ESTÁNDAR ATM EMISOR

Objetivo

Este documento proporciona información acerca de la mensajería ISO: 8583 la cual representa los tipos de mensajes financieros utilizados por **PROSA** con las Entidades que utilizan este mismo método.

Premisas

El presente documento incluye una descripción global del mensaje: sus componentes, la estructura, El control del rechazo, y la diferencia entre el estándar de ISO y el estándar del producto utilizado por **PROSA**.

Historial

Fecha	Versión
16/01/02008	4.00
05/05/02008	4.01
05/03/02009	4.02
29/06/02009	4.03
04/07/2011	4.04
05/07/2011	5.0
18/11/2015	5.1

Control del Cambios

Descripción del Cambio	Versión	Solicitante del Cambio	Fecha de Actualización
Sección Correspondiente a TCP/IP.	4.02	Beatriz Huesca	Mar 02009
Data Element 28 Como Condicional.	4.02	Beatriz Huesca	Abr 02009
Parte del ACVV para Transacciones de VISA, Se Adicionan los de 22 y de 45 Como Condicionales para Estad Transacciones,	4.03	Beatriz Huesca	Jun 02009
Nota Especial para el de 3 Consulta de Cuenta(s).	4.03	Beatriz Huesca	Abr 2010
Tablas de Respuesta	4.03	Beatriz Huesca	Ene 2011
Integración de 23	4.04	Beatriz Huesca	Sept 2011
	5.0	Beatriz Huesca	Sept 2011
Cambio de Formato	5.1	Beatriz Huesca	Nov 2015

Tabla de Aprobación

Nivel	Nombre	Firma	Fecha de Actualización
Elaboración	Beatriz Elena Huesca Guevara		
Revisión	Claudio Copérnico Ávila		

Índice

ESTÁNDAR ATM EMISOR 1

CAPÍTULO 1: INTRODUCCIÓN 8

1.1. Convenciones Utilizadas en este Manual **8**

1.2 Espacios en Blanco **9**

CAPÍTULO 2: MENSAJE EXTERNO ISO 10

2.1 Componentes y Estructura del Mensaje Externo **10**
- 2.1.1 Data Prefix Characters. 10
- 2.1.2 IMS/CICS Transaction Codes 10
- 2.1.3 ISO Literal 10
- 2.1.4 Encabezado del Mensaje Externo (HEADER) 10
- 2.1.5 Tipo de Identificación de Mensajes (Message Type Indentification) 12
- 2.1.6 Message Class: Financial Transaction 13
- FINANCIAL TRANSACTION REQUEST (0200) 13
- FINANCIAL TRANSACTION REQUEST RESPONSE (0210) 13
- 2.1.7 Message Class: Reverse 13
- REVERSAL ADVICE (0420) 14
- REVERSAL ADVICE (0430) 14
- 2.1.8 Message Class: Network/ Administration 14
- NETWORK MANAGEMENT REQUEST (0800) 14
- NETWORK MANAGEMENT REQUEST RESPONSE (0810) 15
- 2.1.9 Timers 15

CAPÍTULO 3: BITMAP PRIMARIO 16

CAPÍTULO 4: DATA ELEMENTS 17

4.1 Mensajes Rechazados **17**

4.2 Variaciones de la Norma de ISO **17**
- 4.2.1 Elemento de Dato P-41 18
- 4.2.2 Elemento de Dato P-54 18
- 4.2.3 Data Element 102 Account Identification 1 18
- 4.2.4 Data Element 103 Account Identification 2 18

4.3 EMV Full Grade **18**

CAPÍTULO 5: ENCRIPCIÓN NIP Y MAC 20

5.1 NIP Encriptado 20

5.2 Llave de Encripción de Llaves ó ZMK (Zone Master Key) 20

5.3 Llave de Encripción de Pin, ZPK (Zone Pin Key) Ó ZWK (Visa) 20

5.4 Proceso de Generación de ZMK 20

CAPÍTULO 6: ISO EXTENAL MESSAGE 21

6.1 Tipos de Configuración de Datos 21

6.2 Tabla DE (Data Elements) 21

6.3 Data Elements Network 23

CAPÍTULO 7: DATA ELEMENTS 24

7.1 Data Elements 1 al 64 24
- 7.1.1 P-1 Secondary Bit Map 26
- 7.1.2 P-3 Processing Code 27
- 7.1.3 P-4 Transaction Amount 29
- 7.1.4 P-7 Transmission Date and Time 30
- 7.1.5 P-11 Systems Trace Audit Number 31
- 7.1.6 P-12 Local Transaction Time 32
- 7.1.7 P-13 Local Transaction Date 33
- 7.1.8 P-17 Capture Date 34
- 7.1.11 P-28 Transaction Fee Amount 38
- 7.1.12 P-32 Acquiring Institution Identification Code 39
- 7.1.13 P-35 Track 2 Data 40
- 7.1.14 P-37 Retrieval Reference Number 42
- 7.1.15 P-38 Authorization Identification Response 43
- 7.1.16 P-39 Response Code 44
- 7.1.17 P-41 Card Acceptor Terminal Identification 45
- 7.1.18 P-42 Card Acceptor Identification Code 46
- 7.1.19 P-43 Card Acceptor Name/Location 47
- 7.1.20 P-44 ATM Additional Response Data 48
- 7.1.22 P-48 ATM Additional Data 51
- 7.1.23 P-49 Transaction Currency Code 53
- 7.1.24 P-52 Personal Identification Number (PIN) Data 54
- 7.1.25 P-53 Security Related Control Information 55
- 7.1.26 P-54 Additional Amounts 56
- 7.1.27 P-60 ATM TERMINAL DATA 57

7.1.28 P-61 ATM Card Issuer and Authorizer Data 58
7.1.29 P-63 ATM PIN Offset 59

7.2 Data Elements 65 al 128 ..... **60**
7.2.1 S-70 Network Management Information Code 60
7.2.2 S-90 Original Data Elements 61
7.2.3 S-95 Replacement Amounts 63
7.2.4 S-100 Receiving Institution Identification Code 64
7.2.5 S-102 Account Identification 1 65
7.2.6 S-103 Account Identification 2 66
7.2.7 S-120 Key Management 67
7.2.8 S-122 Card Issuer Identification Code 68
7.2.9 S-123 Cryptographic Service Message 69
7.2.10 S-125 Account Indicator 75
7.2.12 S-126 Additional Data 76

CAPÍTULO 8: CÓDIGOS RESPUESTA 80

CAPÍTULO 9: TCP / IP HEADER 83

9.1 Configuración Sobre TCP/IP **83**

ANEXO 1: MANEJO DE TRANSACCIONES 85

ANEXO 2: MODELOS DE CONECTIVIDAD 88

2.1 Emisor Un Nodo **88**

2.2 Emisor Dos Nodos 91

GLOSARIO DE TÉRMINOS 95

DOCUMENTOS DE REFERENCIA: 95

----------FIN DEL DOCUMENTO ---------- **95**

Capítulo 1: INTRODUCCIÓN

1.1. Convenciones Utilizadas en este Manual

En esta sección se describe los acuerdos para la utilización de caracteres y formatos especiales.

El manual se describe en 2 idiomas Español e Inglés la parte correspondiente al idioma Inglés contiene los descriptivos internos de los mensajes respetando así la interpretación original de estos.

Mientras que cada Data Element tiene un significado y formato específico, el standard también incluye algunos campos de propósito general y algunos especiales para sistemas o países, los cuales varían sustancialmente en su forma y uso de una implementación a otra.

Cada campo se describe en un formato standard que define el contenido permitido del campo (numérico, binario, etc.) y el largo del campo (variable o fijo), de acuerdo a la siguiente tabla:

FORMAT	Significado
A	Alfanumérico, incluyendo los espacios
N	Sólo valores numéricos
S	Sólo caracteres especiales
AN	Alfanumérico
AS	Sólo caracteres alfanuméricos y especiales
NS	Sólo caracteres numéricos y especiales
ANS	Caracteres Alfabéticos, numéricos y especiales
B	Información binaria
Z	Tracks 2 y 3 code set como se define en la ISO 4909 y en ISO 7813.

Además, cada campo puede tener largo fijo o variable. Si es variable, el largo del campo será precedido por un indicador de largo.

Tipo	Significado
Fixed	Largo Fijo
LLVAR o (...xx)	Donde xx < 100, significa que los dos primeros dígitos indican el largo del campo

LLLVAR o (...xxx)	Donde xxx < 1000, significa que los tres primeros dígitos indican el largo del campo
Un campo LLVAR o LLLVAR puede ser comprimido o ASCII dependiendo del formato del mensaje que puede ser ASCII o Comprimido.	Por ejemplo un campo LLVAR puede tener 1 o 2 bytes, si está comprimido el hexa '23x significa que hay 23 elementos, si es ascii, bytes '32x, '31x significa que hay 21 elementos. Un elemento depende del tipo de dato, si es numérico este estará comprimido, ej. largo 87 se representará por un byte '87x, si es ASCII serán dos bytos '38x y '37x

El formato utilizado para representar la fecha así como la hora será la siguiente:

YY or YYYY = Year
MM = Month
DD = Day
HH = Hour
MM = Minute
SS = Second
Hh = Hundredths of a second
Mmmmmm = Microseconds (millionths of a second)

1.2 Espacios en Blanco

Dentro de este manual será requerido distinguir los espacios en blanco para lo cual se utilizara el símbolo **b-** indicando el espacio mencionado.

Capítulo 2: MENSAJE EXTERNO ISO

El mensaje externo está basado en ISO 8583:1987 publicado por la Organización Internacional de la Estandarización (ISO), permite intercambiar los mensajes entrantes y salientes, que pueden ser configurados individualmente, basados en el sistema de **PROSA** y las necesidades de la Entidad.

2.1 Componentes y Estructura del Mensaje Externo

El mensaje externo está estructurado y se basa en los siguientes elementos:

Componente	Longitud	Requerido
Data prefix characters	0–9 bytes	No
IMS/CICS transaction codes	0–9 bytes	No
ISO literal	3 bytes	Yes
Header	9 bytes	Yes
Message type identifier	4 bytes	Yes
Primary bit map	16 bytes	Yes
Data elements	Variable	Yes

2.1.1 Data Prefix Characters.

No usado.

2.1.2 IMS/CICS Transaction Codes

No usado.

2.1.3 ISO Literal

El aplicativo utilizado por **PROSA** usa y requiere la inclusión de las letras "**ISO**" ya que es un indicador de inicio de mensaje externo. Estos tres caracteres deben estar siempre presentes en todos los mensajes.

Ejemplo:

```
0030  86 C4 B8 94 00 00 03 67 49 53 4F 30 32 35 30 30.....gISO02500
0040  30 30 31 30 30 32 30 30  42 32 33 38 43 34 30 31  00100200B238C401
0050  32 38 41 31 38 30 31 41  30 30 30 30 30 30 30 30  28A1801A00000000
0060  31 30 30 30 30 31 42 43  30 30 30 30 30 30 30 30  100001BC00000000
```

2.1.4 Encabezado del Mensaje Externo (HEADER)

El Encabezado del mensaje externo es requerido para todos mensajes y debe incluir campos ISO en un inicio ya que es el indicador inicial para el Header. El encabezado del mensaje externo contiene 9 caracteres a lo largo del mensaje como se indica a continuación:

Posición	Longitud	Descripción
1-2	**2**	**Product Indicator** Indicates the product with which the message is associated. Valid values are as follows: 00 = Base (network management messages) 01 = ATM
3-4	**2**	**Release Number** Indicates the release of the product with which this message is associated. Many products support both current and previous release message formats. This field has an implied decimal point between the two numeric characters. The value for this field depends on the product and message format being used. The message format is specified in the RELEASE INDICATOR field on the product-specific Host Configuration File (HCF) screen. The following table shows the product, HCF screen number, RELEASE INDICATOR field setting, and the resulting value for this field. DEFAULT = 60
5-7	**3**	**Status** Indicates whether there was a problem with the interpretation of the message. If the message was rejected because of a security failure, this field indicates the reason. Valid values are as follows: 000= Undetermined 196 = Generic key synchronization error1 199 = Security device failure 0210 = MSG key synchronization error 211 = Invalid MSG error2 220 = MAC key synchronization error 221 = Invalid MAC error2 230 = PIN key synchronization error 231 = Invalid PIN error2 If the message was rejected because of bad data in the message, the ISO Host Interface process loads the bit map element number of the offending data element into this field and returns the message to the host.

8	**1**	**Originator Code (Acquirer)** Indicates the network entity that introduced the transaction to. Valid values are as follows: 0 = Undetermined 1 = Device controlled by a process 2 = Device Handler process 3 = Authorization process 4 = ISO Host Interface process 5 = Host 6 = Interchange Interface process or remote banking standard unit interface process 7 = Interchange or remote banking endpoint device 8 = Scheduled Transaction Initiator process 9 = XPNET Billpay Server process
9	**1**	**Responder Code (Issuer)** Indicates the network entity that created the response. Valid values are as follows: 5 = Host

2.1.5 Tipo de Identificación de Mensajes (Message Type Indentification)

La identificación del tipo mensaje es un código de cuatro-dígitos que identifica el propósito general del mensaje y es requerido para todos mensajes.

El estándar ISO 8583 define las clases y tipos de mensajes que determinan el tipo de transacción que se está realizando.

Estas clases y tipos se definen a continuación:

Clase de Mensajes (dos primeras posiciones)
- 02xx Financial transaction
- 04xx Reversal
- 08xx Network Management

Tipos de Mensajes (segundas dos posiciones)
- xx00 Request
- xx10 Request Response
- xx20 Advice
- xx30 Advice Response

2.1.6 Message Class: Financial Transaction

Los mensajes que inician con 02xx son mensajes financieros. Una transacción financiera aprobada afecta el saldo de la cuenta del titular de la tarjeta.

Los mensajes soportados son los siguientes:

Tipo	Descripción
0200	Financial Transaction Request
0210	Financial Transaction Response

FINANCIAL TRANSACTION REQUEST (0200)

Categoría: Interactivo (Requiere una respuesta (0210)
Flujo: Adquirente → **PROSA** → Autorizador (Emisor)
Tiempo: 15 Segundos

Un mensaje Financial Transaction Request (0200) solicita la aprobación de una transacción de:

1. Consulta de Saldo.
2. Disposición.
3. Cambio de Nip (Consultar estándar para cambio de Nip).
4. Venta Genérica (Consultar estándar para Venta Genérica).

El mensaje 0200 requiere una respuesta con un mensaje 0210 con un código de aprobación o rechazo de la transacción de acuerdo a los códigos de respuesta descritos en el Anexo A.

FINANCIAL TRANSACTION REQUEST RESPONSE (0210)

Categoría: Interactivo (Requiere previo un mensaje 0200)
Flujo: Autorizador (Emisor) → **PROSA** → Adquirente
Tiempo: 15 Segundos

Un mensaje 0210 es la respuesta a un mensaje 0200 con un código de aprobación o rechazo de la transacción de acuerdo al Anexo A.

2.1.7 Message Class: Reverse

Los mensajes 04xx se utilizan para realizar reversos de un mensaje de requerimiento que previamente ha sido autorizado.

Los mensajes soportados son los siguientes:

Tipo	Descripción	Restricción
0420	Acquirer Reverse Notice	

0430	Acquirer Reverse Response	Only if the Text Ack messages are configurate in the Issuer

REVERSAL ADVICE (0420)

Categoría: No Interactivo (No es obligatoria la respuesta del mensaje con un 0430)
Flujo: Adquirente → **PROSA** → Autorizador
Tiempo: 15 segundos

Un mensaje 0420 notifica al autorizador el reverso de la transacción que previamente había sido autorizada.

REVERSAL ADVICE (0430)

Categoría: N/A
Flujo: Autorizador (emisor) → **PROSA** → Adquirente
Tiempo: 15 Segundos

Respuesta a la solicitud del mensaje 0420.

2.1.8 Message Class: Network/ Administration

Los mensajes 08xx son usados para la administración de mensajes de la red y para realizar funciones de seguridad.

Los mensajes son los siguientes:

Tipo	Descripción
0800	Network Management Request
0810	Network Management Request Response

Los mensajes de Administración del Emisor manejan el estado operacional de las líneas de comunicación entre el aplicativo utilizado por **PROSA** y el Host.

El aplicativo utilizado en **PROSA** soporta cuatro tipos de mensajes de Administración del Emisor:

- Mensajes de logon
- Mensajes de prueba de Echo
- Mensajes de Log off

Los mensajes de Echo Test, Logon y Log off se mandan como mensajes 0800. El cambio de llave, una nueva llave o repetición de llave son datos que se transportan en los mensajes 0800.

NETWORK MANAGEMENT REQUEST (0800)

Categoría: Interactivo (requiere respuesta 0810)

Flujo: **PROSA** → Autorizador o Emisor
Tiempo: 30 Segundos en caso de no recibir una respuesta enviara un Logon

Es usado para enviar mensajes de Echo Test, Logon, Log off.

NETWORK MANAGEMENT REQUEST RESPONSE (0810)

Categoría: Interactivo (Requiere respuesta 0800)
Flujo: Emisor → **PROSA**
Tiempo: 30 Segundos en caso de no recibir una respuesta enviara un Logon

Es la respuesta del Echo Test, Logon, Log off.

Para mayor especificación consultar el estándar de mensajes 0800 y 0810 para Intercambio de llaves.

2.1.9 Timers

El tiempo establecido para este tipo de transacciones deberá de ser de 15 sec. esto da la salida de la respuesta hacia PROSA.

Capítulo 3: BITMAP PRIMARIO

El BITMAP primario es un campo de 16 posiciones que es requerido para todos los mensajes. Representa los datos de los 64 bits iniciales. En el BITMAP se identifica con 1 la presencia o con 0 la ausencia de los primeros 64 elementos del mensaje.

De los 16 bytes que están en notación hexadecimal al realizar la conversión a binario se despliega los elementos de datos que están presentes o ausentes.

Al convertir los 64 bits a 16 bytes, los primeros 64 bits son divididos en 4 grupos de 16, entonces, a cada grupo de 4 bits se asigna su equivalente hexadecimal según la siguiente tabla:

Valor en Hexadecimal	Valor del Bit	Valor en Hexadecimal	Valor del Bit
0	0000	8	1000
1	0001	9	1001
2	0010	A	1010
3	0011	B	1011
4	0100	C	1100
5	0101	D	1101
6	0110	E	1110
7	0111	F	1111

Estos valores permiten identificar que campos están habilitados en el mensaje, ejemplo:

B	2	3	8	C	4	0	1	2	8	A	1	8	0	1	A
1011	0010	0011	1000	1100	0100	0000	0001	0010	1000	1010	0001	1000	0000	0001	1010
1,3,4	7,	11,12	13	17,18	22,		32	35	37	41,43	48	49		60	61,63

En este caso el armado de la transacción queda de la siguiente forma:

1,3,4,7,11,12,13,17,18,22,32,35,37,41,43,48,49,60,61,63,

Capítulo 4: DATA ELEMENTS

El mensaje externo permite la transmisión de los 128 elementos de datos que forman parte del estándar ISO 8583:1987. Sin embargo, no todos los elementos de datos son utilizados para ser procesados por la aplicación, muchas veces solo un número pequeño de datos es requerido.

Una ventaja del ISO es que permite incluir solo los elementos de datos que realmente se requieren en el mensaje externo dentro de los límites del aplicativo utilizado por **PROSA** y de los requisitos de la norma ISO.

Los valores fijos pueden ser sustituidos por la red Emisora, es decir, incluir o excluir otros elementos de datos en un mensaje. La aplicación permite que la red Emisora realice estas combinaciones en los elementos de datos incluidos en sus mensajes.

Para el intercambio de los mensajes entre entidades debe considerarse el Estándar ISO para garantizar el procesamiento correcto de las transacciones.

4.1 Mensajes Rechazados

Si el aplicativo usado por Prosa recibe un mensaje externo que no puede ser procesado o reformateado para uso interno debido a datos erróneos o fallas en el esquema de seguridad se rechaza el mensaje como sigue:

1. Cambia la primera posición del **Message Type** a un valor de 9 (por ejemplo, un mensaje 0200 lo cambia por un 90200 y un mensaje 0420 lo cambia por un mensaje 90420).

2. La razón del rechazo se indica en el campo de **STATUS** dentro del **Header** en el mensaje externo. Si el mensaje fue rechazado debido al esquema de seguridad, al campo de **STATUS** se le coloca un valor entre 196 y 199. Si el mensaje fue rechazado debido a datos erróneos, en el campo de **STATUS** se indica el número de BIT del elemento de datos que causo el rechazo (por ejemplo, si los datos del Track 2 en P-35 no pueden ser analizados, el campo de **STATUS** presenta el valor 035).

3. Regresa el mensaje externo al EMISOR que originó el mensaje.

Las acciones anteriores aplican a cualquier mensaje que no pueda ser procesado y no simplemente a aquellos que requieren una respuesta.

4.2 Variaciones de la Norma de ISO

El mensaje externo varía de la norma ISO por lo que el Emisor debe considerar la especificación de PROSA en sus desarrollos.

Por ejemplo:

4.2.1 Elemento de Dato P-41

Tiene una longitud de 16 posiciones en lugar de las 8 posiciones prescritas por ISO. Esto permite que el aplicativo utilizado en **PROSA** soporte las 16 posiciones para identificar a los Cajeros Automáticos (ATMs).

4.2.2 Elemento de Dato P-54

Tiene una longitud variable prescrita por ISO, conteniendo un código de montos a seis posiciones. El aplicativo usado por **PROSA** define P-54 como un elemento de datos de longitud fija de 12 posiciones.

4.2.3 Data Element 102 Account Identification 1

Este data element indica el FROM account y no es utilizado en forma mandatorio, se utiliza en casos especiales en donde el cliente lo solicita como parte de la funcionalidad de sus transacciones

4.2.4 Data Element 103 Account Identification 2

Este data element indica el TO account y no es utilizado en forma mandatorio, se utiliza en casos especiales en donde el cliente lo solicita como parte de la funcionalidad de sus transacciones

4.3 EMV Full Grade

Esta sección nos permite conocer cuales elementos son necesarios para el envió de los valores para poder transaccionar con mensajes de EMV FULL.

TOKEN	DESCRIPCION	ADQUIRENTE	EMISOR
B2	REQUEST DATA TOKEN	M	
B3	DISCRETIONARY DATA TOKEN	M	
B4	STATUS TOKEN	M	C
B5	RESPONCE DATA TOKEN		M
B6	SCRIPT DATA TOKEN		M
BJ	RESULT SCRIPT DATA TOKEN	C	

Descripción:

1. ***EMV REQUEST DATA TOKEN (B2)*** Contiene los 13 Data Elements Mínimos para la realización de la transacción de EMV. (*Para mayor información del detalle de campos ir al descriptivo del token B2 descrito en el manual de EMV Full)*

2. ***EMV DISCRETIONARY DATA TOKEN (B3)*** Contiene otros Data Elements definidos en más de una norma de la aplicación del mensaje que ha sido implementado junto al proceso de EMV (*Para mayor información del detalle de campos ir al descriptivo del token B3 descrito en el manual de EMV Full)*

3. ***EMV STATUS TOKEN (B4)*** Contiene el control de información que no es necesariamente especificada para transacciones de EMV (*Para mayor*

información del detalle de campos ir al descriptivo del token B4 descrito en el manual de EMV Full)

4. ***EMV RESPONSE DATA TOKEN (B5)*** Contiene los Data Elements necesarios para generar la respuesta de la transacción, junto con los Falgs para el Script Command (*Para mayor información del detalle de campos ir al descriptivo del token B5 descrito en el manual de EMV Full)*

5. ***EMV SCRIPT DATA TOKEN (B6)*** contiene los comandos necesarios para la realización del Script Command (*Para mayor información del detalle de campos ir al descriptivo del token B6 descrito en el manual de EMV Full)*

6. ***RESULT SCRIPT DATA TOKEN (BJ)*** Contiene La respuesta necesaria para indicar si fue aplicada o no Script Command (*Para mayor información del detalle de campos ir al descriptivo del token B6 descrito en el manual de EMV Full.)*

Todos los elementos viajaran a través de Tokens, los cuales deberán de cumplir con las especificaciones que se indican más adelante en este manual.

Capítulo 5: ENCRIPCIÓN NIP Y MAC

5.1 NIP Encriptado

Procesando el acceso al módulo de seguridad para NIP. Todos los NIPS se manejan bajo las llaves de seguridad de un módulo de seguridad.

Las llaves entre PROSA y el HOST son llamadas llaves de zona ya que establecen "zonas" criptográficas entre entidades.

Se establece una jerarquía de llaves de dos niveles entre Bancos y un Switch.

- Llave "Maestra" intercambiada manualmente (ZMK).
- Llave de "Trabajo" intercambiada electrónicamente (ZPK).

5.2 Llave de Encripción de Llaves ó ZMK (Zone Master Key)

- Debe ser distribuida manualmente.
- Almacenada en la base de datos del Host, en terminología VISA es llamada ZCMK.
- Cualquier otra llave de trabajo deberá ser distribuida electrónicamente bajo encripción de la ZMK.
- Se debe seguir la norma X9.17 la cual especifica el método ECB para la encripción de llaves.

5.3 Llave de Encripción de Pin, ZPK (Zone Pin Key) Ó ZWK (Visa)

- Puede ser también llamada llave de trabajo de zona.
- Se distribuye electrónicamente encriptada bajo una ZMK.

5.4 Proceso de Generación de ZMK

- La llave Maestra de Zona puede ser de longitud sencilla o doble, según se requiera.
- Generación Manual de componentes de ZMK (normalmente se usan de 2 a 3 componentes).
- Encripción manual de cada uno de los componentes.
- Combinación manual de los componentes encriptados.
- Una vez que los componentes se instalan, el valor de verificación se usa para confirmar que se hayan ingresado datos correctos en ambos extremos.

Capítulo 6: ISO EXTENAL MESSAGE

El aplicativo usado en **PROSA** utiliza la siguiente configuración para determinar como un elemento de datos es especificado en el mensaje externo. Esta especificación se utiliza a lo largo de esta sección.

6.1 Tipos de Configuración de Datos

M = Mandatorio. El elemento se requiere en el mensaje.
C = Condicional. El elemento es obligatorio bajo ciertas condiciones.
b- (espacio en blanco) = No Usado. El elemento no es incluido en el mensaje.

El Switch intercambiará los datos Mandatarios y Condicionales entre todas las Entidades y no realiza validaciones para la autorización o rechazo de las transacciones.

6.2 Tabla DE (Data Elements)

Campo	Data Element	0200	0210	0420	0430
P-1	Secondary Bit Map	M	M	M	M
P-3	Processing Code	M	M	M	M
P-4	Transaction Amount	M	M	M	M
P-7	Transmission Date and Time	M	M	M	M
P-11	Systems Trace Audit Number	M	M	M	M
P-12	Local Transaction Time	M	M	M	
P-13	Local Transaction Date	M	M	M	
P-17	Capture Date	M	M	M	
P-22	Point of Service Entry Mode	C	C	C	C
P-23	Card Sequence Number	C	C	C	C
P-28	Transaction fee amount	C	C		
P-32	Acquiring Institution Identification Code	M	M	M	M
P-35	Track 2 Data	M	M	M	M
P-37	Retrieval Reference Number	M	M	M	M
P-38	Authorization Identification Response		M	M	
P-39	Response Code		M	M	M
P-41	Card Acceptor Terminal Identification	M	M	M	M
P-42	Card Acceptor Identification Code	C	C	C	
P-43	Card Acceptor Name/Location	M		M	

P-44	Additional Response Data		C		
P-45	Track I Data	C			
P-48	Additional Data	M			
P-49	Transaction Currency Code	M	M	M	M
P-52	Personal Identification Number (PIN) Data	M			
P-54	Additional Amounts	C	C	C	
P-60	Terminal Data	M	M	M	
P-61	Card Issuer and Authorizer Data	M	M	M	
P-63	PIN OFFSET	C	C	C	
S-90	Original Data Elements			M	M
S-95	Replacement Amounts			C	C
S-100	Receiving Institution Identification Code	M	M	M	
S-102	Account Identification 1	C	C	C	
S-103	Account Identification 2	C	C	C	
S-122	Card Issuer Identification Code		C	C	
S-125	Account Indicator/Statement Print Data	C	C	C	
S-126	Additional Data	C	C	C	C

6.3 Data Elements Network

Campo	Data Element	0800	0810
P-1	Secondary Bit Map	M	M
P-7	Transmission Date and Time	M	M
P-11	Systems Trace Audit Number	M	M
P-39	Response Code		M
P-53	Security Related Control Information	C	C
S-70	Network Management Information Code	M	M
S-120	Issuer Key Management	C	C
S-123	Cryptographic Service Message	C	C

Capítulo 7: DATA ELEMENTS

Los data Elements Descritos a continuación son 128 los cuales están divididos en Campos Primarios y Secundarios los valores que se tienen para cada uno de ellos están descritos en forma individual para su mejor entendimiento, recordando que para la mensajería financiera nacional se han determinado una serie de ellos como Mandatorios y otros como condicionales esto NO IMPIDE QUE ALGUNA INSTITUCION REQUIERA DE OTRA INFORMACION la cual viaja dentro de estos 128 Data Elements como uso personal de las transacciones para lo cual es importante colocarlo como Condicional para no afectar el resto de la funcionalidad actual.

7.1 Data Elements 1 al 64

Los Data Elements son los campos individuales que llevan la información sustancial acerca de la transacción. Hay 128 campos definidos en el standard ISO 8583:1987, y 192 en posteriores releases. La revisión de 1993 agregó nuevas definiciones, eliminó algunas pero sin embargo dejó el formato del mensaje sin cambios.

Mientras que cada Data Element tiene un significado y formato específico, el standard también incluye algunos campos de propósito general y algunos especiales para sistemas o países, los cuales varían sustancialmente en su forma y uso de una implementación a otra.

Cada campo se describe en un formato standard que define el contenido permitido del campo (numérico, binario, etc.) y el largo del campo (variable o fijo), de acuerdo a la siguiente tabla:

FORMAT	Significado
A	Alfanumérico, incluyendo los espacios
N	Sólo valores numéricos
S	Sólo caracteres especiales
AN	Alfanumérico
AS	Sólo caracteres alfanuméricos y especiales
NS	Sólo caracteres numéricos y especiales
ANS	Caracteres Alfabéticos, numéricos y especiales
B	Información binaria
Z	Tracks 2 y 3 code set como se define en la ISO 4909 y en ISO 7813.

Además, cada campo puede tener largo fijo o variable. Si es variable, el largo del campo será precedido por un indicador de largo.

Tipo	Significado
Fixed	Largo Fijo

LLVAR o (…xx)	Donde xx < 100, significa que los dos primeros dígitos indican el largo del campo
LLLVAR o (...xxx)	Donde xxx < 1000, significa que los tres primeros dígitos indican el largo del campo
Un campo LLVAR o LLLVAR puede ser comprimido o ASCII dependiendo del formato del mensaje que puede ser ASCII o Comprimido.	Por ejemplo un campo LLVAR puede tener 1 o 2 bytes, si está comprimido el hexa '23x significa que hay 23 elementos, si es ascii, bytes '32x, '31x significa que hay 21 elementos. Un elemento depende del tipo de dato, si es numérico este estará comprimido, ej. largo 87 se representará por un byte '87x, si es ASCII serán dos bytos '38x y '37x

7.1.1 P-1 Secondary Bit Map

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-1	AN	16	Secondary Bit Map	C	M	M	M

The secondary bit map identifies the presence or absence of data elements 65 through 126 in the System external message. It functions the same as the primary bit map, except that the primary bit map identifies the presence or absence of data elements 1 through 64 and the secondary bit map identifies the presence or absence of data elements 65 through 126.

The secondary bit map is required if any of data elements 65 through 126 are included in the message. Otherwise, it is not used.

The presence or absence of the secondary bit map is identified by bit position 1 in the primary bit map. Data elements 65 through 126 cannot be included in the message if the secondary bit map is not present.

7.1.2 P-3 Processing Code

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-3	N	6	Processing Code	M	M	M	M

The Processing Code data element contains a series of digits used to describe the effect of a transaction on the customer account and the accounts affected.

This data element is mandatory for all messages except network management messages.

The internal transaction codes are translated to and from external transaction codes by the ISO Host Interface processes.
The Valid Values are:

TRAN-CDE (transaction code)
C. ISO VALOR
C. ISO VALOR
01 Servicio Correcto (Disposición)
31 Servicio Correcto (Consulta)
03 Check guarantee (funds guaranteed)
04 Check verification
92 Check cash
21 Deposit
22 Deposito Crédito
37 Consulta SPEI
38 Consulta de cuentas
40 Cardholder accounts transfer
42 SPEI
90 Payment enclosed
91 Message to financial institution
93 Log-only transaction
94 Statement print
96 PIN change
97 EMV PIN Unblock
65 Generic Sale
97 Aviso Cambiar NIP

No account specified
20 Checking account type
10 Savings account type
30 Credit account type
9M Other account type

ISO
00 Not Account Specified

10 Savings
20 Checking
30 Credit

TO-ACCT-TYP (to account type)
00 ISO= Not Account Specified

La consulta de saldo normalmente es de 1 cuenta pero se puede tener multicuentas el desglose de estas depende directamente de la funcionalidad requerida por el cliente y en el caso de solicitar múltiples cuentas se activa un token el cual nos permitirá obtener en pantalla la información requerida.

7.1.3 P-4 Transaction Amount

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-4	N	12	Transaction Amount	M	M	M	M

The Transaction Amount data element contains the amount of funds requested (either for debit or credit) in the currency of the source location of the transaction.

Decimalization of the amount is implied by the Transaction Currency Code (P-49) data element. For example, if the currency code indicates U.S. dollars, 000000001000 would indicate $10.00. However, if the currency code indicates lire, the amount would be 1000 lire.

7.1.4 P-7 Transmission Date and Time

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-7	N	10	Transmission Date and Time	M	M	M	M

The Transmission Date and Time data element contains the time the message is initiated by the message originator. This time is set for each outgoing message and is expressed in Greenwich mean time.

The Transmission Date and Time data element is mandatory for all message types

7.1.5 P-11 Systems Trace Audit Number

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-11	N	6	Systems Trace Audit Number	M	M	M	M

The Systems Trace Audit Number data element contains a number that must be set by a message sender and echoed by a message receiver. It is used for matching responses to original messages and is not intended to remain the same throughout the life of a transaction (for example, a reversal may not have the same number as the original transaction).

The Systems Trace Audit Number data element is mandatory for all messages to and from products.

NETWORK MANAGEMENT

In network management messages, the systems trace audit number is used to match the network management request with its response. The ISO Host Interface process generates the number on outgoing 0800 messages and expects it to be returned in the corresponding 0810 messages. On outgoing 0810 messages, the ISO Host Interface process echoes the number sent in the corresponding 0800 messages

7.1.6 P-12 Local Transaction Time

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-12	N	6	Local Transaction Time	M	M	M	

The Local Transaction Time data element contains the local time at which the transaction began at the card acceptor location.

Since a terminal can be geographically removed from the system by one or more time zones, processes maintain time zone offsets for terminals defined to the system. These offsets allow processes to compute local transaction times and dates for transactions originating at terminals. The time zone offset for a terminal is applied to the system date and time to derive the local date and time for the transaction.

When a transaction originates at an acquirer host, it is assumed that the content of this data element is the terminal local time.

The Local Transaction Time data element carries the time as six characters (HHMMSS). Internally, processes carry this time as eight characters (HHMMSShh), which includes hund Adquiretneths of seconds in the right-most two positions. On incoming messages, the hund Adquiretneths of seconds are set to zeros. On outgoing messages, the hund Adquiretneths of seconds are truncated.

7.1.7 P-13 Local Transaction Date

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-13	N	4	Local Transaction Date	M	M	M	

The Local Transaction Date data element contains the local month and day that the transaction began.

Since a terminal can be geographically removed from the system by one or more time zones, processes maintain time zone offsets for terminals defined to the system. These offsets allow processes to compute local transaction times and dates for transactions originating at terminals. The time zone offset of the terminal is applied to the system date and time to derive the local date and time for the transaction.

When a transaction originates at an acquirer host, it is assumed that the content of this data element is the terminal local date.

The Local Transaction Date data element carries the date as four characters (MMDD). Internally, processes carry this date as six characters (YYMMDD), which includes the year in the left-most two positions. On incoming messages, the year is set to the current year. On outgoing messages, the year is truncated.

7.1.8 P-17 Capture Date

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-17	N	4	Capture Date	M	M	M	

The Capture Date data element contains the month and day the transaction was processed by a process.

This date equates to the date of the transaction log file to which the transaction is logged (each product has its own transaction log file).

Processes move to a new processing date each day at logical network cutover.

The Capture Date data element carries the date as four characters (MMDD). Internally, processes carry this date as six characters (YYMMDD), which includes the year in the left-most two positions. On incoming messages, the year is set to the current year. On outgoing messages, the year is truncated.

7.1.9 P-22 Point of Service Entry Mode

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-22	N	3	Entry Mode	C	C		

The Point of Service Entry Mode data element is a single field that contains two codes. The first code is two digits in length and indicates the method by which Track data or the primary account number (PAN) was entered into the system. The second code is one digit in length and indicates the entry capabilities available at the point of service.

> **Note:** A value of 01 in the first code of the Point of Service Entry Mode indicates that the Track data was entered manually and that the PIN entry capabilities at the point of service are unknown.

Values by position:

Place 1-2
00: Unknown
05: Integrated circuit read
07: Contactless M/Chip
80: FallBack
90: Magnetic stripe read and exact content of
track1 o track2 included
91: Contactless (Track2 o Track1 completo)
95: Integrated circuit card; CVV data may be unreliable

Place 3:
0: Unknown
1: Terminal can accept entry of PINs
2: Terminal cannot accept entry PINs
8: Terminal PIN pad down
Valid values for the first and second digits are listed below.
00 = Unspecified
02 = Magnetic stripe
05 = Integrated circuit card
07 = Integrated circuit card contactless
08–60 = Reserved for ISO use
61–80 = Reserved for national use
81–90 = Reserved for private use
91 = Magnetic stripe contactless
92–99 = Reserved for private use
Valid values for the third digit are listed below.
0 = Unspecified
1 = PIN entry capability
2 = No PIN entry capability

3–5 = Reserved for ISO use
6–7 = Reserved for national use
8–9 = Reserved for private use

7.1.10 P-23 Card Sequence Number

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-23	N	3	Card Sequence Number	C	C	C	C

The Card Sequence Number data element contains the member number for the card that initiated the transaction.

Member numbers are used to differentiate multiple cards issued with the same card number.

The member number must be right-justified and zero-filled, or must contain three zeros.

7.1.11 P-28 Transaction Fee Amount

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-28	N	8	Transaction free amount	C	C		

The Transaction Fee Amount data element contains the amount of an acquirer fee (surcharge or incentive) assessed on an ATM transaction. If the amount is negative (i.e., an incentive), the sign indicator is set to a minus sign (credit). If the amount is positive (i.e., a surcharge), the sign indicator is not needed.

7.1.12 P-32 Acquiring Institution Identification Code

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-32	N	11	Acquiring Institution Identification Code	M	M	M	M

The Acquiring Institution Identification Code data element contains a code that identifies the acquiring institution for the transaction, or its agent. The acquiring institution may be different from the card acceptor.

When a transaction originates at a terminal directly connected to a process, the process sets the value in the Acquiring Institution Identification Code data element from its terminal records. In the United States, this value is normally used for a U.S. Federal Reserve routing number that uniquely identifies financial institutions within the country.

7.1.13 P-35 Track 2 Data

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-35	AN	37	Track 2 Data	M	M	M	M

The Track 2 Data element is the information encoded on Track 2 of the magnetic stripe on the back of the card originating the transaction, excluding start and end sentinel and longitudinal Redundancy check (LRC) characters. The content of Track 2 data is specified in the ISO 7813 standard.

The general format of information in this data element includes the following:

Longitude (Track2) + Tack2 (The content of track2 data is specified in the ISO 7813 standard)

Information from this data element that may be required by includes the PAN, card sequence (member) number, PIN verification data, and expiration date.

Service Code Values
SC: Service Code. 3 digits:

Digit 1 (most significant): Interchange and technology:

0: Reserved for future use by ISO.
1: Available for international interchange.
2: Available for international interchange and with integrated circuit, which should be used for the financial transaction when feasible.
3: Reserved for future use by ISO.
4: Reserved for future use by ISO.
5: Available for national interchange only, except under bilateral agreement.
6: Available for national interchange only, except under bilateral agreement, and with integrated circuit, which should be used for the financial transaction when feasible.
7: Not available for general interchange, except under bilateral agreement.
8: Reserved for future use by ISO.
9: Test.

Digit 2: Authorization processing:

0: Transactions are authorized following the normal rules.
1: Reserved for future use by ISO.
2: Transactions are authorized by issuer and should be online.
3: Reserved for future use by ISO.
4: Transactions are authorized by issuer and should be online, except under bilateral agreement.
5: Reserved for future use by ISO.

6: Reserved for future use by ISO.
7: Reserved for future use by ISO.
8: Reserved for future use by ISO.
9: Reserved for future use by ISO.

Digit 3 (least significant): Range of services and PIN requirements:

0: No restrictions and PIN required.
1: No restrictions.
2: Goods and services only (no cash).
3: ATM only and PIN required.
4: Cash only.
5: Goods and services only (no cash) and PIN required.
6: No restrictions and require PIN when feasible.
7: Goods and services only (no cash) and require PIN when feasible.
8: Reserved for future use by ISO.
9: Reserved for future use by ISO.

7.1.14 P-37 Retrieval Reference Number

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-37	AN	12	Retrieval Reference Number	M	M	M	M

The Retrieval Reference Number data element contains a number assigned by the message initiator to uniquely identify a transaction. This number remains unchanged for all messages throughout the life of a transaction.

When a transaction originates from System, the number is generated as shown below for the different products. When the transaction originates from an acquirer host, the number comes from the original 0200 message from that acquirer.

7.1.15 P-38 Authorization Identification Response

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-38	AN	6	Authorization Identification Response		M	M	

The Authorization Identification Response data element contains a response identification number assigned by the authorizing institution. They may also be generated by an interchange or host.

The external message defaults include the Authorization Identification Response data element as a mandatory data element in a number of cases; however, the Data Element can be changed to indicate that data element P-38 is not used if the response identification number it contains is never required.

7.1.16 P-39 Response Code

The Response Code data element contains a code that indicates the disposition of a message.

Campo	Valor	Posiciones	Data Element	0800	0810
P-39	AN	2	Response Code		M

NETWORK MANAGEMENT

The Response Code data element is mandatory in 0810 messages. Valid values for this code in 0810 messages are as follows:

00 = Approved
05 = Denied
12 = Bad check digits
91 = DPC down

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-39	AN	2	Response Code		M	M	M

ATM

The Response Code data element is mandatory in all financial transaction, statement print, and reversal messages, with the exception of 0200 messages.

The ISO Host Interface process is responsible for translating internal response codes to and from their ISO equivalents.

Refer to Anexo A for the conversion tables.

7.1.17 P-41 Card Acceptor Terminal Identification

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-41	ANS	16	Card Acceptor Terminal Identification	M	M	M	M

The Card Acceptor Terminal Identification data element contains a unique code identifying the terminal at the card acceptor location.

Note: PROSA products use 16 bytes for terminal identification, instead of the 8 bytes specified by ISO8583

7.1.18 P-42 Card Acceptor Identification Code

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-42	ANS	15	Card Acceptor Identification Code	C	C	C	

The Card Acceptor Identification Code data element contains a code used to identify the card acceptor in a transaction if the card acceptor is different from the acquiring institution.

7.1.19 P-43 Card Acceptor Name/Location

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-43	ANS	40	Card Acceptor Name/Location	M		M	

The Card Acceptor Name/Location data element contains the name and location of the card acceptor that defines the point of service in both local and interchange environments.

ATM
The Card Acceptor Name/Location data element is mandatory in all 0200 and 0420 messages.

When a reversal (0420 message) is generated by the ISO Host Interface process because of a late or unsolicited approval response, the regular structure of this data element is not available to be included in the 0420 message. In this case, the following text appears in this data element instead:

** REVERSAL FOR LATE/UNSOL RESPONSE **

In any other reversal situation, this data element is copied from the original transaction request.

The structure of this data element is provided below.

Position	Length	Description
1-22	**22**	**Terminal Owner** The name of the institution owning the terminal.
23-35	**13**	**Terminal City** The city in which the transaction-originating terminal is located.
36-38	**3**	**Terminal State** A code indicating the state or province in which the transaction-originating termianl is located.
39-40	**2**	**Terminal Country** A code indicating the country in which the transaction originating termianl is located.

7.1.20 P-44 ATM Additional Response Data

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-44	ANS	27	Additional Response Data		C		

The Additional Response Data element can be used for additional data in a response message, which can be printed on a screen or receipt at the point of transaction.

This data element is conditional for 0210 messages. It is included in the message if the response code is set to 00 (approved with balances) or 59 (insufficient funds with amount 3).

For 0210 messages, this data element is used for account balance information. If the authorizer wishes to include account balance information in the transaction response, whether on a balance inquiry or any other transaction type, it is this data element that should carry it.

The structure of this data element is provided below.

Position	Length	Description
1-2	**2**	**Field Length Indicator** This field must be set to a value of 025.
3	**1**	**Usage Indicator** A code indicating how the rest of the data should be interpreted. Valid values are as follows: 1 = Ledger balance present only 2 = Available balance present only 3 = both balances present; use ledger balance if only one can be used 4 = both balances present; use available balance if only one can be used
4-15	**12**	**Ledger Balance** The ledger balance for a noncredit account and the current credit account balance for a credit account.
16-27	**12**	**Available Balance**

The available balance for a noncredit account and the available credit for a credit account. The currency for this balance is assumed to be the currency of the database. The currency is identified using the currency code specified in the Institution Definition File record for the institution. If the amount to be expressed is negative, the leftmost byte should contain a minus sign (–); otherwise, it should contain a zero.

7.1.21 P-45 Track I Data

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-45	ANS	76	Track I Data	C			

The Track 1 Data element contains the information encoded on Track 1 of the magnetic stripe of the card being used for the transaction, including start and end sentinel and longitudinal redundancy check (LRC) characters. The content of this data element is specified in the ISO 7813 standard, ***Identification Cards— Financial Transaction Cards.*** The general format of information in this data element is shown below.

Start sentinel (%)
Format code (B for credit cards is the only format code defined)
Primary account number (PAN), left justified (up to 19 digits)
Field separator (^)
Country code (if present; 3 digits)
Name (up to 26 characters)
Field separator (^) Expiration date (YYMM)
Service code (if present; 3 digits)
Discretionary data (up to 21 characters)
End sentinel (?)
Longitudinal redundancy check character

If this data element is present in an incoming transaction and contains information other than spaces, scans the data from the right to compute the length and moves the start sentinel, the data for the computed length and the end sentinel to the Track 1 token. It then adds 2 to the length of the token and adds it to the message

7.1.22 P-48 ATM Additional Data

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-48	ANS	47	Additional Data	M			

The Additional Data element carries sharing information. The Authorization process uses the information from this data element to identify whether not-on-us transactions are to be allowed. A not-on-us transaction is one where the card issuer and card acceptor are not the same.

This data element is mandatory for incoming 0200 messages. Sharing parameters are checked before sending a 0200 message to the host. Therefore, this data element is not required in outgoing 0200 messages.

The structure of this data element is provided below.

Position	Length	Description
1-3	**3**	**Field Length Indicator** This field must be set to a value of 044.
4-27	**24**	**Sharing Group Identifiers (24 at 1 byte each)** A terminal can belong to up to 24 sharing groups within a system. This list of sharing group identifiers is acquirer to the sharing groups for the card issuers; if there is no match, meaning the card issuer and terminal do not have at least one sharing group in common, the transaction is not allowed.
28	**1**	**Termianl Transaction Allowed Code** A code indicating the type of geographical sharing restrictions the terminal owner wishes to apply to the transaction if the transaction is not-on-us (the card issuer and terminal owner are not the same). Valid values are as follows: 0 = Not allowed if not-on-us 1 = Allowed within the county 2 = Allowed within the state 3 = Allowed nationally 4 = Allowed internationally
29-30	**2**	**Terminal State Code** A numeric code indicating the state in which the terminal is located, zero-filled where not applicable.
31-33	**3**	**Terminal Country Code**

		A numeric code indicating the country in which the terminal is located. Zero-filled where not applicable.
34-36	**3**	**Terminal Country Code** A numeric code indicating the country in which the terminal is located. Zero-filled where not applicable.
37-47	**11**	**Terminal Routing Group** The routing group to which the terminal belongs for routing and processing of foreign transactions. The default value is zero.

7.1.23 P-49 Transaction Currency Code

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-49	N	3	Transaction Currency Code	M	M	M	M

The Transaction Currency Code data element contains a code that defines the currency of the source location of the transaction.

Products use numeric currency codes only.

ATM
The code in the Transaction Currency Code data element identifies the currency that applies to the Transaction Amount (P-4) and Transaction Fee Amount (P-28) data elements. It is mandatory for all financial transaction and reversal messages.

For more information consult the ***Official country names used by the ISO 3166/MA***

7.1.24 P-52 Personal Identification Number (PIN) Data

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-52	AN	16	Personal Identification Number (PIN) Data	M			

The Personal Identification Number (PIN) Data element contains a number assigned to a customer intended to uniquely identify that customer at the point of service. This data element can contain the PIN itself or a derivative.

The PIN entered by the cardholder initiating the transaction. If the PIN has already been verified, this field contains zeros.

7.1.25 P-53 Security Related Control Information

Campo	Valor	Posiciones	Data Element	0800	0810
P-53	N	16	Security Related Control Information	C	C

The Security Related Control Information data element contains dynamic key management data. It is conditional for network management messages. It is required when the Network Management Information Code (S-70) data element is set to the value 161, 162, 163, or 164.

The structure of this data element is provided below.

Position	Length	Description
1-2	**2**	**Key Type** A flag identifying the type of key being exchanged. Vlid values are as follows: 00 = PIN key 01 = MAC key
3-4	**2**	**Key Direction** A flag indicating the direction of the key being exchanged. Valid values are as follows: 01 = Outbound key only 02 = Inbound key only 03 = both inbound and outbound keys
5-16	**12**	**Reserved** This field is not used; however, it must be included in the data element.

7.1.26 P-54 Additional Amounts

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-54	ANS	15	Additional Amounts	C	C	C	

The Additional Amounts data element carries the cash back amount for deposits and purchases where cash is being returned to the customer.

This data element is conditional for 0200, 0210, and 0420 messages. If the transaction is a deposit or purchase with cash back, the Additional Amounts data element is required to carry the cash back amount.
The structure of this data element is provided below.

Position	Length	Description
1-3	**3**	**Field Length Indicator**
		This field must be set to a value of 012.
4-15	**12**	**Cash Back Amount**

7.1.27 P-60 ATM TERMINAL DATA

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-60	ANS	15	Terminal Data	M	M	M	

The Terminal Data element carries terminal information required for processing.

For transactions introduced into the system by an acquirer host, these sub elements must come from the original request sent by that host. For transactions originating from System, come from the Terminal Data File.

This data element is mandatory for all financial transaction, reversal, and statement print messages, except for 0430 messages.

The structure of this data element is provided below.

Position	Length	Description
1-3	**3**	**Field Length Indicator** This field must be set to a value of 012.
4-7	**4**	**Terminla Owner FIID** The FIID of the institution owning the terminal.
8-11	**4**	**Terminal Logical Network** The logical network in which the terminal is located.
12-15	**4**	**Terminla Time Offset** The number of minutes to be added to the system time to arrive at the local time of the terminal originating the transaction. The value in this field is expressed as three digits proceeded by a plus or minus sing.

7.1.28 P-61 ATM Card Issuer and Authorizer Data

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-61	ANS	16	Card Issuer and Authorizer Data		M	M	

The Card Issuer and Authorizer Data element contains information that uniquely identifies a financial institution within a system.

The structure of this data element is provided below.

Position	Length	Description
1-3	**3**	**Field Length Indicator** This field must be set to a value of 013.
4-7	**4**	**Card Issuer FIID** The FIID of hte card issuer.
8-11	**4**	**Card Logical Network** The logical network of the card issuer.
12-15	**4**	**Save Account Indicators** Two two-position codes, indicating the actual account types involved in the transaction. The firs code indicates the type of from account; the second code indicates the types of the account.
16	**1**	**Authorizer** A code indicating whether the primary (P) or alternate (A) authorizer the transaction.

7.1.29 P-63 ATM PIN Offset

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
P-63	ANS	19	PIN OFFSET	C	C	C	

The PIN Offset data element is used to carry a PIN offset that supports the capability of allowing ATM customers to select their own PINs. It allows the new PIN offset value to be transmitted to the host, in order to keep the database for the host up-to-date with the database.

This data element is conditional for 0200 (outgoing), 0210, 0220, 0221, and 0420 messages. The ISO Host Interface process includes this data element in an outbound 0200, 0210, 0220, 0221, or 0420 message.

If an outgoing 0210 message for a PIN Change transaction is failed back to the ISO Host Interface process, the ISO Host Interface process checks the message for the presence of this data element. If this data element is present, in the STM is set using the value from this data element. If this data element is not present, the ISO Host Interface process sets in the STM to a value of ZZZZZZZZZZZZZZZZ. The value ZZZZZZZZZZZZZZZZ indicates to the Authorization process.

The structure of this data element is provided below.

Position	Length	Description
1-3	**3**	**Field Length Indicator** This field must be set to a value of 016.
4-9	**16**	**PIN Offset** The PIN Offset (left-justified, blank-filled) that is calculated when a cardholder selects or changes a PIN.

7.2 Data Elements 65 al 128

En esta sección se desglosan los Data Elements secundarios que son utilizados para las transacciones financieras en México.

En esta sección se desglosa el Data Element 126 el cual dentro de su estructura lleva los Tokens que son complementos a las transacciones naturales estos TOKENS son determinados según sea la funcionalidad y se integran en este Data Element.

7.2.1 S-70 Network Management Information Code

Campo	Valor	Posiciones	Data Element	0800	0810
P-70	N	3	Network Management Information Code	M	M

The Network Management Information Code data element contains a code that is used to manage the online processing status between and a host system. This code identifies the purpose of a network management request message.

The following codes are supported:

001 = Logon
002 = Logoff
161 = Change key
162 = New key
163 = Repeat key
164 = Verify key
201 = Cutover
301 = Echo-test

This data element is mandatory for 0800 and 0810 messages.

7.2.2 S-90 Original Data Elements

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
S-90	N	42	Original Data Elements			M	M

The Original Data Elements data element contains a group of five sub-elements included in a reversal or adjustment message. The information in these sub-elements identifies the original transaction being reversed or adjusted.

In the case of adjustments, the first two digits of the Processing Code (P-3) data element contain one of the following values:

02 = Debit adjustment
14 = Cash advance adjustment
19 = Purchase with cash back adjustment
22 = Credit adjustment

Information for data element S-90 is not always available through applications. Therefore, it is recommended that systems interfacing with applications use other information to uniquely identify a transaction. One or more of the following data elements can be used to uniquely identify a transaction:

P-12 Local Transaction Time
P-13 Local Transaction Date
P-35 Primary Account Number (from Track 2 Data)
P-37 Retrieval Reference Number
P-41 Card Acceptor Terminal Identification
P-45 Primary Account Number (from Track 1 Data)

The structure of this data element is provided below.

Position	Length	Description
1-4	**4**	**Original Transaction Type** The transaction type identifying the original transaction.
5-16	**12**	**Original Sequence Number** The sequence number identifying the original transaction.
17-20	**4**	**Transaction Date** The date of the original transaction.
21-28	**8**	**Transaction Time** The time of the original transaction
29-32	**4**	**Original Capture Date**

		The date the original transaction was posted.
33-42	**10**	**Filer**

7.2.3 S-95 Replacement Amounts

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
S-95	AN	42	Replacement Amounts			C	C

The Replacement Amounts data element contains the new transaction amount for a previous transaction. This data element also contains the new surcharge amount for a previous transaction.

ATM
The Replacement Amounts data element is conditional for 0420 and 0430 messages. It is necessary only for partial reversals. On a full reversal, this data element is not included in messages from and need not be present in messages to ATM.

For partial reversals of deposit with cash back transactions, the Actual Transaction Amount field in this data element carries the amount of cash actually dispensed.

For partial reversals of transactions with a surcharge, the Transaction Fee field in this data element carries the actual surcharge applied to the transaction.

The structure of this data element is provided below.

Position	Length	Description
1-12	**12**	**Actual Transaction Amount** The actual completed amount of the transaction.
13-24	**12**	**Settlement Amount** Ignore Acquirer on incoming messages and zero-filler on outgoing messages.
25-33	**9**	**Transaction Fee** The amount of the acquirer fee (surcharge or incentive) assessed on this transaction. If the amount is negative (i.e., an incentive), the first byte of this field is set to a minus sign (–). If the amount is positive (i.e., a surcharge), the first byte of this field remains set to its initialized value.
34-42	**9**	**Settlement Fee** Ignore on incoming messages and zero-filled on outgoing messages.

7.2.4 S-100 Receiving Institution Identification Code

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
S-100	N	11	Receiving Institution Identification Code		M	M	

The Receiving Institution Identification Code data element contains a code that identifies the institution receiving a request message. This data element is included because of its potential need by an acquirer host sending a request through System without knowledge of who the end recipient is to be.

7.2.5 S-102 Account Identification 1

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
S-102	ANS	28	Account Identification 1	C	C	C	

The Account Identification 1 data element contains a series of digits used to identify a customer account, usually some account tied to the primary or card account.

The account number in this data element is left-justified and blank-filled to the right.

ATM

The Account Identification 1 data element is used for the *from* account number involved in the transaction (for example, the debit account in a withdrawal or transfer transaction or the account being inquired upon in a balance inquiry transaction).

This data element is mandatory for statement print messages. It is conditional for all financial transaction and reversal messages. On incoming financial transaction and reversal messages, it should be included if it is known to the host. On outgoing financial transaction and reversal messages, it is sent if it is available

7.2.6 S-103 Account Identification 2

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
S-103	ANS	28	Account Identificacion 2	C	C	C	

The Account Identification 2 data element contains a series of digits used to identify a customer account, usually some account tied to the primary or card account.

The account number in this data element is left-justified and blank-filled to the right.

ATM

The Account Identification 2 data element is used for the *to* account number involved in the transaction (for example, the account being credited in a transfer transaction).

This data element is conditional on all financial transaction and reversal messages, except 0200 messages.

7.2.7 S-120 Key Management

Campo	Valor	Posiciones	Data Element	0800	0810
S-120	ANS	9	Key Management	C	C

The Key Management data element contains check digits for key exchanges. This data element is conditional for network management messages. It must be included in the message if the value in the Network Management Information Code (S-70) data element is 162, 163, or 164.

The structure of this data element is provided below.

Position	Length	Description
1-3	**3**	**Field Length Indicator** This filed must be set to a value of 006.
4-9	**6**	**Check Digits** The check digits for the key being exchanged.

7.2.8 S-122 Card Issuer Identification Code

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
S-122	ANS	14	Card Issuer Identification Code		C	C	

The Card Issuer Identification Code data element contains a value that identifies the institution that issued the card involved in the transaction. This value is used only when the card issuer is different from the receiving institution and has no knowledge of the difference.

The structure of this data element is provided below.

Position	Length	Description
1-3	**3**	**Field Length Indicator** This filed must be set to a value of 011.
4-14	**11**	**Card Issuer ID** The card issuer ID. See the product-specific descriptions that follow for more information on the card issuer ID field.

7.2.9 S-123 Cryptographic Service Message

Campo	Valor	Posiciones	Data Element	0800	0810
S-123	ANS	553	Cryptographic Servie Message	C	C

The ANSI X9. 17 standard, ***Financial Institution Key Management (Wholesale),*** establishes standards for key management. This standard also defines the Cryptographic Service Message (CSM) used for moving key management data between processors when the keys are distributed automatically. CSM information is contained in the Cryptographic Service Message data element (S-123) of the ISO external message.

MESSAGE CLASSES

Supports the following classes of CSMs used in point-to-point environments:

- Request Service Initiation Message (RSI)
- Key Service Message (KSM)
- Response Service Message (RSM)
- Error Service Message (ESM)

MESSAGE FIELDS AND SUBFIELDS

Each CSM class contains several fields, with many of the fields containing subfields. Some fields and subfields are mandatory while others are optional. Because of this flexibility, each field begins with a unique 2- or 3-character identifier and ends with a blank. The CSM itself always begins with the literal CSM, and the message contents are always carried between a pair of parentheses.

The fields shown in the following table are the only ones that appear in the CSMs created by System.

There are five CSM formats because the ESM class can have two formats, depending on the type of error being reported. Each of the CSM formats is described in greater detail, following the table.

CSM Class	RSI	KSM	RSM	ESM	
				With Counts	Without Counts
CSM Fields	MCL	MCL	MCL	MCL	MCL
	RCV	RCV	RCV	RCV	RCV
	ORG	ORG	ORG	ORG	ORG
	SVR	KD		CTP	ERF
		CTP		CTR	

				ERF	

When the interface process receives CSMs generated by an external processor, it searches only for the fields shown in the preceding table. It is recommended, but not mandatory, that the fields in the message be kept in the order shown in the table.

MESSAGE FORMATS

The dynamic key management processing uses the CSM to move key information between the System and the external processor in three of the four key management messages described earlier in this section: Change Key messages, New Key messages, and Repeat Key messages. The verify key message does not use the CSM because it only moves check digits and does not need the additional information contained in the CSM.

The following describes and presents examples of the System supported CSM classes:

Request Service Initiation Message (RSI) — Used when a key change request is being passed between processors. An example of a CSM containing the RSI format is shown below:

CSM(MCL/RSIb-RCV/1234567890123456b-ORG/123456789012346b-SVRb-)

Each field in the message is preceded by one of the following identifiers. The blanks identified by the character J- in the example are required in the message because they act as field terminators. The lengths given in the following field descriptions are for the data in the field, excluding field identifiers and trailing blanks.

MCL/ = Message class (RSI)
Field Length: 3 alphabetical characters

RCV/ = Receiver of the message
Field Length: 4–16 alphanumeric characters

ORG/ = Originator of the message
Field Length: 4–16 alphanumeric characters

SVR/ = Service request
Field Length: 0

Note: The absence of a value following this identifier implies a request for one data key.

Key Service Message (KSM) — Used when a new key is passed between processors. An example of a CSM containing the KSM format for a double-length key is shown below:

CSM(MCL/KSMJ-RCV/1234567890123456J-ORG/1234567890123456J-KD/12345678901234561234567890123456J-CTP/12345678901234J-)

The information in this example is actually a continuous line. It has been broken here due to space constraints. Each field in the message is preceded by one of the following identifiers. The blanks identified by the character J- in the example are required in the message because they act

as field terminators. The lengths given in the following field descriptions are for the data in the field, excluding field identifiers and trailing blanks.

MCL/ = Message class (KSM)
Field Length: 3 alphabetical characters

RCV/ = Receiver of the message
Field Length: 4–16 alphanumeric characters

ORG/ = Originator of the message
Field Length: 4–16 alphanumeric characters

KD/= new key value, generated by the security module for a new key request and taken from the database for a repeat key message
Field Length: 16, 32, or 48 hexadecimal characters

CTP/= Hexadecimal key counter
Field Length: 1–14 hexadecimal characters

Response Service Message (RSM) — used to respond to a KSM that is processed successfully. An example of a CSM containing the RSM format is shown below:

CSM(MCL/RSMJ-RCV/1234567890123456J-ORG/1234567890123456J-)Each field in the message is preceded by one of the following identifiers. The blanks identified by the character J- in the example are required in the message because they act as field terminators. The lengths given in the following field descriptions are for the data in the field, excluding field identifiers and trailing blanks.

MCL/= Message class (RSM)
Field Length: 3 alphabetical characters

RCV/= Receiver of the message
Field Length: 4–16 alphanumeric characters

ORG/= Originator of the message
Field Length: 4–16 alphanumeric characters

Error Service Message (ESM) — used to respond to a Request Service Initiation Message (RSI) or a Key Service Message (KSM) that cannot be processed successfully. The ESM can have two formats, depending on the type of error being reported. The two counter fields are only included in the message when the expected key count (CTP field) and the key count received from the message originator (CTR field) do not match. The error code (ERF field) in the examples below can contain only alphabetical characters. Numbers are used to demonstrate field length.

An example of a CSM containing the ESM format with the key counters is shown below:

CSM(MCL/ESMJ-RCV/1234567890123456J-ORG/1234567890123456JCTP/12345678901234J-CTR/12345678901234J-ERF/1234567890123456J-)

An example of a CSM containing the ESM format without the key counters is shown below:

CSM(MCL/ESMb-RCV/1234567890123456b-ORG/1234567890123456b-ERF/1234567890123456b-)

The information in each of these examples is actually a continuous line. It has been broken here due to space constraints. Each field in the messages is preceded by one of the following identifiers. The blanks identified by the character b- in the example are required in the message because they act as field terminators. The lengths given in the following field descriptions are for the data in the field, excluding field identifiers and trailing blanks.

MCL/ = Message class (ESM)
Field Length: 3 alphabetical characters

RCV/ = Receiver of the message
Field Length: 4–16 alphanumeric characters

ORG/ = Originator of the message
Field Length: 4–16 alphanumeric characters

CTP/ = Hexadecimal key count expected by the receiver of the KSM. This identifier and field are only included in the message when error code P is returned.
Field Length: 1–14 hexadecimal characters

CTR/ = Hexadecimal key count originally sent in the KSM by the message originator. This identifier and field are only included in the message when error code P is returned.
Field Length: 1–14 hexadecimal characters

ERF/ = the following codes identify the errors that were detected during processing.

C = cannot process (general error)
F = Format error
H = Invalid receiver ID or originator ID
P = the value in the CTP field of the KSM does not match the expectd count

Field Length: 1-16 alphabetical characters

Message Length

The use of multiple CSM formats makes the CSM a variable-length element in the ISO external message. The CSM can also be a fixed-length element in the ISO external message.

Fixed-Length Messages. When the CSM is used as a fixed-length element, the data is left-justified within each field of the CSM format being used and each field is blank filled, if necessary, to obtain its maximum length. The CSM format is then left-justified in the external message data element and the data element is blank filled to reach the specified length.

In the fixed-length ISO message, the CSM (S-123) has a length of 150 bytes, excluding the 3-position field length indicator. Although the total length of the CSM is 150 bytes, the longest CSM is currently 114 bytes. Therefore, positions 115 through 150 of the CSM always contain blanks.

The ESM can have two lengths, depending on whether it includes the two key count fields (CTP and CTR). The key count fields are only included when the error code field (ERF) contains a P (counts do not match). Neither key count field is included when the error code is a value other than P.

CSM Format	RSI	KSM	RSM	ESM	
				With Counts	Without Counts
CSM Data Length	60	110	55	114	76

Variable-Length Messages. When the CSM is used as a variable-length element, the length of each field in the CSM is determined by the data it carries. The message format field descriptions presented earlier in this section includes the range of possible lengths for each field.

All fields are required except for the key count fields (CTP and CTR) in the ESM. The key count fields are conditional in the ESM, depending on whether the error code field (ERF) contains a P (counts do not match). Neither key count field is included when the error code is a value other than P. Data element S-123 can have the following lengths (excluding the 3-position field length indicator), depending on the CSM format it contains.

CSM Format	RSI	KSM	RSM	ESM	
				With Counts	Without Counts
Minimum Length	36	57	31	49	37
Maximum Length	60	110	55	114	76

Examples. The following examples show an RSM when the receiver and originator are less than the maximum length of 16 alphanumeric characters. The first example illustrates a variable-length format and the second example illustrates a fixed-length format. The variable-length RSM shown has a length of 36

characters while the fixed-length RSM shown maintains its length of 55 characters because each field is padded with blanks. Blanks are identified by the character b in the examples.

CSM (MCL/ESMbRCV/ABC123bORG/DEFG456b

CSM (MCL/RSMbRCV/ABC123bbbbbbbbbbbORG/DEFG45 6bbbbbbbbbb)

This data element is conditional for network management messages. It must be included in the message if the value in the Network Management Information Code (S-70) data element is 161, 162, or 163.

The structure of this data element is provided below.

Position	Length	Description
1-3	**3**	**Field Length Indicator** This field must contain the length of the Cryptographics Service Message (CSM).
4-553	**550**	**Cryptographic Service Message (CSM)** This field contains the Cryptographic Service Message (CSM). The length of this field depends on the format of the CSM being sent or Received.

7.2.10 S-125 Account Indicator

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
S-125	ANS	375	Account Indicator/Statement Print Data		C	C	

The Account Indicator Data element is used to carry different information depending on the type of message.

7.2.11 Account Indicator

The Account Indicator format of this data element contains a value used in outgoing messages to indicate the account or accounts involved in a two-sided transaction (transfer or payment-from) the host is to process. Values are as follows:

0 = Process both the *from* and *to* accounts
1 = Process only the *from* account
2 = Process only the *to* account

This data element is conditional in 0200 (outgoing), 0210 and 0420 messages and is required only if the code in the Processing Code (P-3) data element indicates that a transaction is two-sided.

The structure of this data element is provided below.

Position	Length	Description
1-3	**3**	**Field Length Indicator**
		This field must be set to a value of 001.
4-	**1**	**Account Indicator**

7.2.12 S-126 Additional Data

Campo	Valor	Posiciones	Data Element	0200	0210	0420	0430
S-126	ANS	800	Additional Data	C	C	C	C

The Additional Data element contains System message tokens. This data element is conditional for all messages. For incoming messages, any token included in the message is appended to the STM. For outgoing messages, the tokens included in this data element are specified in the Token File (TKN). For more information on configuring tokens to be included in outgoing external messages.

The tokens are carried in the external message in the same general structure as they are carried in the internal message. The major difference is that, in the external message, all tokens are in ASCII format.

If token data is added to this data element, the first item following the field length indicator is a Header token. The Header token contains a count of the number of tokens associated with the message and the overall length of all token data. The Header token is added to the message when the first token is added, and is updated each time a subsequent token is added.

The token header for the first token is located after the Header token. Each token that is added to the message has its own token header. Unlike the Header token, which contains information about all tokens in the message, the token header contains information about one specific token. The token header identifies the individual token and contains the length of the individual token. The token header is followed by the token data. Together, the token header and the token data form a single token. The combination of token header and token data is repeated for each token in the message.

TOKEN BASICS AND EXAMPLES

As described previously, the internal message consists of a series of core fields— known as the STM, PSTM, or TSTMH—followed by some number of function-specific tokens. Tokens are only added to the message as they are needed, so it is possible for an internal message to have no tokens associated with it. When the first token is required to process the transaction, the system adds two tokens to the message. The first token is the Header token. The second token is whatever token needed to be added to the message. When subsequent tokens are needed, they are added to the message individually. The general layout of an internal message with message tokens is illustrated below.

STANDARD INTERNAL MESSAGE WITH TOKENS

STM/PSTM/TSTM	Header Token	Token	Token	Token	...

HEADER TOKEN

The Header token contains a count of the number of tokens associated with the message and the overall length of all token data. The Header token is added to the message when the first token is added, and is updated each time a subsequent token is added. The Header token is illustrated below.

Eye Catcher	Count	Length
&	02	30

The first field in the Header token contains an eye catcher. The eye catcher makes it easy to locate token information when viewing internal messages. The eye catcher in the Header token is an ampersand **(&)**.

The second field contains the token count. In the example, the token count field contains the value 2. This indicates that there are two tokens in the internal message—the Header token plus one additional token.

Among the symbol **(&)** Eye catcher and the Count will exist a space the one which this represented by " ".

The final field contains the overall length of token data. The length includes the total length of the Header token, plus the length of each individual token added to the message.

DESCRIPTION HEADER TOKEN:

Position	Level	Field Name and Description	Data Type
1-12		**HEADER-TKN**	
1	**02**	**EYE-CATCHER** Indicates the start of token data. The only valid value is an Ampersand (&).	**PIC X(1)**
2	**02**	**USER-FLD1** Space " "	**PIC X(1)**
3-7	**02**	**CNT** The count of the number of tokens, including the Header Token that is present in the token data buffer.	**PIC 9(5)**
8-12	**02**	**LGTH** The length of all token data, including the Header token and Token header structures present in a token data buffer.	**PIC 9(5)**

TOKEN HEADERS

Each token that is added to the message has its own token header. Unlike the Header token, which contains information about all tokens in the message, the token header contains information about one specific token. The token header identifies the individual token and contains the binary length of the individual token. The token header is followed by the token data. Together, the token header and the token data form a single token. The general format of a token is illustrated below.

Data Token

Eye Catcher	Token ID	Token	Length Token Data
!	13	30	11101361109261209...

The first field in the data token is another eye catcher. The eye catcher separates each token in the message from the previous token. The eye catcher in data tokens is always an exclamation point **(!)**.

Among the symbol **(!)** Eye Catcher and the Token ID will exist a space the one which this represented by " ".
The tokens are carried in their entirety in ASCII format. The general structure of this data element is provided below:

DESCRIPTION TOKEN HEADER:

Position	Level	Field Name and Description	Data Type
1-10		**TKN-HEADER**	
1	**02**	**EYE-CATCHER** Indicates the start of an individual token. The only valid value is an exclamation point (!). Note: If the Super Extract process converts a token to EBCDIC, the exclamation point in this field is translated to a vertical bar (|).	**PIC X(1)**
2	**02**	**USER-FDL1** Space " "	**PIC X(1)**
3-4	**02**	**TKN-ID** The two-byte ASCII representation of the token ID the token ID uniquely identifies a token.	**PIC X(2)**
5-7	**02**	**LGTH** The length of the token data for the token identifield by the TKN-ID field.	**PIC 9(5)**
10	**02**	**USER-FLD2** Space " "	**PIC X(1)**

DESCRIPCIÓN GENERAL DE TOKEN:

Position	Length	Description
1-3	**3**	**Field Length Indicator** The field length indicator value is the sum of the lengths of the Header token, all token headers, and token data begin used.
4-15	**12**	**Header Token**
15-24	**10**	**Token Header**
a-b	**N**	**Token Data**
…	**…**	**…**
w-x	**10**	**Token Header**
y-z	**n**	**Token Data**

Capítulo 8: CÓDIGOS RESPUESTA

CODIGOS DE RESPUESTA ISO	
00	Approved or completed successfully
01	Refer to card Issuer
02	Refer to special conditions of card issuer
03	Invalid merchant
04	Pick-up
05	Do not honor
06	Error
07	Pick-up card, special condition
08	Honor with identification
09	Request in progress
10	Approved for partial amount (not supported)
11	Approved (VIP)
12	Invalid transaction
13	Invalid amount
14	Invalid card number (no such number)
15	No such issuer
16	Approved, update track 3 (not supported)
17	Customer cancellation
18	Customer dispute
19	Re-enter transaction
20	Invalid response
21	No action taken
22	Suspected malfunction
23	Unacceptable transaction fee
30	Format error
31	Bank not supported by switch

32	Completed partially
33	Expired card
34	Suspected fraud
35	Card acceptor contact acquirer, pick-up
36	Restricted card
37	Card acceptor call acquirer security
38	Allowable PIN tries exceded
39	No credit account
40	Requested function not supported
41	Lost card
42	No universal account
43	Stolen card, pick-up
44	No investment account
51	Not sufficient funds
52	No chequing account
53	No savings account
54	Expired card
55	Incorrect personal identification number
56	No card record
57	Transaction not permitted to Cardholder
58	Transaction not permitted to terminal
59	Suspected fraud
60	Card acceptor contact acquirer
61	Exceeds withdrawal amount limit
62	Restricted card
63	Security violation
65	Exceeds withdrawal frequency limit
66	Card acceptor call security department of acquirer
67	Hard capture (requires that card be picked up at ATM)
75	Allowable number of PIN tries exceeded

76	Reserved for private use or Inelegible Account
77	Reserved for private use or No sharing between the card issuer and terminal owner
78	Reserved for private use or Contact card issuer
79	Reserved for private use or Approved transaction inside window
80	Reserved for private use or Approved transaction outside window
81	Reserved for private use or Approved transaction balance anytime
86	Reserved for private use or No statement information for the account
87	Reserved for private use or Statement information not available
88	Reserved for private use or System error
89	Reserved for private use or Database problem
90	Cutoff is in process— a switch is ending business for a day and starting the next (transaction can be sent again in a few minutes)
91	Issuer or switch is inoperative
92	Financial institution or intermediate network facility cannot be found for routing
93	Transaction cannot be completed due to a violation of law
94	Duplicate transmission
95	Reconcile error
96	System malfunction
05	ARQC Failure Decline
05	Security Module Parameter Error
05	Security Module Failure
05	KEY1 Record Not Found
05	ATC Check Falure
05	CVR Decline
05	TVR Decline
05	Fallback Decline
67	ARQC Failure Capture
67	CVR Capture
67	TVR Capture

Capítulo 9: TCP / IP HEADER

9.1 Configuración Sobre TCP/IP

Formato del Header de TCP.

El header del TCP utilizado para la comunicación con el sistema de **PROSA** deberá de estar precedido por dos byte que indiquen la longitud del mensaje.

El siguiente ejemplo ilustra la situación:

Associated Data - 69 bytes

```
000:  0043  4953  4F30  3233   30430  3030  3130  3038 .CISO02340001008
008:  3030  3832  3230  3030   3030  3030  3030  3030 00820200000000000
010:  3030  3034  3030  3030   3030  3030  3030  3030 0004000000000000
018:  3030  3035  3132  3133   3138  3330  3030  3030 0005121318300000
020:  3637  3030  3100                    67001
```

0043 = .C PARA LA LONGITUD DEL MENSAGE

0043 = HEX(0043) 69 bytes (67) + 2 bytes =

El ejemplo muestra como antes de enviar la información en el formato ISO es necesario anunciar de qué longitud irá. La primera validación se realiza al tomar como premisa que los datos en formato ISO tendrán una longitud de 67 bytes, aun cuando los datos asociados sean 69 bytes.

Es importante tomar en cuenta que estos dos primeros bytes siempre deberán de traer la longitud real del mensaje en formato ISO, ya que de no ser así el primer rechazo será por longitud inválida.

A continuación se presenta un ejemplo en donde la longitud que se marca es incorrecta:

Associated Data - 464 bytes

```
000:  CEFF  4953  4F30  3233   30430  3030  3130  3032 N.ISO02340001002
008:  3030  4232  3345  3834   3231  3241  4131  3830 00B23E84212AA180
010:  3138  3030  3030  3030   3030  3130  3030  3031 10800000000100001
018:  4243  3030  3030  3030   3030  3030  3030  3030 BC00000000000000
```

*** CONTINUA MAS INFORMACION**

El valor CEFF representa una longitud de 52991 bytes y si sumamos los dos primeros bytes (En donde debe venir definida la longitud del mensaje en ISO) tenemos un total de 52993 .El valor real de los datos asociados es de 464 y quitando los 2 primeros bytes la longitud del mensaje ISO es de 462.Este mensaje es rechazado por longitud inválida al mencionar 52991 bytes y enviar 462.

Se anexan ejemplos de datos asociados dentro de la configuración de TCP/IP; no deben ser tomados como los mismos que muestra este documento (Análisis de mensajes 0800,0200, 0400) ya que los BIT-MAPS son diferentes:

Associated Data - 69 bytes

```
000: 0043 4953 4F30 3233 30430 3030 3130 3038 .CISO02340001008
008: 3030 3832 3230 3030 3030 3030 3030 3030 00820200000000000
010: 3030 3034 3030 3030 3030 3030 3030 3030 0004000000000000
018: 3030 3035 3132 3133 3138 3330 3030 3030 0005121318300000
020: 3637 3030 3100                               67001
```

Mensaje 0810 70 **+ 2 de la longitud**

Associated Data - 72 bytes

```
000: 0046 4953 4F30 3233 30430 3030 3134 3038 .FISO02340001408
008: 3130 3832 3230 3030 3030 3032 3030 3030 10820200000020000
010: 3030 3034 3030 3030 3030 3030 3030 3030 0004000000000000
018: 3030 3035 3132 3133 3138 3330 3030 3030 0005121318300000
020: 3637 3030 3030 3103                     6700001.
```

Anexos

Anexo 1: MANEJO DE TRANSACCIONES

Este capítulo nos habla de los tipos de transacciones que existen así como el manejo de los mismos la descripción de esto será deberá de tomar como apoyo al entendimiento de las transacciones aquí nombradas.

Para los Adquirentes como se menciona en el Data Element 3 (TIPO DE TRANSACCION) se cuenta con los valores validos por ISO 8583 para una transacción financiera.

01 Disposición
La cual nos está indicando que un tarjeta habiente de alguna institución ha realizado un retiro a través del cajero automático, este retiro ha viajado en una transacción financiera 0200 hacia la institución generadora de la tarjeta y la cual en su respuesta (0210) ha aprobado la entrega de la cantidad solicitada.

31 Consulta
La cual nos está indicando que un tarjeta habiente de alguna institución ha solicitado saber el saldo que actualmente cuenta en su tarjeta (esta puede ser de Débito o Crédito) recordando que para esta última cuando el valor es positivo deberá de aparecer con in "-"antes dl total a mostrar o imprimir y que nos está indicando que esta tarjeta tiene un saldo positivo o de más en esta tarjeta esta viaja a través de un mensaje 0200.

02 Check guarantee (funds guaranteed)

04 Check verification
La cual nos indica que la transacción será para validar que la tarjeta este activa o sea una tarjeta válida para el banco emisor correspondiente, normalmente se da este tipo de transacción para cuando son tarjetas extrajeras y que le sirve al adquirente para asegurar la transacción y la cual viaja en un mensaje 0200.

92 Check cash

21 Deposit
La cual nos indica que se realizará un depósito a una cuenta del mismo banco, en este tipo de transacciones no hay ningún retiro solo se aplica el traspaso de la cantidad solicitada en el ATM hacia la cuanta destino la cual viaja en el mismo ISO 8583 en el Data Element 102. (*Para mayor información solicitar el estándar de Depósitos On-line)*

22 Deposito Crédito

La cual nos indica que se realizará un depósito a una cuenta del mismo banco, en este tipo de transacciones no hay ningún retiro solo se aplica el traspaso de la cantidad solicitada en el ATM hacia la cuanta destino la cual viaja en el mismo ISO 8583 en el Data Element 102. (*Para mayor información solicitar el estándar de Depósitos On-line)*

37 Consulta SPEI
(*Para mayor información solicitar el estándar de SPEI al comercial correspondiente)*

38 Consulta de cuentas
Este tipo de transacción deberá de aparecer en el ATM y solo se muestra así por seguridad del tarjeta habiente, esto le servirá para poder realizar algún traspaso de fondos a cualquiera de las cuentas que tenga, esta información viaja en una transacción de tipo 0200.

40 Cardholder accounts transfer
La cual nos indica que se realizara a través de una transacción de tipo 0200 un traspaso de fondos a una de las cuentas relacionadas.

42 SPEI
(*Para mayor información solicitar el estándar de SPEI al comercial correspondiente)*

90 Payment enclosed
La cual nos indica que a través del ATM se estará realizando un pago a algún prestador de servicios como puede ser SKY, GAS, TELEFONO, etc, etc.

91 Message to financial institution
(No usado)

93 Log-only transaction
(No usado)

94 Statement print
(No Usado)

96 PIN change
La cual nos indica que el tarjeta habiente acaba o está solicitando el cambio del Número de identificación personal PIN esto solo aplica para transacciones de Banda para la parte de Chip NO esta normado realizar este tipo de transacción.

97 EMV PIN Unblock
La cual le está indicando al emisor correspondiente que se requiere que desbloquee el Pin del Chip, esta funcionalidad no está activa para México por lo que no se podrá utilizar.

65 Generic Sale

La cual nos indica que se está realizando compra de tiempo aire para celular esta transacción viaja en un mensaje 0200.

97 Aviso Cambiar NIP

La cual nos indica que por algún motivo dentro de la banda tenga algún contador de tiempo el cual al llegar a caducar obliga al tarjeta habiente a realizar el cambio de Nip, Normalmente esto se da cuando la tarjeta es Nueva lo primero que solicita el cajero es un cambio de Numero confidencial.

Anexo 2: MODELOS DE CONECTIVIDAD

En este capítulo se muestran los diferentes tipos de conectividad que se manejan en PROSA,

- **Emisor un Nodo – Prosa: Sta. Fe y KIO**

  1. Emisor un nodo y una tarjeta de red
  2. Emisor un nodo y dos tarjetas de red

- **Emisor Dos Nodos – Prosa: Sta. Fe y KIO**

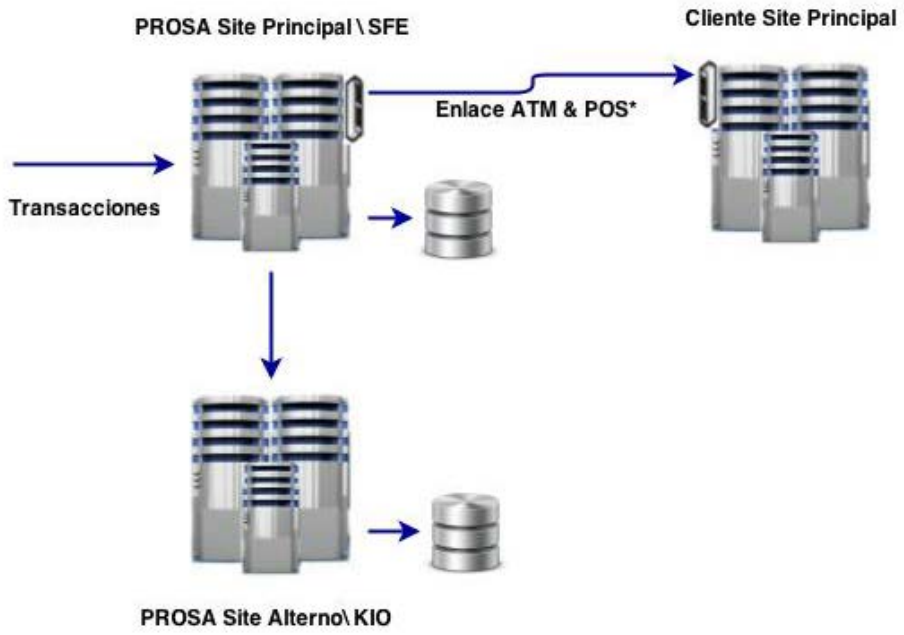
  1. Emisor primer nodo activo y segundo nodo en DRP
  2. Emisor ambos nodos activos

- **Emisor Tres o más Nodos – Prosa: Sta. Fe y KIO**

  1. En este esquema se pueden presentar varias topologías de conectividad por lo que es necesario contar con la configuración y operativa de los tres o más nodos del adquirente para dar la configuración a operar.

2.1 Emisor Un Nodo

Modelo Emisor un nodo y una tarjeta de **red DRP.**



Modelo DRP - Este modelo es el más clásico en donde el cliente no tiene la oportunidad de tener más de 2 conexiones (1 atm y 1 pos) y su plataforma no tiene forma de recibir transacciones por más de 1 solo puerto el cual es separado en ATM y POS, trabajando solo por el equipo primario.

Nota: Este esquema este en desuso y su implementación requerirá la autorización de las áreas de Seguridad Lógica y Switch

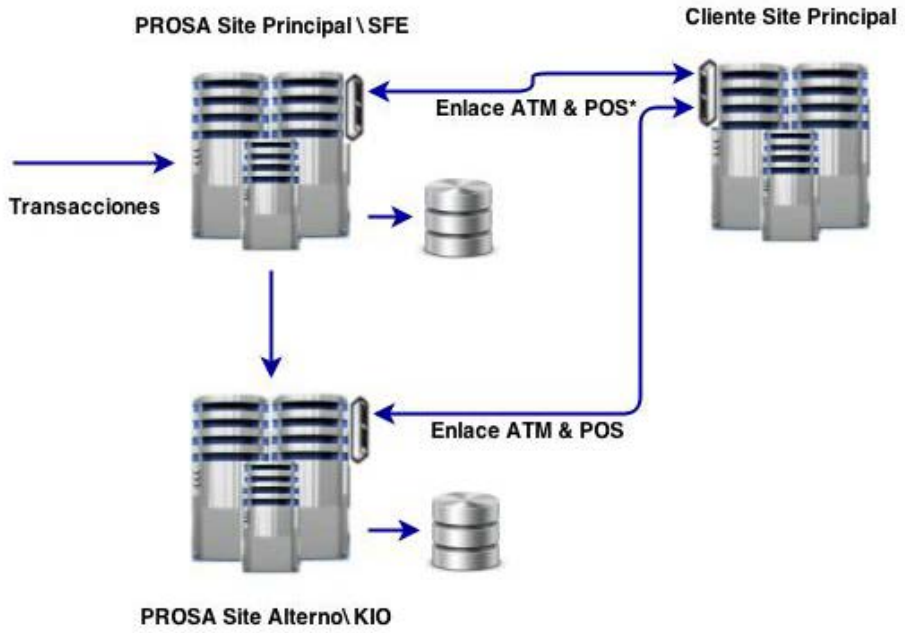
En el caso de una caída el cliente quedaría fuera de línea para estos casos el tiempo de recuperación es de **5 horas** en el caso de una contingencia mayor, en el caso contrario a través del área de Centro de Control Operativo la desconexión será atendida bajo los tiempos establecidos en el contrato con el cliente.

2. Emisor un nodo y dos tarjetas de red **Modelo Activo-Pasivo**

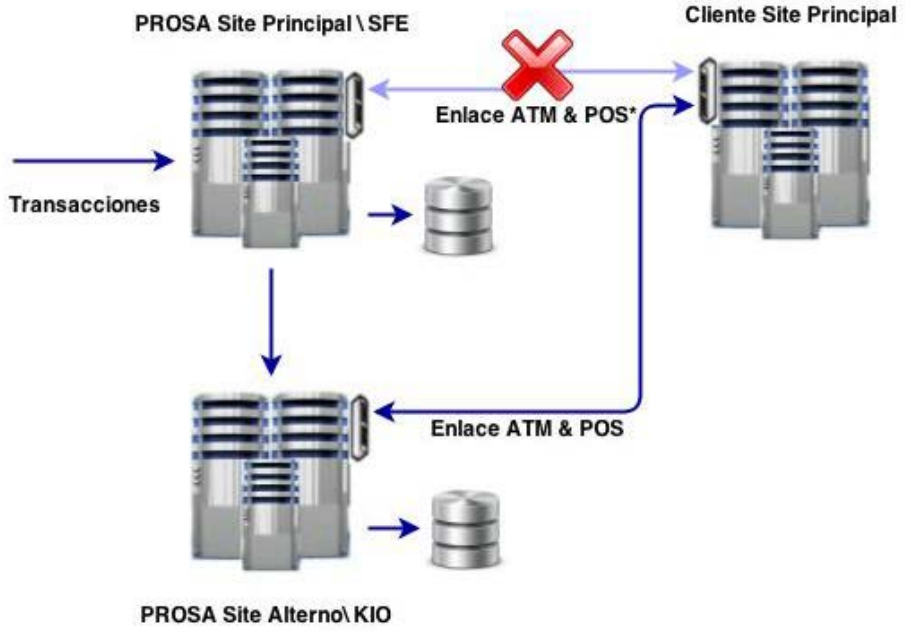
Modelo Hotsite (Pasivo-Activo) - Este modelo nos indica que el cliente puede llegar a tener enlaces desde un servidor hacia 2 servidores de PROSA pudiendo recibir y enviar información por cualquiera de ellos, trabajando desde su equipo con conexiones a los equipos en PROSA.

En el caso de una caída de los enlaces podrá seguir transaccionando a través de la otra línea de comunicación.

Se recomienda no balancear 50x50 en este modelo ya que en caso de una contingencia se podría perder las transacciones del canal con problemas, es recomendable utilizar ambas en todas las transacciones.



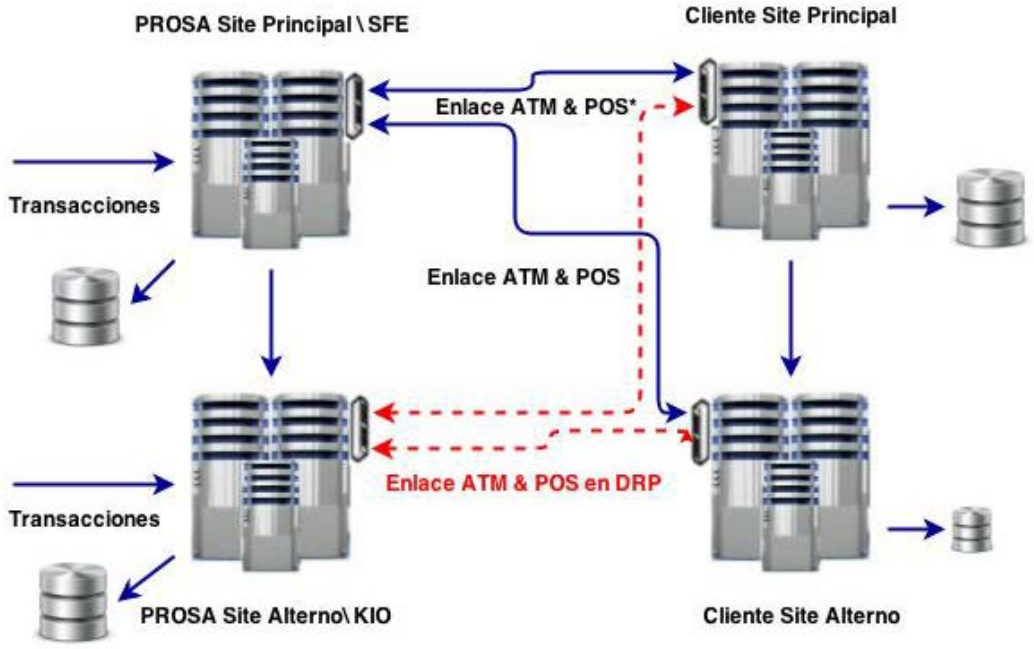
En el caso de presentarse una desconexión de cualquiera de los enlaces el cliente podrá seguir realizando transacciones por la otra conexión, la idea es que siempre estén utilizando ambas líneas para mejorar las capacidades transaccionales y en el caso que suceda lo que se indica logre seguir realizando estas transacciones con normalidad.



2.2 Emisor Dos Nodos

1. Emisor primer nodo activo y segundo nodo en DRP

Para este modelo es importante que el cliente se asegure que puede estar interconectado en sus plataformas ya que en el momento de un DRP pueda seguir realizando transacciones normalmente.

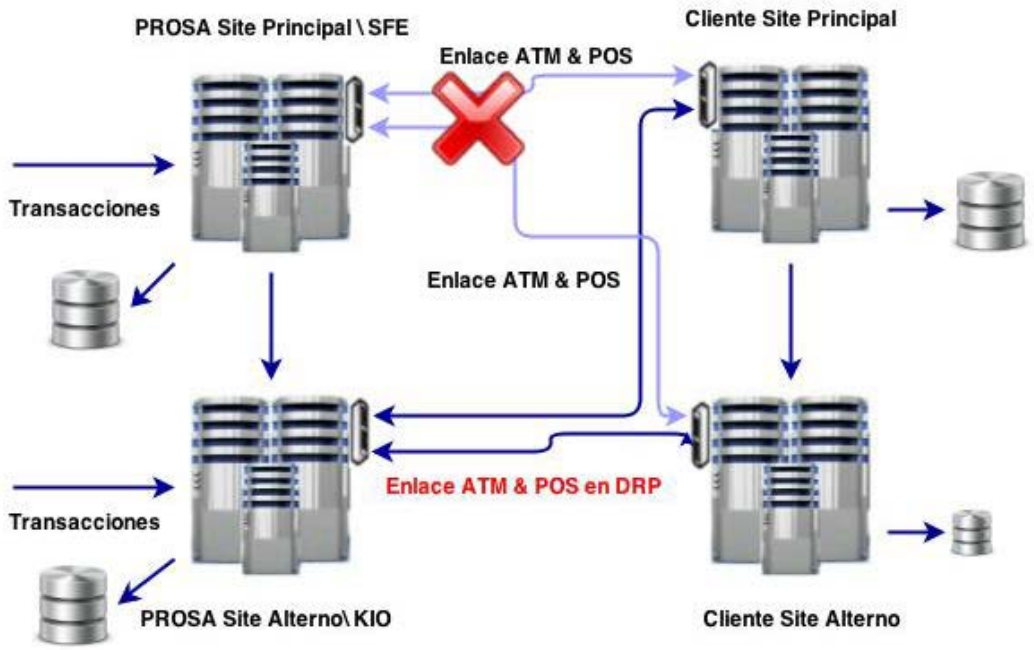


Para este caso sucede lo siguiente:

a) Cuando suceda el evento el área de CCO (Centro de control Operativo) de PROSA estará realizando una llamada al centro de cómputo del cliente para informar del evento, de ahí se tomaran las acciones para levantar el enlace de respaldo.

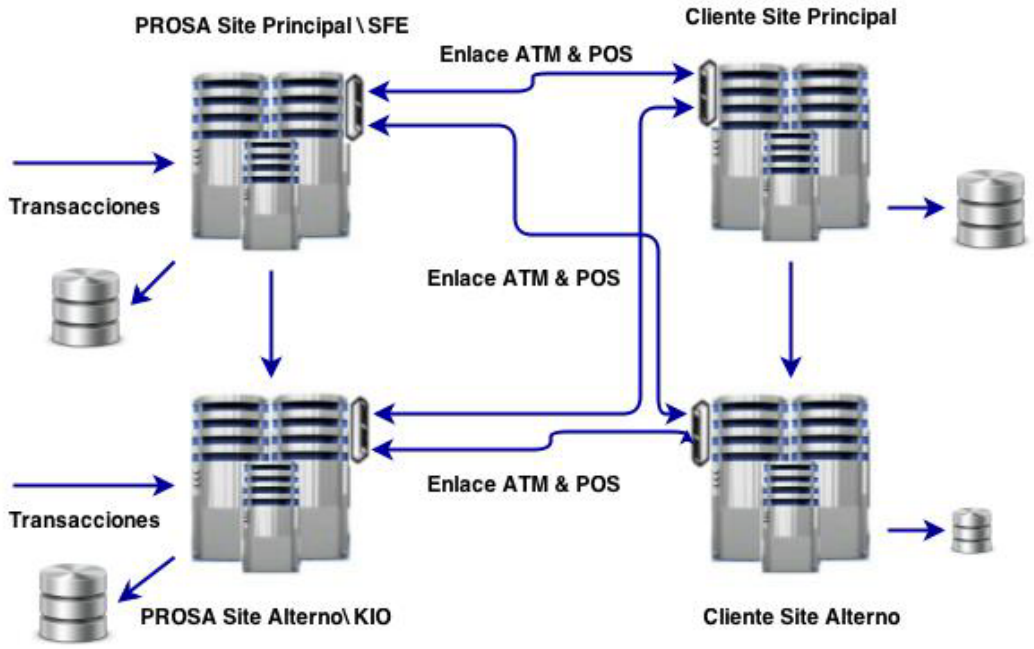
b) Una vez restablecido el enlace por la línea de respaldo el cliente podrá seguir realizando sus transacciones normalmente y podrá en conjunto con sus representantes de comunicaciones arreglar el problema, esto mismo sucede con el respaldo de PROSA que en su caso estará tomando las medidas pertinentes.

c) Este modelo es cuando el cliente al tener 2 nodos puede enlazar sus 2 plataformas en forma cruzada hacia los sistemas de PROSA, pero al no tenar conectividad entre sus Nodos no es posible el recibir y enviar por ambos lados por lo que su nodo secundario queda fuera de servicio hasta que el cliente indique que los va a activar desactivando los principales.



2. Emisor ambos nodos activos **Modelo Activo-Activo**

Modelo Active-Active – Este modelo nos indica que el cliente puede llegar a tener enlaces desde 2 o más servidores hacia 2 servidores de PROSA pudiendo recibir y enviar información por cualquiera de ellos y conectándose de forma cruzada esto es que desde cualquier servidor pueden llegar a cualquiera de los servidores de PROSA.

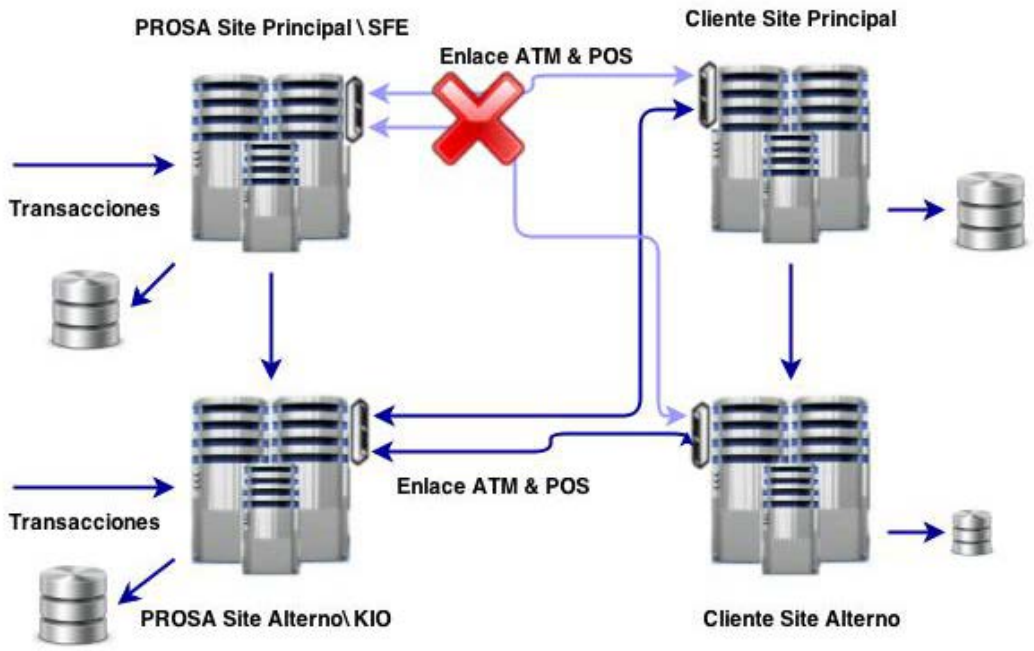


Para este modelo se recomienda al cliente que sus site's puedan intercambiar la información de transacciones esto para asegurar la integridad de los mismos.

Este modelo es el más completo ya que en el caso de una caída en cualquiera de los enlaces o bien en cualquiera de los equipos se podrá seguir realizando las transacciones sin ningún tipo de alteración o intervención del personal para seguir con las transacciones, los niveles de servicios superan lo establecido y solo hará la necesidad de en coordinación con sus prestadores de servicios arreglar y verificar que sucedió.

En esta lámina se muestra que el adquirente puede tener las *nnnn* conexiones hacia PROSA desde ambos Nodos pudiendo enviar y recibir transacciones simultáneamente.

Esto se podrá repetir un *nnn* Nodos sin ningún problema:



Lamina ejemplo de caída ya de un Site o enlace de cualquiera de los Nodos.

Glosario de Términos

ABM	Asociación de Bancos de México
ASCII	American Standard Code for Information Interchange
ATM	Automated Teller Machine
BIC	Base 24 Interchange
CSM	Cryptographic Service Message
DE	Data Element
ISO	International Organization for Standardization
MO/TO	Mail Order/Telephone Order
NIP	Número de Identificación Personal
POS	Point Of Sale
PROSA	Promoción y Operación S.A. De C.V.
DATA ELEMENT	Unidad de almacenaje de información con una estructura definida para transportar información específica en el estándar ISO 8583
TOKEN	Unidad de Almacenaje de con estructura que no cubre ninguno de los Data Elements del ISO 8583.

Documentos de Referencia:

1.-PROSA: Especificación Técnica, Estándar ATM EMISOR. Ver. 5.0; Sept. 2011; Clave C-008

----------FIN DEL DOCUMENTO ----------