitud de actualización de archivos aprobando o negando la operación.
  - ✓ Mensaje de aviso de actualización de archivos (1324): Informa de una operación previamente completada.
  - ✓ Mensaje de repetición de aviso de actualización de archivos (1325): Este mensaje se utiliza cuando no se recibió el mensaje 1124 indicando al receptor sobre un posible mensaje duplicado.
  - ✓ Mensaje de respuesta al aviso de actualización de archivos (1334): Reconoce la recepción de un mensaje 1324/1325.

- Mensajes de Reversión

  - ✓ Mensaje de reversión de aviso de actualización de archivos (1420): Este mensaje revierte una operación previamente ejecutada.

  - ✓ Mensaje de repetición de una reversión (1421): Este mensaje es exactamente al 1420.

  - ✓ Mensaje de respuesta a una reversión (1430): Este mensaje reconoce la recepción de un mensaje 1420/1421.

  - ✓ Mensaje de notificación de una reversión (1440): Notifica al emisor sobre la recepción del mensaje.

- Mensajes de Red

  - ✓ Mensaje de solicitud de administración de red (1804): Se utiliza este mensaje para la gestión dinámica de contraseñas, inicio y cierre de sesión de mensajes.

  - ✓ Mensaje de repetición de una solicitud de administración de red (1805): Indica al receptor de un posible mensaje duplicado. Este mensaje se utiliza cuando no se recibió el mensaje 1804.

  - ✓ Mensaje de respuesta a una solicitud de administración de red (1814): Este mensaje se lo utiliza como respuesta a un mensaje 1804/1805.

2.1.2 Bit map primario

Es un campo con 16 posiciones requeridas en todos los mensajes. Representa 64 bits de la información que identifica la presencia o ausencia de los primeros 64 elementos de datos del mensaje.

La información representada por estos 64 bits es convertida a 16 bytes utilizando los equivalentes hexadecimales.

2.1.3 Elementos de datos

Los elementos de datos son campos que contienen la información esencial sobre una transacción. La norma ISO 8583:1993 permite la transmisión de todos los elementos de datos que conforman el estándar. No todos estos elementos de datos son utilizados, de hecho muchas veces se utilizan pocos de ellos. Estos elementos son los siguientes:

Tabla 3: Campos de datos

N	Nombre	Formato/Longitud	Descripción
P1	Secondary Bit Map	AN 16	Este bit map secundario define la presencia o la ausencia de elementos de datos desde el 65 hasta el 128
P2	Primary Account Number	LLVAR N ..19	Contiene el número de cuenta primaria (PAN) del titular de la tarjeta que participa en la solicitud de transacción o actualización que está siendo procesada.

Tabla 3: Campos de datos

P3	Processing Code	AN 6	Contiene el código de procesamiento asociado a la transacción. Este dato es obligatorio para todos los mensajes, excepto para la gestión de red y los mensajes de actualización de archivos.
P4	Amount, Transaction	N 12	Contiene la cantidad de fondos solicitados (ya sea de débito o crédito) en la moneda utilizada por el software del switch transaccional para procesar la transacción.
P5	Amount, Reconciliation	N 12	Contiene la cantidad de fondos que se transfieren entre el adquirente y emisor de la tarjeta.
P6	Amount, Cardholder Billing	N 12	Contiene el importe[1] facturado al titular de la tarjeta en la moneda su cuenta y exclusiva de facturación titular fees.
P7	Transmission Date and Time	N10 (MMDDhhmmss)	Contiene la fecha y hora del mensaje iniciado por el autor. Este tiempo se fija para cada mensaje de salida, y se expresa en hora media de Greenwich (GMT).
P8			No es utilizado por la ISO 8583:1993

Tabla 3: Campos de datos

P9	Conversion Rate, Reconciliation	N 8	Contiene el factor utilizado en la conversión de transacción a la cantidad de reconciliación[6]. El importe de la operación se multiplica por este factor para obtener la cantidad de reconciliación.
P10	Conversion Rate, Cardholder Billing	N 8	Contiene el factor utilizado en la conversión de transacción a la cantidad de facturación del titular de la tarjeta. El importe de la operación se multiplica por este factor para obtener el importe de facturación titular de la tarjeta.
P11	Systems Trace Audit Number	N 6	Contiene un número que deberá ser fijado por el remitente del mensaje y se hizo eco del receptor de mensajes. Se utiliza para hacer coincidir las respuestas a los mensajes originales y no está destinado a seguir siendo el mismo a lo largo de la vida de una transacción.
P12	Date and Time, Local Transaction	N12 (YYMMDDhhmmss)	Contiene la fecha y hora locales en los que la operación se inició, en el lugar donde se acepta la tarjeta.

[6] Cantidad de reconciliación: es una comparación que se hace entre los apuntes contables que lleva una empresa de su cuenta con un banco y los ajustes que el propio banco realiza sobre la misma cuenta.

Tabla 3: Campos de datos

P13	Date, Effective	N 4 (YYMM)	Contiene el año y el mes en el que el instrumento (por ejemplo, la tarjeta) esté en vigencia.
P14	Date, Expiration	N 4 (YYMM)	Contiene el año y el mes en el que el instrumento (por ejemplo, la tarjeta) expira.
P15	Date, Settlement	N 6 (YYMMDD)	Contiene el año, mes y día en que se transfieren los fondos entre el adquirente de transacciones y el instrumento emisor.
P16	Date, Conversion	N 4 (MMDD)	Contiene el mes y el día en el que la tasa de conversión[7] es eficaz para convertir la cantidad de la transacción desde la moneda original de reconciliación.
P17	Date, Capture	N 4 (MMDD)	Contiene el mes y el día en que los datos de las transacciones se registran en la fuente de datos Diario (Journal) del software del switch transaccional.
P18	Merchant Type	N 4	Contiene el código de clasificación del vendedor involucrado en la transacción según el Estándar Industrial (SIC).
P19	Country Code, Acquiring Institution	N 3	Contiene el código del país donde se encuentra la entidad adquirente.

[7] Tasa de conversión: es el porcentaje de usuarios que finalmente compran o realizan alguna acción deseada.

Tabla 3: Campos de datos

P20			No es utilizado por la ISO 8583:1993
P21	Country Code, Forwarding Institution	N 3	Contiene el código de país del país donde se encuentra la institución de reenvío.
P22	Point of Service Data Code	AN 12	Contiene el punto de datos de servicio asociado con la transacción, utilizado para indicar las condiciones específicas que son (o eran) presentes en el momento de que una transacción se llevó a cabo en el punto de servicio y/o cuando se inició todo.
P23	Card Sequence Number	N 3	Contiene el número de tarjeta utilizado para distinguir entre tarjetas separadas que tengan la misma cuenta principal.
P24	Function Code	N 3	Contiene el código de función asociada a la transacción.
P25	Message Reason Code	N 4	Contiene el código de la razón del mensaje que proporciona el receptor de la solicitud.
P26	Card Acceptor Business Code	N 4	Contiene un código de clasificación del tipo de negocio que está realizando el que acepta la tarjeta para esta transacción.
P27	Approval Code Length	N 1	Contiene la longitud máxima del código de aprobación.

Tabla 3: Campos de datos

P28	Date, Reconciliation	N 6 (YYMMDD)	Contiene el año, mes y día en el que los totales financieros se concilian entre el adquiriente y el emisor de la tarjeta.
P29	Reconciliation Indicator	N 3	Contiene un valor que se utiliza para permitir la reconciliación de los plazos en las fechas de reconciliación. Este elemento de datos está actualmente reservado para uso futuro.
P30	Amounts, Original	N 24	Contiene los elementos de datos de la cantidad de la transacción original.
P31			No es utilizado por la ISO 8583:1993
P32	Acquirer Institution ID Code	LLVAR N ..11	Contiene un código que identifica la entidad adquirente de la transacción.
P33	Forwarding Institution ID Code	LLVAR N ..11	Contiene un código que identifica a la institución de reenvío (o proveedor).
P34	Primary Account Number, Extended	LLVAR NS ..28	Contiene un número que identifica la cuenta del cliente o la relación que participa en la solicitud de transacción o actualización que se está procesando.

Tabla 3: Campos de datos

P35	Track 2 Data	LLVAR Z ..37	Contiene la información codificada en la pista 2 de la banda magnética en la parte posterior de la tarjeta que origina la transacción.
P36	Track 3 Data	LLLVAR Z ..104	Contiene la información codificada en la pista 3 de la banda magnética como se define en la norma ISO 4909.
P37	Retrieval Reference Number	ANP 12	Contiene un número asignado por el iniciador del mensaje para identificar de forma única una transacción. Este número se mantendrá para todos los mensajes en toda la vida de una transacción.
P38	Approval Code	ANP 6	Contiene un código asignado por la entidad que autoriza la transacción indicando su aprobación.
P39	Action Code	N 3	Contiene el código de acción asociado a la transacción que define las medidas adoptadas o que se adopten, así como la razón de esta acción.
P40	Service Code	N 3	Contiene el código de servicio asociados con la transacción identificando la disponibilidad del servicio.
P41	Card Acceptor Terminal Identification	ANS 16	Contiene un código único que identifica el terminal en la ubicación del que acepta la tarjeta.

Tabla 3: Campos de datos

P42	Card Acceptor Identification Code	ANS 15	Contiene un código utilizado para identificar al que acepta la tarjeta en una transacción, se observa si el que acepta la tarjeta es diferente de la entidad adquirente.
P43	Card Acceptor Name/Location	LLVAR ANS ..99	Contiene el nombre y la ubicación del que acepta la tarjeta.
P44	Additional Response Data	LLVAR ANS ..99	Contiene hasta diez códigos de acción asociados a un mensaje de actualización de archivos.
P45	Track 1 Data	LLVAR ANS ..76	Contiene la información codificada en la pista 1 de la banda magnética de la tarjeta utilizada para la transacción.
P46	Amounts, Fees	LLLVAR ANS ..204	Contiene el honorario asociado con la transacción.
P47			No es utilizado por la ISO 8583:1993
P48	Additional Data – Private Data Element	LLLVAR ANS..999	Se utiliza para un número de propósitos, en función de la información transportada.
P49	Currency Code, Transaction	A 3 or N 3	Contiene la moneda local de la entidad adquirente o la fuente de la ubicación de la transacción.
P50	Currency Code, Reconciliation	A 3 or N 3	Contiene el código que define la moneda reconciliación.

Tabla 3: Campos de datos

P51	Currency Code, Cardholder Billing	A 3 or N 3	Contiene el código de la definición de la moneda de los importes realizados en la cantidad, facturación y honorarios del titular de la tarjeta.
P52	Personal Identification Number (PIN)	AN 16	Contiene el número de identificación personal (PIN) asignado a un cliente para identificar de forma exclusiva a ese cliente en el punto de servicio.
P53	Security Related Control Information	N 16	Contiene datos de gestión de claves.
P54	Amounts, Additional	LLLVAR ANS ..120	Contiene una devolución de dinero o cantidades de saldo durante la transacción.
P55	Integrated Circuit Card System Related	LLLVAR ANS ..510	Contiene datos EMV[8].

[8] EMV: estándar de interoperabilidad de tarjetas IC ("Tarjetas con microprocesador") y *TPV* con soporte IC, para la autentificación de pagos mediante tarjetas de crédito y débito.

Tabla 3: Campos de datos

P56	Original Data Elements	LLVAR N ..35	Contiene los elementos de datos del mensaje original previsto para la adaptación de la transacción. Este elemento está formado por: • Identificador original del tipo de mensaje • Número de auditoría de seguimiento del sistema original • Fecha y hora original, transacción local La adquisición de código de identificación
P57	Authorization Life Cycle Code	N 3	Contiene un valor en días, horas o minutos que define el período de tiempo durante el cual el adquirente ha solicitado una garantía de los fondos, o que el emisor de la tarjeta le garantiza los fondos para una operación financiera que puede seguir.
P58	Authorizing Agent Institution ID Code	LLVAR N ..11	Contiene un código de identificación de la entidad agente del orden público.

Tabla 3: Campos de datos

P59	Transport Data	LLLVAR ANS ..999	Contiene los datos del remitente del mensaje que debe ser devuelto e inalterado en un mensaje de respuesta.
P60	CSM Reserved	LLLVAR ANS ..999	El elemento de datos CSM[9] está reservado para el uso del cliente al momento de realizar modificaciones.
P61			No es utilizado por la ISO 8583:1993
P62	Primary Reserved Private	LLLVAR ANS ..999	Se utiliza para un número de propósitos en función de la información transportada.
P63			No es utilizado por la ISO 8583:1993
P64	Primary Message Authentication Code	AN 16	Transporta el código de autenticación de mensajes (MAC) para el mensaje.
S65			No es utilizado por la ISO 8583:1993
S66			No es utilizado por la ISO 8583:1993

[9] CMS: es un programa que permite crear una estructura de soporte (framework) para la creación y administración de contenidos, principalmente en páginas web, por parte de los administradores, editores, participantes y demás roles.

Tabla 3: Campos de datos

S67	Extended Payment Code	N 2	Es un elemento condicional. Especifica un periodo de reembolso para portadores de MasterCard con el fin de realizar pagos diferidos para una determinada transacción
S68	Country Code, Receiving Institution	N 3	Este elemento contiene el código del país donde la institución receptora se encuentra.
S69			No es utilizado por la ISO 8583:1993
S70	Country Code, Authorizing Agent Institution	N 3	Este elemento contiene el código del país donde se encuentra la institución emisora de autorización
S71	Message Number	N 8	Contiene un número asignado al mensaje por la transacción original. Se lo utiliza para monitorear la integridad y la continuidad del intercambio de dicho elemento
S72	Data Record	LLLVAR ANS ..999	Contiene información requerida para el soporte de una operación administrativa o actualización de archivos
S73			No es utilizado por la ISO 8583:1993

Tabla 3: Campos de datos

S74			No es utilizado por la ISO 8583:1993
S75			No es utilizado por la ISO 8583:1993
S76			No es utilizado por la ISO 8583:1993
S77			No es utilizado por la ISO 8583:1993
S78			No es utilizado por la ISO 8583:1993
S79			No es utilizado por la ISO 8583:1993
S80			No es utilizado por la ISO 8583:1993
S81			No es utilizado por la ISO 8583:1993
S82			No es utilizado por la ISO 8583:1993
S83			No es utilizado por la ISO 8583:1993
S84			No es utilizado por la ISO 8583:1993
S85			No es utilizado por la ISO 8583:1993
S86			No es utilizado por la ISO 8583:1993
S87			No es utilizado por la ISO 8583:1993

Tabla 3: Campos de datos

S88			No es utilizado por la ISO 8583:1993
S89			No es utilizado por la ISO 8583:1993
S90			No es utilizado por la ISO 8583:1993
S91			No es utilizado por la ISO 8583:1993
S92			No es utilizado por la ISO 8583:1993
S93	Transaction Destination Institution Identification Code	LLVAR N ..11	Contiene información que identifica a la institución receptora de la transacción.
S94	Transaction Originator Institution Identification Code	LLVAR N ..11	Contiene información que identifica a la institución emisora de la transacción
S95			No es utilizado por la ISO 8583:1993
S96	Key Management Data	LLVAR N ..11	Contiene campos asociados con la administración de mensajes clave
S97			No es utilizado por la ISO 8583:1993

Tabla 3: Campos de datos

S98			No es utilizado por la ISO 8583:1993
S99			No es utilizado por la ISO 8583:1993
S100	Receiving Institution ID Code	LLVAR N ..11	Es un elemento condicional. Se incluye cuando la institución receptora no es la misma que el destino final del mensaje
S101			No es utilizado por la ISO 8583:1993.
S102	Account Identification 1	LLVAR ANS ..28	Contiene una serie de dígitos y/o caracteres utilizados para identificar la cuenta de un cliente especifico o de una conexión
S103	Account Identification 2	LLVAR ANS ..28	Contiene una serie de dígitos y/o caracteres utilizados para identificar la cuenta de un cliente especifico o una conexión
S104			No es utilizado por la ISO 8583:1993
S105			No es utilizado por la ISO 8583:1993
S106			No es utilizado por la ISO 8583:1993
S107			No es utilizado por la ISO 8583:1993
S108			No es utilizado por la ISO 8583:1993

Tabla 3: Campos de datos

S109			No es utilizado por la ISO 8583:1993
S110			No es utilizado por la ISO 8583:1993
S111			No es utilizado por la ISO 8583:1993
S112			No es utilizado por la ISO 8583:1993
S113			No es utilizado por la ISO 8583:1993
S114			No es utilizado por la ISO 8583:1993
S115			No es utilizado por la ISO 8583:1993
S116			No es utilizado por la ISO 8583:1993
S117			No es utilizado por la ISO 8583:1993
S118			No es utilizado por la ISO 8583:1993
S119			No es utilizado por la ISO 8583:1993
S120			No es utilizado por la ISO 8583:1993
S121			No es utilizado por la ISO 8583:1993
S122			No es utilizado por la ISO 8583:1993

Tabla 3: Campos de datos

S123	Reserved for Private Use	LLLVAR ANS ..999	Se lo utiliza para diferentes propósitos dependiendo de la información del mensaje.
S124			No es utilizado por la ISO 8583:1993
S125			No es utilizado por la ISO 8583:1993
S126			No es utilizado por la ISO 8583:1993
S127	Reserved for Private Use	LLLLVAR ANS ..9999	Se lo utiliza para diferentes propósitos dependiendo de la información que el mensaje contiene.
S128	Secondary Message Authentication Code	AN 16	Contiene información de autentificación del mensaje. Está configurado para la interfaz donde se trabaja con la norma ISO 8583:1993

Fuente: Base 24 External Message
Elaborada por: Juan Pablo Baquero, David Murillo
Traducida por: Juan Pablo Baquero, David Murillo

2.2 Ventajas y Desventajas

2.2.1 Ventajas

Para la norma ISO 8583:1993 se consideran las mismas ventajas mencionadas en el capítulo 1 en el punto 1.2.1 y además se nombraran otras ventajas específicas que hacen diferente a esta versión:

- El número de campos se reduce de siete a tres lo cual optimiza el uso de memoria en la transmisión de datos.

- El elemento de dato P22 solo contiene información del punto de servicio asociado a la transacción ejecutada. En la versión anterior este elemento contiene dos tipos de códigos: el método que se utilizo para ingresar el número de cuenta del titular y las capacidades disponibles en el punto de servicio, lo cual hace más especifica la información.

- La norma ISO 8583:1993 utiliza un elemento de dato para verificar que el mensaje original sea el mismo que el mensaje recibido, empleando el tipo de identificador, el número de seguimiento del sistema, la fecha de la transacción y un código identificado de la institución financiera, fortaleciendo así la seguridad al momento de realizar la transacción.

- La norma emplea un mensaje de notificación de autorización que advierte al emisor sobre la recepción del mensaje, gracias a esta advertencia el emisor puede asegurarse que su mensaje fue recibido correctamente evitando percances en la comunicación.

- Cuando se realizan transacciones financieras también se utiliza un mensaje de notificación para advertir al emisor sobre la recepción del mensaje, advirtiendo cualquier error al momento de realizar la transacción.

2.2.2 Desventajas

- Cambios de versión: Al existir una nueva versión de la norma en la que los cambios sean drásticos y puedan afectar al sistema de la institución financiera en donde es aplicada no sería factible o el proceso demandaría de esfuerzo desperdiciando así tiempo y dinero para la organización.

2.3 Usos y Aplicaciones

En cualquiera de los casos que se vaya a utilizar una tarjeta de crédito, de débito, o para realizar un retiro en un cajero automático la información que contiene la transacción que se realiza en este proceso es enviada de un sistema hacia otro. Por ejemplo una compra efectuada en una tienda particular puede ser procesada a través de una terminal, hacia uno o más sistemas conectados mediante una red, con el fin de notificar al banco de la cuenta del cliente de que esta transacción es solicitada. La transacción contiene información sobre el tipo de transacción, el uso de la tarjeta, el comerciante, el monto de la transacción, información de seguridad, entre otros. La respuesta a esta solicitud, autorizando o rechazando la transacción, debe ser retornada por la misma ruta hacia la terminal.

La información entre terminales necesita basarse en un formato estándar para integración, intercambio e interoperabilidad. La ISO 8583 intercambia especificaciones de mensajes adoptadas por un gran segmento de la industria de pagos. Este estándar puede ser extendido a través de los sistemas por donde las transacciones toman su rumbo. La ISO 8583 establece una estructura de mensaje, un formato y contenido, los elementos de datos y sus valores. El estándar puede ser implementado de acuerdo a las necesidades de la institución financiera que lo vaya a utilizar.

Las transacciones originadas a través de una tarjeta de crédito incluyen compras, retiros, depósitos, devoluciones, reversiones, consultas de saldo, pagos y transferencias interbancarias. La ISO 8583 define mensajes determinados de sistema a sistema para intercambios seguros o cualquier otro propósito administrativo.

Los usos y aplicaciones para esta versión son los mismos ya mencionados en el punto 1.4 del capítulo anterior con la diferencia de que en esta versión se reforzó la seguridad en varios aspectos para garantizar transacciones resguardadas.

Capítulo III: Definición de un procedimiento para la migración que se realice de la norma ISO 8583 de 1987 a la norma ISO 8583 de 1993

3.1 Análisis comparativo entre las normas ISO 8583 de 1987 e ISO 8583 de 1993

La siguiente tabla expondrá los tipos de mensajes más importantes que manejan las dos normas y sus diferentes usos:

Tabla 4: Tipos de mensajes

Clase de mensaje	Tipo de Mensaje ISO 87	Tipo de Mensaje ISO 93	Descripción
Autorización	0100	1100/1101	Solicitud de Autorización/Repetición
	0110	1110	Respuesta a la solicitud de Autorización
	0120/0121	1120/1121	Aviso de Autorización/Repetición
	0130	1130	Respuesta al Aviso de Autorización
		1140	Notificación de Autorización
Transacción Financiera	0200	1200/1201	Solicitud de Transacción Financiera/Repetición
	0210	1210	Respuesta a la Solicitud de Transacción Financiera
	0220/0221	1220/1221	Aviso de Transacción Financiera/Repetición
	0230	1230	Respuesta al Aviso de una Transacción Financiera
		1240	Notificación Financiera
Actualización de Archivos	0300	1304/1305	Solicitud de Actualización de Archivos/Repetición
	0310	1314	Respuesta a la Solicitud de Actualización de Archivos
		1324/1325	Aviso de Actualización de Archivos/Repetición
		1334	Respuesta al Aviso de Actualización de Archivos

Tabla 4: Tipos de mensajes

Reversión	0420/0421	1420/1421	Mensaje de Reversión/Repetición
	0430	1430	Respuesta a una Reversión
Red	0800	1804/1805	Solicitud de Administración de Red/Repetición
	0810	1814	Respuesta a una Solicitud de Red

Fuente: Base 24 External Message, BASE24-eps ISO 8583:1993 Host External Message Specifications
Elaborada por: Juan Pablo Baquero, David Murillo

La siguiente tabla expondrá los elementos de datos más importantes que manejan las dos normas y sus diferentes usos:

Tabla 5: Elementos de datos

	ISO 8583:1987		**ISO 8583:1993**		
N	**Nombre**	**Formato/ Longitud**	**Nombre**	**Formato/ Longitud**	**Diferencias**
P1	Secundary bit map	AN 16	Secondary Bit Map	AN 16	
P2	Primary Acount Number	AN 19 N 19	Primary Account Number	LLVAR N ..19	Formato/Longitud
P3	Processing Code	AN 6 N 6	Processing Code	AN 6	Funcionamiento Formato/Longitud
P4	Transaction Amount	N 12	Amount, Transaction	N 12	
P5	Settlement Amount	N 12	Amount, Reconciliation	N 12	Funcionamiento
P6	Cardholder Billing Amount	N 12	Amount, Cardholder Billing	N 12	Funcionamiento

Tabla 5: Elementos de datos

P7	Transmission Date and Time	N10	Transmission Date and Time	N 10	
P8	Cardholder Billing Free Amount	N 8			No existe en la norma ISO8583:1993
P9	Settlement Conversion Rate	N 8	Conversion Rate, Reconciliation	N 8	Funcionamiento
P10	Cardholder Billing Conversion Rate	N 8	Conversion Rate, Cardholder Billing	N 8	Funcionamiento
P11	Systems Trade Audit Number	N 6	Systems Trace Audit Number	N 6	
P12	Local Transaction Time	N 6	Date and Time, Local Transaction	N 12	Formato/Longitud
P13	Local Transaction Date	N 4	Date, Effective	N 4	
P14	Expiration Date	N 4	Date, Expiration	N 4	
P15	Settlement Date	N 4	Date, Settlement	N 6	Longitud
P16	Conversion Date	N 4	Date, Conversion	N 4	
P17	Capture Date	N 4	Date, Capture	N 4	
P18	Merchant Type	N 4	Merchant Type	N 4	
P19	Acquiring Institution Country Code	N 3	Country Code, Acquiring Institution	N 3	Funcionamiento
P20	Country Code Primary Account Number Extended	N 3			No existe en la norma ISO 8583:1993

Tabla 5: Elementos de datos

P21	Forwarding Institution Country Code	N 3	Country Code, Forwarding Institution	N 3	Funcionamiento
P22	Point of Service Entry Mode	N 3	Point of Service Data Code	AN 12	Formato/Longitud
P23	Car Sequence Number	N 3	Card Sequence Number	N 3	
P24	Network International Identifier	N 3	Function Code	N 3	Funcionamiento
P25	Point of Service Condition Code	N 2	Message Reason Code	N 4	Longitud
P26	Point of Service PIN Capture Code	N 2	Card Acceptor Business Code	N 4	Longitud
P27	Authorization Identification Response	N 1	Approval Code Length	N 1	Funcionamiento
P28	Transaction Fee Amount	X + N 8	Date, Reconciliation	N 6	Funcionamiento Formato/Longitud
P29	Settlement Fee Amount	X + N 8	Reconciliation Indicator	N 3	Funcionamiento Formato/Longitud
P30	Transaction Processing Fee Amount	X + N 8	Amounts, Original	N 24	Funcionamiento Formato/Longitud

Tabla 5: Elementos de datos

P31	Settlement Processing Fee Amount	X + N 8			Funcionamiento Formato/Longitud
P32	Acquiring Institution Identification Code	N..11	Acquirer Institution ID Code	LLVAR N ..11	Formato
P33	Forwarding Institution Identification Code	N..11	Forwarding Institution ID Code	LLVAR N ..11	Formato
P34	Extended Primary Account Number	AN..28	Primary Account Number, Extended	LLVAR NS ..28	Formato
P35	Track 2 Data	ANS..37	Track 2 Data	LLVAR Z ..37	Formato
P36	Track 3 Data	ANS..104	Track 3 Data	LLLVAR Z ..104	Formato
P37	Retrieval Reference Number	AN 12	Retrieval Reference Number	ANP 12	Formato
P38	Authorization Identification Response	AN 6	Approval Code	ANP 6	Funcionamiento Formato
P39	Response Code	AN 2	Action Code	N 3	Funcionamiento Formato/Longitud
P40	Service Restriction Code	AN 3	Service Code	N 3	Funcionamiento Formato

Tabla 5: Elementos de datos

P41	Card Acceptor Terminal Identification	ANS 16	Card Acceptor Terminal Identification	ANS 16	
P42	Card Acceptor Identification Code	ANS 15	Card Acceptor Identification Code	ANS 15	
P43	Card Acceptor Name/Location	ANS 40	Card Acceptor Name/Location	LLVAR ANS ..99	Formato/Longitud
P44	Additional Response Data	ANS 27	Additional Response Data	LLVAR ANS ..99	Funcionamiento Formato/Longitud
P45	Track 1 Data	ANS..76	Track 1 Data	LLVAR ANS ..76	Formato
P46	ISO Additional Data	ANS 999	Amounts, Fees	LLLVAR ANS ..204	Funcionamiento Formato/Longitud
P47	National Additional Data	ANS 999			No existe en la norma ISO 8583:1993
P48	atm Additional Data	ANS 47	Additional Data – Private Data Element	LLLVAR ANS..999	Funcionamiento Formato/Longitud
P49	Transaction Currency Code	N 3	Currency Code, Transaction	A 3 or N 3	Formato
P50	Settlement Currency Code	N 3	Currency Code, Reconciliation	A 3 or N 3	Funcionamiento Formato
P51	Cardholder Billing Currency Code	N 3	Currency Code, Cardholder Billing	A 3 or N 3	Funcionamiento Formato

Tabla 5: Elementos de datos

P52	Personal Identification Number (PIN) Data	AN 16	Personal Identification Number (PIN) Data	AN 16	
P53	Security Related Control Information	N 16			No existe en la norma ISO 8583:1993
54	Additional Amounts	ANS 15	Amounts, Additional	LLLVAR ANS ..120	Formato/Longitud
P55	Through P-56 ISO Reserved	ANS..99	Integrated Circuit Card System Related Data Data Element	LLLVAR ANS ..510	Funcionamiento Formato/Longitud
P56			Original Data Elements	LLVAR N ..35	No existe en la norma ISO 8583:1987
P57	National Reserved	ANS..99	Authorization Life Cycle Code	N 3	Funcionamiento Formato/Longitud
P58	Financial Token	ANS 135	Authorizing Agent Institution ID Code	LLVAR N ..11	Funcionamiento Formato/Longitud
P59	CAF Update Token	ANS 17	Transport Data	LLLVAR ANS ..999	Funcionamiento Formato/Longitud
P60	Terminal Data	ANS 15	CSM Reserved	LLLVAR ANS ..999	Funcionamiento Formato/Longitud
P61	Card Issuer and Authorizer	ANS 16			No existe en la norma ISO 8583:1993
P62	Postal Code	ANS 13	Primary Reserved Private	LLLVAR ANS ..999	Funcionamiento Formato/Longitud
P63	PIN Offset	ANS 19			No existe en la norma ISO 8583:1993

Tabla 5: Elementos de datos

P64	Primary Message Authentication Code	AN 16	Primary Message Authentication Code	AN 16	
S65	Extended Bit Map	No definido			No existe en la norma ISO 8583:1993
S66	Settlement Code	N 1			No existe en la norma ISO 8583:1993
S67	Extended Payment Code	N 2	Extended Payment Data	N 2	Funcionamiento
S68	Receiving Institution Country Code	N 3	Country Code, Receiving Institution	N 3	Funcionamiento
S69	Settlement Institution Country Code	N 3			No existe en la norma ISO 8583:1993
S70	Network Management Information Code	N 3	Country Code, Authorizing Agent Institution	N 3	Funcionamiento
S71	Message Number	N 4	Message Number	N 8	Funcionamiento Longitud
S72	Message Number Last	N 4	Data Record	LLLVAR ANS ..999	Formato/Longitud
S73	Action Date	N 6			No existe en la norma ISO 8583:1993
S74	Number Credits	N 10			No existe en la norma ISO 8583:1993
S75	Reversal Number Credits	N 10			No existe en la norma ISO 8583:1993

Tabla 5: Elementos de datos

S76	Number Debits	N 10			No existe en la norma ISO 8583:1993
S77	Reversal Number Debits	N 10			No existe en la norma ISO 8583:1993
S78	Number Transfer	N 10			No existe en la norma ISO 8583:1993
S79	Reversal Number Transfer	N 10			No existe en la norma ISO 8583:1993
S80	Number Inquiries	N 10			No existe en la norma ISO 8583:1993
S81	Number Authorizations	N 10			No existe en la norma ISO 8583:1993
S82	Processing Fee Amount Credits	N 12			No existe en la norma ISO 8583:1993
S83	Transaction Fee Amount Credits	N 12			No existe en la norma ISO 8583:1993
S84	Processing Fee Amount Debits	N 12			No existe en la norma ISO 8583:1993
S85	Transaction Fee Amount Debits	N 12			No existe en la norma ISO 8583:1993
S86	Amount Credits	N 16			No existe en la norma ISO 8583:1993
S87	Reversal Amount Credits	N 16			No existe en la norma ISO 8583:1993
S88	Amount Debits	N 16			No existe en la norma ISO 8583:1993

Tabla 5: Elementos de datos

S89	Reversal Amount Debits	N 16			No existe en la norma ISO 8583:1993
S90	Original Data Elements	N 42			No existe en la norma ISO 8583:1993
S91	File Update Code	AN 1			No existe en la norma ISO 8583:1993
S92	File Security Code	AN 2			No existe en la norma ISO 8583:1993
S93	Response Indicator	AN 5	Transaction Destination Institution Identification Code	LLVAR N ..11	Funcionamiento Formato/Longitud
S94	Service Indicator	AN 7	Transaction Originator Institution Identification Code	LLVAR N ..11	Funcionamiento Formato/Longitud
S95	Replacement Amounts	AN 42			No existe en la norma ISO 8583:1993
S96	Message Security Code	AN 16	Key Management Data	Variable based on the tags included	Funcionamiento Formato/Longitud
S97	Net Settlement Amount	X+N 16			No existe en la norma ISO 8583:1993
S98	Payee	ANS 25			No existe en la norma ISO 8583:1993
S99	Settlement Institution Identification Code	N ..11			No existe en la norma ISO 8583:1993

Tabla 5: Elementos de datos

S100	Receiving Institution Identification Code	N ..11	Receiving Institution Identification Code	LLVAR N ..11	Formato/Longitud
S101	File Name	ANS 4			No existe en la norma ISO 8583:1993
S102	Account Identification 1	ANS ..28	Account Identification 1	LLVAR ANS ..28	Formato
S103	Account Identification 2	ANS ..28	Account Identification 2	LLVAR ANS ..28	Formato
S104	Transaction Description	ANS 63			No existe en la norma ISO 8583:1993
S105	ISO Reserved	ANS ..999			No existe en la norma ISO 8583:1993
S106	ISO Reserved	ANS ..999			No existe en la norma ISO 8583:1993
S107	ISO Reserved	ANS ..999			No existe en la norma ISO 8583:1993
S108	ISO Reserved	ANS ..999			No existe en la norma ISO 8583:1993
S109	ISO Reserved	ANS ..999			No existe en la norma ISO 8583:1993
S110	ISO Reserved	ANS ..999			No existe en la norma ISO 8583:1993
S111	ISO Reserved	ANS ..999			No existe en la norma ISO 8583:1993

Tabla 5: Elementos de datos

S112	from host maintenance Enhanced Preauthorized Hold Information	ANS 105			No existe en la norma ISO 8583:1993
S113	Override Token	ANS ..157			No existe en la norma ISO 8583:1993
S114	from host maintenance Automated Hot Card Update Information	ANS ..276			No existe en la norma ISO 8583:1993
S114	from host maintenance Application File and Table Information	AN ..429 / ANS ..276			No existe en la norma ISO 8583:1993
S114	WHFF Inquiry Token—Part 1	ANS ..429			No existe en la norma ISO 8583:1993
S115	WHFF Inquiry Token—Part 2	ANS 389			No existe en la norma ISO 8583:1993
S115	from host maintenance CAF and PBF Base User Information	ANS 153			No existe en la norma ISO 8583:1993

Tabla 5: Elementos de datos

S116	WHFF Inquiry Token—Part 3	ANS 389			No existe en la norma ISO 8583:1993
S116	from host maintenance CAF Non–Currency Dispense	ANS 155			No existe en la norma ISO 8583:1993
S117	PBF Update Token	ANS 7			No existe en la norma ISO 8583:1993
S117	from host maintenance CAF EMV	ANS 32			No existe en la norma ISO 8583:1993
S118	from host maintenance CAF and PBF Data	ANS 52 / ANS 71	Reserved for Private Use	LLLVAR ANS ..999	No existe en la norma ISO 8583:1993
S118	SPF Update Token	ANS 103			No existe en la norma ISO 8583:1993
S119	from host maintenance Self- Service Banking Check Information	ANS 67 / ANS 13			No existe en la norma ISO 8583:1993
S119	WHFF Update Token	ANS 83			No existe en la norma ISO 8583:1993
S120	Key Management	ANS 9	Reserved for Private Use	LLLLVAR ANS ..9999	Formato/Longitud

Tabla 5: Elementos de datos

S121	Terminal Address-Branch-Region	ANS 36	Secondary Message Authentication Code	AN 16	Funcionamiento Formato/Longitud
S122	Card Issuer Identification Code	ANS 14	Secondary Bit Map	AN 16	Funcionamiento Formato/Longitud
S123	Deposit Credit Amount	N 15	Primary Account Number	LLVAR N ..19	Funcionamiento Formato/Longitud
S124	Depository Type	ANS 4	Processing Code	AN 6	Funcionamiento Formato/Longitud
S125	Account Indicator/Statement Print Data	ANS 4 / ANS 375	Amount, Transaction	N 12	Funcionamiento Formato/Longitud
S126	Additional Data	ANS ..800	Amount, Reconciliation	N 12	Funcionamiento Formato/Longitud
S127	User Data	ANS ..200	Amount, Cardholder Billing	N 12	Funcionamiento Formato/Longitud
S128	Secondary Message Authentication Code	AN 16	Transmission Date and Time	N 10	Funcionamiento Formato/Longitud

Fuente: Base 24 External Message, BASE24-eps ISO 8583:1993 Host External Message Specifications
Elaborada por: Juan Pablo Baquero, David Murillo

En la tabla mostrada anteriormente, las filas que se encuentran subrayadas con color azul representan una diferencia entre los elementos de datos de ambas normas. Las diferencias se basan en el formato, longitud, nombre, funcionalidad o simplemente inexistencia del elemento en una o en ambas normas. La descripción de cada uno de estos elementos de datos se encuentra en los capitulos I y II.

Tabla 6: Tipos de formato (Elementos de datos)

Abreviatura	Significado
A	Alfanuméricos, incluyendo los espacios.
N	Sólo valores numéricos.
S	Sólo caracteres oficiales.
AN	Alfanumérico.
AS	Sólo caracteres alfanuméricos y especiales.
NS	Sólo caracteres numéricos y especiales.
ANS	Caracteres numéricos, alfanuméricos y especiales.
B	Información binaria
Z	Tracks 2 y 3 code set como se define en la ISO 4909 y en ISO 7813.
LLVAR	Significa que los dos primeros dígitos indican el largo del campo
LLLVAR	Significa que los tres primeros dígitos indican el largo del campo

Fuente: es.wikipedia.org/wiki/ISO_8583
Elaborada por: Juan Pablo Baquero, David Murillo

3.2 Matriz con los principales elementos a considerar en la migración a la versión actualizada de la norma

Tabla 7: Elementos principales a considerar en la migración

N	Aspecto	Descripción
1	Migrar lo más fácil	Se debe comenzar con la migración de estaciones de trabajo y servicios que tengan poca prioridad en el funcionamiento del sistema que maneje información de tarjetas de crédito o débito. Este proceso no representara ninguna diferencia de operatividad o rendimiento dentro del sistema.
2	Documentar todo el proceso	Se debe recolectar toda información de todos los procesos, procedimientos, resolución de problemas y datos que se encuentren dentro del marco del sistema que maneje los datos de tarjetas de crédito.

Tabla 7: Elementos principales a considerar en la migración

3	Involucrar a todos los usuarios	Todos los usuarios que forman parte del área pueden estar involucrados en el uso del sistema en el cual forma parte la norma ISO 8583, por lo que este puede decir cuáles son sus necesidades y cuáles son las nuevas funcionalidades o características que va a tener el sistema con la migración. El usuario también puede manifestar si se va a presentar mejoras en los procesos y por ultimo brindar sugerencias sobre el nuevo sistema.
4	Proporcionar toda información necesaria previamente a la migración	Explicar por qué se va a desarrollar una migración, sus elementos principales, las consecuencias de la migración y los beneficios de ésta. De esta manera todo el personal que esté involucrado con los sistemas que manejen la información de tarjetas de crédito estará al tanto de este proceso.
5	Compatibilidad del software que maneja el estándar	Este elemento determina si el software tiene la capacidad de trabajar conjuntamente con el hardware, programas y aplicaciones de la organización.
6	Aprobación del usuario final	El usuario final tiene la última palabra al decidir si fue factible la migración del estándar en base a las pruebas aplicadas previamente.
7	Costo del entrenamiento al personal técnico	El costo para el soporte debe ser planteado mediante un análisis minucioso con el fin de que bambas partes en este caso la empresa y el usuario salgan beneficiados.
8	Tiempo y costo del desarrollo del software que maneja el estándar actualizado	En base a los requerimientos y un estudio detallado se podrá determinar el tiempo costo y alcance de la migración tomando en cuenta futuras modificaciones a los requerimientos y a un previo análisis.
9	Dependencia de la organización con el software que maneja el estándar anterior	Una vez establecido un inventario de hardware y software se puede definir todas las dependencias que existen entre los elementos recogidos en el inventario y la norma que se maneja actualmente.

Fuente: Juan Pablo Baquero, David Murillo
Elaborada por: Juan Pablo Baquero, David Murillo

3.3 Definir el nivel de riesgo que tienen los elementos en la migración a la versión actualizada de la norma

Tabla 8: Niveles de riesgo

Elemento	Alto	Medio	Bajo
Migrar lo más fácil			X
Documentar todo el proceso		X	
Involucrar a todos los usuarios	X		
Proporcionar toda información necesaria previamente a la migración	X		
Compatibilidad del software que maneja el estándar	X		
Aprobación del usuario final		X	
Costo del entrenamiento al personal técnico		X	
Tiempo y costo del desarrollo del software que maneja el estándar actualizado	X		
Dependencia de la organización con el software que maneja el estándar anterior	X		

Fuente: Juan Pablo Baquero, David Murillo
Elaborada por: Juan Pablo Baquero, David Murillo

3.4 Evaluación del riesgo que tendría una institución financiera de la migración a la versión actualizada de la norma

El objetivo del proceso de reconocimiento de riesgos es identificar las principales fuentes de riesgo al desarrollar la migración de la norma ISO 8583. Este proceso debe basarse en un análisis minucioso donde todo el personal que se encuentre involucrado pueda discutir sus puntos de vista, compartir experiencias y desarrollar propuestas en base a datos históricos de otros proyectos similares. Posteriormente se puede establecer las consecuencias de cada uno de los riesgos previamente identificados y ver si es factible o no el desarrollo de la migración.

Con los elementos examinados en el punto 3.3 y el nivel del riesgo que contiene cada uno, se visualiza que el riesgo de migrar a la nueva norma seria alta ya que la mayoría de puntos recae en este campo luego de un estudio minucioso, y las consecuencias de una falla en estos elementos sería muy perjudicial para el funcionamiento de la organización por lo que la recomendación dada después de este análisis seria desarrollar un plan de contingencia que provea una solución para cada uno de los elementos mencionados previamente.

En la actualidad BANRED solo ha realizado la migración de la norma ISO 8583:1993 a la norma ISO 8583:1993 al Banco del Pichincha para poder proveerles el servicio llamado Stan-In que consiste en la inserción del saldo de la cuenta en la base de datos del switch transaccional para poder realizar cualquier movimiento en caso de que el sistema del Banco del Pichincha no este en funcionamiento. Es importante destacar que este servicio notifica a ambas partes de cualquier movimiento transaccional con el propósito de mantener actualizado la información en ambas bases de datos.

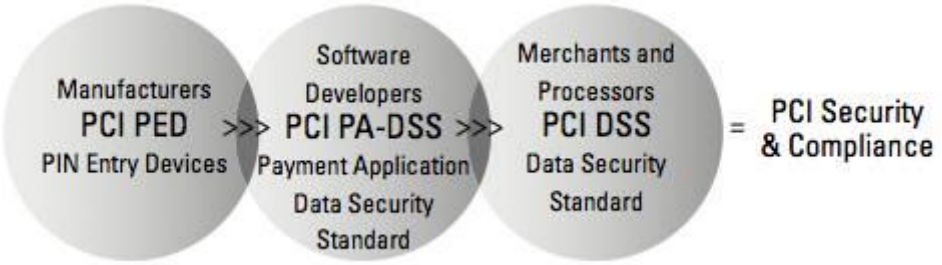
Capítulo IV: Propuesta de requerimientos para certificarse en PCI DSS

4.1 Analizar los requerimientos para construir y mantener una red segura, para proteger la información, de los tarjetahabientes, en tránsito, que exige la certificación PCI DSS, para asegurar la calidad transaccional bancaria

La información personal de los consumidores ha estado comprometida durante años. Más de 300 millones de registros en diferentes bases de datos han sufrido de alguna violación de seguridad durante los últimos años. Los datos más importantes son: datos del titular de la tarjeta, el número de cuenta y los datos confidenciales que se utilizan para la autentificación de las transacciones que se realiza con la tarjeta de crédito o débito. El punto más vulnerable de esta información se genera en los negocios que utilicen transacciones financieras. Como se conoce los negocios pequeños normalmente son los que tienen una seguridad menor y son los más atractivos para las personas que quieran robar información. El número de ataques a sistemas de procesamiento de tarjetas de crédito ha aumentado en los últimos 5 años.

El estándar PCI DSS se divide en tres sub estándares: PCI DSS aplicado para negocios u organizaciones que manejen pagos a través de tarjetas de crédito o débito, PA DSS se enfoca en los fabricantes de POS utilizados en los puntos de ventas y PED para los desarrolladores de software para el uso de tarjetas de crédito y débito.

Ilustración 3: Partes División del estándar PCI



Fuente: PCI compliance for dummies
Elaborado por: Sumedh Thakar, Terry Ramos

El estándar PCI es la clave principal para ayudar a los comerciantes a proteger la información de sus clientes protegiendo principalmente la información que contienen las tarjetas de banda magnética o chip.

Las tarjetas de banda magnética como cómo su nombre lo indica son tarjetas que tienen una banda magnética que contiene varios códigos e información del usuario de la tarjeta para poder identificarla rápidamente, estas pueden ser utilizadas para varios propósitos como: tarjetas de crédito o débito, cerraduras electrónicas, cajas fuertes, programas de fidelización, etc.

La banda magnética es de color marrón o negro y está localizada en la parte de atrás de la tarjeta, está hecha de finas partículas magnéticas en una resina. La banda está compuesta por tres pistas en las que se meten los datos dependiendo por la entidad que va a ser usada. Las pistas de la banda magnética y sus características se representaran en la siguiente tabla:

Tabla 9: Pistas de la banda magnética

# Pista	Densidad de grabación (bit por pulgada)	Información de contenido
1	210	79 caracteres alfanuméricos
2	27	40 caracteres numéricos
3	210	107 caracteres numéricos

Fuente: www.sesdi.com/cb/cgcodifica.html
Elaborada por: Juan Pablo Baquero, David Murillo

Este estándar está estructurado en base a seis objetivos que incluyen doce requerimientos. A continuación se describirán a detalle estos doce requerimientos para cumplir con los objetivos planteados en el estándar.

- **Construir y mantener una red segura**

  La red conecta terminales de pago de tarjetas, sistemas de procesamiento y el comercio en general. Identificando las vulnerabilidades de la red, un criminal puede tener acceso a la información de los titulares de las tarjetas de crédito. Por lo que es esencial que los comerciantes implementen los controles de este estándar con el fin de asegurar sus redes internas y las conexiones hacia redes externas que son utilizadas por terceros que procesan los datos de los titulares de las tarjetas de crédito.

  - **Instalar y mantener una configuración del firewall para proteger la información del titular de la tarjeta:** El firewall es una herramienta fundamental de seguridad que todo comerciante debe utilizar cuando la información de sus clientes dentro de su red interna es expuesta en el

internet. El firewall controla el tráfico de datos dentro de la red interna y entre redes internas y externas.

PCI demanda que se utilice procesos adecuados para asegurar que el firewall bloquee cualquier tipo de información maliciosa, también exige que se utilice estándares dentro de los routers que deben ser probados cada vez que se cambie o modifique un equipo o alguna configuración, esto debe realizarse cada seis meses. Además la configuración del firewall debe negar todo el tráfico de los datos del titular, exceptuando a los usuarios autorizados.

La configuración del firewall debe prohibir el acceso no autorizado a los componentes del sistema que contienen la información de los titulares de las tarjetas. El acceso a componentes no esenciales y los puertos también deben ser bloqueados. Se debe estar seguro que se instale software para configurar el firewall a cada dispositivo que administre este tipo de información.

- **No utilizar información predeterminada subministrada por el proveedor para contraseñas del sistema y otros parámetros de seguridad:** Es vital para los comerciantes utilizar contraseñas de alto nivel de seguridad. El error más común cometido por los comerciantes es no cambiar la contraseña por defecto. Estas contraseñas son fáciles de recuperar mediante un motor de búsqueda.

  El estándar PCI dicta a los comerciantes que desarrollen estándares de configuración para todos los componentes del sistema. Esto incluye cambiar las contraseñas por defecto de los equipos inalámbricos y cifrar cualquier acceso administrativo.

- **Proteger la información del titular de la tarjeta**

  Existen varias técnicas para proteger la información como: encriptación de los datos, método de truncamiento[10], enmascaramiento[11] de datos y método hash, entre otros. La información del titular esta impresa y almacenada en una tarjeta de crédito. Esta información se encuentra en la banda magnética o en un chip dentro de la tarjeta. El número de cuenta junto con el nombre del titular y la fecha de caducidad son los datos más importantes de una tarjeta de crédito. Esta información es procesada o almacenada dentro de la infraestructura del comerciante para luego ser transmitida mediante sistemas de redes.

  En la siguiente tabla se detallara como se deben manejar los tipos de datos al momento de que el usuario utiliza una tarjeta de crédito o débito.

Tabla 10: Tipos de información

Tipo de dato	Elemento de dato	Permitir almacenamiento	Solicitar protección	Ilegible
Datos del titular	Número de cuenta	Si	Si	Si
	Nombre del titular	Si	Si	No
	Código de servicio	Si	Si	No
	Fecha de expiración	Si	Si	No

[10] Truncamiento: es el término usado para reducir el número de dígitos a la derecha del separador decimal, descartando los menos significativos.

[11] Enmascaramiento: proceso que garantiza que la información original nunca estará disponible para el usuario final

Datos de autentificación	Datos de la banda magnética	No		
	CAV2/CVC2/ CVV2/CID	No		
	PIN/PIN block	No		

Fuente: PCI compilance for dummies
Elaborada por: Sumedh Thakar, Terry Ramos
Traducida por: Juan Pablo Baquero, David Murillo

- **Proteger la información almacenada del titular:** El estándar le indica al comerciante que debe mantener almacenada la información de sus clientes al mínimo y crear políticas de eliminación, retención de dicha información y limitar esta práctica estrictamente para propósitos de negocios o legales. Además se le indica al comerciante no almacenar información de autentificación ya que podría ser perjudicial para este y para los clientes.

  Las situaciones más comunes donde se reúne información del titular son en donde la tarjeta no está presente ya sea vía correo electrónico, teléfono o una aplicación web. La mayoría de robos de información ocurren cuando el comerciante no está al tanto de que dicha información se encuentra almacenada en su infraestructura. El estándar aconseja al comerciante analizar las aplicaciones que procesan la información de los titulares de las tarjetas con el fin de descubrir exactamente donde se encuentra esta información y eliminar todos los datos de autentificación.

Los comerciantes siempre deben hacer que el número de cuenta de la tarjeta sea ilegible incluyendo las copias de seguridad en los dispositivos de almacenamiento portátiles y también en los medios de redes inalámbricas. Existen tres soluciones generales para enmascarar el número de cuenta de las tarjetas de crédito:

- ✓ Utilizar funciones hash unidireccionales que solo muestren los datos de los índices que apuntan a los registros en la base de datos.
- ✓ Utilizar truncamiento para suprimir un segmento de datos y solo mostrar los últimos cuatro dígitos del número de cuenta de la tarjeta de crédito.
- ✓ Utilizar procedimientos de encriptación y procesos de administración de contraseñas. Estas contraseñas deben ser protegidas de divulgación y uso indebido por parte del comerciante.

- o **Encriptar la transmisión de los datos a través de redes públicas abiertas:** Los datos del titular que se trasladan a través de redes públicas abiertas deben estar encriptados para impedir que se vean comprometidos por terceras personas. El estándar PCI requiere que se utilice encriptación y protocolos de seguridad como SSL/TLS[12] o IPSec[13] para proteger la información durante la transmisión, también sugiere el uso de las mejores prácticas del estándar de la industria para implementar una fuerte encriptación para la autentificación y transmisión de datos.

[12] SSL/TLS: Secure Sockets Layer, en español capa de conexión segura/Transporter Layer Security en español seguridad de la capa de transporte

[13] IPSec: Internet Protocol security es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

- **Mantener un programa de administración de vulnerabilidad**

  La administración de la vulnerabilidad es un proceso que todo comerciante debe utilizar con el propósito de evitar el abuso de las debilidades en la infraestructura de pago con tarjeta. PCI señala los siguientes pasos para la administración de vulnerabilidad.

  - ✓ asegurar que las políticas de seguridad trabajen conjuntamente con el proceso de la administración de vulnerabilidad.
  - ✓ Mantener un seguimiento de los activos de TI para priorizar los elementos más importantes para la protección de los datos de los titulares de las tarjetas de crédito.
  - ✓ Desarrollar sistemas de exploración de vulnerabilidad.
  - ✓ Verificar las vulnerabilidades contra inventario.
  - ✓ Clasificar los riesgos de vulnerabilidad.
  - ✓ Realizar pruebas, desarrollar correcciones y generar soluciones.
  - ✓ Realizar un análisis para verificar cumplimientos.
  - **Utilizar y actualizar regularmente antivirus:** PCI solicita a los comerciantes que utilicen software de antivirus en todos sus sistemas que manejen información de titulares de tarjetas de crédito. PCI exige que se mantenga actualizados los antivirus y que siempre se estén ejecutando en cada dispositivo que administre datos de tarjetas de crédito.

- **Desarrollar y mantener aplicaciones y sistemas seguros:** Los ladrones de datos con frecuencia explotan las vulnerabilidades en los sistemas y aplicaciones que trabajan con información de tarjetas de crédito. Al adquirir aplicaciones de pago con tarjeta de crédito o débito se debe verificar que estén aprobadas por el consejo de estándares de seguridad PCI.

  Todos los días aparecen nuevas vulnerabilidades, por esto los comerciantes deben realizar auditorías y reparar las debilidades encontradas lo más pronto posible. El proceso de aplicación de parches requiere que los comerciantes utilicen estrategias para mantener sus aplicaciones y sistemas seguros, este proceso requiere los siguientes pasos:

  - ✓ Instalar el más reciente parche para los sistemas y aplicaciones de pago con tarjeta dentro de un mes de su lanzamiento.
  - ✓ Aplicar parches a sistemas y aplicaciones lo más pronto posible, basado en prioridades definidas por el proceso de administración de vulnerabilidades.
  - ✓ Seguir un proceso para asegurar que no se pase por alto una nueva vulnerabilidad.
  - ✓ Si se desarrolla su propia aplicación de pago con tarjeta, se debe seguir las mejores prácticas de la industria.
  - ✓ Estar al tanto de los procedimientos de cambio de control cada vez que se modifique el sistema de pagos con tarjetas o sus configuraciones.

- ✓ Basarse en instrucciones de codificación segura para aplicaciones web y utilizar un proceso para revisar y descubrir vulnerabilidades.

- ✓ Utilizar herramientas de pruebas de aplicaciones web para protegerlas de cualquier software malicioso. También se puede instalar in firewall de aplicaciones web.

- **Implementar medidas de control de acceso:** El control de acceso permite a los comerciantes autorizar o denegar a los medios físicos o técnicos para acceder al número de cuenta del titular o a otra información.

  - **Restringir el acceso a los datos de titulares de tarjetas:** PCI requiere que los comerciantes garanticen los derechos de al mínimo para sus empleados.

    Para implementar este requerimiento se debe desarrollar un sistema de control de acceso por cada elemento de la información del titular de la tarjeta.

  - **Asignar un identificador único a cada persona con acceso a la información:** Esto permite al comerciante rastrear todas las acciones electrónicas que realiza un determinado empleado. PCI sugiere implementar los siguientes pasos.

    - ✓ Asignar un nombre de usuario único a cada empleado antes de conceder derechos de acceso al sistema que administra la información de tarjetas de crédito.

    - ✓ Cada usuario se debe autentificar al sistema por medio de una contraseña. El estándar sugiere utilizar una autentificación remota, un controlador de acceso terminal o una red virtual privada.

- ✓ Todas las contraseñas deben ser ilegibles para cada componente que maneje información de tarjetas de crédito, tanto en el almacenamiento como en la transmisión de datos utilizando métodos de encriptación basando en estándares.

- ✓ Para empleados que no maneje esta información asegurarse de utilizar autentificación de usuario y derechos de acceso en todos los componentes del sistema.

- **Restringir el acceso físico a la información de titulares de tarjetas de crédito:** PCI indica a los comerciantes sobre la restricción física tanto para la información de las tarjetas de crédito como para los respaldos, este requerimiento se divide en 10 sub requerimientos:

  - ✓ Monitorear y limitar el acceso físico a los sistemas que administran y almacenan esta información.

  - ✓ Utilizar cámaras de video en puntos de entrada y salida y almacenar las grabaciones de estas por al menos tres meses.

  - ✓ Utilizar carnets de identificación para conocer para diferenciar entre un empleado y un visitante.

  - ✓ Autorizar la entrada a todos los visitantes antes de que ingresen a cualquier área donde se encuentre esta información.

  - ✓ Almacenar la información de todos los visitantes así como también todas sus actividades.

  - ✓ Asegurar los lugares que contengan respaldos de la información.

  - ✓ Asegurar toda información física y digital.

  - ✓ Controlar la distribución de esta información.

- ✓ Aprobar formalmente cualquier acción sobre esta información.
- ✓ Controlar el almacenamiento y accesibilidad de dicha información.
- ✓ Destruir cualquier medio que contenga esta información cuando ya no se la necesite.

- **Realizar pruebas a los sistemas y procesos de seguridad:** El estándar PCI sugiere desarrollar pruebas a los sistemas y procesos que manejen información de tarjetas de crédito con la intención de descubrir vulnerabilidades existentes. Los principales componentes que deben ser analizados son: Software personalizado, procesos, servidores, redes cableadas e inalámbricas. Es esencial realizar pruebas en el caso de efectuar modificaciones radicales como la ejecución de cambios en la configuración de los sistemas o la implementación de un nuevo software.

  Cada 90 días se deben ejecutar estas pruebas tanto en las redes internas como en las externas. PCI propone los siguientes puntos en relación a dichas pruebas:

  - ✓ Emplear un servicio de escaneo de vulnerabilidades en redes cableadas externas. Las redes internas deben ser analizadas por personal de nuestra organización mediante herramientas de escaneo.
  - ✓ Para redes inalámbricas, podemos emplear un analizador inalámbrico, una herramienta de detección de intrusiones o un servicio de prevención de intrusiones.
  - ✓ Monitorear el tráfico de datos en los sistemas mediante herramientas de detección de intrusiones.

- ✓ Utilizar software de monitoreo de integridad de archivos. Esto nos alerta cuando se realicen modificaciones no autorizadas a archivos del sistema, archivos de configuración o a cualquier archivo que perjudique nuestra información.

Al examinar las vulnerabilidades de los sistemas se exige que se presente un reporte con todos los resultados por cada uno de los componentes. Es necesario que el reporte organice la información mediante un sistema de clasificación de vulnerabilidad. PCI expone lo anterior con el siguiente ejemplo:

- ✓ Urgente: Virus troyano, lectura y escrito en archivos, ejecución remota de comandos
- ✓ Critico: Virus troyano, lectura de archivos
- ✓ Alto: Lectura de archivos, búsqueda en directorio de archivos
- ✓ Medio: Piratas cibernéticos pueden obtener información importante en archivos de configuración del sistema
- ✓ Bajo: Se puede leer archivos de configuración del sistema

- **Mantener una política de seguridad para la información:** Una organización comercial debe regir las actividades de seguridad PCI con sus políticas de seguridad. Basarse en buenas políticas ayuda al personal de TI a descubrir vulnerabilidades, remediar los agujeros de seguridad y generar la documentación esperada.

  - **Mantener una política que aborde la seguridad de la información para empleados y contratistas:** Las políticas y los controles de la organización comercial deben ser aplicadas a todo elemento que maneje información de tarjetas de crédito (computadores, servidores, redes internas y externas, aplicaciones). La siguiente lista describe a fondo lo anterior:

- ✓ Política formal: La política de seguridad debe cumplir con todos los requerimientos que señala el estándar PCI. Se necesita un proceso específico para identificar y evaluar las vulnerabilidades y sus riesgos.
- ✓ Procedimientos diarios: Asegurarse que las actividades de sus procedimientos diarios cumplan con los requerimientos del estándar.
- ✓ Políticas de uso: Todo empleado debe emplear políticas de uso en cada componente que maneje información de tarjetas de crédito.
- ✓ Responsabilidades claras: Los empleados y contratistas deben comprender claramente sus responsabilidades de seguridad de la información.
- ✓ Responsabilidades asignadas: Asignar responsabilidades a empleados específicos.
- ✓ Programa de seguridad: Instruir a los empleados sobre la importancia de la seguridad de la información de titulares de tarjetas de crédito.
- ✓ Selección de empleados: Se debe escoger cuidadosamente a los empleados que tendrán acceso a esta información.
- ✓ Selección de servicios por terceros: Si se comparte información con terceras personas, asegurarse que también cumplan con los requerimientos del estándar.
- ✓ Plan de respuesta a incidentes: Estar preparado con un plan detallado en respuesta a cualquier violación.

4.2 Definición del procedimiento para la migración a la versión actualizada de la norma, incluyendo requerimientos de hardware y software

La definición del procedimiento de migración a la norma actualizada de divide en seis etapas:

- Etapa I: Recolección de información

  En esta fase se recolectará toda la información sobre el capital humano, el hardware y el software de la institución financiera.

  - ✓ Capital humano: En esta sub fase se debe desarrollar encuestas al personal técnico y al usuario final con el propósito de saber el grado de conocimiento que tiene cada persona con respecto al estándar ISO:8583. Estas encuestas se emplearan para la capacitación de estas personas
  - ✓ Hardware: Es importante determinar el total de hardware que se tiene para la implementación del estándar y desarrollar un analizas de compatibilidad entre el hardware y el estándar.
  - ✓ Software: Se debe realizar un levantamiento de información sobre todos los programas y aplicaciones que se manejen en cada uno de los ordenadores con el fin de identificar cuáles de estos son de uso crítico.

- Etapa II: Capacitación

  El entrenamiento es esencial dentro del proceso de migración. Esta fase se divide en dos elementos:

  - ✓ Capacitación del personal: El propósito de la capacitación en el personal es facilitar el proceso de migración y que estos puedan dar soporte durante y después de este proceso.
  - ✓ Capacitación del usuario final: Una capacitación al usuario final posibilitara la adaptación y familiarización con el nuevo estándar.

- Etapa III: Migración parcial

  - ✓ Instalación de software: Mediante la recopilación de información previa se podrá desarrollar un análisis para identificar que programas o aplicaciones podrán ser instaladas. Además se debe documentar las aplicaciones y programas que serán eliminados o reemplazado.

  - ✓ Pruebas de software: Se debe realizar pruebas de compatibilidad entre el hardware y el software durante todo el proceso de migración. Estas pruebas tienen como objetivo determinar los riesgos de implementación y actualización del estándar. Es necesario tomar en cuenta los siguientes puntos:

    - ➢ Verificar la estabilidad del software que utiliza el nuevo estándar.

    - ➢ El software del nuevo estándar debe cumplir con las exigencias de la institución.

    - ➢ Cerciorarse que todas las funcionalidades del estándar puedan efectuarse.

    - ➢ Comprobar la compatibilidad del nuevo software con el hardware.

  - ✓ Pruebas de hardware: En este punto se verifica el buen funcionamiento de todo el hardware para identificar que elementos deben ser cambiados en cuanto a capacidad o velocidad al momento de ejecutar un proceso. También se podrá establecer cualquier elemento que no sea compatible con la nueva versión del estándar.

- Etapa IV: Migración total

  En base a las etapas anteriores se podrá ejecutar los pasos finales para la migración total del estándar tomando en cuenta cada uno de los elementos que intervienen en este proceso.

- Etapa V: Soporte a la migración desarrollada

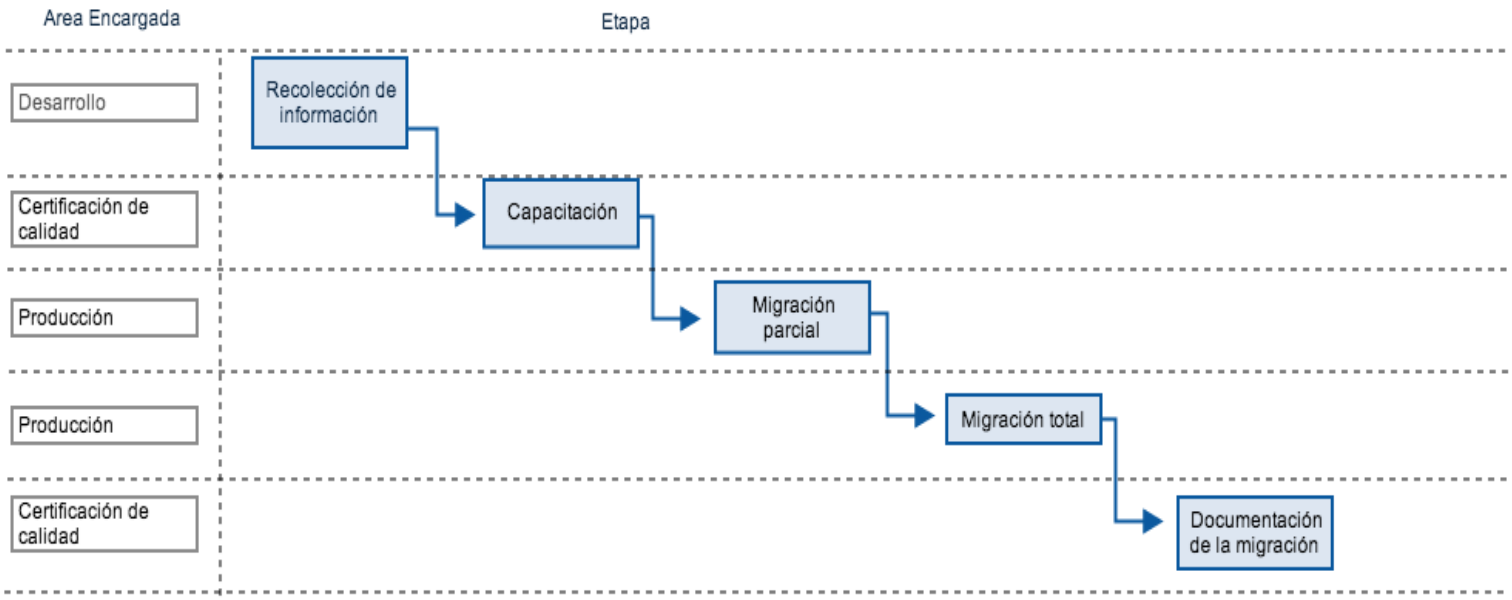
  En esta etapa el personal de soporte técnico estará encargado de solucionar todo problema relacionado a la migración. La cantidad de personal de soporte técnico dependerá de las necesidades y la tecnología que maneje la institución financiera.

- Etapa VI: Documentación de la migración

  En esta etapa se deberá documentar todo el proceso de migración. Es necesario documentar todas las modificaciones que se han realizado tanto en hardware como en software, igualmente se debe documentar cada una de las prueba efectuadas y sus resultados respectivos.

A continuación se presentará un diagrama de procesos en base al procedimiento de migración.

Ilustración 4: Diagrama de procesos Etapas de la migración



Fuente: Juan Pablo Baquero, David Murillo

Elaborado por: Juan Pablo Baquero, David Murillo

4.3 Matriz de elementos de mayor impacto para la implementación de la de la certificación PCI DSS para asegurar la calidad transaccional bancaria

Para la implementación del estándar PCI se debe tomar en cuenta todos los componentes del sistema. Estos componentes son conformados por: cualquier componente de la red, del servidor o de la aplicación que trabajan dentro del dominio de los datos del titular de la tarjeta. Este entorno administra y almacena toda la información del titular de la tarjeta y datos confidenciales de autentificación.

Los componentes de la red abarcan firewalls, routers, puntos de acceso, y cualquier aplicación de red o de seguridad. Al hablar de servidores tenemos la web, aplicaciones, correo electrónico, protocolos de red, entre otros. Por último las aplicaciones incluyen todo software o programa tanto interno o externo. La matriz presentada a continuación muestra los elementos más importantes a considerar al momento de instaurar el estándar.

Tabla 11: Elementos de impacto al momento de migrar

Elemento	Descripción
Segmentación de red	Este elemento no es requisito formal del estándar, sin embargo se aconseja utilizarlo para disminuir: • El riesgo de las empresas. • El costo de la evaluación del estándar. • La dificultad y el costo de la implementación y del mantenimiento de los controles del estándar. • El alcance de la evaluación del estándar. Para reducir el alcance del dominio de los datos del titular se debe comprender y analizar las necesidades de la organización y sus procesos correlacionados con el procesamiento almacenamiento y transferencia de datos. La adecuada segmentación de la red aísla los sistemas que almacenan, procesan o transfieren estos datos de los sistemas que no realizan estas operaciones.
Medios inalámbricos	Si se utiliza tecnología inalámbrica para gestionar la información del titular de la tarjeta se debe aplicar implementar los requerimientos y procedimientos de evaluación del estándar. La organización debe calcular el riesgo cuidadosamente al momento de usar esta tecnología.

Tabla 11: Elementos de impacto al momento de migrar

Tercerización	En el caso de proveedores de servicios que almacenan, procesan y transfiere este tipo de datos deben realizar una evaluación del estándar por su cuenta y justificar mediante pruebas a sus clientes para demostrar el cumplimiento de las seguridades.
Control de las instalaciones de la empresa y de los componentes del sistema	Para evaluar los requerimientos del estándar, el asesor debe seleccionar muestras representativas tanto de las instalaciones de la empresa como de los componentes del sistema. Estos ejemplares deben ser seleccionados tomando en cuenta lo siguiente: • Si existen procesos necesarios que cumplan con el estándar PCI en cada instalación, la muestra puede ser menos de lo que sería necesario y así asegurar que cada instalación esté estructurada de acuerdo al estándar. • La muestra debe ser lo suficientemente grande si existiera mas de un tipo de proceso estándar implementado. • Si no existen procesos estándares de PCI implementados, el tamaño de la muestra debe ser mayor para asegurar que todas las instalaciones conozcan e implementen de forma adecuada los requerimientos del estándar.
Controles de compensación	El asesor deberá revisar, validar documentar todos los controles de compensación e incluirlos en un informe de cumplimiento.

Fuente: exa.unne.edu.ar
Elaborada por: Sumedh Juan Pablo Baquero, David Murillo

4.4 Desarrollo de una propuesta con los elementos más importantes requeridos por la certificación PCI DSS, que sirva como guía práctica alineando a la realidad de BANRED

En este punto se tratará los elementos más importantes para cumplir con el estándar PCI. Todo comerciante que almacene, transmita o procese información de tarjetas de crédito debe cumplir con los requerimientos del estándar para poder asegurase de que los datos del cliente se están manejando con las mejores prácticas de seguridad. A continuación se redactará una guía para cumplir con el cometido.

1) **Comprender los principios esenciales del estándar PCI:** Antes de implementar todo lo que requiere el estándar se debe comprender las bases y requerimientos más importantes planteados por este. Estos requerimientos deben ser implementados de acuerdo a las necesidades del comerciante asegurándose de tener todos los elementos y la tecnología necesaria.

2) **Determinar los riesgos que existen al manejar la información de tarjetas de crédito:** El comerciante debe entender la naturaleza de los riesgos que amenazan a esta información durante todo el proceso de aceptación al momento de usar una tarjeta de crédito o de débito para realizar un pago. El estándar PCI describe los riesgos que recaen directamente en la responsabilidad del comerciante.

3) **Desarrollar y mantener una red segura:** Una red mantiene conectado las terminales de pago de tarjetas, sistemas de procesamiento de información y el comercio en general. Los comerciantes deben utilizar controles para proteger su red interna para evitar accesos no autorizados.

4) **Proteger la información de tarjetas de crédito que son almacenadas o transmitidas:** Un comerciante debe utilizar métodos te protección como encriptación de datos, truncamiento o enmascaramiento de datos. Estos métodos ayudan a que la información sea ilegible por terceras personas.

5) **Mantener un programa de administración de vulnerabilidades:** La administración de vulnerabilidades es un proceso que nos ayuda a evitar la explotación de debilidades en la infraestructura de pago con tarjeta. Se debe tener en cuenta que cada día se generan nuevas vulnerabilidades debido a defectos en el software, configuraciones deficientes en las aplicaciones o errores humanos. Este proceso regula continuamente el uso de herramientas de seguridad y el flujo de trabajo para eliminar riesgos.

6) **Implementar medidas de control de acceso:** Manejar el control de acceso nos permite aceptar denegar el uso de medios físicos o técnicos para acceder a la información de la tarjeta de crédito de un titular. Es necesario ejecutar políticas de acceso lógico y físico tanto a los registros físicos como a los digitales.

7) **Monitorear redes:** Se debe monitorear y supervisar todas las redes con el propósito de encontrar y resolver vulnerabilidades. Para redes externas se debe contratar un proveedor que realice pruebas trimestralmente. Si se realizan modificaciones a la infraestructura del sistema inmediatamente se debe ejecutar un escaneo de una red y se debe utilizar herramientas que almacenen registros de seguridad.

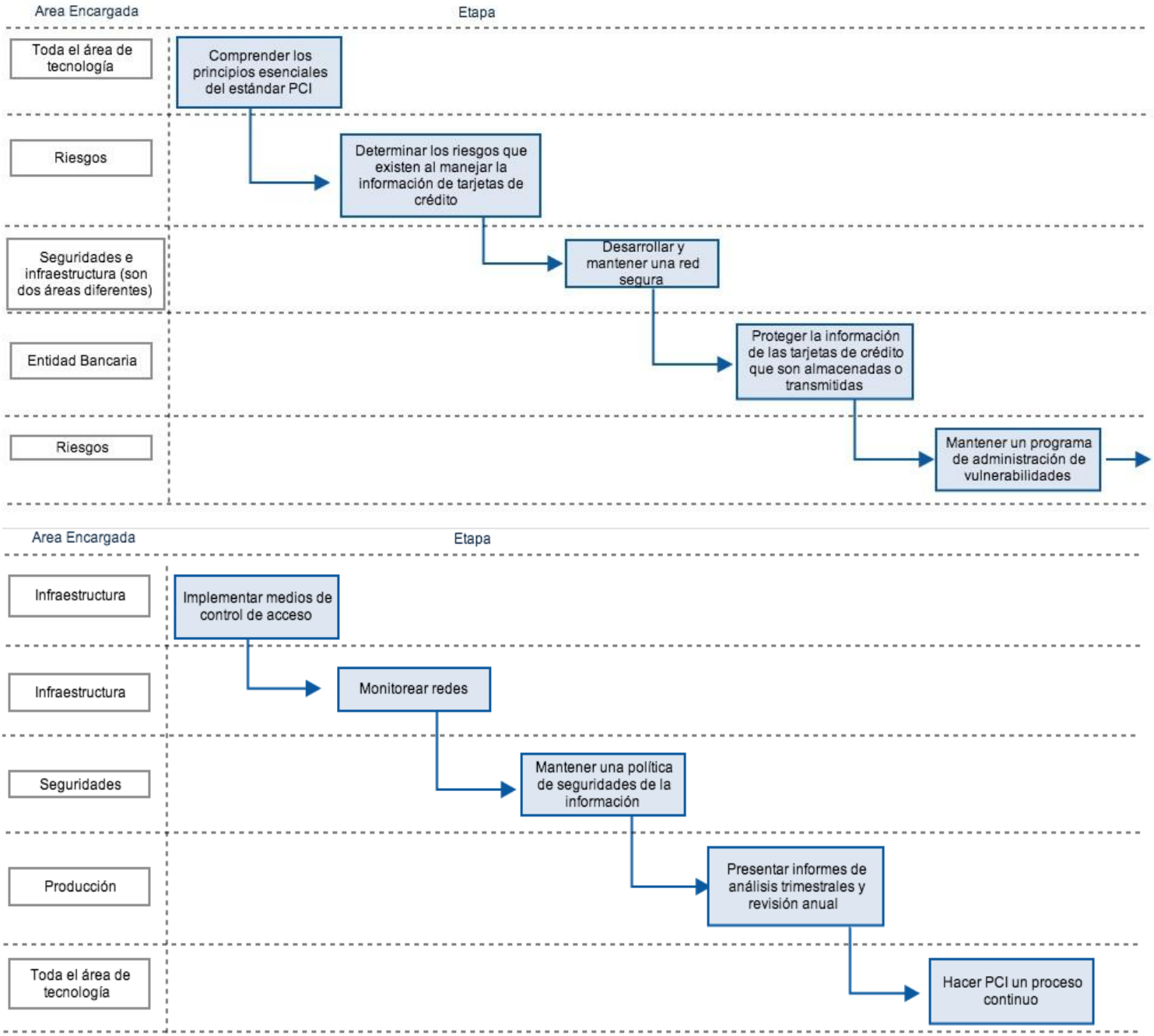
8) **Mantener una política de seguridad de la información:** Las políticas hacen que sea más fácil desarrollar y cumplir con los requerimientos del estándar PCI. Estas políticas colaboran con el hallazgo de vulnerabilidades, a remediar brechas de seguridad y a generar las debidas documentaciones.

9) **Presentar informes de análisis trimestrales y revisión anual:** Para cumplir con los requisitos del estándar se debe someter a un cuestionario de autoevaluación anual y trimestral, y desarrollar un análisis de los reportes generados por un proveedor aprobado. Alcanzar la certificación PCI e esencial para prevenir sanciones por parte de empresas financieras.

10) **Hacer a PCI un proceso continuo:** El comerciante debe persistir con el proceso de evaluación, corrección y presentación de informes con el fin de garantizar la seguridad continua de los datos de titulares de tarjetas de crédito.

A continuación se presentará un diagrama de procesos en base a los elementos más importantes de la certificación PCI DSS y las áreas encargadas.

Ilustración 5: Diagrama de procesos Guía de PCI DSS



Fuente: Juan Pablo Baquero, David Murillo
Elaborado por: Juan Pablo Baquero, David Murillo

Capítulo V: Conclusiones y recomendaciones

5.1 Conclusiones

- Generalmente la migración a un nuevo estándar en entornos profesionales es un proceso con nivel de complejidad alto pero no imposible. Por lo tanto debe asumirse con rigor y seriedad.

- Las pasividades técnicas del estándar ISO:8583 de 1993 son netamente superiores a las del estándar ISO:8583 de 1987 en cuanto a su acceso a los campos de datos para su adaptación y mejora en programas que sea utilizado. Sin embargo adaptar el estándar ISO:8583 de 1993 es un proceso que requiere un alto nivel de especialización el cual debe valorarse correctamente.

- La migración a un nuevo estándar requiere una correcta planificación y gestión del proceso. Es necesario valora con mucho esfuerzo los múltiples factores que influyen en el proceso y realizar planes de migración adecuaos para cada entorno.

- El proceso de migración consume cantidades importantes de recursos económicos y humanos. Por lo tanto se requiere de una planificación correcta de este proceso para luego no tener que lidiar con perdidas económicas de alto nivel.

- La migración requiere de mucho apoyo por parte de los gerentes de cada área que conforman la organización. La resistencia a los cambios es fuerte, por lo tanto es necesario que los gerentes de cada área brinden el apoyo con alto nivel de determinación.

- La certificación PCI DSS es una herramienta que proporciona credibilidad en la institución que lo sustenta. Esto facilita el acceso a cualquier tipo de mercados y ayuda al diseño y desarrollo de productos acordes a las necesidades de los consumidores por lo que mejora su competitividad.

- Es muy fácil realizar la clonación de una tarjeta ya que solo se debe se utiliza una máquina con un chip que permite copiar la información de las bandas magnéticas, estas maquinas suelen estar ubicadas en la puerta de cajeros automáticos o en los cajeros y receptores de compra en red., una vez que la tarjeta fue leída con esta máquina los datos se traspasan a un computador y son copiados a una tarjeta virgen.

- En sus esfuerzos por cumplir con los estándares PCI DSS para proteger los datos de las tarjetas de crédito o débito, muchas instituciones se han enfocado solo en el estándar, en lugar de concentrarse en la consecución de un nivel de seguridad que soporte el estándar.

- La clave del éxito de cumplimiento de PCI DSS es la construcción una infraestructura adecuada para ofrecer un nivel de seguridad conveniente. Identidad y gestión de acceso pueden ser una parte importante de dicha infraestructura, ayudando al mismo tiempo a cumplir con los objetivos específicos de las PCI DSS para el mantenimiento de una red segura, manejo de la vulnerabilidad, la aplicación de control de acceso fuerte y el control de la red.

5.2 Recomendaciones

- Los cambios de funcionalidad que produce la norma ISO:8583 de 1993 podrían afectar a las aplicaciones, scripts, procesos de mantenimiento y cualquier otro aspecto relacionado con el proceso de migración, por lo que es necesario que se ponga atención a estos cambios y se planifique como abordarlos antes de realizar la migración.

- Realizar la migración en un entorno de pruebas permitirá conocer posibles problemas, evaluar el impacto sobre el entorno y hallar una solución ante cualquier problema.

- Se deben realizar varias tareas previas a la migración para tener un proceso satisfactorio o en caso de que la migración tenga algún problema en el futuro estas tareas son: realizar una copia de la base de datos, guardar los valores de los parámetros de configuración, verificar que las bases de datos estén preparadas para la migración, etc.

- Un factor muy importante para realizar la migración es el análisis en profundidad de la situación de partida, el conocimiento detallado de los documentos o las aplicaciones de base de datos evita realizar ajustes imprevistos durante la migración y permite el establecimiento de planes de actuación con suficiente anticipación.

- Para una efectiva implementación de los programas de seguridad, y en especial para iniciar un proceso de certificación, es prudente que la empresa inicie por algo más elemental, como definir una cultura orientada a la excelencia en cuanto al manejo seguro de datos de los clientes.

Anexos

Laboratorio

Objetivos:

- Determinar los elementos principales de una banda magnética de una tarjeta.
- Definir cada una de las tres pistas dentro de una banda magnética.
- Analizar la información que se genera en un archivo de texto al utilizar una tarjeta y un lector de tarjetas de crédito.

Trabajo:

La banda magnética es una banda de color negra que forma parte de una tarjeta. Estas tarjetas pueden ser utilizadas como o para:

- Tarjetas de crédito
- Tarjetas de debito
- Cajas fuertes
- Cerraduras electrónicas

Esta banda magnética contiene información codificada que se utiliza para una determinada función. Esta información puede ser captada mediante un lector de tarjetas, además está distribuida en diferentes pistas. La estructura y el formato de esta información se encuentran regularizados por dos normas ISO (ISO7813 e ISO4909).

Ilustración 6: Ejemplo de una banda magnética

Fuente: http://ditechnology.com/mscri.html, tomado el 27 de octubre del 2013

La banda magnética contiene tres pistas:

- Track 1 (IATA)
- Track 2 (ABA)
- Track 3 (THRIFT-TTS)

Track 1

La pista Track 1 fue desarrollada por la Asociación Internacional de Transporte Aéreo (IATA). Esta pista contiene información alfanumérica y un máximo de 79 caracteres.

Track 2

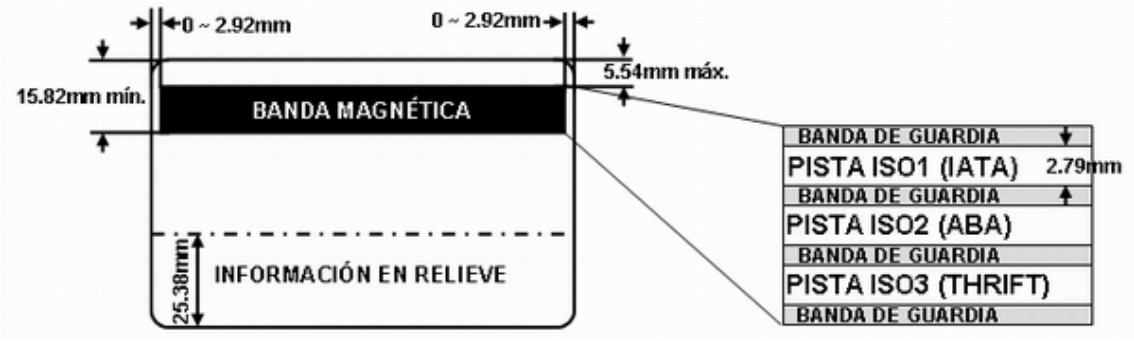
La pista Track 2 fue desarrollada por la Asociación Americana de Banqueros (ABA)

Esta pista contiene información alfanumérica y un máximo de 40 caracteres. Es utilizada constantemente por sistemas que requieren un número de identificación e información de control.

Track 3

Esta pista contiene información que puede ser actualizada en cada transacción que se realice. La información dentro de esta pista tiene un formato alfanumérico y un máximo de 107 caracteres.

Ilustración 7: Pistas de la banda magnética



Fuente: http://ditechnology.com/mscri.html, tomado el 27 de octubre del 2013

Para este laboratorio se necesitó una tarjeta que tenga banda magnética, un lector de tarjetas de banda magenta y una computadora. Con estas herramientas pudimos obtener la información de la tarjeta deslizándola por la cabeza del lector e inmediatamente todos los datos se desplegaron en un archivo de texto. Se observó que la información de la tarjeta estaba codificada con la excepción del nombre del titular de la tarjeta.

Ilustración 6: Lector de banda magnética

Fuente: http://ditechnology.com/mscri.html, tomado el 27 de octubre del 2013

Conclusiones:

- Al deslizar la tarjeta en un lector de banda magnética se pudo generar la información dentro de un archivo de texto.
- La información dentro de una tarjeta de crédito se encuentra codificada exceptuando el nombre del dueño de la tarjeta.
- No se necesita de ningún tipo de programa o software para observar la información de una tarjeta con banda magnética, solamente el lector y abrir un programa de texto.

Bibliografía

- ACI Worldwide Inc. (2010). *Base24-eps ISO 8583:1993 Host External Message Specifications.* Estados Unidos.

- ACI Worldwide Inc. (2007). *Base24 External Message.* Estados Unidos.

- Thakar S, Ramos T. (2009). *PCI Compliance for Dummies.* Inglaterra.

- Edwars J. (2001). Descripción ISO 8583. Recuperado el 21 de agosto del 2013, de http://es.scribd.com/doc/68082371/Descripcion-ISO-8583

- Suman K. (2010). Introduction to ISO 8583. Recuperado el 12 de septiembre del 2013, de http://www.codeproject.com/Articles/100084/Introduction-to-ISO-8583

- Herrera A. (2011). Migracion de Datos. Recuperado el 23 de junio del 2013, de http://www.mailxmail.com/curso-migracion-datos/migracion-datos

- González R. (2013). Cómo funciona: Tarjeta de banda magnértica. Recuperado el 2 de noviembre del 2013, de http://nosoloingenieria.com/como-funciona-tarjetas-banda-magnetica/

- Rouse M. (2012). PCI DSS. Recuperado 14 de septiembre del 2013, de http://searchdatacenter.techtarget.com/es/definicion/PCI-DSS-20

- Consejo PCI Security Standards, LLC. (2013). PCI DSS. Recuperado 5 de noviembre del 2013, de https://www.pcisecuritystandards.org/organization_info/contact.php

- Chile-Offshore. (2009). PCI DSS. Recuperado 5 de noviembre del 2013, de http://www.chileoffshore.com/es/articulos-interesantes/115-todo-sobre-iso8583