UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

T.30

Enmienda 1
(07/97)

SERIE T: TERMINALES PARA SERVICIOS DE TELEMÁTICA

Procedimientos de transmisión de documentos por facsímil por la red telefónica general conmutada

Enmienda 1

Recomendación UIT-T T.30 – Enmienda 1

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES DE LA SERIE T DEL UIT-T

TERMINALES PARA SERVICIOS DE TELEMÁTICA

Para más información, véase la Lista de Recomendaciones del UIT-T.

RECOMENDACIÓN UIT-T T.30

PROCEDIMIENTOS DE TRANSMISIÓN DE DOCUMENTOS POR FACSÍMIL POR LA RED TELEFÓNICA GENERAL CONMUTADA

ENMIENDA 1

Resumen

La Recomendación T.30 define los protocolos para los terminales facsímil del grupo 3.

La enmienda 1 define los cambios propuestos al texto principal de la Recomendación T.30 y la introducción de los nuevos anexos G, H e I.

Los cambios relativos al texto principal se refieren a la introducción de las nuevas señales fin de selección (EOS, e*nd of selection*), señal de página parcial - fin de selección (PPS-EOS, *partial page signal – end of selection*), campo no válido (FNV, *field not valid*), subdirección para interrogación secuencial, nueva denominación de la contraseña para la transmisión de ID del remitente (SID) y modificaciones referentes a la introducción de los nuevos anexos.

El anexo G describe la utilización del sistema de gestión de claves HKM, del sistema de cifrado HFX40 y del sistema troceador HFX40-I (todos ellos descritos en la Recomendación T.36).

El anexo H describe la utilización del algoritmo RSA.

Los procedimientos propuestos en los anexos G y H se basan en los definidos en el cuerpo principal y en los anexos A y C de la Recomendación T.30.

El anexo I contiene las modificaciones necesarias para contemplar la utilización de una comunicación con imágenes en color y en escala de grises empleando el esquema de codificación sin pérdidas definido en la Recomendación T.43.

Orígenes

La Recomendación UIT-T T.30, enmienda 1, ha sido preparada por la Comisión de Estudio 8 (1997-2000) del UIT-T y fue aprobada por el procedimiento de la Resolución N.° 1 de la CMNT el 2 de julio de 1997.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución N.° 1 de la CMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT a recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Página

1 Sección 1 Introducción de nuevas señales y modificaciones de señales existentes 1

2 Sección 2 13

Anexo G – Procedimientos para la transmisión segura de documentos por facsímil grupo 3 mediante la utilización de los sistemas HKM y HFX 13

G.1 Introducción 13

G.2 Descripción del procedimiento de transmisión segura de documentos por facsímil 14

G.3 Referencias 15

G.4 Definiciones 15

G.5 Abreviaturas 15

G.6 Procedimientos facsímil 16

G.7 Diagramas de flujo 18

G.8 Diagramas de flujo 19

1 Sección 1 Introducción de nuevas señales y modificaciones de señales existentes 1

1.1) Modifíquese 5.3.6.1.2 5) para que diga lo siguiente: 1

1.2) Añádase el nuevo apartado 6) a 5.3.6.1.2 siguiente: 1

1.3) Modifíquese 5.3.6.1.3 5) para que diga: 1

1.4) En 5.3.6.1.6, añádase un nuevo apartado 7) posterior al mensaje que diga: 1

1.5) Renumérense las actuales secciones 5.3.6.1.6 7) a 5.3.6.1.6 9) como 5.3.6.1.6 8) a 5.3.6.1.6 10), respectivamente. 1

1.6) Añádase el nuevo apartado 3) a 5.3.6.1.8 siguiente: 2

1.7) Añádase una nueva subcláusula 5.3.6.2.11 que diga lo siguiente: 2

1.8) Añádase la nueva subcláusula 5.3.6.2.12 siguiente: 2

1.9) Añádase la subcláusula 5.3.6.2.13 siguiente: 6

1.10) Remplácese el cuadro 2/T.30 existente por el siguiente: 6

1.11) En la figura A.1/T.30, modifíquese la descripción del FCF2 de modo que se lea: 13

1.12) Definición de la señal PPS-EOS 13

2 Sección 2 13

G.1 Introducción 13

G.2 Descripción del procedimiento de transmisión segura de documentos por facsímil 14

G.3 Referencias 15

G.4 Definiciones 15

G.5 Abreviaturas 15

G.6 Procedimientos facsímil 16

G.7 Diagramas de flujo 18

G.8 Diagramas de flujo 19

1 Sección 1 Introducción de nuevas señales y modificaciones de señales existentes 1

1.1) Modifíquese 5.3.6.1.2 5) para que diga lo siguiente: 1

1.2) Añádase el nuevo apartado 6) a 5.3.6.1.2 siguiente: 1

1.3) Modifíquese 5.3.6.1.3 5) para que diga: 1

1.4) En 5.3.6.1.6, añádase un nuevo apartado 7) posterior al mensaje que diga: 1

1.5) Renumérense las actuales secciones 5.3.6.1.6 7) a 5.3.6.1.6 9) como 5.3.6.1.6 8) a 5.3.6.1.6 10), respectivamente. 1

1.6) Añádase el nuevo apartado 3) a 5.3.6.1.8 siguiente: 2

1.7) Añádase una nueva subcláusula 5.3.6.2.11 que diga lo siguiente: 2

1.8) Añádase la nueva subcláusula 5.3.6.2.12 siguiente: 2

1.9) Añádase la subcláusula 5.3.6.2.13 siguiente: 6

1.10) Remplácese el cuadro 2/T.30 existente por el siguiente: 6

1.11) En la figura A.1/T.30, modifíquese la descripción del FCF2 de modo que se lea: 13

1.12) Definición de la señal PPS-EOS 13

2 Sección 2 13

Anexo G Procedimientos para la transmisión segura de documentos por facsímil grupo 3 mediante la utilización de los sistemas HKM y HFX 13

G.1 Introducción 13

G.2 Descripción del procedimiento de transmisión segura de documentos por facsímil 14

G.3 Referencias 15

G.4 Definiciones 15

G.5 Abreviaturas 15

G.6 Procedimientos facsímil 16

G.7 Diagramas de flujo 18

G.8 Diagramas de flujo 19

Recomendación T.30

PROCEDIMIENTOS DE TRANSMISIÓN DE DOCUMENTOS POR FACSÍMIL POR LA RED TELEFÓNICA GENERAL CONMUTADA

ENMIENDA 1

(Ginebra, 1997)

1 Sección 1 Introducción de nuevas señales y modificaciones de señales existentes

1.1) Modifíquese 5.3.6.1.2 5) para que diga lo siguiente:

5) *Interrogación secuencial selectiva* (SEP, *selective polling*) – Esta señal opcional indica que la siguiente información FIF es:

   a) una subdirección para el modo interrogación secuencial; o

   b) un número de documento específico.

   (Véase el punto 5.3.6.2.9/T.30, formato para la codificación de SEP.) SEP se envía únicamente si el bit 47 está puesto en DIS.

Formato: 1000 0101

NOTA – Cuando se utilizan juntas las señales PSA y SEP en el modo interrogación secuencial, se aplica la opción b).

1.2) Añádase el nuevo apartado 6) a 5.3.6.1.2 siguiente:

6) *Subdirección interrogada* (PSA, *polled subaddress*) – Esta señal opcional indica que la siguiente información FIF es una subdirección para interrogación secuencial (véase el punto 5.3.6.2.13/T.30 sobre formato para la codificación de PSA). PSA se envía únicamente si el bit 35 está puesto en DIS.

Formato: 1000 0110

1.3) Modifíquese 5.3.6.1.3 5) para que diga:

"5) *Identificación al remitente* (SID, *sender identification*) – Esta señal opcional indica que la información FIF siguiente es la identidad del remitente (véase el punto 5.3.6.2.11/T.30 formato para codificación de SID). SID se envía únicamente si el bit 50 está puesto en DIS.

Formato: X100 0101"

1.4) En 5.3.6.1.6, añádase un nuevo apartado 7) posterior al mensaje que diga:

"Formato: X111 1000

7) *Fin de selección* (EOS, *end of selection*) – Esta instrucción opcional desde el transmisor de interrogación secuencial con capacidad de SEP múltiple al receptor de interrogación secuencial con capacidad de SEP deberá utilizarse para indicar que se ha llegado al final (última página o último bloque) del documento seleccionado en ese instante y que se espera una vuelta a la fase B para reducir toda nueva petición de documento seleccionado por la SEP. La señal EOS puede transmitirse únicamente si el bit 34 está puesto en la DTC del receptor."

1.5) Renumérense las actuales secciones 5.3.6.1.6 7) a 5.3.6.1.6 9) como 5.3.6.1.6 8) a 5.3.6.1.6 10), respectivamente.

1.6) Añádase el nuevo apartado 3) a 5.3.6.1.8 siguiente:

"3) Campo no válido (FNV, *field not valid*). Esta señal opcional indica que la última señal PWD, SEP, SUB, SID, TSI, PSA o de fax seguro recibida (o una combinación de éstas) no es válida o no se acepta. FNV se envía únicamente si el bit 33 está puesto en DIS/DTC y DCS.

NOTA – FNV se enviará en lugar de CFR/FTT cuando el FIF de una o más señales opcionales asociadas con DCS no sea válido o no se acepte. FNV se enviará también en respuesta al DTC cuando una o más de las señales opcionales conexas no sea válida o no se acepte. FNV también puede enviarse en respuesta a las señales DEC, DES, DTR o DER (como se define en el anexo H/T.30).

Formato: X101 0011"

1.7) Añádase una nueva subcláusula 5.3.6.2.11 que diga lo siguiente:

"**5.3.6.2.11 Formato para la codificación de SID**

El campo de información facsímil de la señal SID consistirá en 20 cifras numéricas codificadas como se indica en el cuadro 3 pero excluyendo el carácter "+". El bit menos significativo de la cifra menos significativa será el primer bit transmitido. Los octetos sin utilizar en el campo de información se rellenarán con el carácter "espacio" y la información debe justificarse a la derecha."

1.8) Añádase la nueva subcláusula 5.3.6.2.12 siguiente:

"**5.3.6.2.12 Formato para la codificación de FNV**

La estructura del FIF para la señal FNV es la siguiente:

Octetos de motivo	Octeto de número de trama	Octetos de información de diagnóstico

En el FIF de la señal FNV se requiere al menos un octeto de motivo. Los otros octetos son opcionales pero es necesario un octeto de número de trama si están presentes algunos de los octetos de información de diagnóstico. La utilización de los octetos facultativos depende de la aplicación. Los terminales que emplean la señal FNV deberán poder recibir estos octetos, pero no están obligados a tratarlos, ni a reaccionar a los mismos.

Formato de los octetos de motivo

El primer octeto se denomina octeto de motivo y se utiliza para identificar los casos en que el contenido del campo de información facsímil (FIF, *facsimile information field*) para las señales especificadas no es válido. Los valores aplicados a este octeto se encuentran en el cuadro que aparece a continuación. La puesta de un bit a "0" indica "correcto" y un bit puesto a "1" indica "inválido". El bit 8 es un bit de ampliación que se pondrá a "1" si hay octetos de motivo adicionales en el FIF. Si el bit de ampliación se pone a "0", no hay octetos de motivo adicionales.

N.° del bit	Significado
1	Contraseña incorrecta (PWD)
2	Referencia de interrogación secuencial selectiva (SEP) desconocida
3	Subdirección (SUB) desconocida
4	Identidad del remitente (SID) desconocida
5	Error de fax seguro
6	Identificación del abonado de transmisión (TSI) no aceptada
7	Subdirección interrogada secuencialmente (PSA) no conocida
8	Bit de ampliación – por defecto a "0"
NOTA – A medida que se definan octetos de motivo adicionales deberán tener una estructura de bits coherente con el primer octeto de motivo. Los primeros siete bits identificarán los motivos (o estarán reservados) y el octavo bit es un bit de ampliación para los octetos de motivo.	

Formato para el número de trama del FNV

Se trata de un número binario de 8 bits. El número de trama 0-255 (el número máximo es 255) se utiliza para identificar el número de secuencia de una trama FNV. La trama 0 es la primera trama que debe transmitirse en una serie de tramas FNV. El bit menos significativo se transmite en primer lugar.

Formato para octetos de información de diagnóstico de FNV

La información de diagnóstico para una o más señales puede presentarse de forma opcional. La información de diagnóstico para cada señal se presenta en una serie de octetos utilizando una codificación del tipo, la longitud y el valor. El orden de transmisión para los octetos de información de diagnóstico deberá ser de izquierda a derecha y el bit menos significativo (a la derecha) deberá ser el primero que se transmite, salvo indicación contraria (véanse más adelante las reglas para los octetos de valor).

El formato para la información de diagnóstico de cada señal es el siguiente:

Tipo	Longitud	Valor – Contenido FIF no válido (número variable de octetos)

Tipo – Especificado basándose en la inversa de campo de control de facsímil (FCF, *facsimil control field*) de la señal u otra denominación característica. Se utilizan normalmente identificadores de un octeto pero se dispone de un método de ampliación. Los tipos se definen de la forma siguiente:

Tipo	Descripción
1100 0001	Contraseña incorrecta (PWD)
1010 0001	Referencia de interrogación secuencial selectiva (SEP) desconocida
1100 001X	Subdirección (SUB) desconocida
1010 001X	Identidad del remitente (SID) desconocida
0000 1000	Error de fax seguro
0100 001X	Identificación del abonado de transmisión (TSI) no aceptada
0110 0001	Subdirección interrogada secuencialmente no conocida
NOTA – X se define como indica 5.3.6.1/T.30.	

Longitud – Número de octetos del valor que sigue. Se utiliza normalmente un octeto pero se dispone de un método de ampliación.

Valor – Contiene la parte de FIF que no fue válida para el tipo de señal u otra información de diagnóstico. En los casos en que se devuelve todo o parte del FIF no aceptado, los datos deberán presentarse en el mismo orden de bits y octetos como se transmitieron originalmente.

Si se dispone de información de diagnóstico para más de una señal, el octeto de "tipo" para la segunda señal irá inmediatamente después del último octeto de "valor" para la señal anterior. De forma similar, toda la información de diagnóstico para todas las señales se presentará en el FIF del FNV hasta que se transmita toda la información de diagnóstico. En los casos en que el volumen de información de diagnóstico a transmitir rebase los límites de una sola trama T.30, la información de diagnóstico restante se situará en tramas FNV adicionales y el número de trama se incrementará en una unidad para cada nueva trama. Para tales tramas adicionales, el contenido de los octetos de motivo deberá ser idéntico a la primera trama FNV y el contenido de los octetos de información de diagnóstico deberá ser el de la trama previa.

Sintaxis del campo de información facsímil FNV

A continuación se presenta la sintaxis detallada del campo de información facsímil FNV en formato Backus-Naur (BNF). Los símbolos utilizados en el BNF se definen en H.6.1.4.5/T.30.

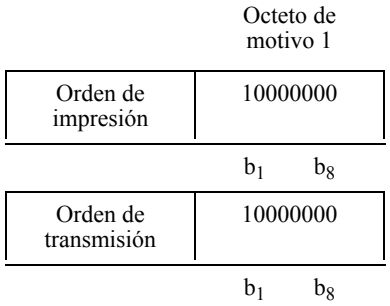
```
<bit>          ::= <0> | <1>
<octet>        ::= <bit><bit><bit><bit><bit><bit><bit><bit>
<8_bit_tag>    ::= <octet>
<extend_octet> ::= {<1><1><1><1><1><1><1><1>}
```

<FNV_type> ::= <8_bit_tag>|<extend octet><8_bit_tag><8_bit_tag>
<parameter_value> ::= <octet>{<octet>}
<count_extend_octet> ::= <0><0><0><0><0><0><0><0>
<parameter_length> ::= <octet>|<count_extend_octet> <octet> <octet>
<Diagnostic_Information> ::= {<FNV_type><parameter_length><parameter_value>}
<frame_number> ::= <octet>
<FNV_Reason_Octets> ::= <octet>{<octet>}
<FIF_of_FNV> ::= <FNV_Reason_Octets>[<frame_number>< Diagnostic_Information>]

Ejemplos de código para campos de información facsímil FNV

Caso A)

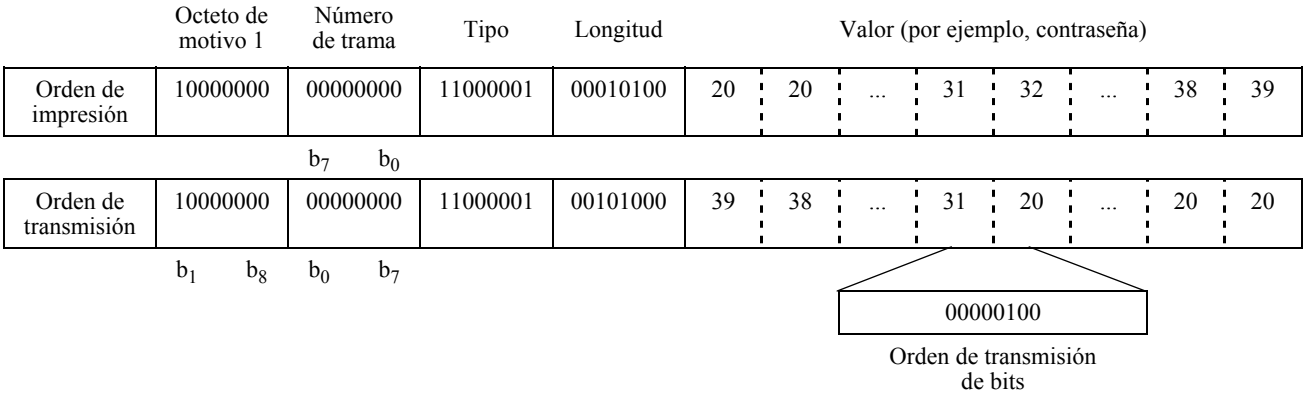
La contraseña no es válida y no se envía información de diagnóstico.



Caso B)

La contraseña no es válida y se envía la información de diagnóstico.

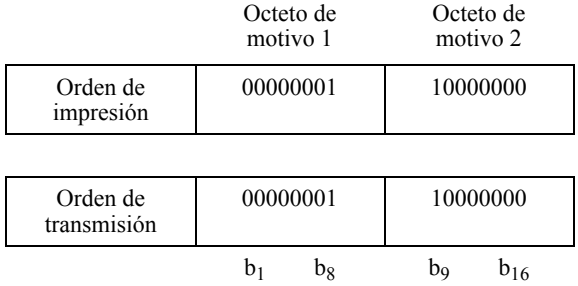
El ejemplo de la contraseña es "123456789"



Caso C)

Se definen nuevos bits de error en el segundo octeto de motivo.

Aparece un error en el bit 1 del segundo octeto de motivo y no se envía información de diagnóstico.



Caso D)

Se define un nuevo bit de error en el segundo octeto de motivo.

Aparece un error en el bit 1 del segundo octeto de motivo y se envía información de diagnóstico para el caso en que se devuelve el FIF de la señal no válida.

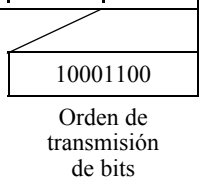
	Octeto de motivo 1	Octeto de motivo 2	Número de trama		Tipo	Longitud	Valor
Orden de impresión	00000001	10000000	00000000		FCF (orden inverso)	Longitud	Devolución de FIF (orden inverso)
			b_7 b_0				
Orden de transmisión	00000001	10000000	00000000		FCF (orden normal)	Longitud	Devolución de FIF (orden normal)
	b_1 b_8	b_9 b_{16}	b_0 b_7				

Caso E)

Se definen nuevos bits de error en el segundo octeto de motivo. Una parte de la subdirección no es válida (véase el bit 3) y se indica un error en el bit 9 del segundo octeto de motivo. Se incluye la información de diagnóstico para ambos errores. El ejemplo de la subdirección es "SSSSSSSSSSS1002#2002" y únicamente se rechaza la ampliación 1002. Una parte del valor de la información de diagnóstico para el segundo error se extiende sobre la frontera de trama, de manera que se transmite una segunda trama con la continuación del valor. La información de diagnóstico para el segundo error no incluye la devolución de un FIF previo, de forma que se aplica la regla general para el orden de transmisión de bits (se transmite en primer lugar el bit menos significativo que es el que se encuentra más a la derecha).

Primera Trama

	Octeto de motivo 1	Octeto de motivo 2	Número de trama	Tipo 1 (SUB)	Longitud (4)	Valor (parte devuelta de FIF)			
Orden de impresión	00100001	10000000	00000000	11000011	00000100	31	30	30	32
			b_7 b_0		longitud del primer bloque				
Orden de transmisión	00100001	10000000	00000000	11000011	00100000	32	30	30	31
	b_1 b_8	b_9 b_{16}	b_0 b_7						



Primera trama (continuación)

	Tipo 2	Longitud (128)	Valor
Orden de impresión	Tipo	10000000	Valor

Orden de transmisión	Tipo (orden del bit menos significativo)	00000001	Valor (orden del bit menos significativo)

Segunda trama

	Octeto de motivo 1	Octeto de motivo 2	Número de trama (2)	Valor (continuación)
Orden de impresión	00100001	10000000	00000001	Valor (continuación)
			b_7 b_0	
Orden de transmisión	00100001	10000000	10000000	Valor (en primer lugar el bit menos significativo)
	b_1 b_8	b_9 b_{16}	b_0 b_7	

1.9) Añádase la subcláusula 5.3.6.2.13 siguiente:

"**5.3.6.2.13 Formato de codificación de PSA**

El campo de información facsímil de la señal PSA constará de 20 dígitos numéricos codificados como se muestra en el cuadro 3/T.30, pero excluyendo el carácter "+". El bit menos significativo del dígito menos significativo será el primero en transmitirse. Los octetos no utilizados del campo de información se rellenarán con el carácter "espacio" y la información estará justificada a la derecha."

1.10) Remplácese el cuadro 2/T.30 existente por el siguiente:

Cuadro 2/T.30

N.° del bit	DIS/DTC	Nota	DCS	Nota
1	Reservado	1	Reservado	1
2	Reservado	1	Reservado	1
3	Reservado	1	Reservado	1
4	Reservado	1	Reservado	1
5	Reservado	1	Reservado	1
6	Capacidades V.8	23	No válido	24
7	"0" = 256 octetos preferido "1" = 64 octetos preferido	23, 42	No válido	24
8	Reservado	1	Reservado	1
9	Preparado para transmitir un documento facsímil (interrogado secuencialmente)	18	Poner a "0"	
10	Receptor funcionamiento fax	19	Receptor funcionamiento fax	20
11, 12, 13, 14 0, 0, 0, 0 0, 1, 0, 0 1, 0, 0, 0 1, 1, 0, 0 0, 0, 1, 0 0, 1, 1, 0 1, 0, 1, 0 1, 1, 1, 0 0, 0, 0, 1 0, 1, 0, 1 1, 0, 0, 1 1, 1, 0, 1 0, 0, 1, 1 0, 1, 1, 1 1, 0, 1, 1 1, 1, 1, 1	Velocidad de señalización de datos Rec. V.27 *ter* modo repliegue Rec. V.27 *ter* Rec. V.29 Recs. V.27 *ter* y V.29 No utilizado Reservado No utilizado No válido No utilizado Reservado No utilizado Recs. V.27 *ter*, V.29 y V.17 No utilizado Reservado No utilizado Reservado	3 32 	Velocidad de señalización de datos 2400 bit/s, Rec. V.27 *ter* 4800 bit/s, Rec. V.27 *ter* 9600 bit/s, Rec. V.29 7200 bit/s, Rec. V.29 No válido No válido Reservado Reservado 14 400 bit/s, Rec. V.17 12 000 bit/s, Rec. V.17 9600 bit/s, Rec. V.17 7200 bit/s, Rec. V.17 Reservado Reservado Reservado Reservado	33 31 31

Cuadro 2/T.30 *(continuación)*

N.° del bit	DIS/DTC	Nota	DCS	Nota
15	R8 × 7,7 líneas /mm y/o 200 × 200 pels/25,4 mm	10, 11, 13, 25	R8 × 7,7 líneas /mm y/o 200 × 200 pels/25,4 mm	10, 11, 13
16	Capacidad de codificación bidimensional		Codificación bidimensional	
17, 18 (0,0) (0,1) (1,0) (1,1)	Capacidad de anchura registrable Longitud de línea de exploración de 215 mm ± 1% Longitud de línea de exploración de 215 mm ± 1% y Longitud de línea de exploración de 255 mm ± 1% y Longitud de línea de exploración de 303 mm ± 1% Longitud de línea de exploración de 215 mm ± 1% y Longitud de línea de exploración de 255 mm ± 1% No válido	27 6	Anchura registrable Longitud de línea de exploración de 215 mm ± 1% Longitud de línea de exploración de 303 mm ± 1% Longitud de línea de exploración de 255 mm ± 1% No válido	27
19, 20 (0,0) (0,1) (1,0) (1,1)	Capacidad de longitud máxima registrable A4 (297 mm) Ilimitada A4 (297 mm) y B4 (364 mm) No válido	2	Longitud máxima registrable A4 (297 mm) Ilimitada B4 (364 mm) No válido	2
21, 22, 23 (0,0,0) (0,0,1) (0,1,0) (1,0,0) (0,1,1) (1,1,0) (1,0,1) (1,1,1)	Capacidad de tiempo mínimo de la línea de exploración en el receptor 20 ms para 3,85 l/mm: $T_{7,7} = T_{3,85}$ 40 ms para 3,85 l/mm: $T_{7,7} = T_{3,85}$ 10 ms para 3,85 l/mm: $T_{7,7} = T_{3,85}$ 5 ms para 3,85 l/mm: $T_{7,7} = T_{3,85}$ 10 ms para 3,85 l/mm: $T_{7,7} = 1/2\ T_{3,85}$ 20 ms para 3,85 l/mm: $T_{7,7} = 1/2\ T_{3,85}$ 40 ms para 3,85 l/mm: $T_{7,7} = 1/2\ T_{3,85}$ 0 ms para 3,85 l/mm: $T_{7,7} = T_{3,85}$	4, 8, 23	Tiempo mínimo de la línea de exploración 20 ms 40 ms 10 ms 5 ms 0 ms	8, 24
24	Extender el campo	5	Extender el campo	5
25	Reservado	1, 41	Reservado	1, 41
26	Modo sin compresión		Modo sin compresión	
27	Modo de corrección de errores	9, 17, 23, 25	Modo de corrección de errores	9, 17, 24, 34
28	Poner a "0"		Longitud de trama 0 = 256 octetos Longitud de trama 1 = 64 octetos	7, 24
29	Reservado	1	Reservado	1
30	Reservado	1	Reservado	1
31	Capacidad de codificación Rec. T.6	9, 17	Capacidad para codificación Rec. T.6	9, 17
32	Extender el campo	5	Extender el campo	5
33	Capacidad no válida de campo		Capacidad no válida de campo	
34	Capacidad de interrogación selectiva múltiple		Poner a "0"	
35	Subdirección interrogada	26, 44, 45	Poner a "0"	
36	Codificación T.43	17, 25, 34, 35, 37, 39, 40	Codificación T.43	17, 25, 34, 35, 37, 39, 40
37	Intercalado de planos	25, 46	Intercalado de planos	25, 46
38	Reservado	1	Reservado	1
39	Reservado	1	Reservado	1
40	Extender el campo	5	Extender el campo	5

Cuadro 2/T.30 *(continuación)*

N.° del bit	DIS/DTC	Nota	DCS	Nota
41	R8 × 15,4 líneas/mm	10	R8 × 15,4 líneas/mm	10, 34
42	300 × 300 pels/25,4 mm	34	300 × 300 pels/25,4 mm	34
43	R16 × 15,4 líneas/mm y/o 400 × 400 pels/25,4 mm	10, 12, 13	R16 × 15,4 líneas/mm y/o 400 × 400 pels/25,4 mm	10, 12, 13, 34
44	Se prefiere la resolución basada en pulgadas	13, 14	Selección de tipo de resolución "0": sist. métrico "1": pulgadas	13, 14
45	Se prefiere la resolución basada en unidades métricas	13, 14	Intrascendente ("don't care")	
46	Capacidad de tiempo mínimo de la línea de explotación para resoluciones más altas "0": $T_{15,4} = T_{7,7}$ "1": $T_{15,4} = 1/2\ T_{7,7}$	15	Intrascendente ("don't care")	
47	Interrogación secuencial selectiva	26, 44	Poner a "0"	
48	Extender campo	5	Extender campo	5
49	Capacidad de subdireccionamiento		Capacidad de subdireccionamiento	26
50	Contraseña	26	Transmisión de contraseña	26
51	Preparado para transmitir un fichero de datos (interrogación secuencial)	17, 21	Poner a "0"	
52	Reservado	1	Reservado	1
53	Transferencia de fichero binario (BFT, *binary file transfer*)	16, 17, 21	Transferencia de fichero binario (BFT, *binary file transfer*)	16, 17
54	Modo transferencia de documento (DTM, *document transfer mode*)	17, 21	Modo transferencia de documento (DTM, *document transfer mode*)	17
55	Intercambio electrónico de datos (EDI, *electronic data interchange*)	17	Intercambio electrónico de datos (EDI, *electronic data interchange*)	17
56	Extender campo	5	Extender campo	5
57	Modo transferencia básica (BTM, *basic transfer mode*)	17, 21	Modo transferencia básica (BTM, *basic transfer mode*)	17
58	Reservado	1	Reservado	1
59	Preparado para transmitir un documento en modo de caracteres o modo mixto (interrogación secuencial)	17, 22	Poner a "0"	
60	Modo de caracteres	17, 22	Modo de caracteres	17, 22
61	Reservado	1	Reservado	1
62	Modo mixto (Anexo D/T.4)	17, 22	Modo mixto (Anexo D/T.4)	17, 22
63	Reservado	1	Reservado	1
64	Extender campo	5	Extender campo	5
65	Modo procesable 26 (Rec. T.505)	17, 22	Modo procesable 26 (Rec. T.505)	17, 22
66	Capacidad de red digital	43	Capacidad de red digital	43
67 (0) (1)	Capacidades dúplex y semidúplex Funcionamiento dúplex solamente Funcionamiento dúplex y semidúplex		Capacidades dúplex y semidúplex Funcionamiento semidúplex Funcionamiento dúplex	
68	Codificación JPEG	25, 34, 35, 39, 40	Codificación JPEG	25, 34, 35, 39, 40
69	Modo color total	25, 35	Modo color total	25, 35
70	Poner a "0"	36	Se prefieren tablas Huffman	25, 36

Cuadro 2/T.30 *(continuación)*

N.° del bit	DIS/DTC	Nota	DCS	Nota
71	Componente 12 bit/pel	25, 37	Componente 12 bits/pel	25, 37
72	Extender campo	5	Extender campo	5
73	Ningún submuestreo (1:1:1)	25, 38	Ningún submuestreo (1:1:1)	25, 38
74	Iluminante específico	25, 39	Iluminante específico	25, 39
75	Gama de color específica	25, 40	Gama de color específica	25, 40
76	Capacidad de formato de carta norteamericano (215,9 × 279,4 mm)	28	Formato de carta norteamericano (215,9 × 279,4 mm)	
77	Capacidad de formato legal norteamericano (215,9 × 355,6 mm)	28	Capacidad de formato legal norteamericano (215,9 × 355,6 mm)	
78	Capacidad básica de codificación secuencial de progresión única (Rec. T.85)	17, 29, 30	Capacidad básica de codificación secuencial de progresión única (Rec. T.85)	17, 29
79	Capacidad L0 opcional de codificación secuencial de progresión única (Rec. T.85)	17, 29, 30	Capacidad L0 opcional de codificación secuencial de progresión única (Rec. T.85)	17, 29
80	Extender campo	5	Extender campo	5
81	Capacidad de gestión de clave HKM		Gestión de clave HKM seleccionada	
82	Capacidad de gestión de clave RSA		Gestión de clave RSA seleccionada	47
83	Anular la capacidad de modo		Anular modo seleccionado	
84	Capacidad de cifrado HX40		Cifrado HFX40 seleccionado	
85	Capacidad de número de cifrado alternativo 2		Número de cifrado alternativo 2 seleccionado	
86	Capacidad de número de cifrado alternativo 3		Número de cifrado alternativo 3 seleccionado	
87	Capacidad de troceado HFX40-I		Troceado HFX40-I seleccionado	
88	Campo de ampliación	5	Campo de ampliación	5
89	Capacidad de número de sistema de troceado alternativo 2		Número de sistema de troceado alternativo 2 seleccionado	
90	Capacidad de número del sistema de troceado alternativo 3		Número de sistema de troceado alternativo 3 seleccionado	
91	Reservado para futuras características de seguridad	1	Reservado para futuras características de seguridad	1
92	Reservado	1	Reservado	1
93	Reservado	1	Reservado	1
94	Reservado	1	Reservado	1
95	Reservado	1	Reservado	1
96	Campo de ampliación	5	Campo de ampliación	5

NOTA 1 – Los bits indicados como "Reservado" se pondrán a "0".

NOTA 2 – Los terminales facsímil normalizados conformes a la Recomendación T.4 deberán tener la capacidad siguiente: longitud de papel = 297 mm.

NOTA 3 – Cuando la trama de DIS o DTC define las capacidades de la Recomendación V.27 *ter*, cabe suponer que el terminal puede funcionar a 4800 ó 2400 bit/s.

Cuando la trama DIS o DTC define las capacidades de la Recomendación V.29, cabe suponer que el terminal puede funcionar a 9600 ó a 7200 bit/s conforme a la Recomendación V.29; cuando define las capacidades de la Recomendación V.17, cabe suponer que el terminal puede funcionar a 14 400 bits/s, 12 000 bits/s, 9600 bits/s o 7200 bits/s según la Recomendación V.17.

Cuadro 2/T.30 *(continuación)*

NOTA 4 – $T_{7,7}$ y $T_{3,85}$ se refieren a los tiempos de la línea de exploración que deben utilizarse cuando la resolución vertical es de 7,7 líneas/mm (o 200 líneas/25,4 mm o 300 líneas/25,4 mm) o de 3,85 líneas/mm, respectivamente (véase más arriba el bit 15). $T_{7,7} = 1/2\ T_{3,85}$ indica que cuando la resolución vertical es 7,7 líneas/mm o 200 líneas/25,4 mm o 300 líneas/25,4 mm, el tiempo de la línea de exploración puede reducirse a la mitad.

NOTA 5 – El campo normalizado FIF para las señales DIS, DTC y DCS tiene una longitud de 24 bits. Si el bit (o los bits) "extender el campo" es (son) "1", el campo FIF se extenderá en 8 bits adicionales.

NOTA 6 – El terminal existente puede enviar la condición no válido (1,1) para los bits 17 y 18 de su señal DIS. Si se recibe esta señal, hay que interpretarla como (0,1).

NOTA 7 – El valor del bit 28 en la instrucción DCS sólo es válido cuando el bit 27 invoca el modo de corrección de errores de la Recomendación T.4.

NOTA 8 – El modo corrección de errores facultativo Recomendación T.4 requiere la capacidad de 0 ms de tiempo mínimo de línea de exploración. Los bits 21-23 de las señales DIS/DTC indican el tiempo mínimo de línea de exploración de un receptor, independientemente de la disponibilidad del modo corrección de errores.

En el caso del modo corrección de errores, el emisor envía la señal DCS con los bits 21-23 puestos a "1,1,1", indicando la capacidad de 0 ms.

En el caso de transmisión normal, el emisor envía la señal DCS con los bits 21-23 puestos en los valores apropiados según las capacidades de los dos terminales.

NOTA 9 – La capacidad del esquema de codificación de la Recomendación T.6 especificada por el bit 31 es válida solamente cuando el bit 27 (modo corrección de errores) se pone a "1".

NOTA 10 – Las resoluciones de R8 y R16 se definen como sigue:

R8 = 1728 pels/(215 mm ± 1%) para ISO A4, carta y legal norteamericano.

R8 = 2048 pels/(255 mm ± 1%) para ISO B4.

R8 = 2432 pels/(303 mm ± 1%) para ISO A3.

R16 = 3456 pels/(215 mm ± 1%) para ISO A4, carta y legal norteamericano.

R16 = 4096 pels/(255 mm ± 1%) para ISO B4.

R16 = 4864 pels/(303 mm ± 1%) para ISO A3.

NOTA 11 – El bit 15, cuando está puesto a "1", se interpreta según los bits 44 y 45, como sigue:

bit 44	bit 45	Interpretación
0	0	(no válido)
1	0	200 × 200 pels/25,4 mm
0	1	R8 × 7,7 líneas/mm
1	1	R8 × 7,7 líneas/mm y 200 × 200 pels/25,4 mm

"1" en el bit 15 sin los bits 41, 42, 43, 44, 45 y 46, indica R8 × 7,7 líneas/mm.

NOTA 12 – El bit 43, cuando está puesto a "1", se interpreta según los bits 44 y 45, como sigue:

bit 44	bit 45	Interpretación
0	0	(no válido)
1	0	400 × 400 pels/25,4 mm
0	1	R16 × 15,4 líneas/mm
1	1	R16 × 15,4 líneas/mm y 400 × 400 pels/25,4 mm

NOTA 13 – Los bits 44 y 45 se utilizan sólo junto con los bits 15 y 43. El bit 44 de DCS, cuando se utiliza, indicará correctamente la resolución del documento transmitido, lo que significa que el bit 44 del DCS no siempre se corresponderá a la indicación de los bits 44 y 45 de DIS/DTC. La selección cruzada causará distorsión y reducción del área reproducible.

Cuando un receptor indica en DIS que prefiere recibir información en unidades métricas y el transmisor sólo tiene la información equivalente en pulgadas (o viceversa), la comunicación no dejará de establecerse.

NOTA 14 – Los bits 44 y 45 no necesitan características adicionales en el terminal para indicar a los usuarios que transmiten o reciben si la información fue transmitida o recibida en métrico-métrico, pulgada-pulgada; métrico-pulgada o pulgada-métrico.

NOTA 15 – $T_{15,4}$ se refiere a los tiempos de la línea de exploración que debe utilizarse cuando la resolución vertical es de 15,4 líneas/mm o 400 líneas/mm.

$T_{15,4} = 1/2\ T_{7,7}$ indica que, cuando $T_{7,7}$ es 10, 20 ó 40 ms, el tiempo de la línea de exploración puede reducirse a la mitad en el modo de alta resolución.

Cuadro 2/T.30 *(continuación)*

Cuando $T_{7,7}$ es 5 ms [o sea (bit 21, bit 22, bit 23) = (1, 0, 0), (0, 1, 1)] ó 0 ms [o sea (1, 1, 1)], el bit 46 en DIS/DTC se deberá poner a "0" ($T_{15,4} = T_{7,7}$).

NOTA 16 – El protocolo de transferencia de fichero binario se describe en la Recomendación T.434.

NOTA 17 – Cuando cualquiera de los bits 31, 36, 51, 53, 54, 55, 57, 59, 60, 62, 65, 78 y 79 se ponga a "1", el bit 27 se pondrá también a "1".

NOTA 18 – El bit 9 indica que hay un documento facsímil preparado para ser interrogado secuencialmente desde el terminal de respuesta. No es una indicación de capacidad.

NOTA 19 – El bit 10 indica que el terminal de respuesta tiene capacidades de recepción.

NOTA 20 – El bit 10 es una instrucción al terminal receptor para que él mismo se ponga en el modo recepción.

NOTA 21 – El bit 51 indica que hay un fichero de datos preparado para ser interrogado secuencialmente desde el terminal de respuesta. No es indicación de una capacidad. Este bit se puede utilizar junto con los bits 53, 54 y 57.

NOTA 22 – El bit 59 indica que hay un documento en modo mixto o codificado en carácter preparado para ser interrogado secuencialmente desde el terminal de respuesta. No es una indicación de una capacidad. Este bit puede utilizarse junto con los bits 60, 62 y 65.

NOTA 23 – Cuando se utiliza el procedimiento facultativo definido en el anexo C/T.30, los bits 6 y 7 en DIS/DTC se pondrán a "0", y los bits 21 a 23 y 27 se pondrán a "1".

NOTA 24 – Cuando se utiliza el procedimiento facultativo definido en el anexo C/T.30, los bits 6, 7 y 28 en DCS se pondrán a "0", y los bits 21 a 23 y 27 se pondrán a "1".

NOTA 25 – En el anexo E/T.30 y en el I/T.30 se describen, respectivamente, los protocolos opcionales del modo de color de tono continuo y el modo de escala de grises (modo JPEG), y el modo opcional de codificación sin pérdidas de color y de escala de grises (modo T.43). Si el bit 68 en la trama DIS/DTC se pone a "1", esto indica capacidad de modo JPEG. Si los bits 36 y 68 están puestos a "1", esto indica que también está disponible la capacidad de T.43. El bit 36 de la trama DIS/DTC únicamente se pondrá a "1" cuando el bit 68 también se haya puesto a "1". Además, los bits 15 y 27 de la trama DIS/DTC deberán también ponerse a "1", si el bit 68 o los bits 36 y 68 se han puesto también a "1". El bit 15 indica una capacidad de resolución de 200 × 200 pels/25,4 mm, que es básica para el facsímil de color. El bit 27 indica la capacidad de modo de corrección de errores, que es obligatoria para el facsímil de color. Los bits 69 a 71 y 73 a 75 son pertinentes únicamente si el bit 68 se pone a "1". El bit 73 es pertinente solamente para el modo JPEG. Los bits 69, 71, 74 y 75 son pertinentes para el modo JPEG y/o modo T.43. El bit 37 es pertinente solamente cuando el bit 36 se ha puesto a "1" – véanse también las notas 39 y 40.

NOTA 26 – Para proporcionar un mecanismo de recuperación de errores, cuando se envían las tramas PWD/SEP/SUB/SID/PSA con DCS o DTC, los bits 49 y 50 en DCS o los bits 47, 50 y 35 en DTC deberán ponerse a "1". En el bit 47, la puesta a "1" para DTC significa transmisión de interrogación secuencial selectiva y para DIS significa capacidad de interrogación secuencial selectiva. En el bit 50, la puesta a "1" para DTC significa transmisión de contraseña y para DIS significa capacidad de contraseña o ID de remitente. En el bit 35, la puesta a "1" para DTC significa transmisión de subdirección interrogada y para DIS significa capacidad de subdirección interrogada. Los terminales conformes a las versiones de 1993 de esta Recomendación pueden poner los bits anteriores a 0 aun cuando se transmitan las tramas PWS/SEP/SUB.

NOTA 27 – Las longitudes de línea de exploración correspondientes para resoluciones basadas en la pulgada pueden encontrarse en 2.2/T.4.

NOTA 28 – Cuando se utilizan los bits 76 y 77 en DIS/DTC, es necesario que el terminal pueda recibir documentos ISO A4 con cualquier combinación de los bits 76 y 77. Los transmisores de A4, B4 y A3 pueden ignorar el valor fijado para de los bits 76 y 77.

NOTA 29 – El esquema de codificación indicado por los bits 78 y 79 se define en la Recomendación T.85.

NOTA 30 – Cuando el bit 79 en DIS se pone a "1", también se pondrá a "1" el bit 78.

NOTA 31 – Algunos terminales que eran conformes a la versión de 1994 y versiones anteriores de la presente Recomendación pueden haber utilizado este secuencia de bit para indicar utilización del sistema de modulación de la Recomendación V.33.

NOTA 32 – Algunos terminales que eran conformes a la versión de 1994 y versiones anteriores de la presente Recomendación pueden haber utilizado esta secuencia de bits para indicar capacidades de las Recomendaciones V.27 *ter*, V.29 y V.33. Para mantener la compatibilidad con tales terminales un terminal que tenga la capacidad de recibir utilizando el sistema de modulación definido en la Recomendación V.17 debe ser capaz también de recibir utilizando el sistema de modulación definido en la Recomendación V.33. Además, un terminal que tenga la capacidad de recibir utilizando el sistema de modulación definido en la Recomendación V.33 debe ser capaz también de recibir utilizando el sistema de modulación definido en la Recomendación V.29.

NOTA 33 – Cuando se utilice el sistema de modulación definido en la Recomendación V.34, los bits 11 a 14 de la DCS no son válidos y deben ponerse a "0".

NOTA 34 – El bit 68 puesto a "0" indica que el modo JPEG y el modo T.43 del terminal llamado no están disponibles y este terminal no puede decodificar datos codificados en JPEG o T.43. En una trama DCS, el bit 68 puesto a "1" indica que se utiliza el modo JPEG del terminal llamante y que se envían datos de imagen codificados en JPEG. El bit 68 puesto a "0" y el bit 36 puesto a "1" indica que se utiliza el modo T.43 del terminal llamante y que se envían datos de imagen codificados en el modo T.43. Si el bit 68 o el bit 36 de la trama DCS está puesto a "1", los bits 41 o 42 o 43, y el bit 27 de la trama DCS deberán ponerse también a "1". Los bits 42 y 43 indican las resoluciones 300 × 300 y 400 × 400 pels/25,4 mm, respectivamente. El bit 68 y el bit 36 puestos a "0" indica que no se utiliza ni el modo JPEG ni el modo T.43, y que la imagen no está codificada en los modos JPEG ni en la Recomendación T.43.

Cuadro 2/T.30 *(continuación)*

NOTA 35 – En la trama DIS/DTC, el bit 69 puesto a "1" indica que el terminal llamado tiene capacidad de color completa. Este terminal puede aceptar datos de imagen de color completo en el espacio CIELAB. Si el bit 36 está también puesto a "1", dicho terminal puede aceptar también datos de imagen de color definidos en la Recomendación T.43. El bit 69 puesto a "0" y el bit 68 o los bits 68 y 36 puestos a "1" indica que el terminal llamado dispone solamente del modo de escala de grises, que acepta solamente el componente de claridad (el componente L*) en la representación CIELAB para el modo JPEG y para el modo T.43, respectivamente. En una trama DCS, el bit 68 y el bit 69 puestos a "1" indica que el terminal llamante envía imagen en representación de color completo en el espacio CIELAB, en el modo JPEG. En una trama DCS, el bit 36 y el bit 69 puestos a "1" indica que el terminal llamante envía imagen de color codificada en el modo Rec. T.43. El bit 68 o el bit 36 puestos s "1" y el bit 69 puesto a "0" indica que el terminal llamante envía solamente el componente de claridad (el componente L*) en la representación CIELAB para el modo JPEG o el modo T.43, respectivamente. Nota: Las imágenes en color sólo se transmitirán si, o bien el bit 68 y el bit 69 están fijados a "1" o el bit 36 y el bit 69 están fijados a "1", ambos.

NOTA 36 – El bit 70 se denomina "indicación de tablas Huffman por defecto". Proporciona un medio para indicar al terminal llamado que las tablas Huffman son las tablas por defecto. Las tablas por defecto se especifican solamente para la resolución de intensidad de imagen por defecto (8 bits/pel/componente). Las tablas Huffman por defecto deben determinarse (por ejemplo, tablas K.3/T.81-K.6/T.81). En una trama DIS/DTC, el bit 70 no se utiliza y se pone a cero. En una trama DCS, el bit 70 puesto a 0 indica que el terminal llamante no identifica las tablas de Huffman que utiliza para codificar los datos de imagen como las tablas por defecto. El bit 70 puesto a 1 indica que el terminal llamante identifica las tablas de Huffman que utiliza para codificar los datos de imagen como las tablas por defecto.

NOTA 37 – En una trama DIS/DTC, el bit 71 puesto a "0" indica que el terminal llamado sólo puede aceptar datos de imagen que hayan sido digitalizados a 8 bits por componente para el modo JPEG. Esto es también válido para el modo T.43 si el bit 36 está también fijado a "1". El bit 71 puesto a "1" indica que el terminal llamado sólo puede aceptar datos de imagen que hayan sido digitalizados a 12 bits por componente para el modo JPEG. Esto es también válido para el modo T.43 si el bit 36 está también puesto a "1". En una trama DCS, el bit 71 puesto a "0" indica que el terminal llamante transmite datos de imagen que han sido digitalizados a 8 bits por componente para el modo JPEG. Esto es asimismo válido para el modo T.43 si el bit 36 está también puesto a "1". El bit 71 puesto a "1" indica que el terminal llamante transmite datos de imagen que han sido digitalizados a 12 bits por componente para el modo JPEG. Esto es asimismo válido para el modo T.43 si el bit 36 está también puesto a "1".

NOTA 38 – En una trama DIS/DTC, el bit 73 puesto a 0 indica que el terminal llamado espera una relación de submuestreo de las componentes de crominancia de los datos de imagen de 4:1:1; las componentes a* y b* en la representación de espacio de color CIELAB se submuestrean en una relación de cuatro veces a una con respecto a la componente L*. Los detalles se describen en el anexo E/T4. La puesta a "1" del bit 73 indica que el terminal llamado, como una opción, acepta el no submuestreo de las componentes de crominancia en los datos de imagen. En una trama DCS, el bit 73 puesto a "0" indica que el terminal llamado utiliza una relación de submuestreo de las componentes a* y b* en los datos de imagen de 4:1:1. El bit 73 puesto a 1 indica que el terminal llamado no efectúa submuestreo.

NOTA 39 – En una trama de DIS/DTC la puesta del bit 74 a "0" indica que el terminal llamado espera la utilización del iluminante D50 de la norma CIE en los datos de imagen de color, como se especifica en la Recomendación T.42. La puesta del bit 74 a "1" indica que el terminal llamado también puede aceptar otros tipos de iluminantes además del D50. La puesta del bit 68 a "1" indica que el terminal tiene la capacidad de codificación JPEG, como se describe en el anexo E/T.4. La puesta del bit 36 a "1" indica que el terminal tiene la capacidad de codificación de color, como se describe en la Recomendación T.43. En una trama DCS, la puesta del bit 74 a "0" y del bit 68 o el bit 36 a "1", indica que el terminal llamante utiliza el iluminante D50 en la representación de los datos de imagen de color, como se especifica en la Recomendación T.42. La puesta del bit 74 a "1" indica que se está utilizando otro tipo de iluminante. Cuando los bits 68 y 74 se ponen a "1", la especificación se incluye en la sintaxis JPEG como se describe en el anexo E/T.4. Cuando los bits 36 y 74 se ponen a "1", la especificación se incluye en la sintaxis de la Recomendación T.43, como se describe en dicha Recomendación.

NOTA 40 – En una trama DIS/DTC, la puesta del bit 75 a "0" indica que el terminal llamado espera que los datos de imagen de color se representen utilizando la extensión de la gama de colores por defecto especificada en la Recomendación T.42. La puesta del bit 75 a "1" indica que el terminal llamado también puede aceptar otras extensiones de la gama de colores. La puesta del bit 68 a "1" indica que el terminal tiene la capacidad de codificación JPEG, como se describe en el anexo E/T.4. La puesta del bit 36 a "1" indica que el terminal tiene la capacidad de codificación en color, como se describe en la Recomendación T.43. En una trama DCS, la puesta del bit 75 a "0" y el bit 68 o el bit 36 a "1", indica que el terminal llamante utiliza la extensión de la gama de colores por defecto como se especifica en la Recomendación T.42. La puesta del bit 75 a "1" indica que el terminal llamante utiliza una extensión de la gama de colores distinta. Cuando los bits 68 y 75 se ponen a "1", la especificación se incluye en la sintaxis JPEG como se describe en el anexo E/T.4. Cuando los bits 36 y 75 se ponen a "1", la especificación se incluye en la sintaxis de la Recomendación T.43 como se describe en dicha Recomendación.

NOTA 41 – Algunos terminales conformes con las versiones de esta Recomendación anteriores a 1996 pueden poner este bit a "1" . Tales terminales darán una secuencia de respuesta como se muestra en la figura III.2/T.30.

NOTA 42 – Se sobreentiende que para la compatibilidad regresiva un terminal transmisor puede pasar por alto la petición de una trama de 64 octetos y, en consecuencia, el terminal receptor debe estar preparado para manejar, de alguna manera, tramas de 256 octetos.

NOTA 43 – Véase C.7.2/T.30.

NOTA 44 – Aclaración sobre la utilización de la interrogación secuencial selectiva basada en los valores del bit 47 y del bit 35 dados en el punto 5.3.6.1.2 5)/T.30.

NOTA 45 – Aclaración sobre la utilización de subdirección para interrogación secuencial basada en los valores del bit 35 dados en el punto 5.3.6.1.2 6)/T.30.

Cuadro 2/T.30 *(fin)*

NOTA 46 – En una trama DIS/DTC, la puesta del bit 37 a "0" indica que el terminal llamado puede aceptar únicamente datos de imagen intercalados por entrelazado por barra (128 líneas/barra o menos). La puesta del bit 37 a "1" indica que el terminal llamado puede aceptar también datos de imagen entrelazados por plano. En una trama DCS, la puesta del bit 37 a "0" indica que los datos de imagen del terminal llamante están intercalados a través del entrelazado de barra. La puesta del bit 37 a "1" indica que los datos de imagen del terminal llamante están intercalados a través de entrelazado plano. Los detalles de ambos métodos de entrelazado se describen en la Recomendación T.43.

NOTA 47 – DCS no se emite en el contexto del anexo H/T.30; FIF de DCS se incluye en la nueva señal "DEC" (véase H.6.1/T.30) donde el correspondiente bit 82 debe ponerse a "1".

1.11) En la figura A.1/T.30, modifíquese la descripción del FCF2 de modo que se lea:

FCF2 Campo de control facsímil 2: instrucción posterior a mensaje (NULL, MPS, EOM, EOP, EOS, y PRI-Q)

1.12) Definición de la señal PPS-EOS

En A.4.3 la figura A.1/T.30, modifíquese la Nota 1 para que diga:

FCF2	Significado
0000 0000	Código NULL, que indica el límite de página parcial
1111 0000	EOM, en el modo de corrección de errores opcional de la Recomendación T.4
1111 0010	MPS, en el modo de corrección de errores opcional de la Recomendación T.4
1111 0100	EOP, en el modo de corrección de errores opcional de la Recomendación T.4
1111 1000	EOS, en el modo de corrección de errores opcional de la Recomendación T.4
1111 1001	PRI-EOM, en el modo de corrección de errores opcional de la Recomendación T.4
1111 1010	PRI-MPS, en el modo de corrección de errores opcional de la Recomendación T.4
1111 1100	PRI-EOP, en el modo de corrección de errores opcional de la Recomendación T.4

2 Sección 2

Introducción del nuevo anexo G:

Anexo G

Procedimientos para la transmisión segura de documentos por facsímil grupo 3 mediante la utilización de los sistemas HKM y HFX

G.1 Introducción

G.1.1 Este anexo describe el protocolo utilizado por los terminales facsímil grupo 3 para proporcionar comunicaciones seguras utilizando los sistemas HKM y HFX. Los procedimientos aplicados se basan en los definidos en el texto principal de esta Recomendación y en los anexos A/T.30 y C/T.30.

G.1.2 La utilización de este anexo es facultativa.

G.1.3 Es obligatoria la corrección de errores definida en los anexos A/T.30 o C/T.30 (según proceda).

G.2 Descripción del procedimiento de transmisión segura de documentos por facsímil

G.2.1 Los sistemas HKM y HFX proporcionan las siguientes capacidades para comunicaciones de documentos seguras entre entidades (terminales u operadores de terminales):

- autenticación mutua de entidades;
- establecimiento de claves de sesión secretas;
- confidencialidad de los documentos;
- confirmación de recepción;
- confirmación o rechazo de la integridad del documento.

G.2.2 Funciones

Se proporciona la gestión de claves utilizando el sistema HKM definido en el anexo B/T.36. Se definen dos procedimientos: el primero es el registro y el segundo la transmisión segura de una clave secreta. El registro establece el secreto mutuo y permite efectuar con seguridad todas las transmisiones subsiguientes, en las que el sistema HKM proporciona autenticación mutua, una clave de sesión secreta para la confidencialidad e integridad del documento, la confirmación de recepción y una confirmación o rechazo de la integridad del documento.

La confidencialidad del documento se proporciona utilizando el cifrado definido en el anexo D/T.36. El cifrado utiliza una clave de 12 cifras decimales que equivale aproximadamente a 40 bits.

La integridad del documento se proporciona utilizando el sistema definido en el anexo E/T.36. La Recomendación T.36 define el algoritmo de troceado (hashing), incluidos los cálculos y el intercambio de información asociados.

G.2.3 Método

En el modo de registro, los dos terminales intercambian información que permite a las entidades identificarse inequívocamente entre sí, basándose en el acuerdo entre los usuarios de una clave secreta que se utiliza una sola vez. Cada entidad almacena un número de 16 cifras que está asociado únicamente con la entidad con la cual ha efectuado el registro.

Cuando tiene que enviar un documento con seguridad, el terminal transmisor transmite el número secreto de 16 cifras asociado con la entidad receptora junto con un número aleatorio y una clave de sesión criptada como una petición de identificación (challenge) a la entidad receptora. El terminal receptor responde transmitiendo la clave de 16 cifras asociada con la entidad transmisora junto con un número aleatorio y una versión recriptada de la petición de identificación de la entidad transmisora. Al mismo tiempo, transmite un número aleatorio y una clave de sesión encriptada como una petición de identificación a la entidad transmisora. El terminal transmisor responde con un número aleatorio y una versión recriptada de la solicitud de identificación de la entidad receptora. Este procedimiento permite que las dos entidades se autentiquen entre sí. Al mismo tiempo, el terminal transmisor transmite un número aleatorio y una clave de sesión criptada que se ha de utilizar para la cripción y el troceado.

Después de transmitir el documento, el terminal transmisor transmite un número aleatorio y una clave de sesión encriptada como una petición de identificación a la entidad receptora. Al mismo tiempo, envía un número aleatorio y un valor de troceado encriptado que permite a la entidad receptora asegurar la integridad del documento recibido. El terminal receptor transmite un número aleatorio y la versión reencriptada de la petición de identificación de la entidad transmisora. Al mismo tiempo, envía un número aleatorio y un documento de integridad criptado como confirmación o rechazo de la integridad del documento recibido.

El algoritmo de troceado utilizado para la integridad del documento se aplica en todo el documento.

Se proporciona otro modo que no conlleva el intercambio de señales de seguridad entre los dos terminales. Los usuarios acuerdan una clave de sesión secreta que se utiliza una sola vez y que se ha de introducir manualmente. Esta clave es utilizada por el terminal transmisor para cifrar el documento y por el terminal receptor para descifrar el documento.

G.3 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

– Recomendación UIT-T T.4 (1996), *Normalización de terminales facsímil de grupo 3 para transmisión de documentos.*

– Recomendación UIT-T T.36 (1997), *Procedimientos de utilización del sistema de gestión de claves HKM para la transmisión segura de documentos por facsímil.*

G.4 Definiciones

G.4.1 Funcionamiento por la red telefónica pública conmutada que utiliza los sistemas de modulación V.27 *ter*, V.29, V.17 y V.34 (modo semidúplex)

Las señales y definiciones utilizadas con los procedimientos de transmisión segura de documentos por facsímil son las indicadas en el texto principal y el anexo A/T.30 junto con las detalladas en G.6.1/T.30.

G.4.2 Funcionamiento por la red telefónica pública conmutada que utiliza el sistema de modulación V.34 (modo dúplex) y por la red digital de servicios integrados

Las señales y definiciones utilizadas con los procedimientos seguros de transmisión de documentos facsímil son las indicadas en el anexo C/T.30, junto con las detalladas en G.6.1/T.30.

G.5 Abreviaturas

G.5.1 Las abreviaturas utilizadas para la transmisión segura de documentos facsímil son las definidos en el texto principal de la presente Recomendación y en los anexos A/T.30 y C/T.30 junto con las especificadas a continuación.

ESHx Valor de troceado aleatorizado criptado del transmisor (*encrypted scrambled hash value from the transmitter*)

ESIMy Mensaje de integridad aleatorizado criptado del receptor (*encrypted scrambled integrity message from the receiver*)

ESSC1x Clave de petición de identificación secreta aleatorizada criptada del transmisor (*encrypted scrambled secret challenge key from the transmitter*)

ESSC1y Clave de petición de identificación secreta aleatorizada criptada del receptor (*encrypted scrambled secret challenge key from the receiver*)

ESSC2x Clave de petición de identificación secreta aleatorizada criptada del transmisor (*encrypted scrambled secret challenge key from the transmitter*)

ESSR1x Clave de respuesta secreta aleatorizada criptada del transmisor (*encrypted scrambled secret response key from the transmitter*)

ESSR1y Clave de respuesta secreta aleatorizada criptada del receptor (*encrypted scrambled secret response key from the receiver*)

ESSR2y Clave de respuesta secreta aleatorizada criptada del receptor (*encrypted scrambled secret response key from the receiver*)

ESSS1x Clave de sesión secreta aleatorizada criptada del transmisor (*encrypted scrambled secret session key from the transmitter*)

RCNx Número de criptación registrado (16 cifras decimales en 16 octetos) asociado con el transmisor [*registered crypt number (16 decimal digits in 16 octets) associated with the transmitter*]

RCNy Número de criptación registrado (16 cifras decimales en 16 octetos) asociado con el receptor [*registered crypt number (16 decimal digits in 16 octets) associated with the receiver*]

RK Claves del receptor – véase G.6.1/T.30 (*receiver keys*)

RNC1x Número aleatorio asociado con una petición de identificación secreta del transmisor (*random number associated with a secret challenge from the transmitter*)

RNC1y Número aleatorio asociado con una petición de identificación secreta del receptor (*random number associated with a secret challenge from the receiver*)

RNC2x Número aleatorio asociado con una petición de identificación secreta del transmisor (*random number associated with a secret challenge from the transmitter*)

RNIMy Número aleatorio asociado con un mensaje de integridad del receptor (*random number associated with an integrity message from the receiver*)

RNSR1x Número aleatorio asociado con una respuesta secreta del transmisor (*random number associated with a secret response from the transmitter*)

RNSR1y Número aleatorio asociado con una respuesta secreta del receptor (*random number associated with a secret response from the receiver*)

RNSR2y Número aleatorio asociado con una respuesta secreta del receptor (*random number associated with a secret response from the receiver*)

RNSS1x Número aleatorio asociado con una clave de sesión secreta del transmisor (*random number associated with a secret session key from the transmitter*)

RTC Retorno a control – definida en la Recomendación T.4 (*return to control*)

TK Claves del transmisor (*transmitter keys*) – véase G.6.1/T.30

TKx Clave de transferencia proporcionada por el transmisor (*transfer key provided by the transmitter*)

TKy Clave de transferencia proporcionada por el receptor (*transfer key provided by the receiver*)

TNR Transmisor no preparado (*transmitter not ready*) – véase G.6.1/T.30

TR Transmisor preparado (*transmitter ready*) – véase G.6.1/T.30

NOTA 1 – Todos los valores de números aleatorios son 4 cifras decimales en 4 octetos.

NOTA 2 – Todos los valores aleatorizados encriptados son 12 cifras decimales en 12 octetos.

G.6 Procedimientos facsímil

G.6.1 Campo de control facsímil

El sistema de gestión de claves HKM utiliza las tramas de claves del transmisor (TK) y de claves del receptor (RK) de la Recomendación T.30. El contenido del campo de información facsímil (FIF, *facsimile information field*) de estas señales varía de acuerdo con la utilización y se enumera en G.6.2/T.30. Cada señal TK y RK tiene un sufijo de una cifra para la referencia cruzada con los diagramas de flujo y los diagramas de secuencias de señales de este anexo.

Cada clave transferida (distinta a las transferidas durante el registro) está en el formato aleatorizado encriptado (ES, *encrypted scrambled*) y está acompañada por un número aleatorio (RN, *random number*) asociado.

1) *Transmisor no preparado (TNR)* – Esta señal se utiliza para indicar que el transmisor no está preparado aún para transmitir.

   Formato:
   X101 0111

2) *Transmisor preparado (TR)* – Esta señal se utiliza para preguntar el estado del transmisor.

   Formato:
   X101 0110

3) *Claves del transmisor (TK)* – Esta señal se utiliza para transportar claves de seguridad, etc., del transmisor del documento al receptor del documento. El contenido FIF de esta señal se define ulteriormente en este anexo y variará de acuerdo con las circunstancias en las cuales se utiliza.

   Formato:
   1101 0010

4) *Clave del receptor (RK)* – Esta señal se utiliza para transportar claves de seguridad, etc., del receptor del documento al transmisor del documento. El contenido del FIF de esta señal se define ulteriormente en este anexo y variará de acuerdo con las circunstancias en las cuales se utiliza.

   Formato:
   0101 0010

G.6.2 Campos de información facsímil

La codificación de las claves será la indicada en el cuadro 3/T.30 y el bit menos significativo de la cifra menos significativa será el primer bit transmitido.

G.6.2.1 Registro y autenticación mutuos

Véase el cuadro G.1/T.30.

Cuadro G.1/T.30

Señal	Octetos FIF	Contenido FIF
TK0	1 2 length 3-18 19-22 23-34	0000 0000 0010 0000 TKx RNC0x ESSC0x
RK1	1 2 length 3-18 19-34 35-38 39-50 51-54 55-66	0000 0001 0100 0000 RCNy TKy RNSR0y ESSR0y RNC0y ESSC0y
TK2	1 2 length 3-18 19-22 23-34	0000 0010 0010 0000 RCNx RNSR0x ESSR0x

G.6.2.2 Señales previas al mensaje: autenticación mutua e intercambio de clave de sesión secreta

Véase el cuadro G.2/T.30.

Cuadro G.2/T.30

Señal	Octetos FIF	Contenido FIF
TK8	1 2 length 3-18 19-22 23-34	0000 1100 0010 0000 RCNy RNC1x ESSC1x
RK9	1 2 length 3-18 19-22 23-34 35-38 39-50	0000 1001 0011 0000 RCNx RNSR1y ESSR1y RNC1y ESSC1y
TK10	1 2 length 3-6 7-18 19-21 23-34	0000 1010 0010 0000 RNSR1x ESSR1x RNSS1x ESSS1x
NOTA – Si el documento no está cifrado, RNC1x y ESSS1x se ponen a todos ceros.		

G.6.2.3 Procedimiento durante la transmisión del mensaje

Del transmisor al receptor. Los formatos y las señales específicas del procedimiento durante la transmisión del mensaje son las definidas en el anexo A/T.4.

G.6.2.4 Señales posteriores al mensaje: confirmación e integridad del documento (transmisión normal)

Véase el cuadro G.3/T.30.

Cuadro G.3/T.30

Señal	Octetos FIF	Contenido FIF
TK16	1 2 length 3-6 7-18 19-42	0001 0000 0010 1000 RNC2x ESSC2x ESHx
RK17	1 2 length 3-6 7-18 19-22 23-34	0001 0001 0010 0000 RNSR2y ESSR2y RNIMy ESIMy
NOTA 1 – Si el documento no tiene una verificación de integridad, ESHx, RNIMy y ESIMy se ponen a todos ceros. NOTA 2 – La trama TK16 no se proporciona si DCS indica que no hay cifrado. NOTA 3 – La trama RK17 no se proporciona si no se proporciona TK16.		

G.6.2.5 Notas generales

1) Durante el registro, son obligatorias las peticiones de identificación y las respuestas. El mecanismo de petición/respuesta se define en la Recomendación T.36.

2) Durante las llamadas normales, todas las peticiones y respuestas válidas deben tener un número aleatorio no cero. Los números aleatorios puestos a cero en peticiones o respuestas indican que no se admite la autenticación mutua.

3) TK16/RK17 se envían normalmente con PPS-EOP o después, salvo en el caso de interrogación secuencial, cuando se pueden enviar con PPS-EOM o después.

4) El troceado y la encripción son determinados por el primer intercambio de DIS/DCS y se aplican a cada documento transmitido en esa sesión.

G.7 Diagramas de flujo

G.7.1 Funcionamiento por la red telefónica pública conmutada que utiliza los sistemas de modulación V.27 *ter*, V.29, V.17 y V.34 (modo semidúplex)

Los diagramas de flujo de la figura G.7-1/T.30 muestran la fase B, los procedimientos previos al mensaje, la fase C, el procedimiento durante la transmisión del mensaje, la fase D, el procedimiento posterior al mensaje y la fase E, liberación de la llamada, para los terminales transmisor y receptor.

Se debe hacer referencia también a los procedimientos definidos en la Recomendación T.36.

G.7.2 Reglas de los diagramas de flujo

Los diagramas de flujo siguen dos reglas simples:

1) Todas las líneas tienen una flecha en el destino solamente.

2) Las líneas no se cruzan.

G.7.3 Temporizadores utilizados en los diagramas de flujo

T1	35 s ± 5 s
T2	6 s ± 1 s
T3	10 s ± 5 s
T4	4,5 s ± 15% para unidades manuales
T4	3,0 s ± 15% para unidades automáticas
T5	60 s ± 5 s

G.7.4 Abreviaturas y descripciones utilizadas en los diagramas de flujo

A menos que se defina otra cosa, la definición de los términos de los diagramas de flujo es la indicada en el texto principal y/o en el anexo A/T.30.

Authen reqd? Comprobación para ver si se requiere autenticación mutua al principio de la transmisión.

NOTA 1 – Una vez que se ha completado la autenticación mutua, dentro de la misma sesión se ha de seguir siempre la salida "No".

Reg mode? Comprobación para ver si se requiere registro de seguridad.

First page? Comprobación para ver si se requiere autenticación mutua al principio de la transmisión.

NOTA 2 – Una vez que se ha completado la autenticación mutua, dentro de la misma sesión se ha de seguir siempre la salida "No".

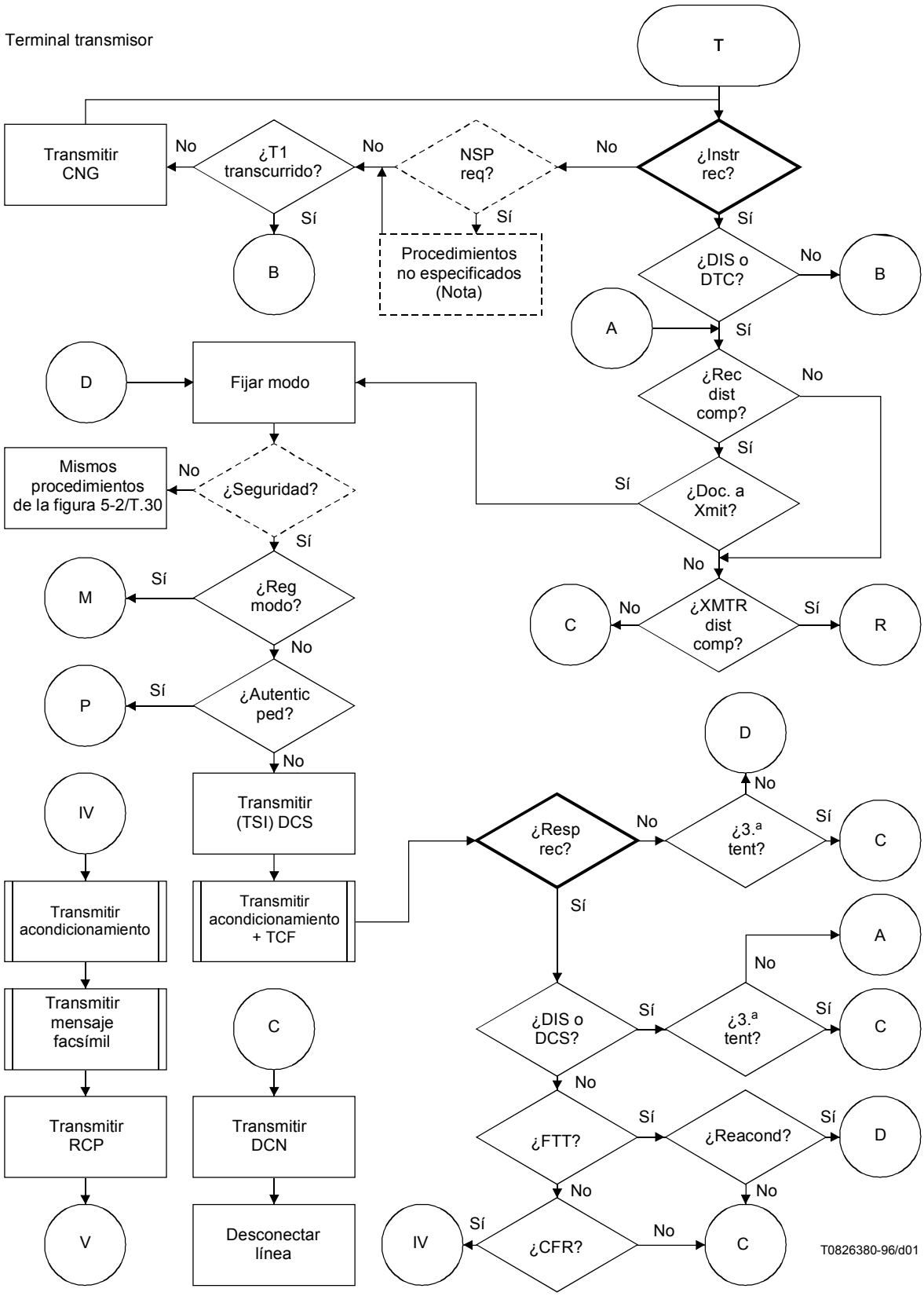
G.8 Diagramas de flujo

G.8.1 Funcionamiento por la red telefónica pública conmutada que utiliza el sistema de modulación V.34 (modo dúplex) y por la red digital de servicios integrados

El funcionamiento para transmitir documentos facsímil seguros por la red telefónica pública conmutada que utiliza el sistema de modulación V.34 (dúplex) y por la RDSI es exactamente como se define en el anexo C/T.30, con las excepciones mostradas en los siguientes diagramas de flujo.

Los diagramas de flujo de la figura G.8/T.30 muestran la fase B, los procedimientos previos al mensaje, la fase D, el procedimiento posterior al mensaje y la fase E, liberación de la llamada, para los terminales transmisor y receptor.

Se debe hacer referencia también a los procedimientos definidos en la Recomendación T.36.



NOTA – El procedimiento no especificado (NSP) designa un procedimiento que tarda tres segundos o menos en completarse. Puede no ser necesariamente una secuencia de señales definible.

Figura G.7-1/T.30 (hoja 1 de 20)

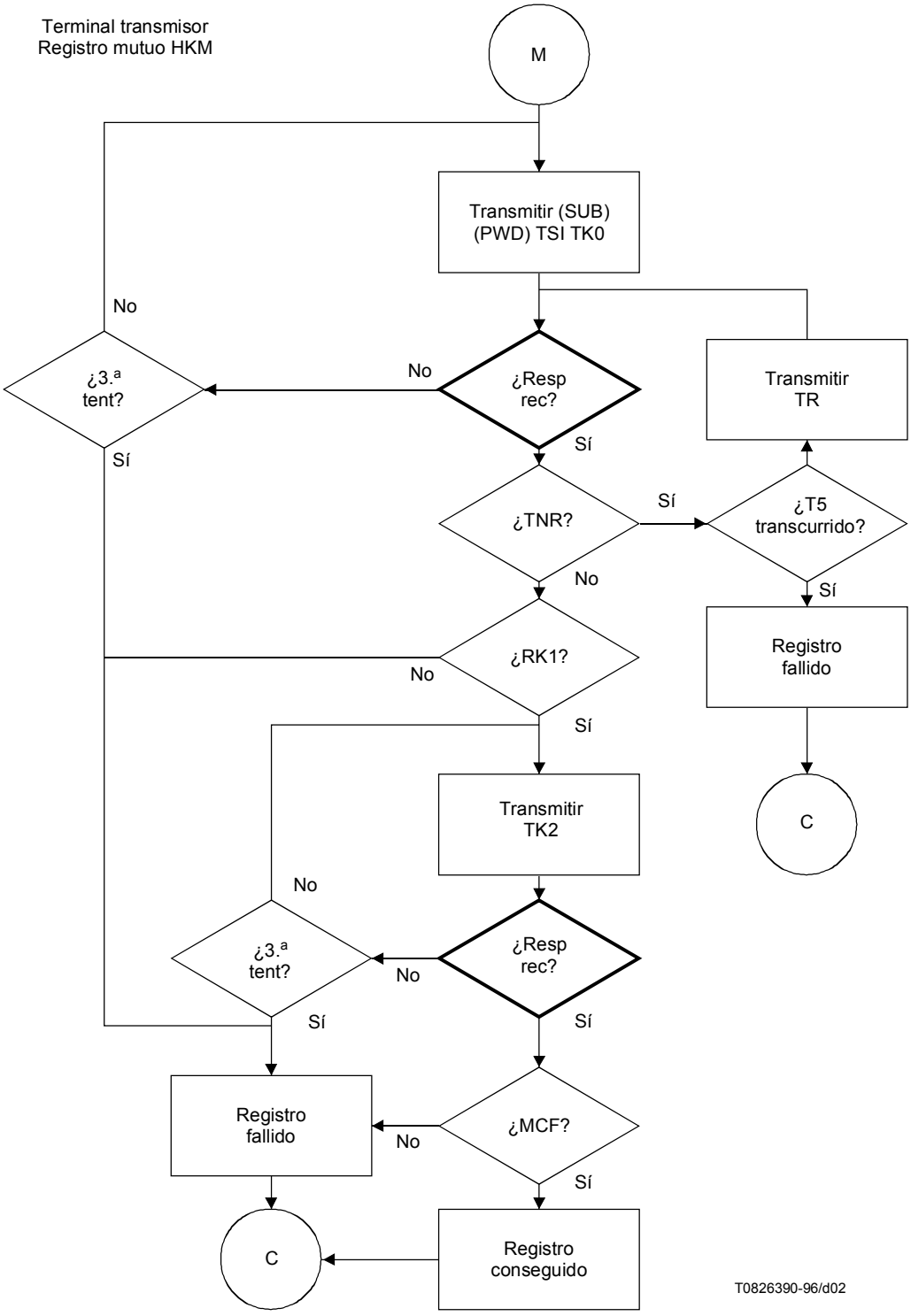


Figura G.7-1/T.30 (hoja 2 de 20)

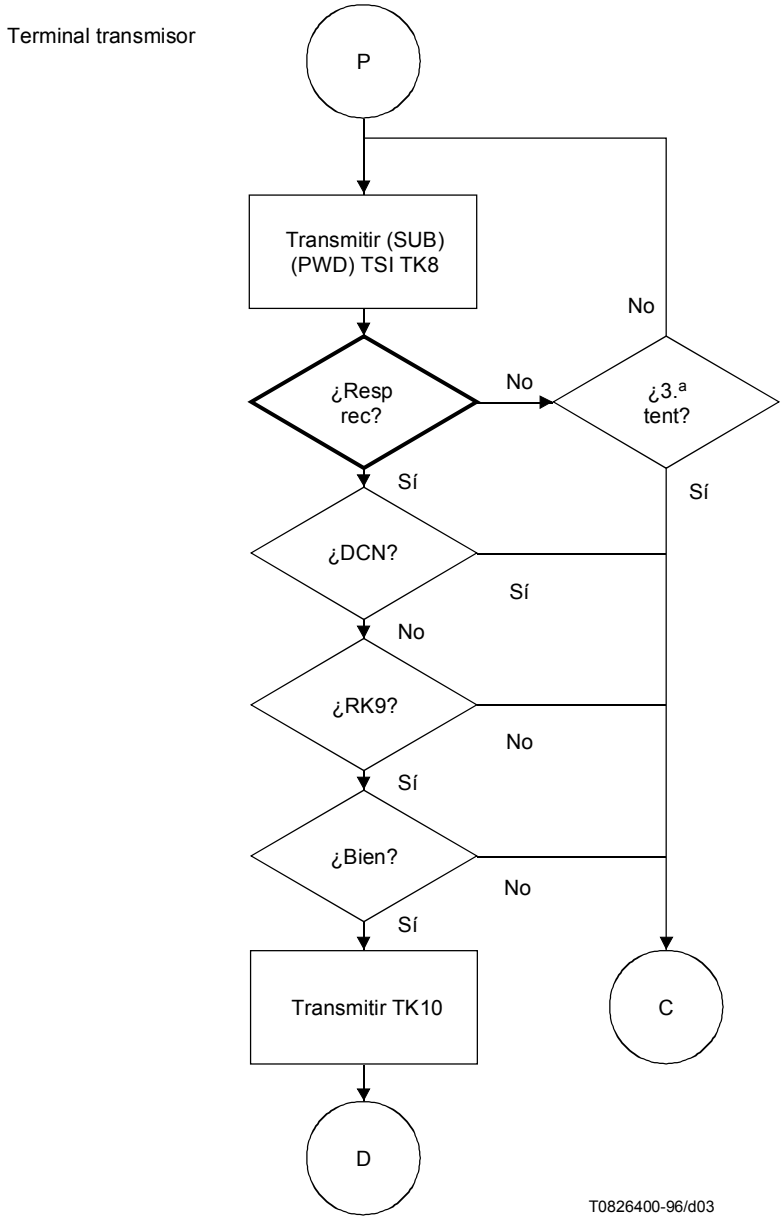


Figura G.7-1/T.30 (hoja 3 de 20)

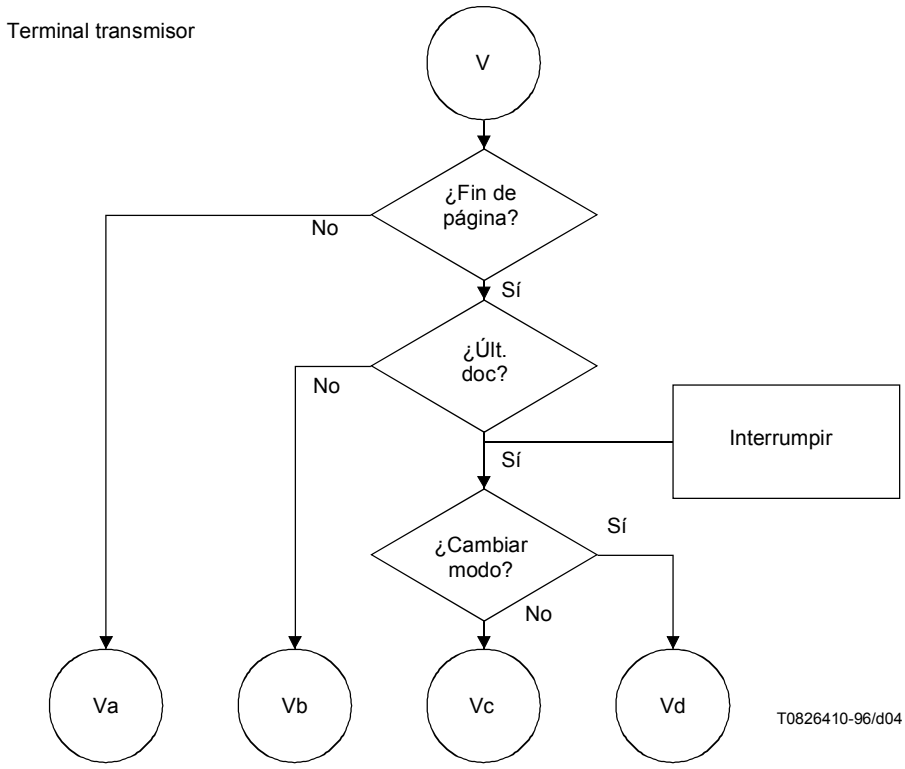


Figura G.7-1/T.30 (hoja 4 de 20)

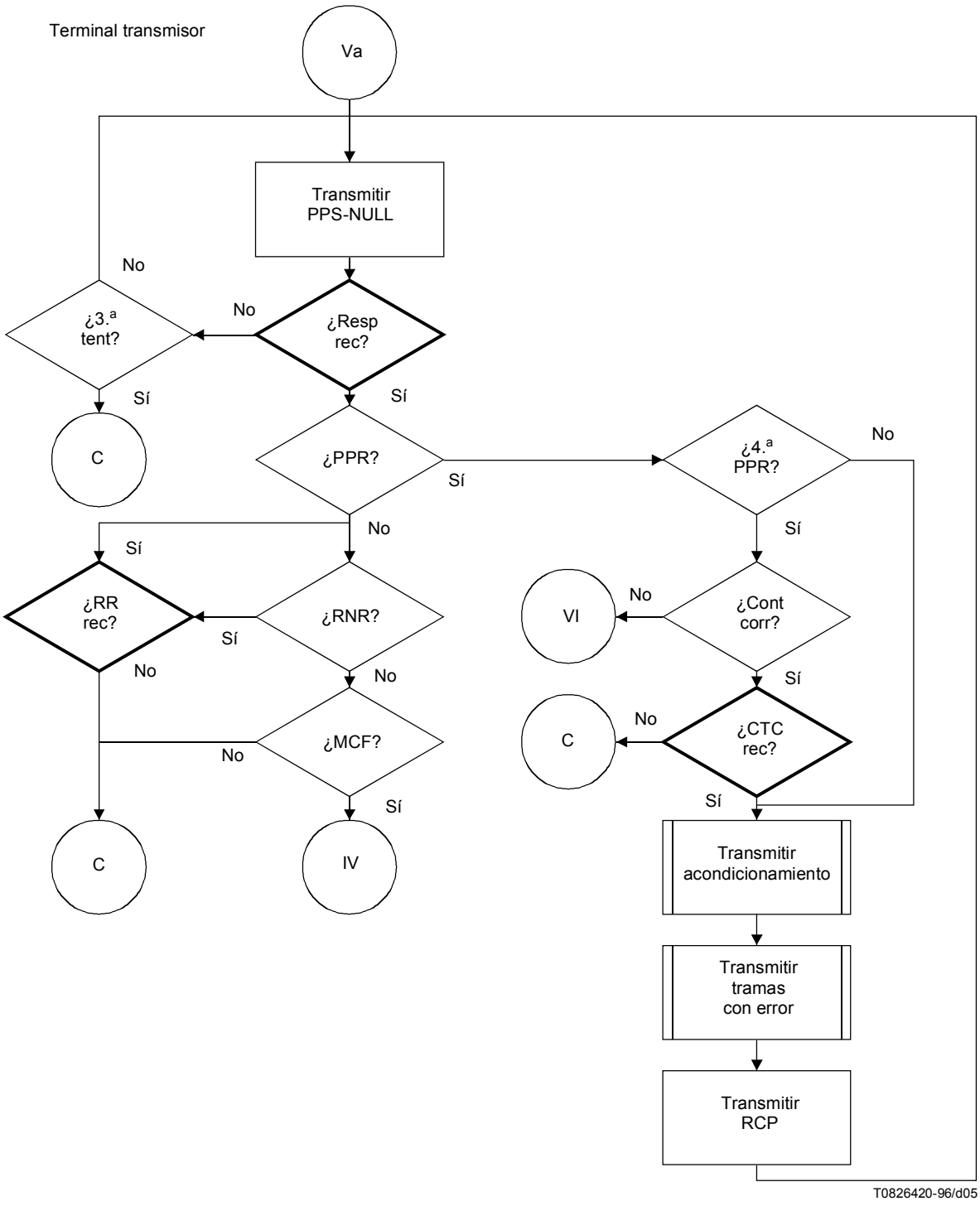


Figura G.7-1/T.30 (hoja 5 de 20)

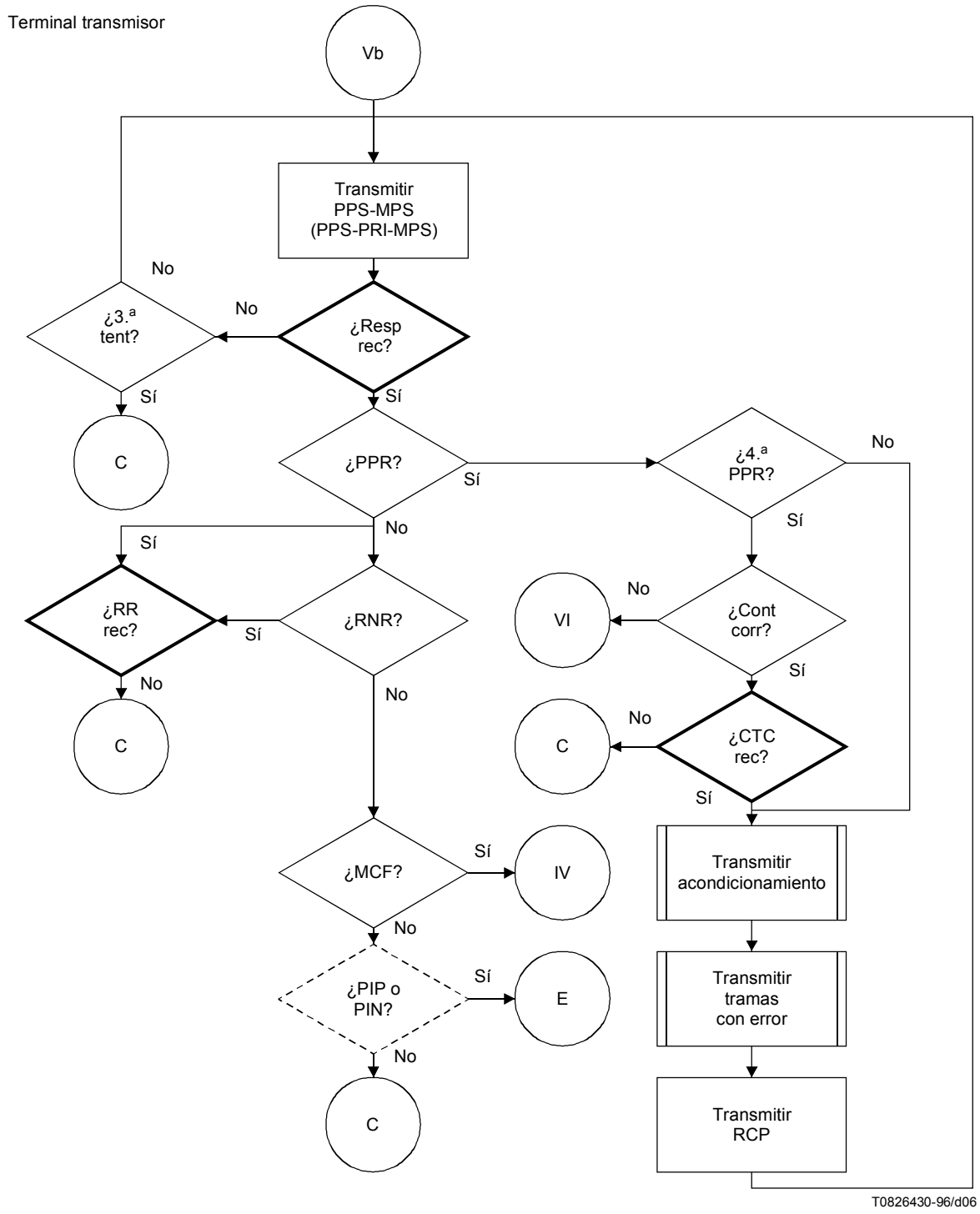


Figura G.7-1/T.30 (hoja 6 de 20)

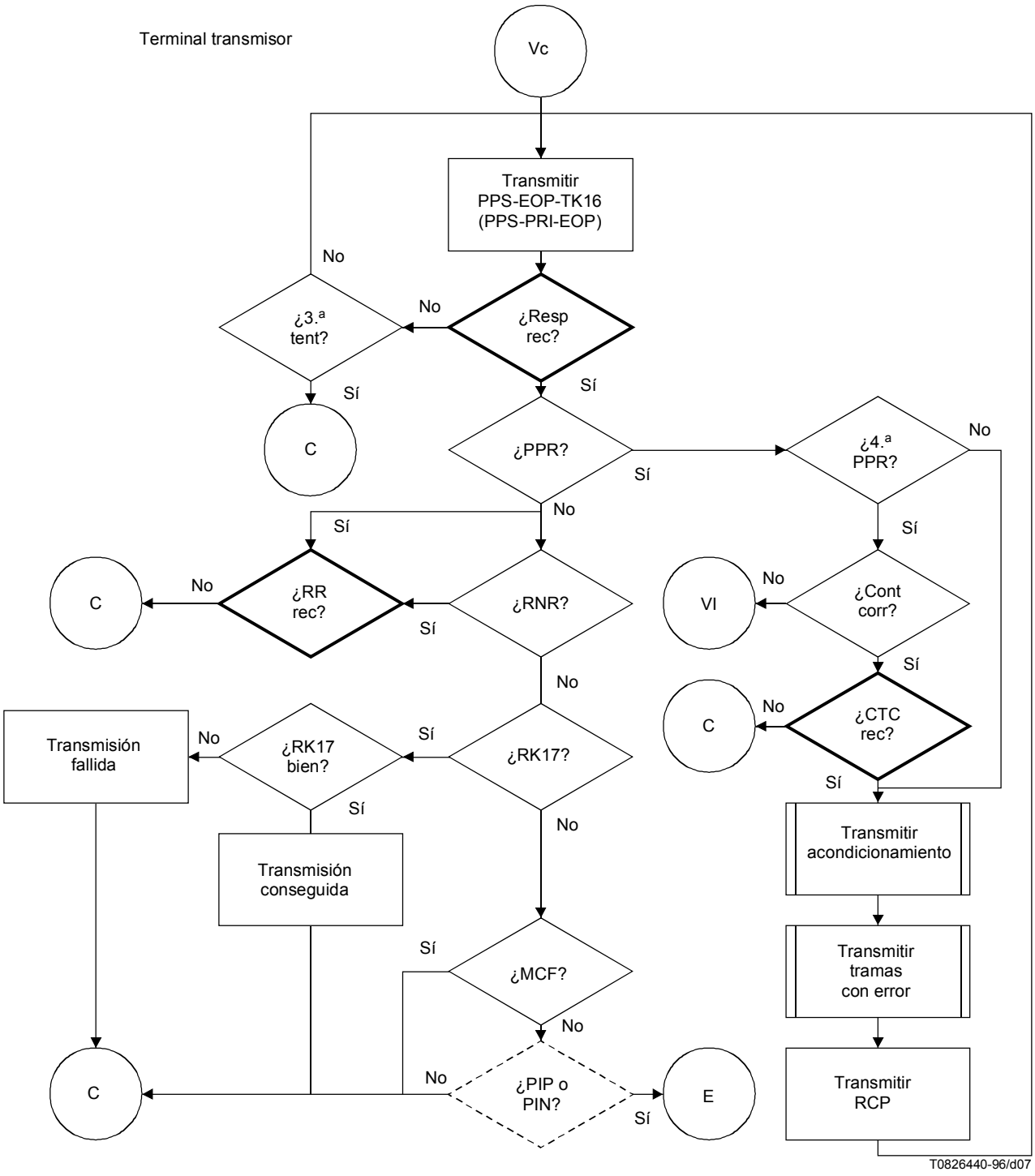


Figura G.7-1/T.30 (hoja 7 de 20)

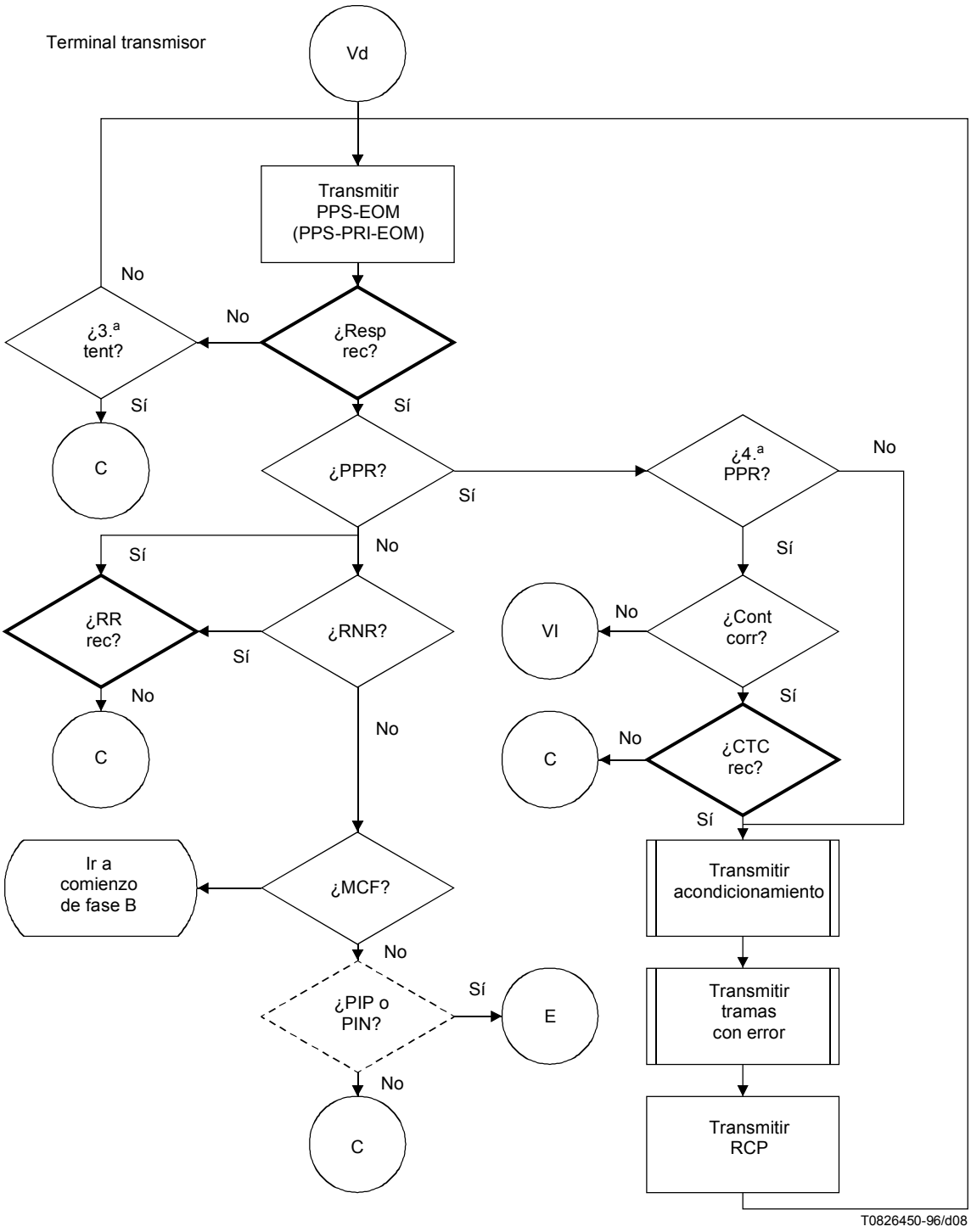


Figura G.7-1/T.30 (hoja 8 de 20)

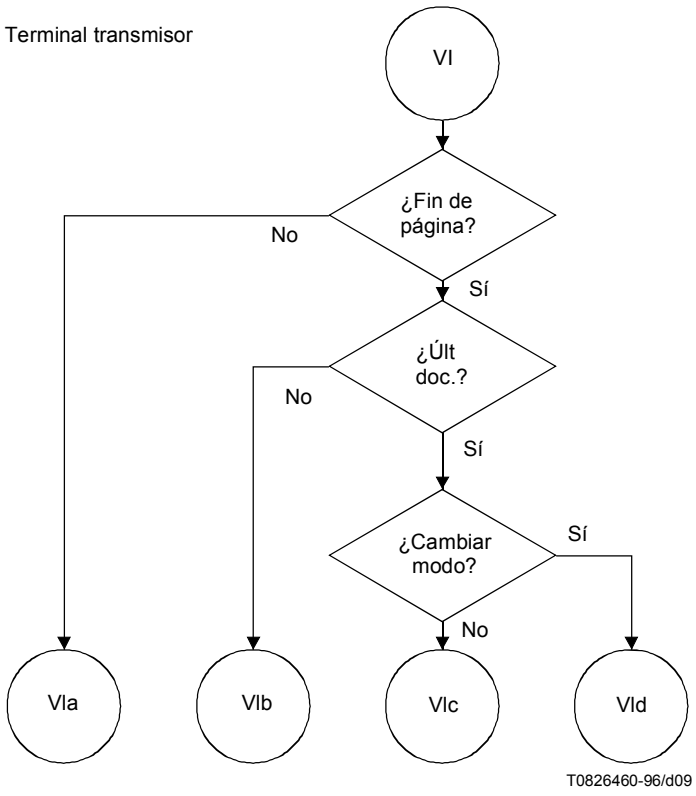


Figura G.7-1/T.30 (hoja 9 de 20)

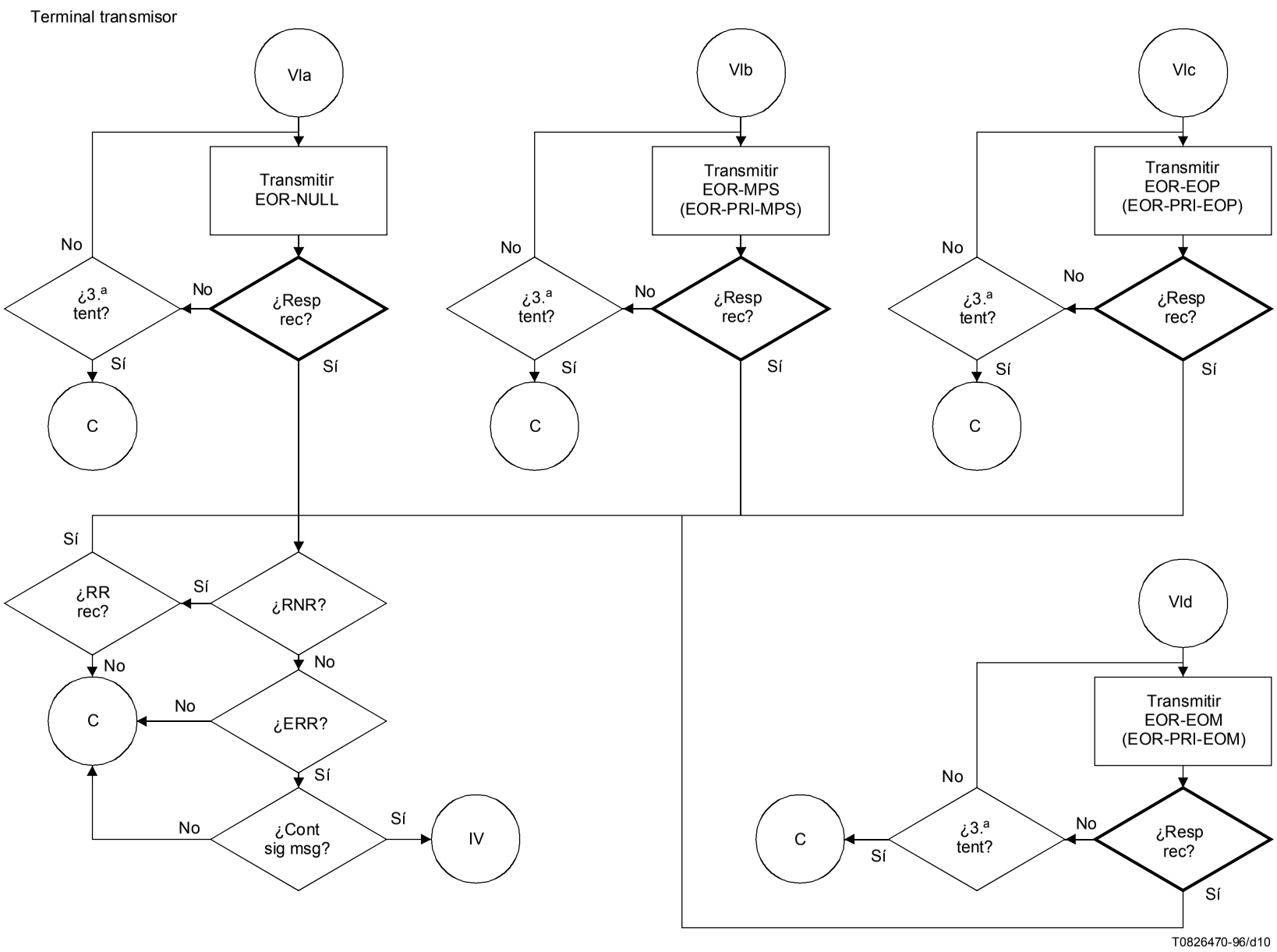


Figura G.7-1/T.30 (hoja 10 de 20)

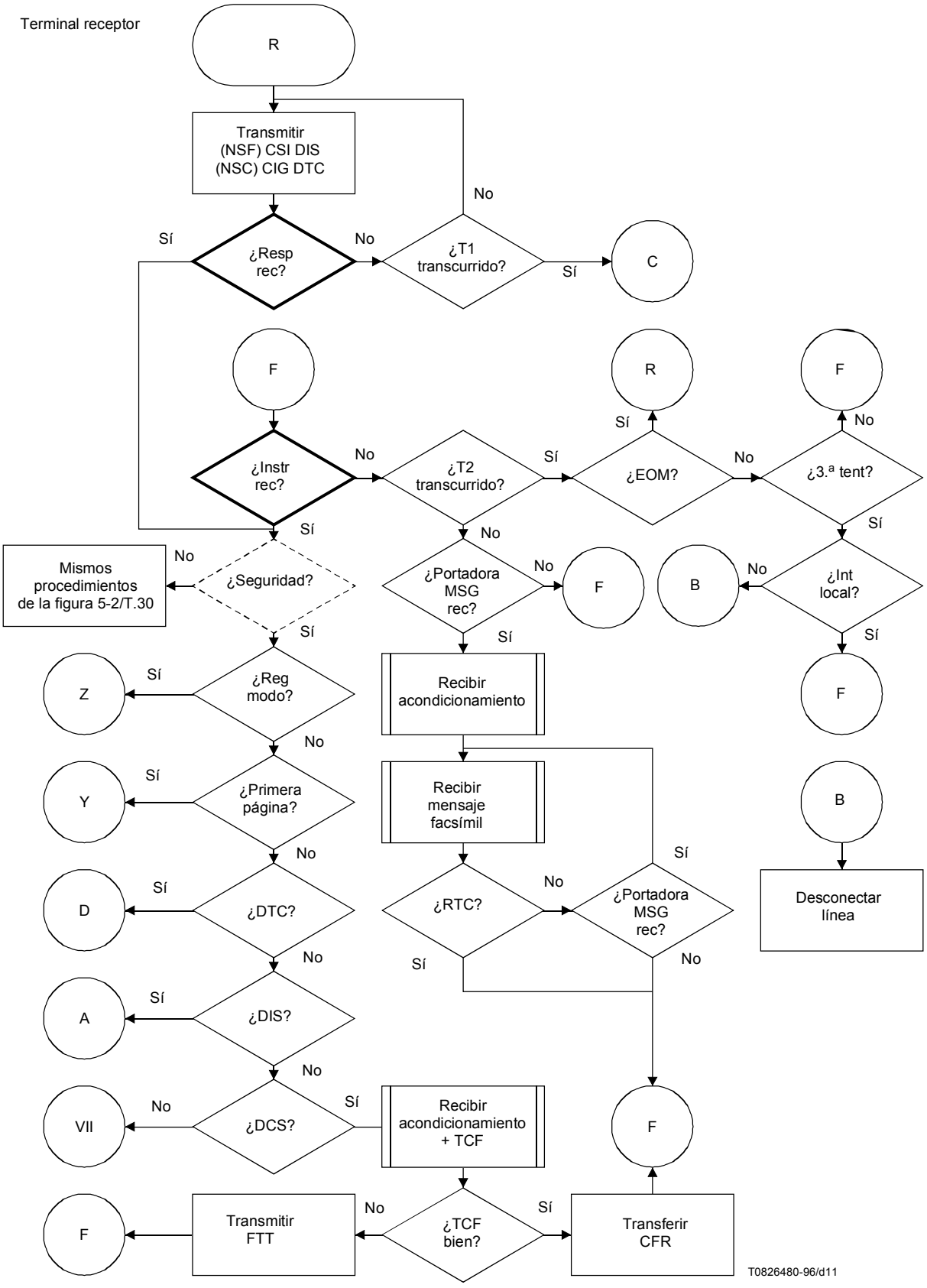


Figura G.7-1/T.30 (hoja 11 de 20)

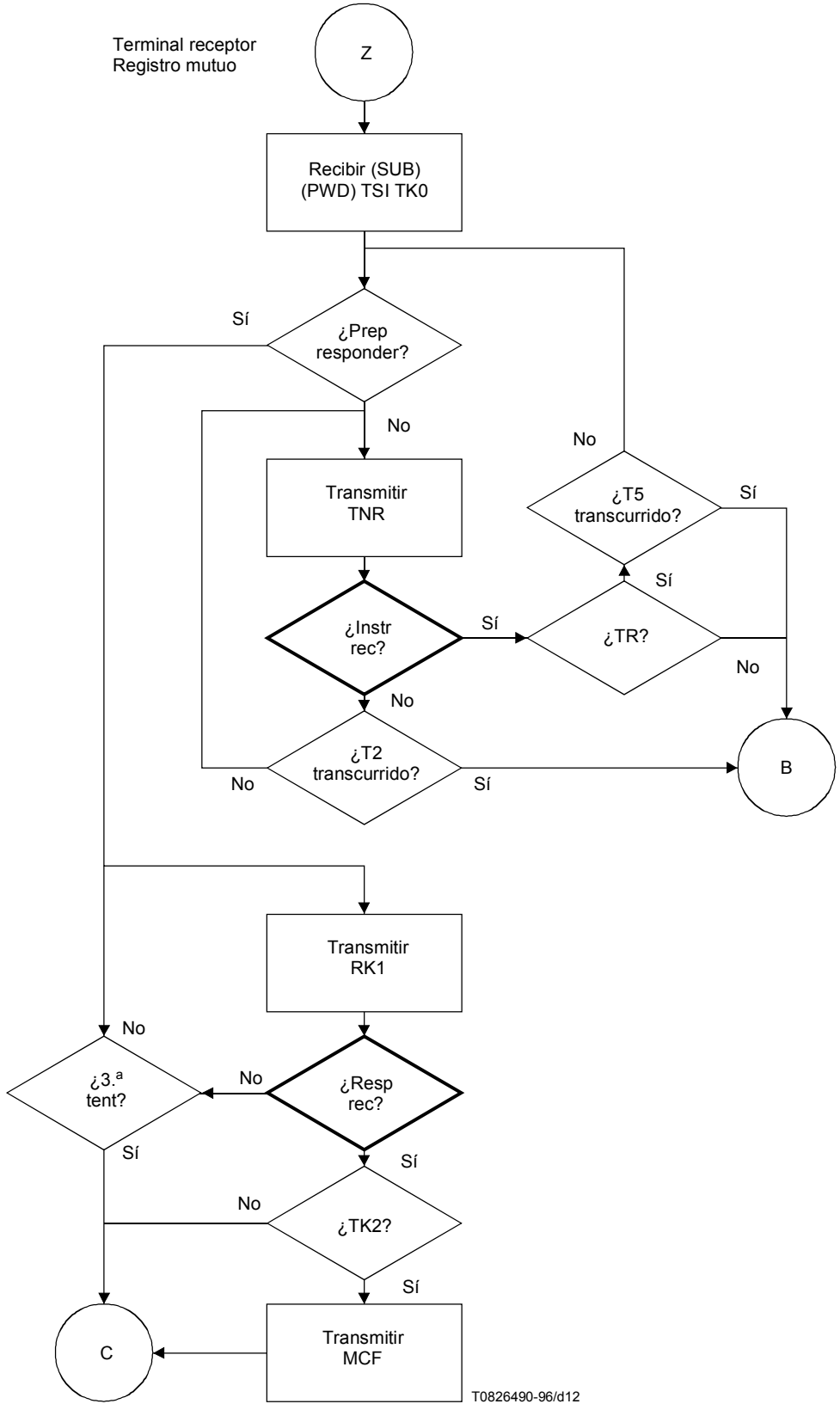


Figura G.7-1/T.30 (hoja 12 de 20)

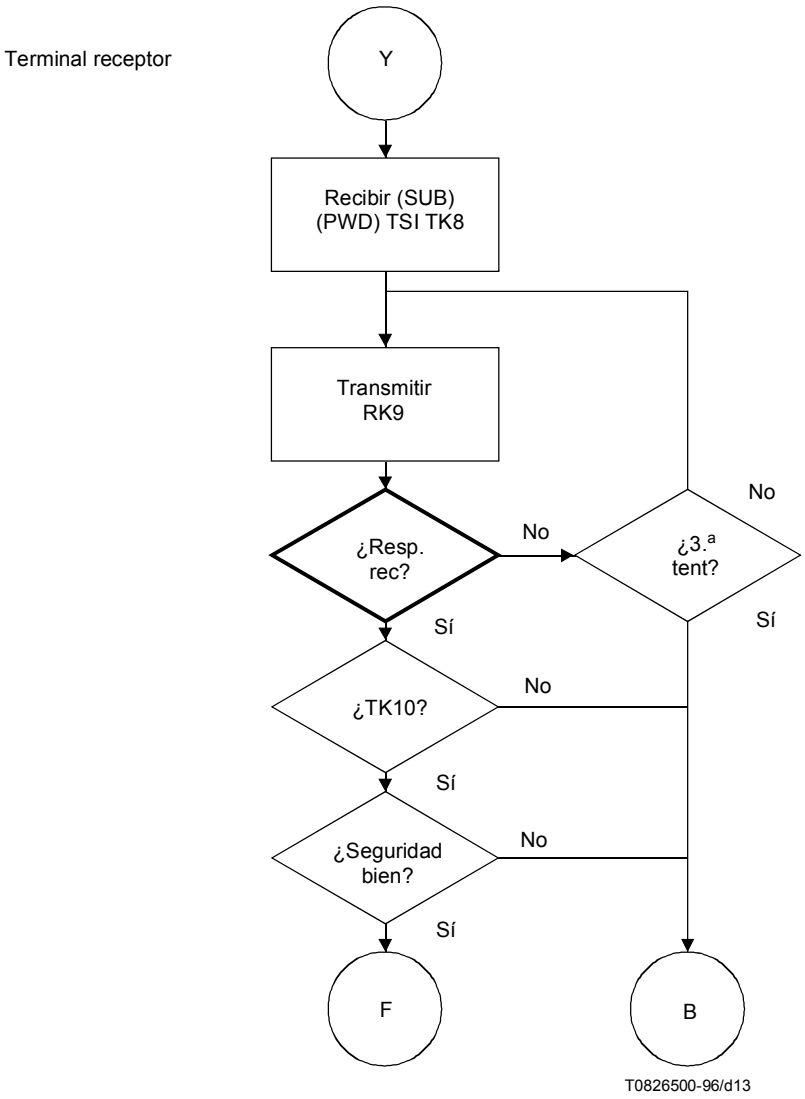


Figura G.7-1/T.30 (hoja 13 de 20)

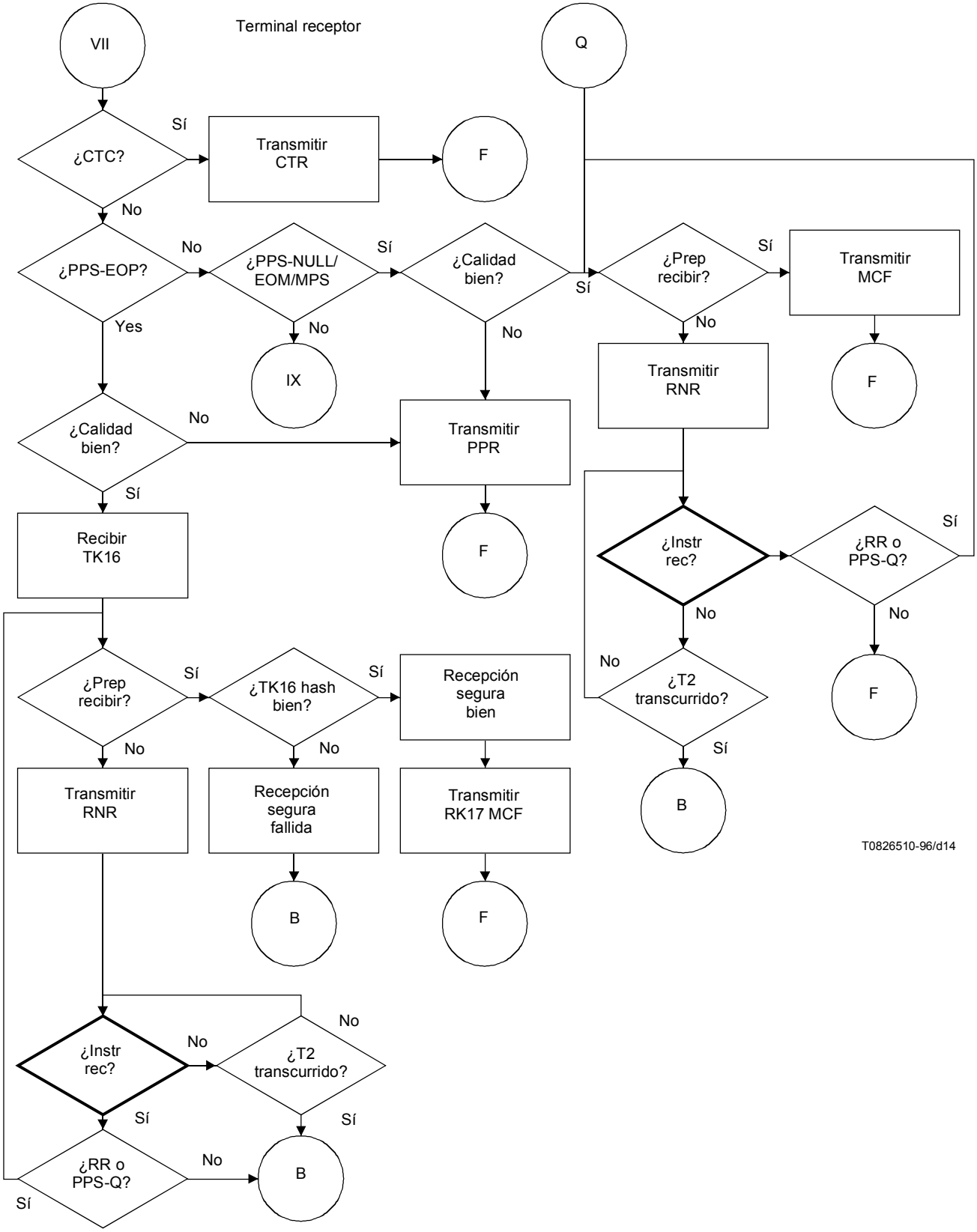


Figura G.7-1/T.30 (hoja 14 de 20)

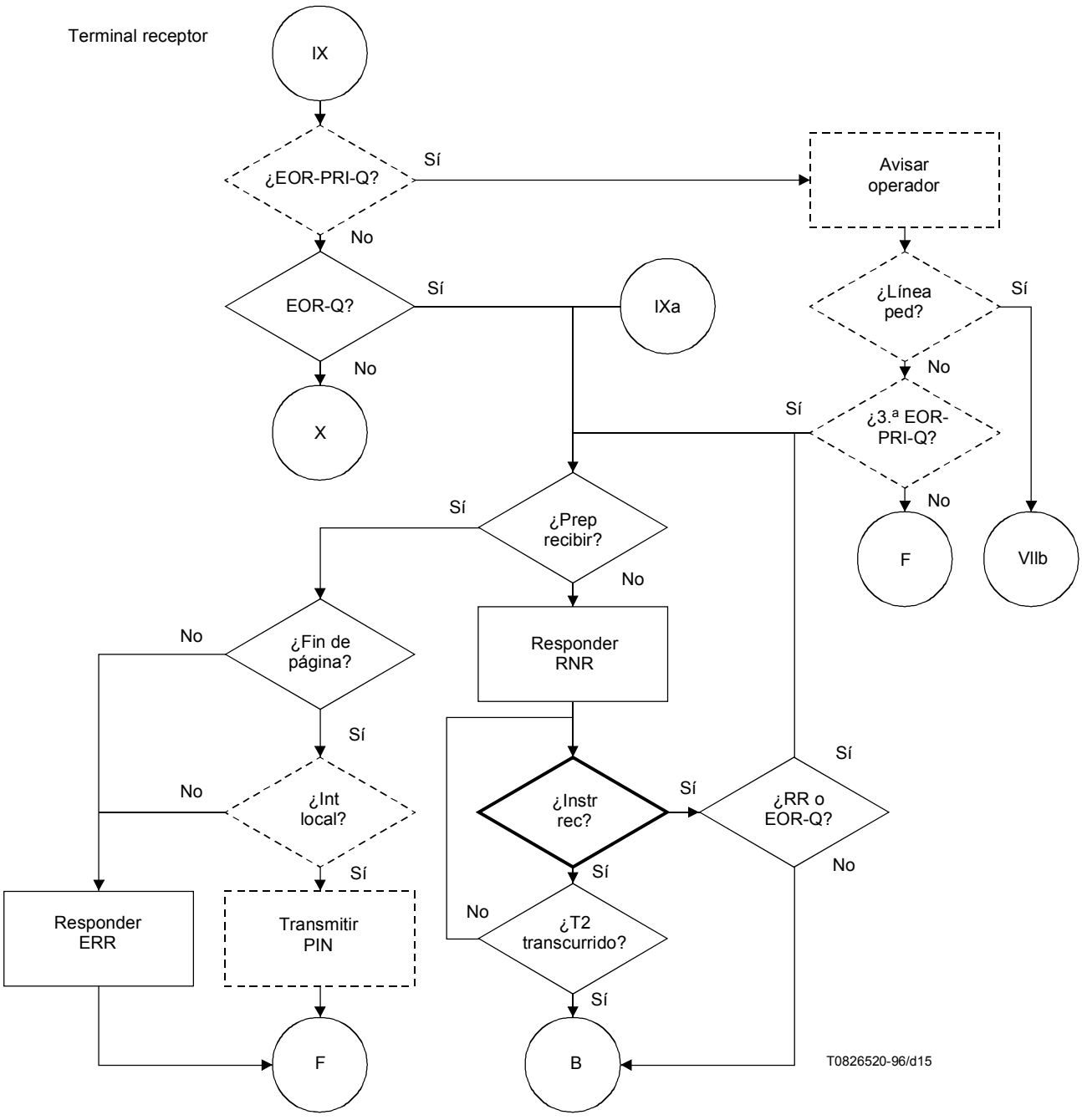


Figura G.7-1/T.30 (hoja 15 de 20)

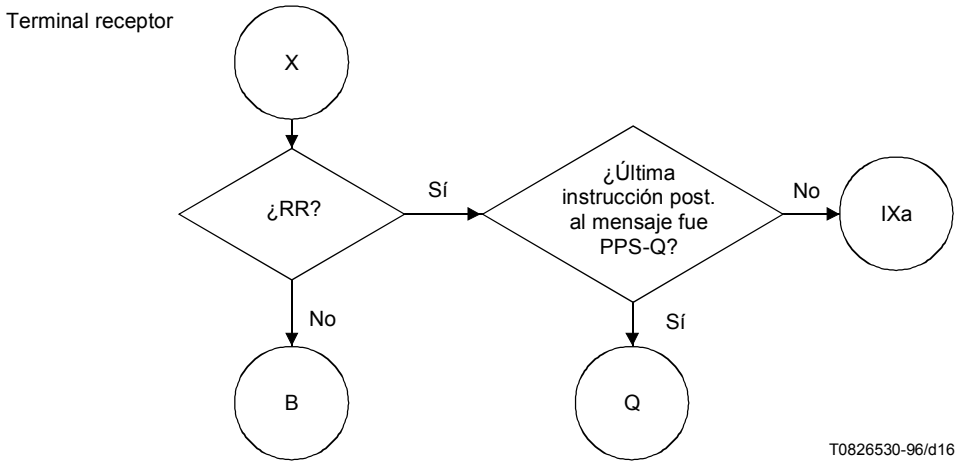


Figura G.7-1/T.30 (hoja 16 de 20)

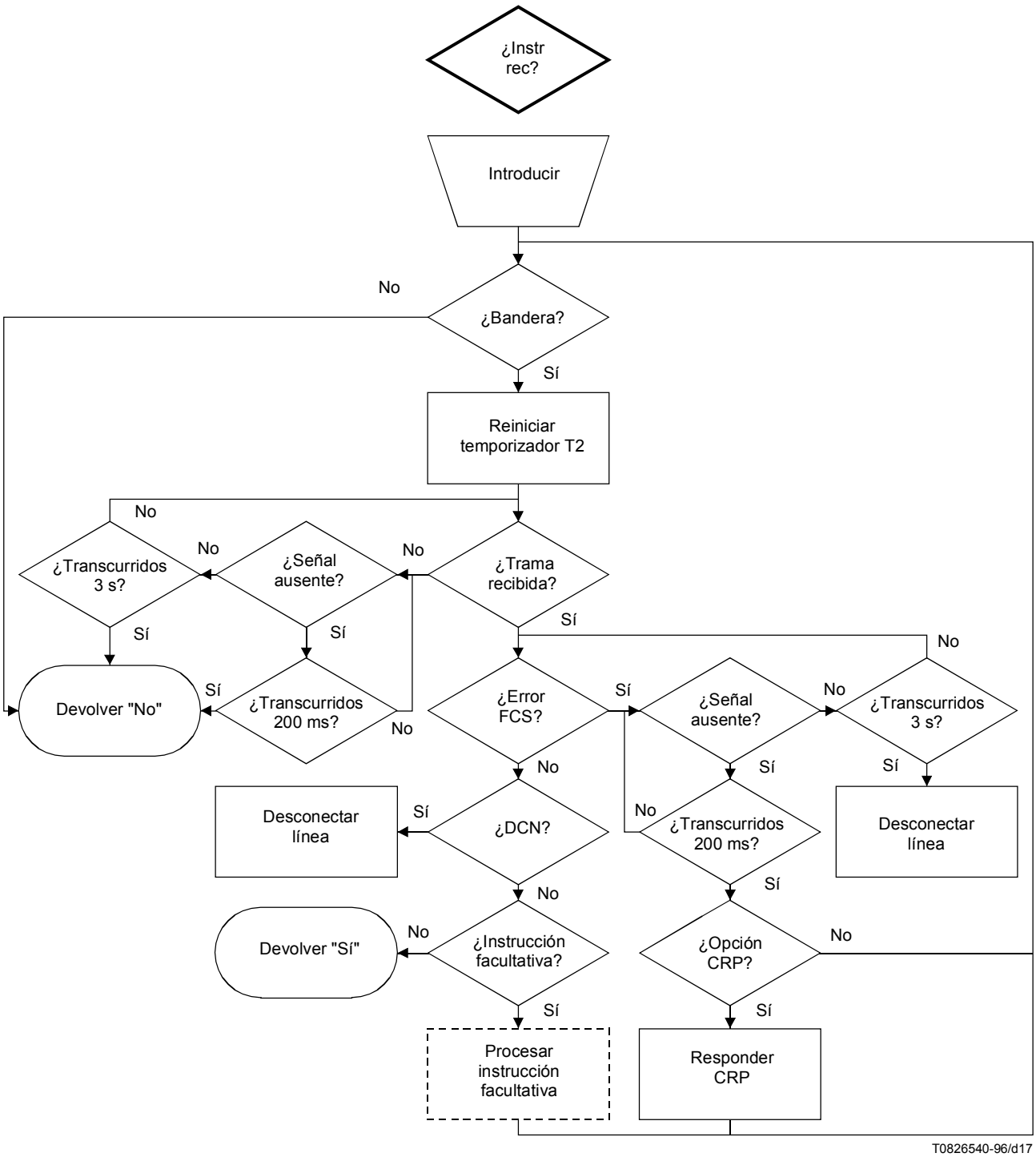


Figura G.7-1/T.30 (hoja 17 de 20)

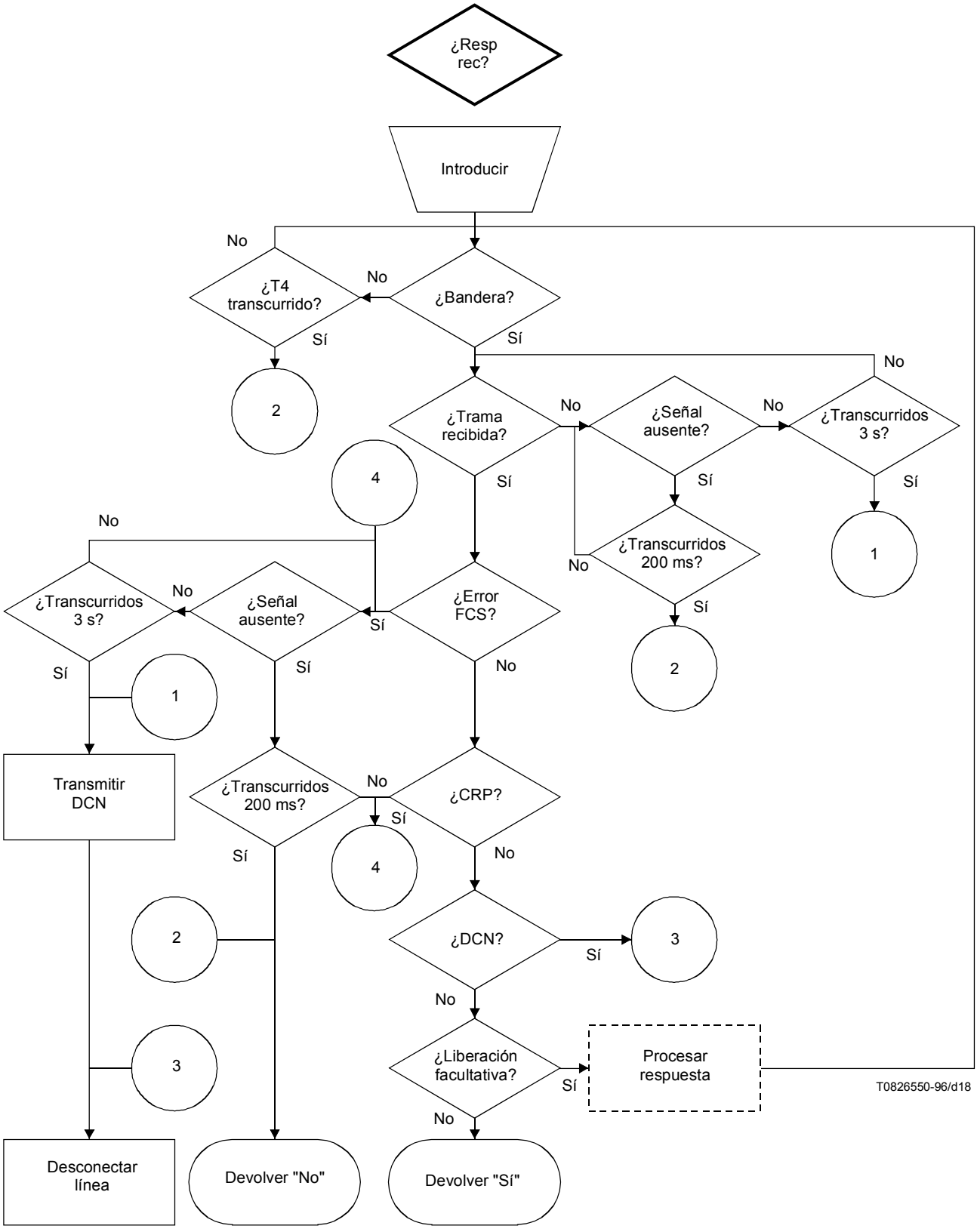


Figura G.7-1/T.30 (hoja 18 de 20)

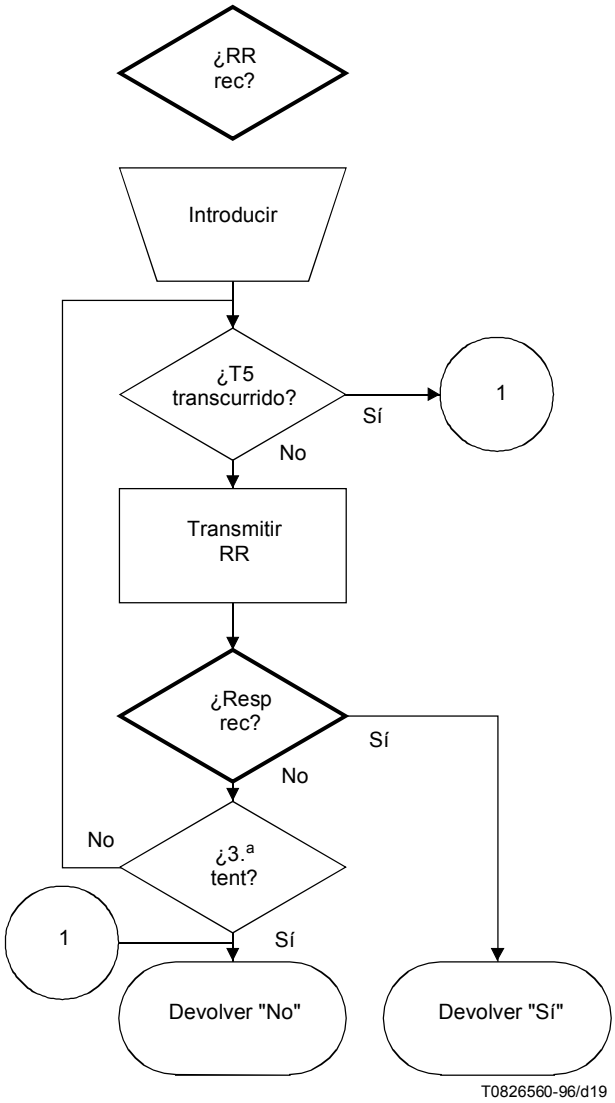


Figura G.7-1/T.30 (hoja 19 de 20)

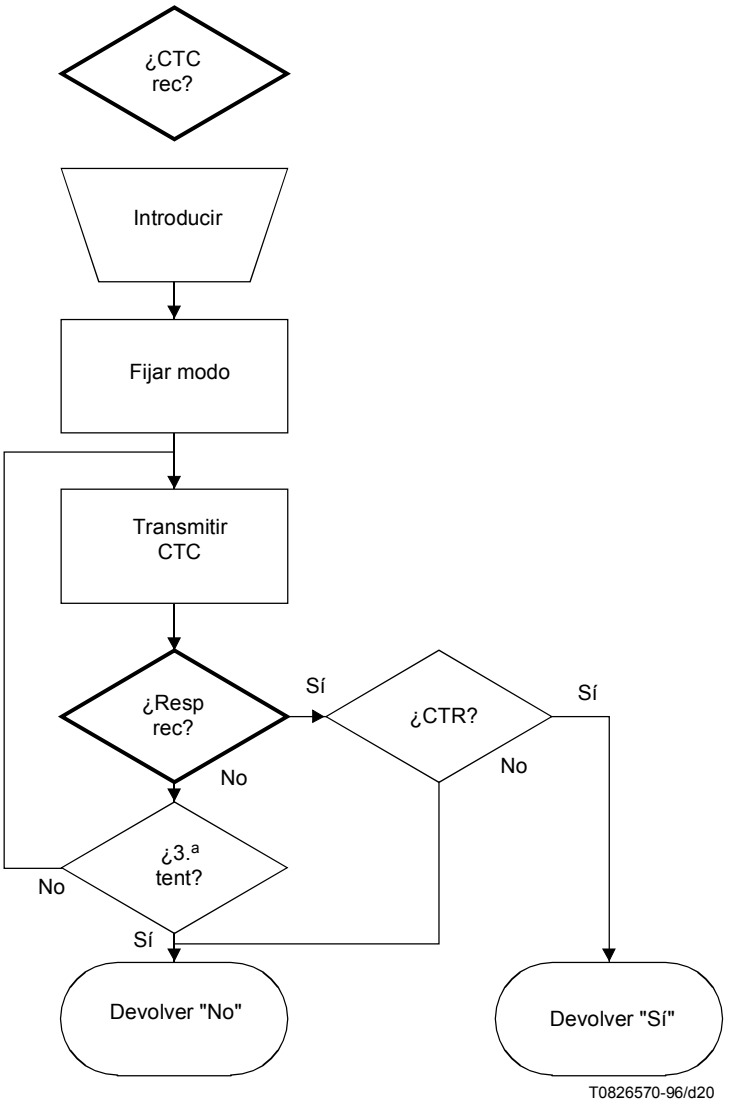


Figura G.7-1/T.30 (hoja 20 de 20)

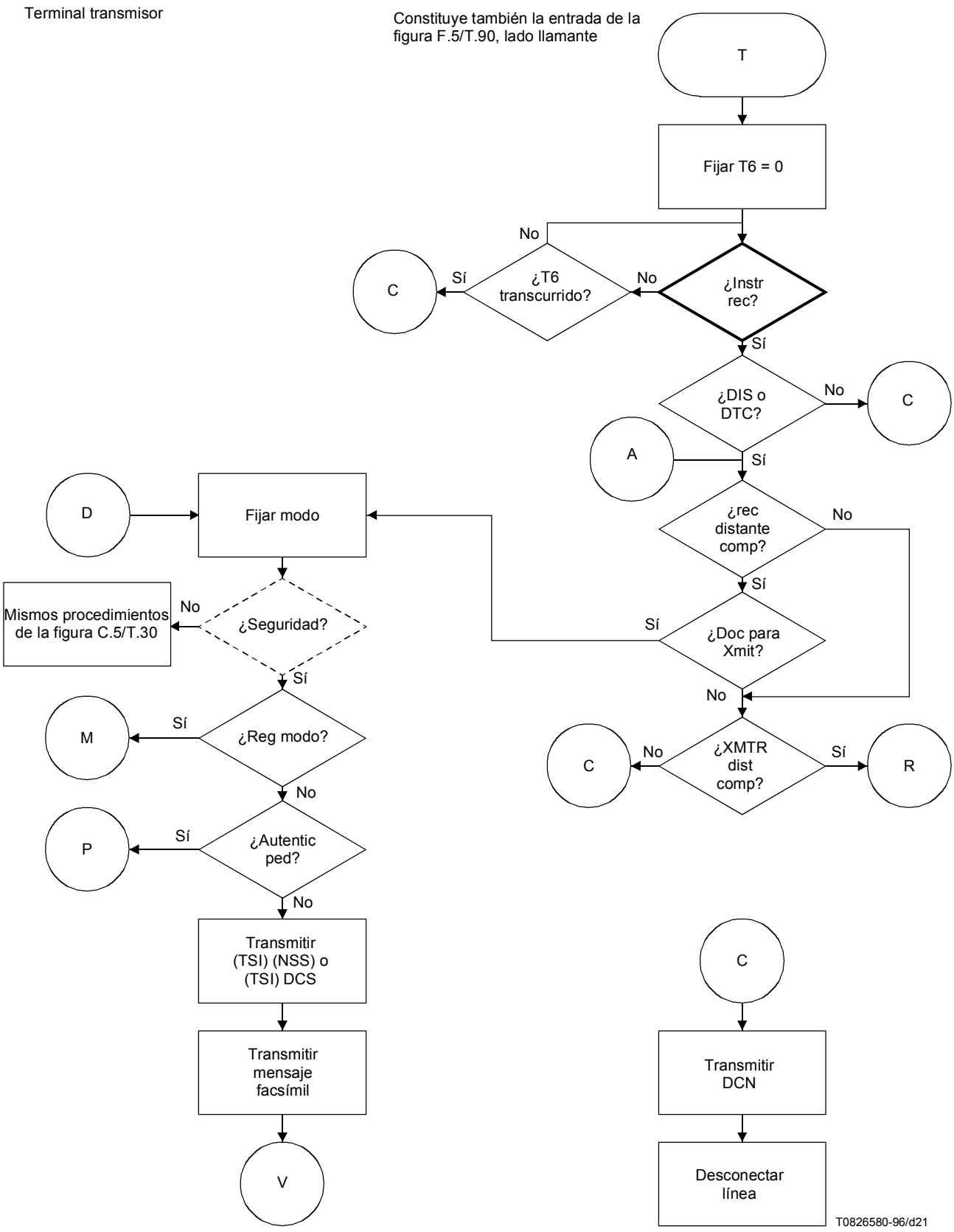


Figura G.8-1/T.30 (hoja 1 de 3) (Utilizada en lugar de la figura C.5/T.30) Dúplex

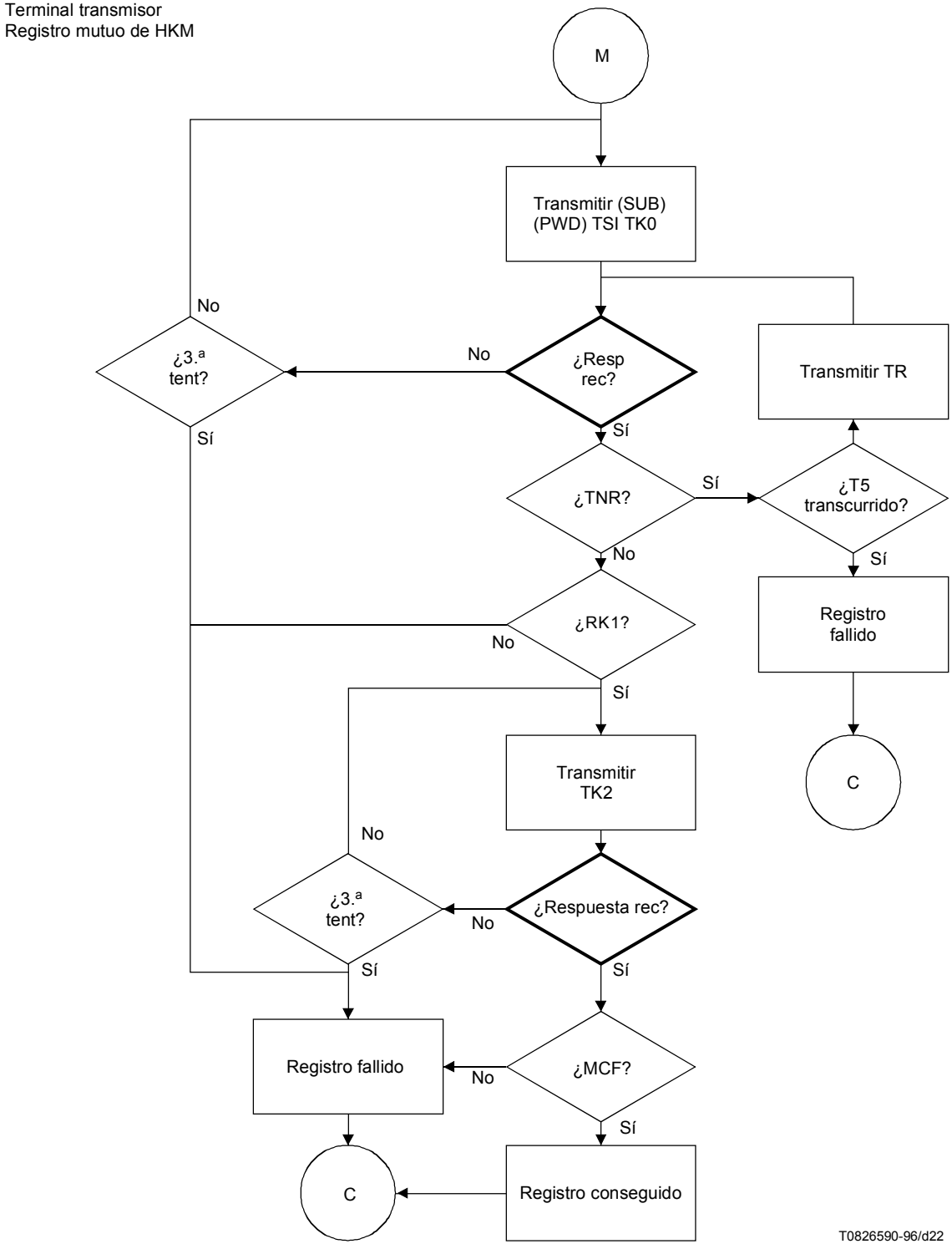


Figura G.8-1/T.30 (hoja 2 de 3) (Utilizada en lugar de la figura C.5/T.30) Dúplex

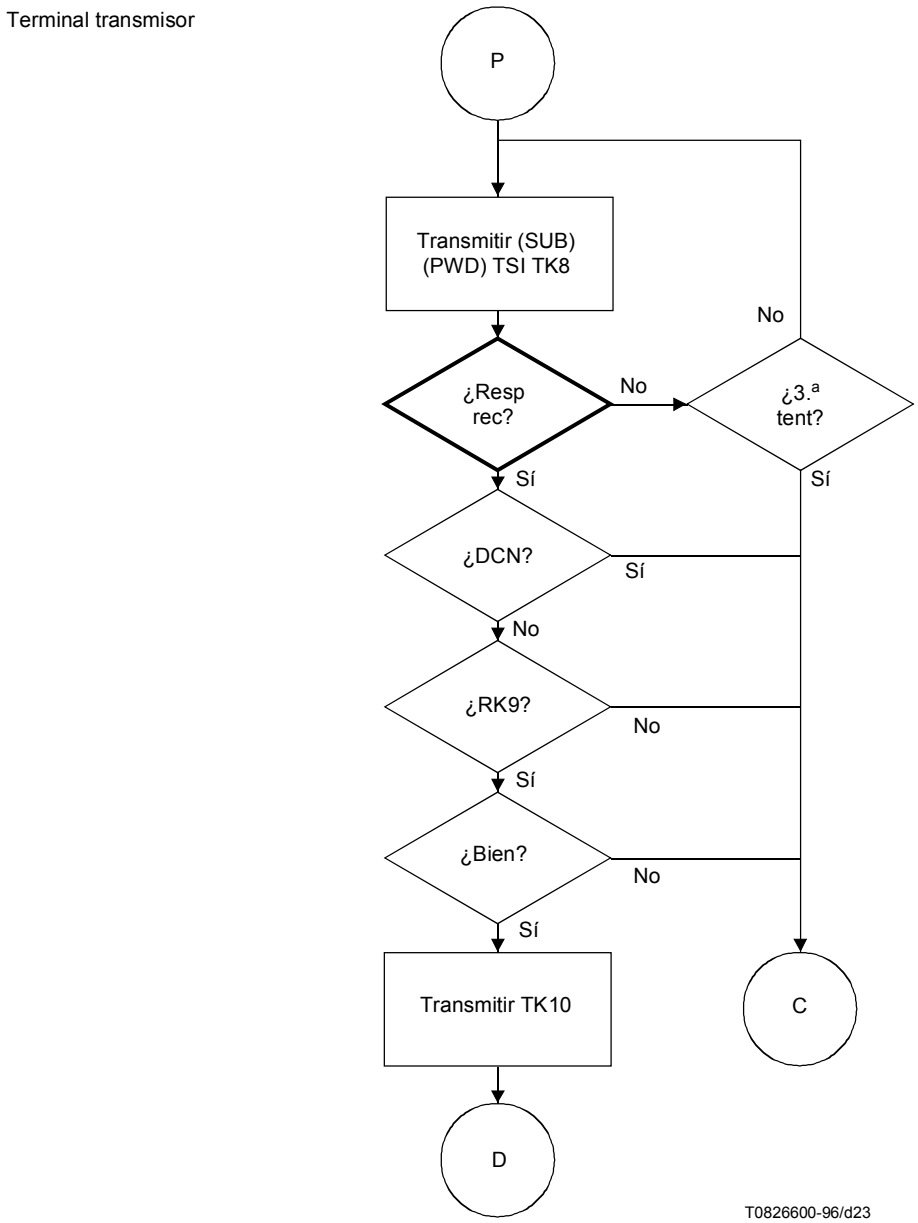


Figura G.8-1/T.30 (hoja 3 de 3) (Utilizada en lugar de la figura C.5/T.30) Dúplex

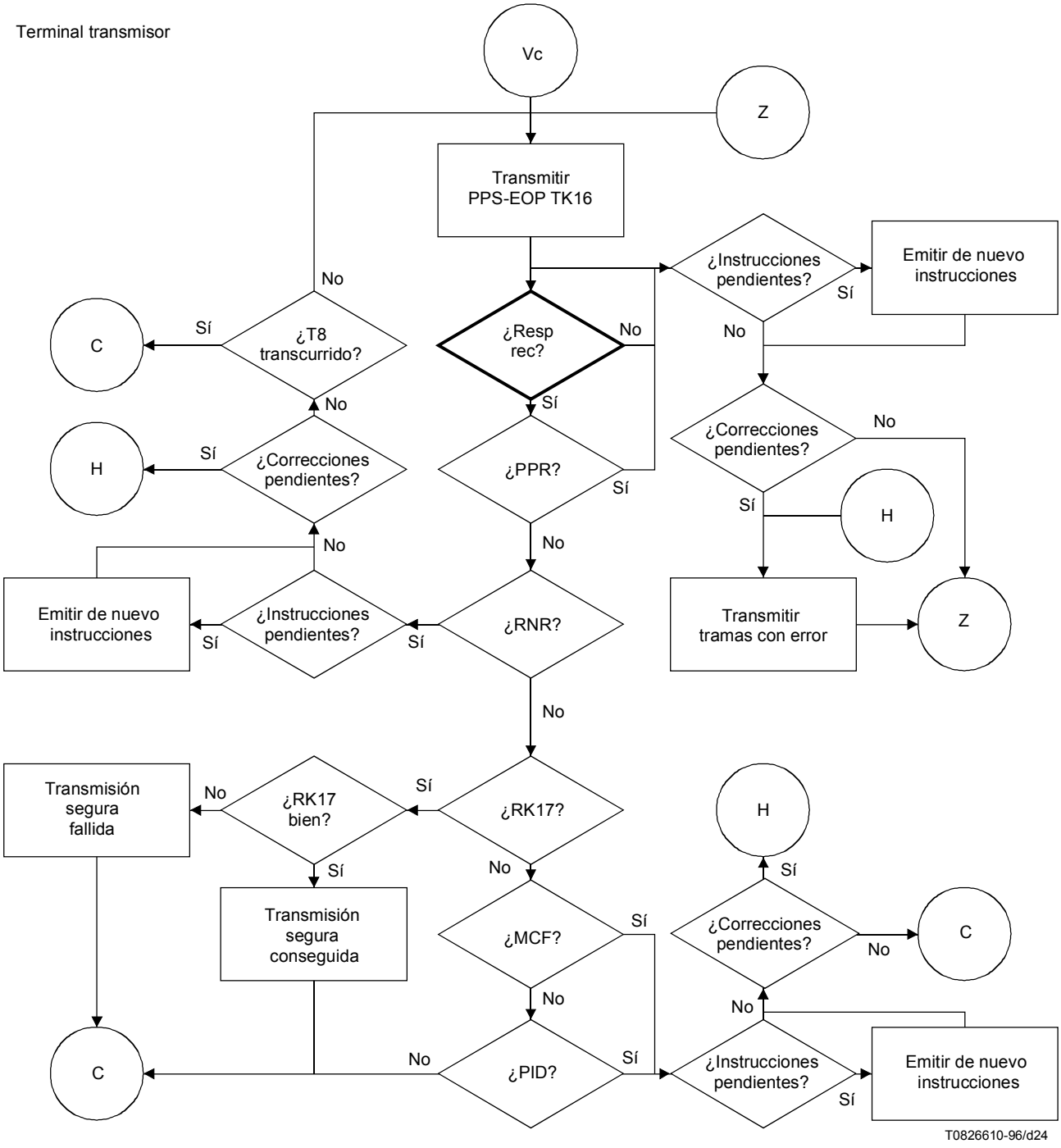


Figura G.8-2/T.30 (Utilizada en lugar de la figura C.9/T.30) Dúplex

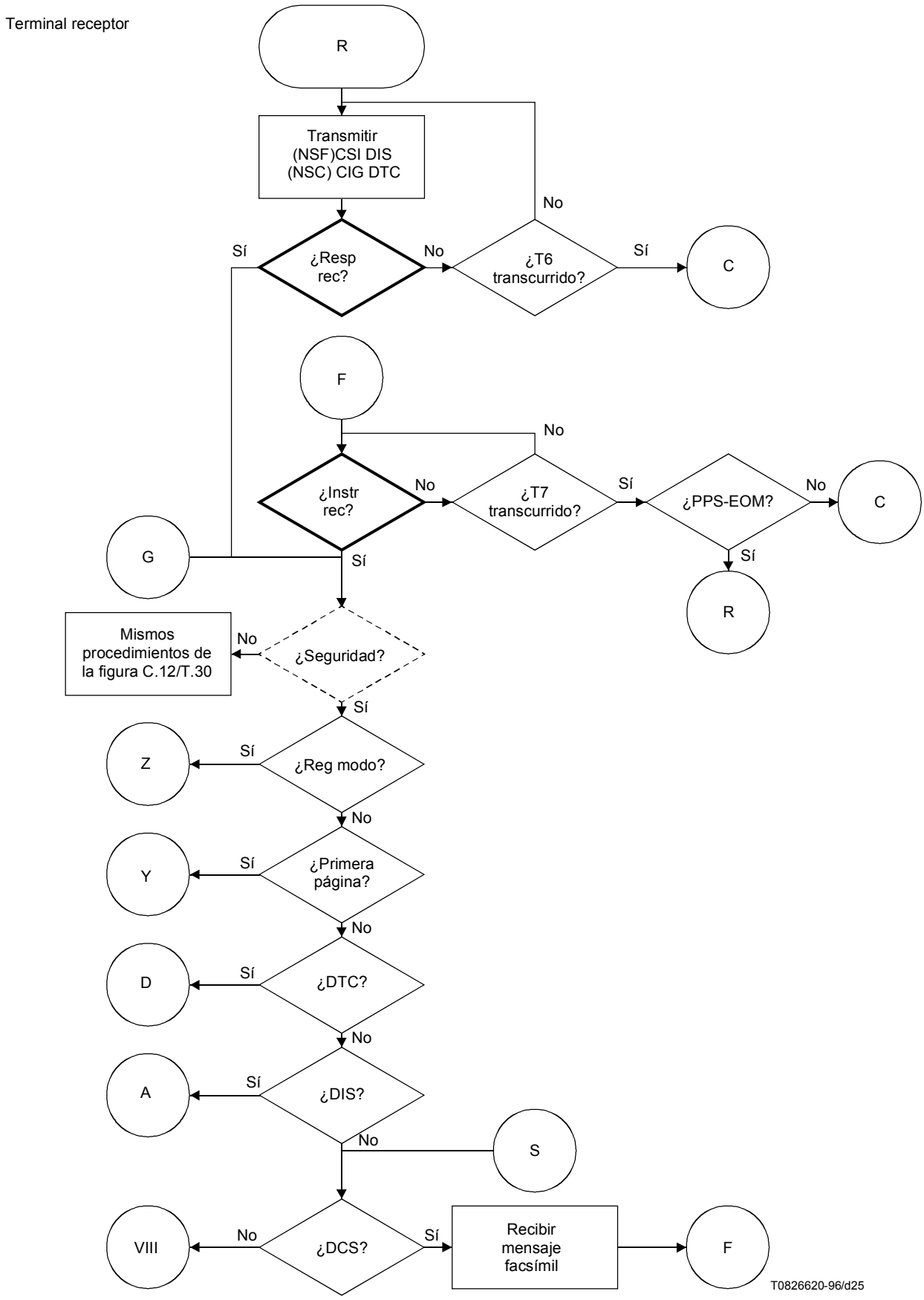


Figura G.8-3/T.30 (hoja 1 de 3) (Utilizada en lugar de la figura C.12/T.30) Dúplex

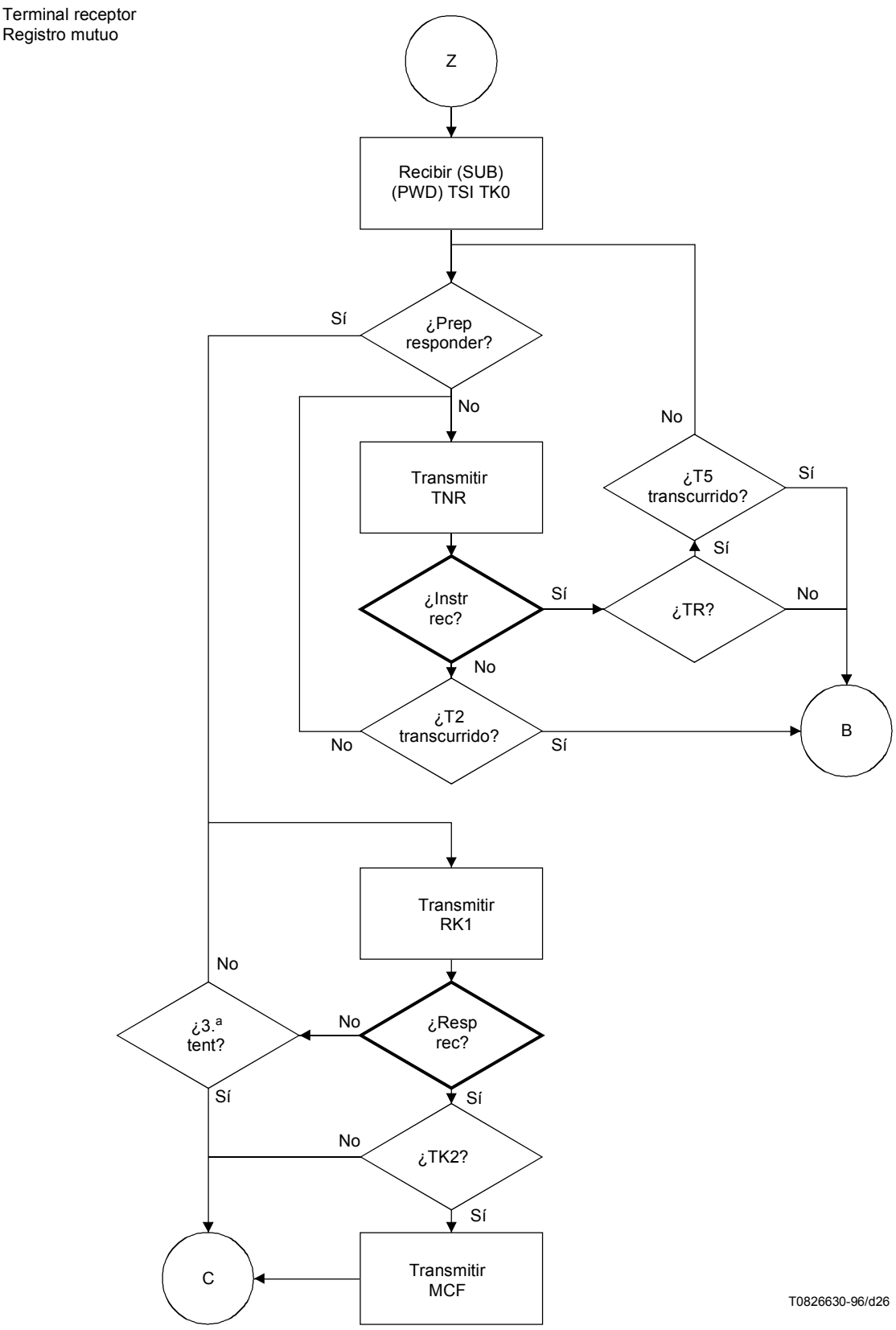


Figura G.8-3/T.30 (hoja 2 de 3) (Utilizada en lugar de la figura C.12/T.30) Dúplex

Terminal receptor

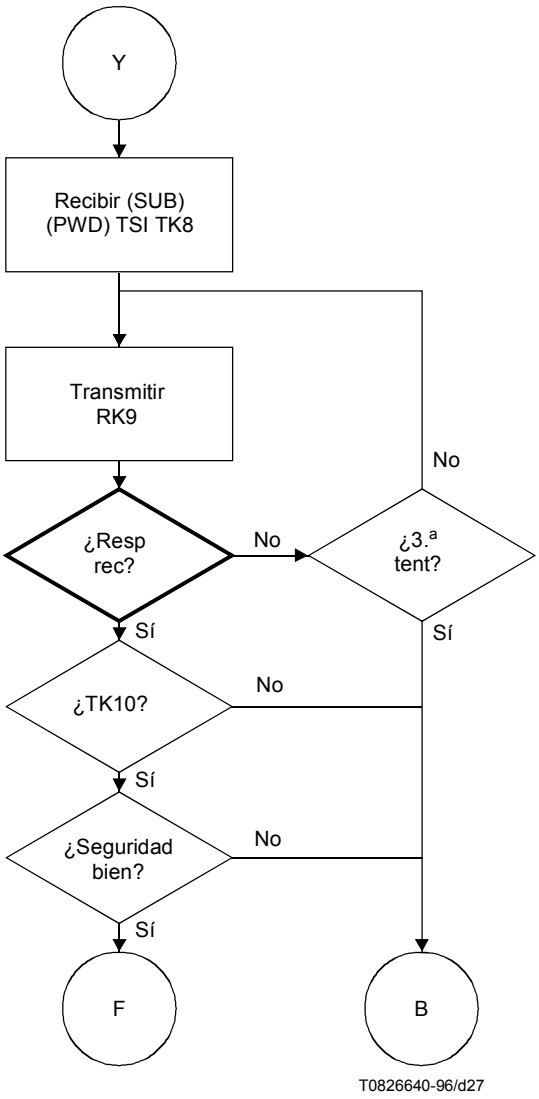


Figura G.8-3/T.30 (hoja 3 de 3) (Utilizada en lugar de la figura C.12/T.30) Dúplex

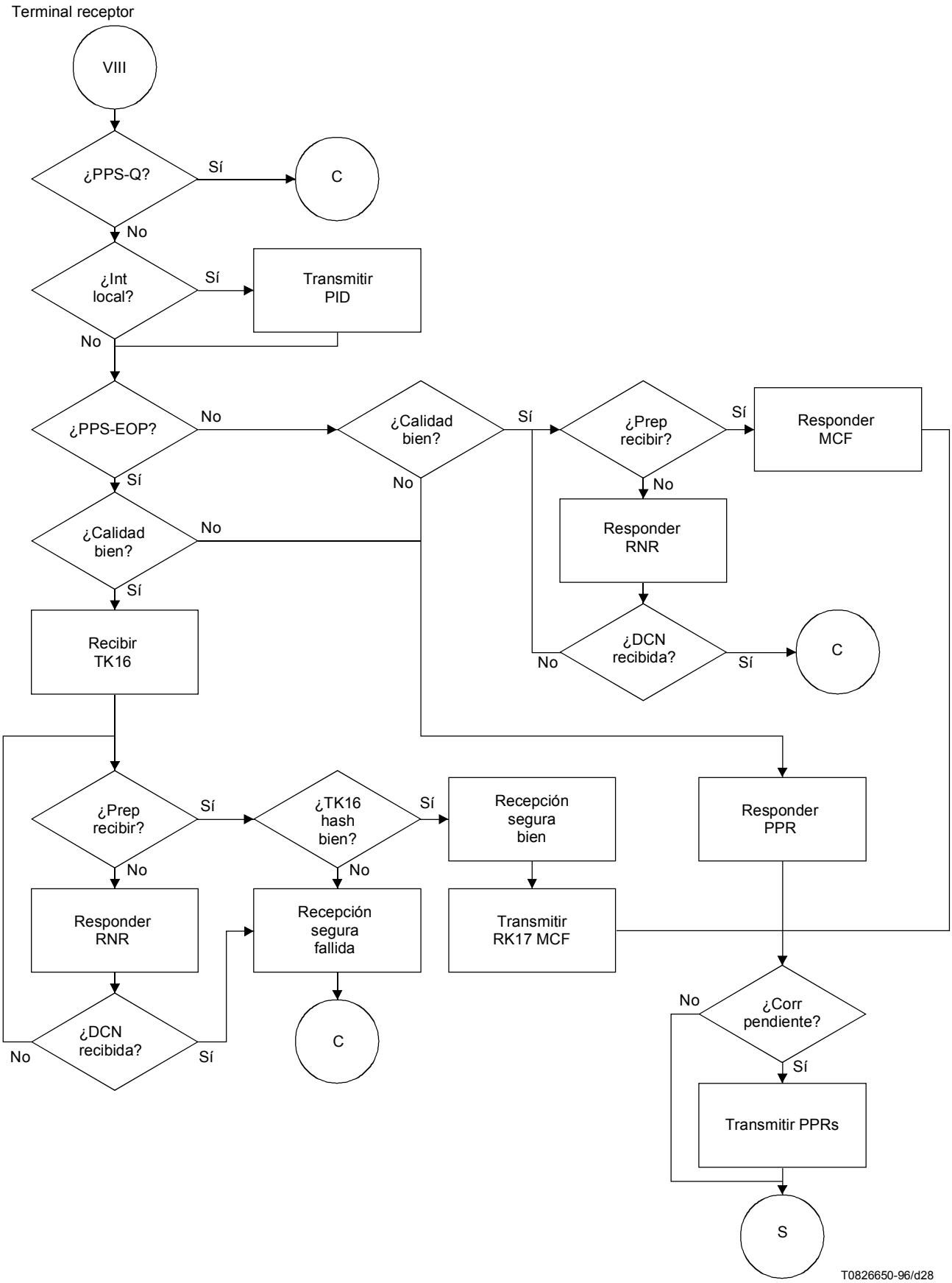


Figura G.8-4/T.30 (Utilizada en lugar de la figura C.13/T.30) Dúplex

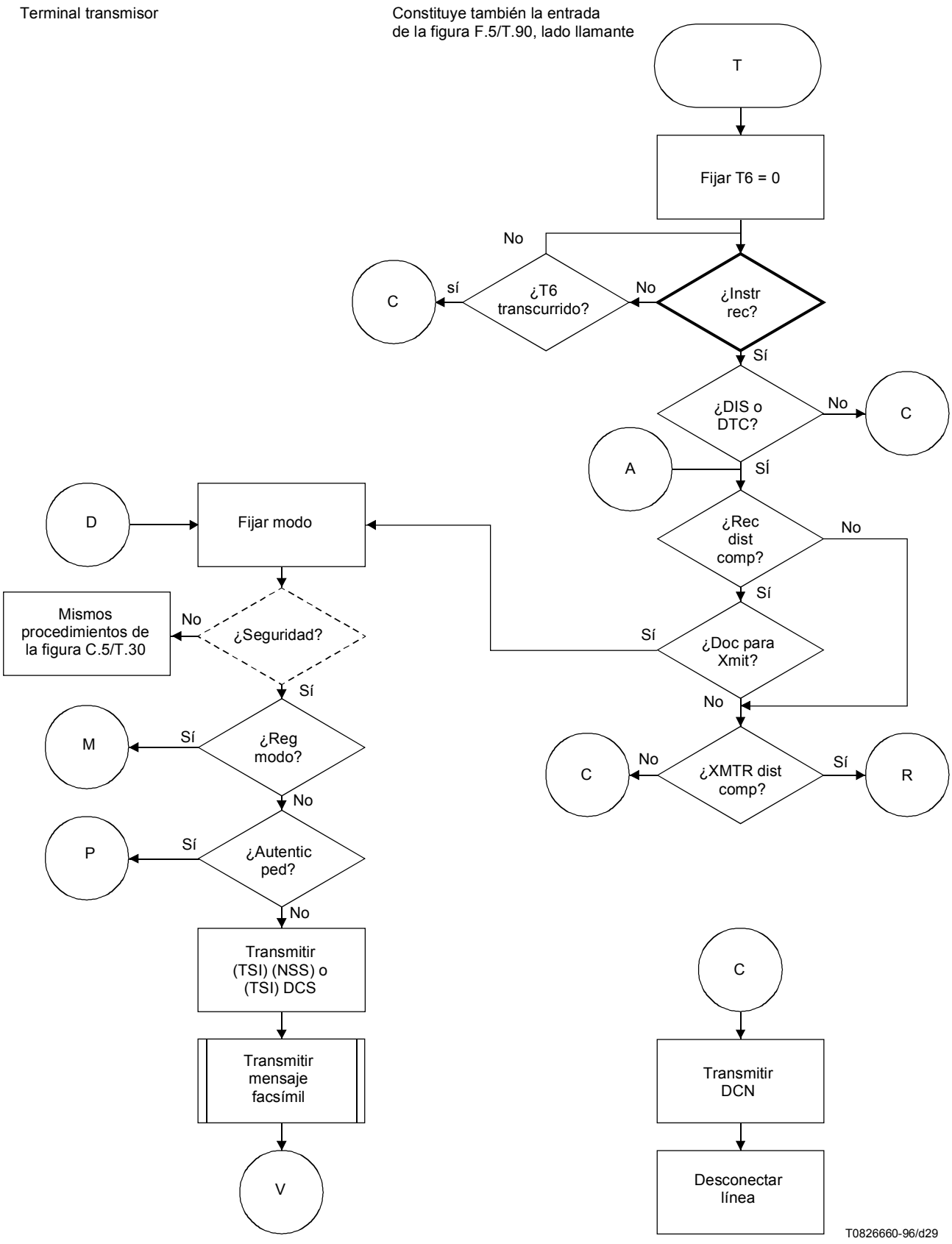


Figura G.8-5/T.30 (hoja 1 de 3) (Utilizada en lugar de la figura C.14/T.30) Dúplex

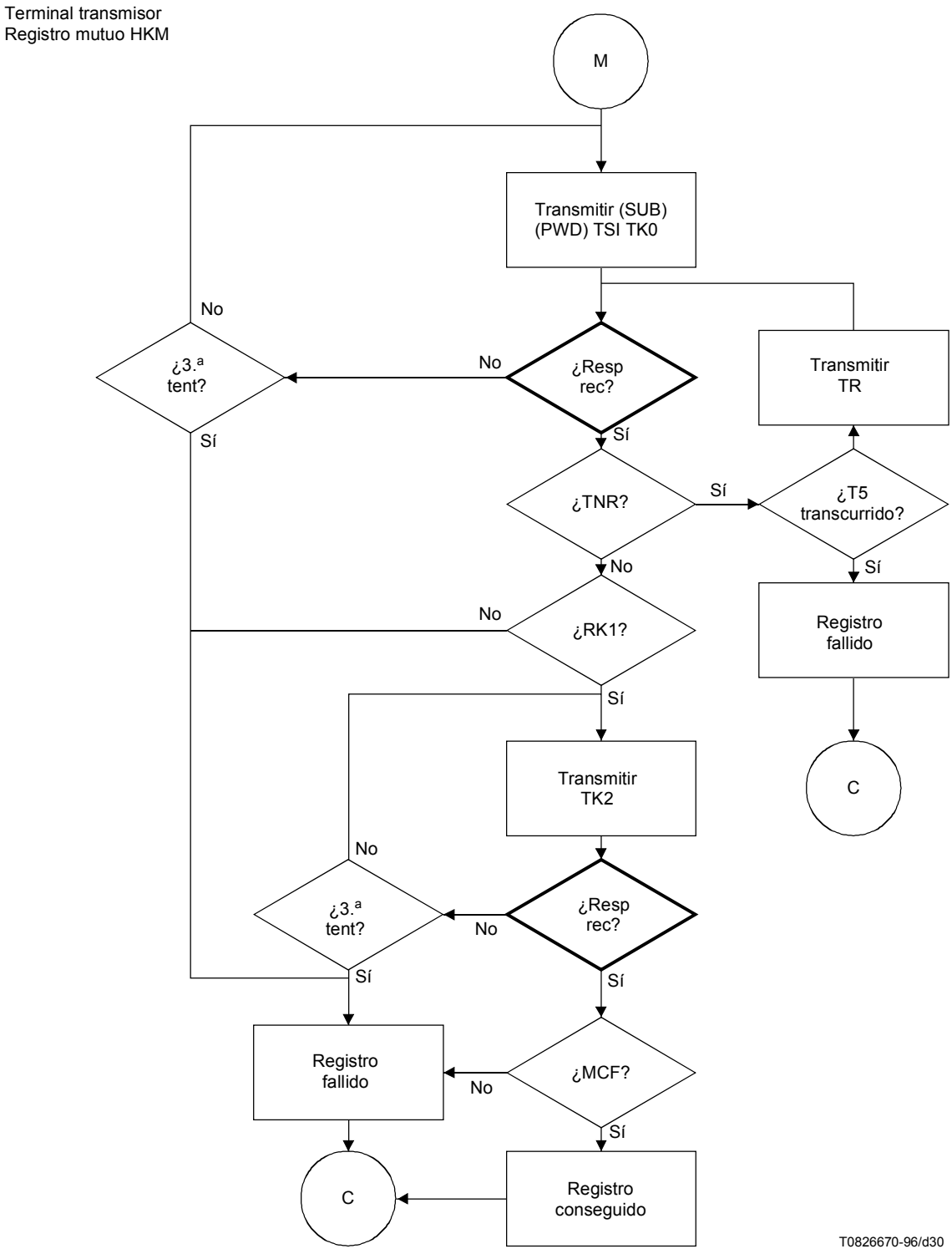


Figura G.8-5/T.30 (hoja 2 de 3) (Utilizada en lugar de la figura C.14/T.30) Dúplex

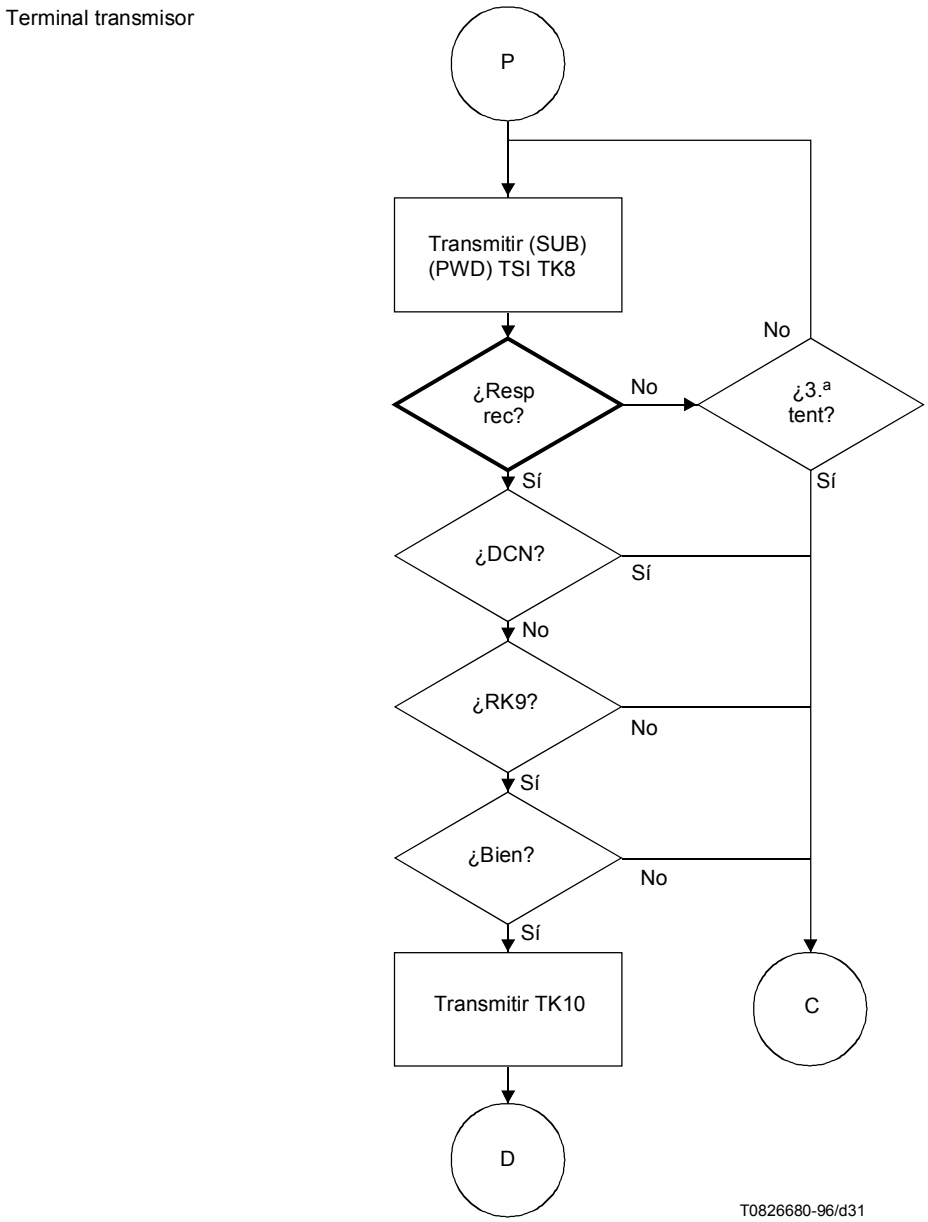


Figura G.8-5/T.30 (hoja 3 de 3) (Utilizada en lugar de la figura C.14/T.30) Dúplex

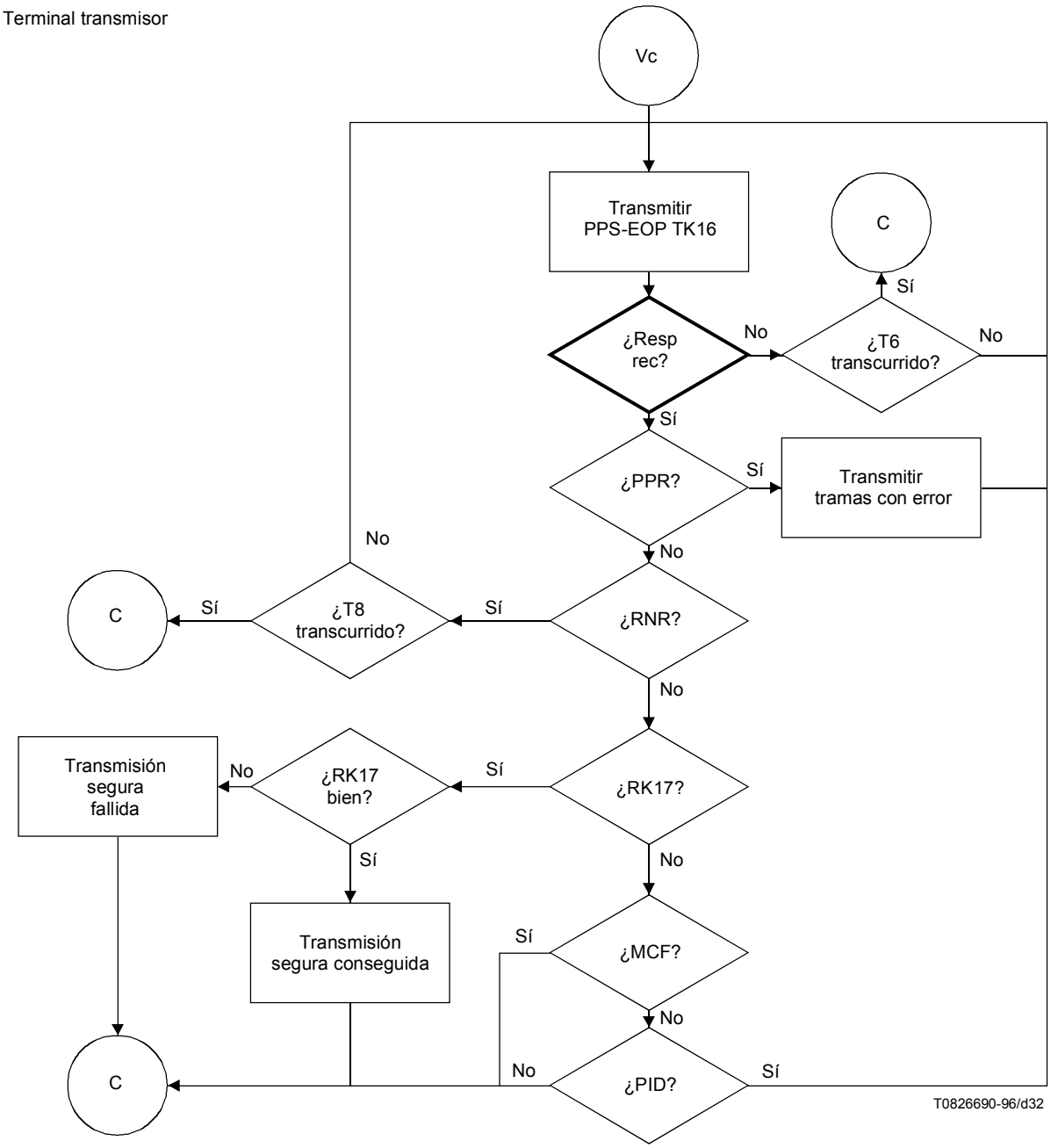


Figura G.8-6/T.30 (Utilizada en lugar de la figura C.18/T.30) Dúplex

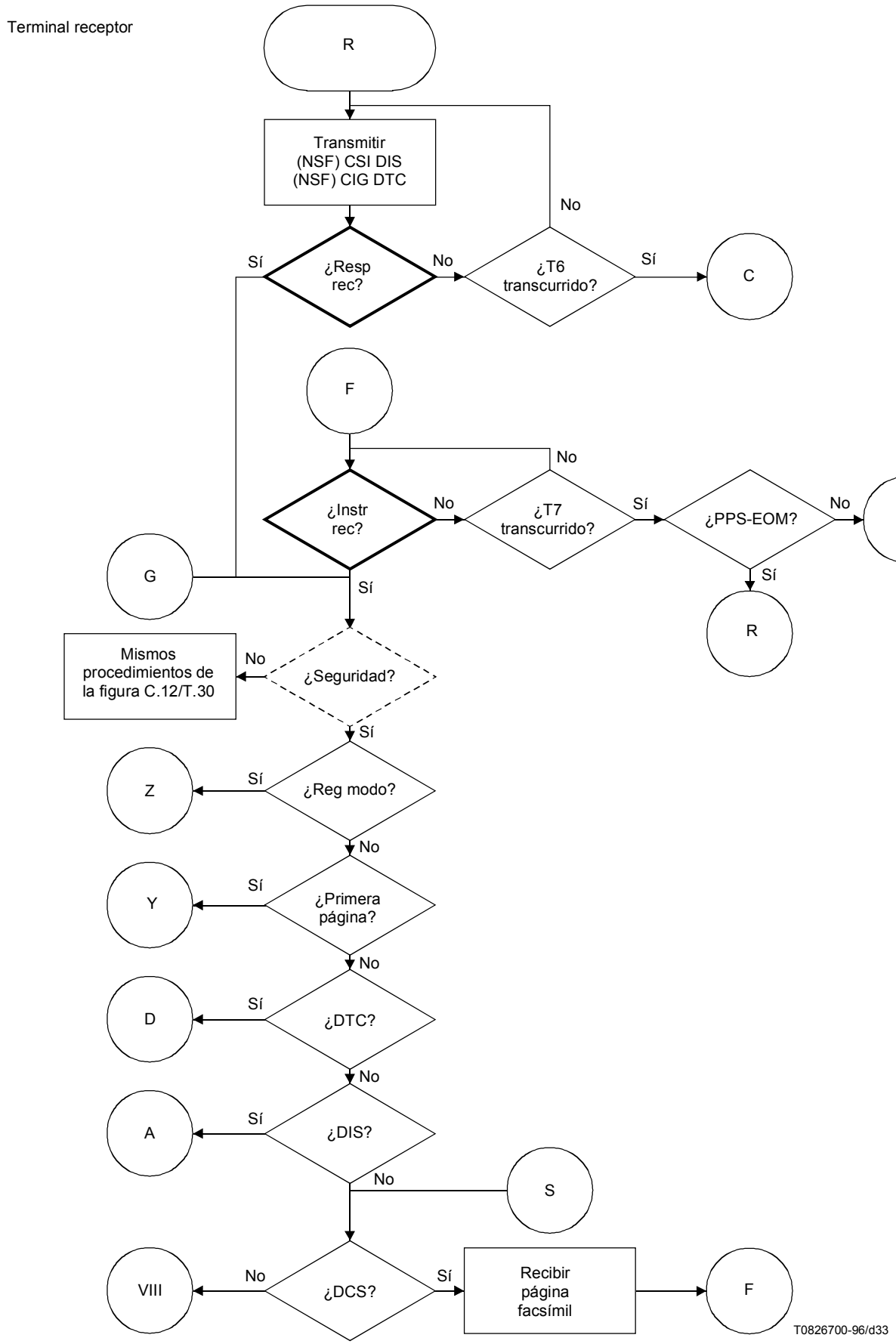


Figura G.8-7/T.30 (Utilizada en lugar de la figura C.21/T.30) Dúplex

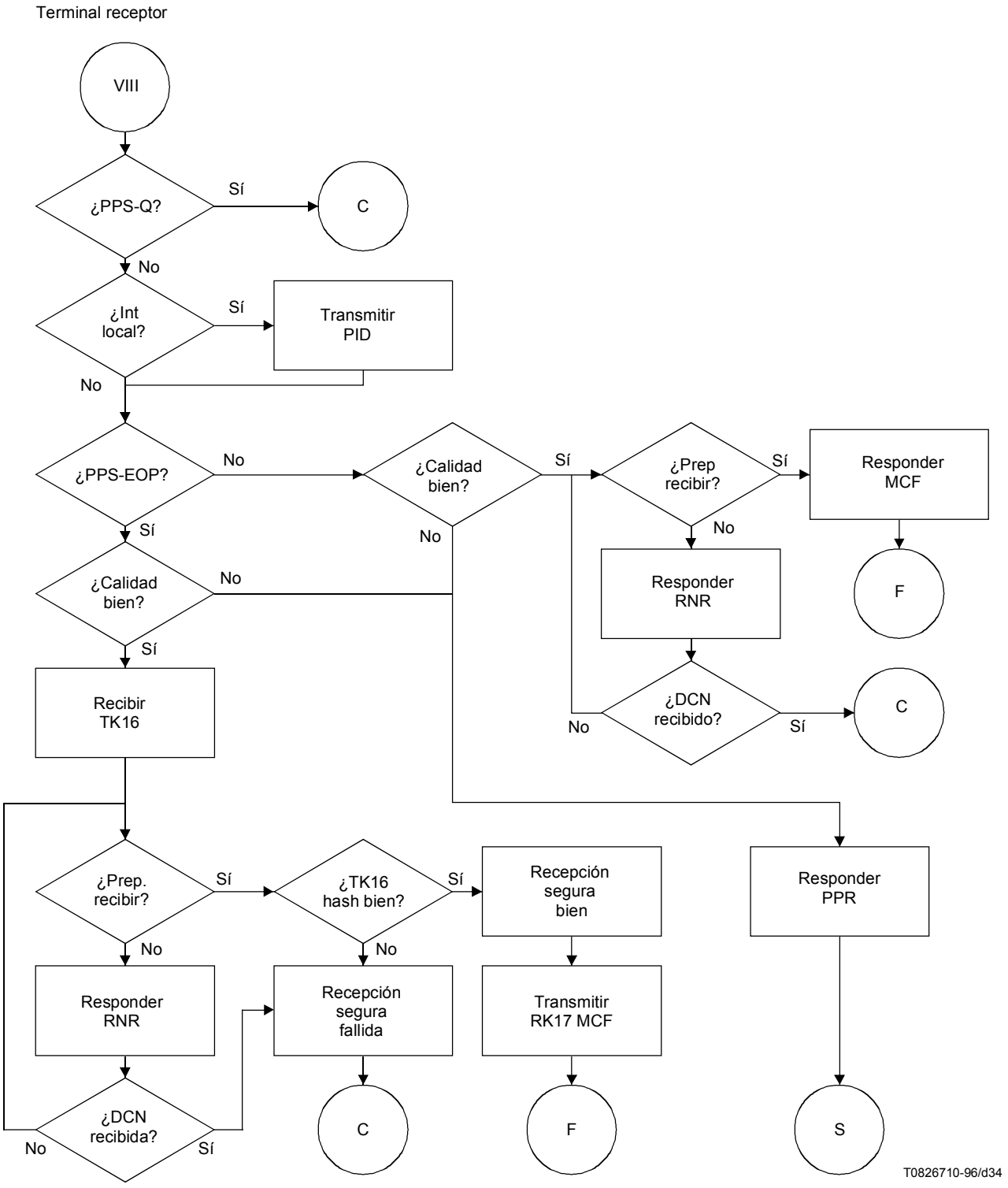


Figura G.8-8/T.30 (Utilizada en lugar de la figura C.22/T.30) Dúplex

G.8.2 Reglas de diagrama de flujo

Los diagramas de flujo siguen dos reglas simples:

1) Todas las líneas tienen una flecha en el destino solamente.

2) Las líneas no se cruzan.

G.8.3 Temporizadores utilizados en los diagramas de flujo

T1	35 s ± 5 s
T2	6 s ± 1 s
T3	10 s ± 5 s
T4	4,5 s ± 15% para unidades manuales
T4	3,0 s ± 15% para unidades automáticas
T5	60 s ± 5 s
T6	5 s ± 0,5 s
T7	6 s ± 1 s
T8	10 s ± 1 s
T9	Duración de 256 banderas

G.8.4 Abreviaturas y descripciones utilizadas en los diagramas de flujo

Salvo que se haya definido diferentemente más arriba, la definición de los términos del organigrama se da en el cuerpo de la Recomendación y/o en el anexo A/T.30.

Authen reqd? Comprobación para ver si se requiere autenticación mutua al principio de la transmisión.

NOTA 1 – una vez que se ha completado la autenticación mutua, dentro de la misma sesión se ha de seguir siempre la salida "No".

Reg mode? Comprobación para ver si se requiere registro de seguridad.

First page? Comprobación para ver si se requiere autenticación mutua al principio de la transmisión.

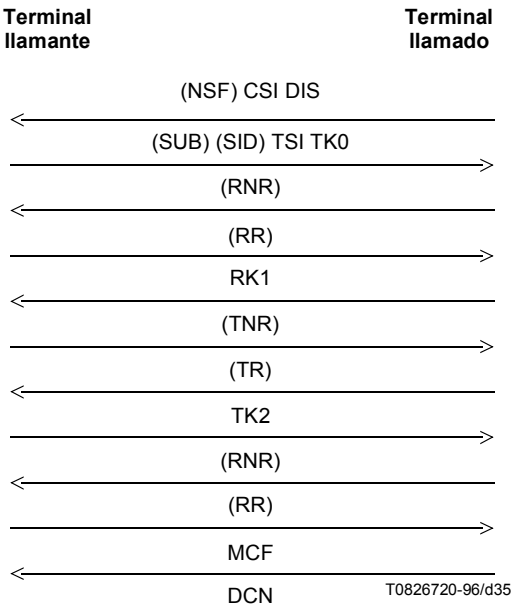
NOTA 2 – una vez que se ha completado la autenticación mutua, dentro de la misma sesión se ha de seguir siempre la salida "No".

G.9 Ejemplo de secuencias de señales en caso del procedimiento de transmisión segura de documentos facsímil

Los ejemplos de las figuras G.9-1/T.30-G.9-2/T.30 se basan en los diagramas de flujo y sólo tienen un fin ilustrativo y didáctico. No se debe interpretar que establecen o limitan el protocolo. Los intercambios de las diversas señales y respuestas están limitados solamente por las reglas especificadas en la presente Recomendación.

NOTA – La señales de obtención, RNR/RR y TNR/TR, se pueden utilizar en cualquier momento durante la fase B y la fase D para que el receptor o el transmisor puedan realizar cualquier procesamiento para calcular valores de seguridad o para obtener claves del almacenamiento o, en el caso de registro, del operador.

G.9.1 Registro mutuo de HKM



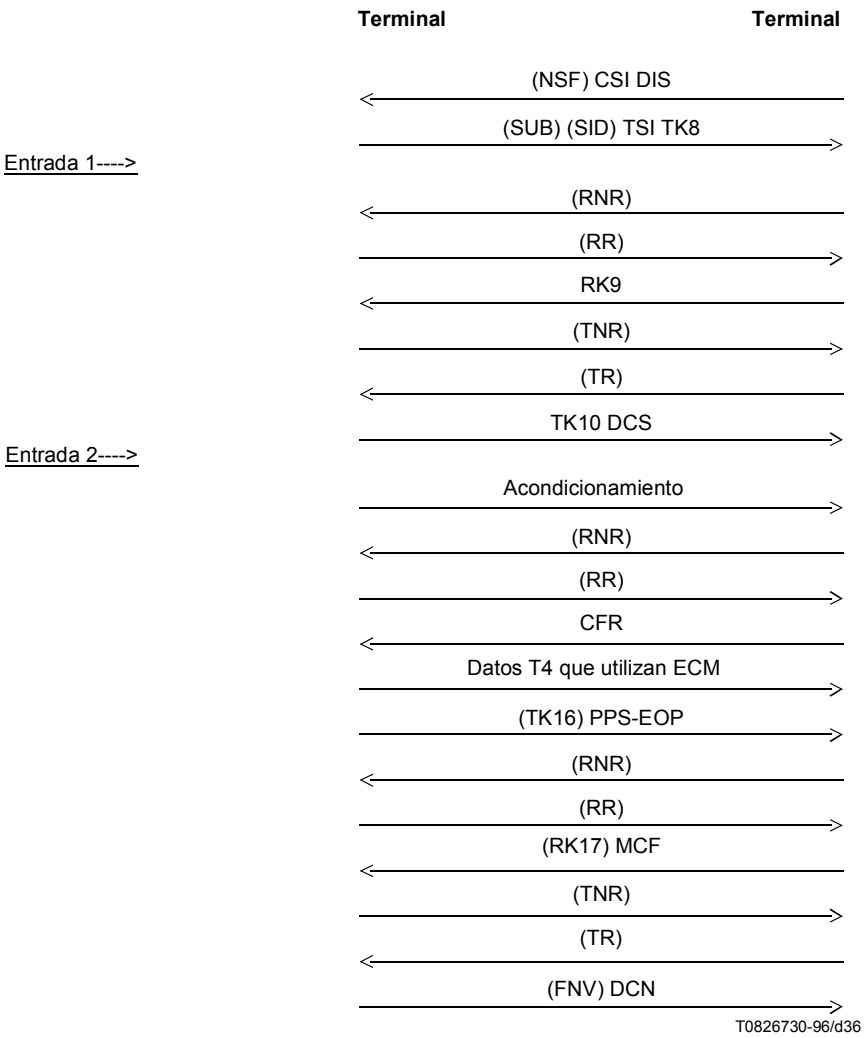
NOTA 1 – El operador del terminal llamado puede necesitar tiempo para introducir la clave que se utiliza una sola vez. Si ésta está siendo introducida manualmente en tiempo real, se utiliza RNR/RR para obtener el terminal llamante. RNR/RR proporciona un retardo de hasta 65 segundos.

NOTA 2 – La señal SUB se puede utilizar para identificar un individuo dentro del dominio del terminal llamado con el cual se solicita el registro.

NOTA 3 – La señal SID, identificación del emisor, se puede utilizar para identificar un individuo dentro del dominio del terminal llamante que está solicitando el registro.

Figura G.9-1/T.30

G.9.2 Transmisión segura de HKM con criptación y troceado facultativos



NOTA 1 – La señal SUB se puede utilizar para identificar a un individuo dentro del dominio del terminal llamado para recibir el documento facsímil seguro.

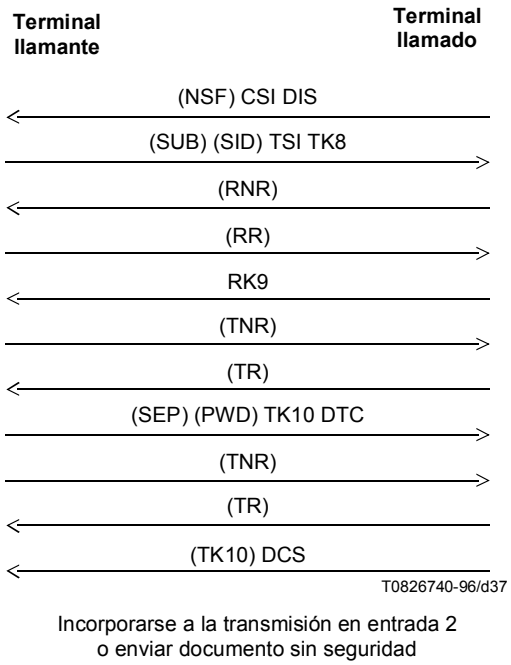
NOTA 2 – La señal SID, identificación del emisor, se puede utilizar para identificar un individuo dentro del dominio del terminal llamante que está enviando el documento facsímil seguro.

NOTA 3 – Los datos que se han de transmitir deben estar exactamente en el mismo formato que estarían si no se hubiese utilizado el cifrado, es decir, completos con cualquier relleno, etc. El cifrado se efectúa inmediatamente antes de que estos datos se transmitan realmente. Cuando el terminal receptor descifra los datos, debe hacerlo inmediatamente antes del procesamiento normal.

Figura G.9-2/T.30

G.9.3 Interrogación secuencial segura de HKM con criptación y troceado facultativos

Véase la figura G.9-3/T.30.



NOTA 1 – La señal SUB se puede utilizar para identificar a un individuo dentro del dominio del terminal llamado para recibir el documento facsímil seguro.

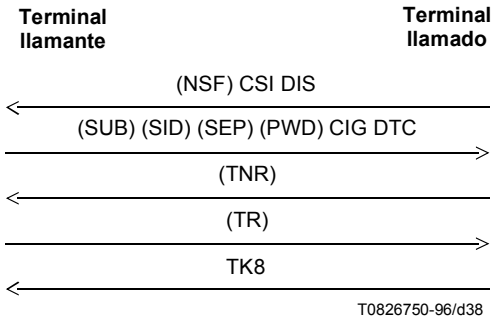
NOTA 2 – La señal SID, identificación del emisor, se puede utilizar para identificar un individuo dentro del dominio del terminal llamante que está enviando el documento facsímil seguro.

NOTA 3 – Los datos que se han de transmitir deben estar exactamente en el mismo formato que estarían si no se hubiese utilizado el cifrado, es decir, completos con cualquier relleno, etc. El cifrado se efectúa inmediatamente antes de que estos datos se transmitan realmente. Cuando el terminal receptor descifra los datos, debe hacerlo inmediatamente antes del procesamiento normal.

Figura G.9-3/T.30

G.9.4 Interrogación secuencial segura de HKM (iniciada por el sistema interrogado) con criptación y troceado facultativos

Véase la figura G.9-4/T.30.



Incorporarse a la transmisión en la entrada 1

NOTA 1 – La señal SUB se puede utilizar para identificar a un individuo dentro del dominio del terminal llamado para proporcionar el documento facsímil seguro.

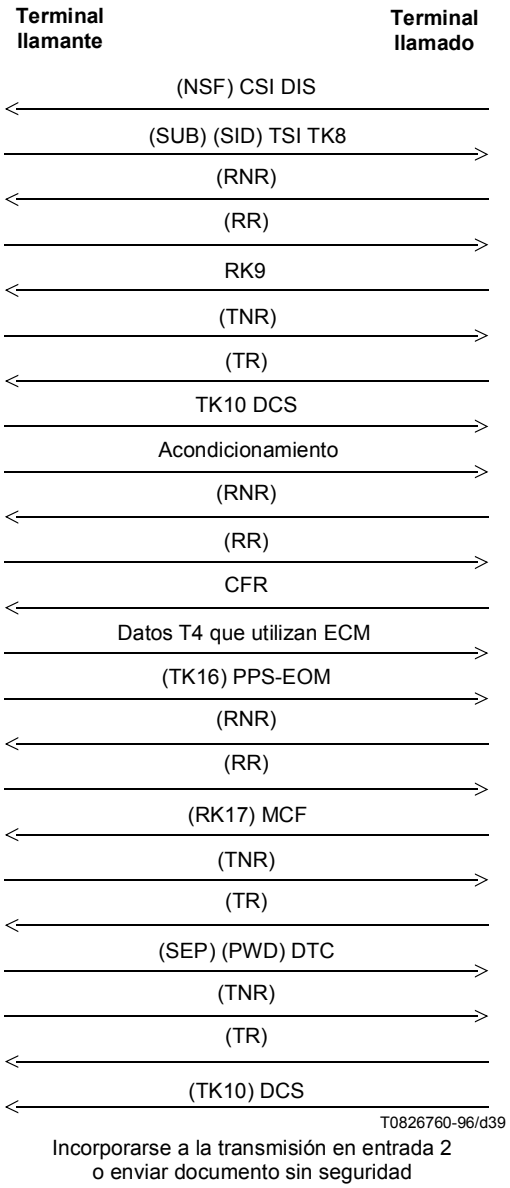
NOTA 2 – La señal SID, identificación del emisor, se puede utilizar para identificar un individuo dentro del dominio del terminal llamante que está interrogando sobre el documento facsímil seguro.

NOTA 3 – Los datos que se han de transmitir deben estar exactamente en el mismo formato que estarían si no se hubiese utilizado el cifrado, es decir, completos con cualquier relleno, etc. El cifrado se efectúa inmediatamente antes de que estos datos se transmitan realmente. Cuando el terminal receptor descifra los datos, debe hacerlo inmediatamente antes del procesamiento normal.

Figura G.9-4/T.30

G.9.5 Interrogación segura de HKM en los dos sentidos con criptación y troceado facultativos

Véase la figura G.9-5/T.30.



NOTA 1 – La señal SUB se puede utilizar para identificar a un individuo dentro del dominio del terminal llamado para recibir el documento facsímil seguro.

NOTA 2 – La señal SID, identificación del emisor, se puede utilizar para identificar un individuo dentro del dominio del terminal llamante que está enviando el documento facsímil seguro.

NOTA 3 – Los datos que se han de transmitir deben estar exactamente en el mismo formato que estarían si no se hubiese utilizado el cifrado, es decir, completos con cualquier relleno, etc. El cifrado se efectúa inmediatamente antes de que estos datos se transmitan realmente. Cuando el terminal receptor descifra los datos, debe hacerlo inmediatamente antes del procesamiento normal.

NOTA 4 – TK10 es facultativo y, si está presente, contendrá una nueva clave de sesión con los valores de respuesta puestos a cero.

Figura G.9-5/T.30

3 Sección 3

Introducción del nuevo anexo H:

Anexo H

Seguridad en facsímil del grupo 3 basada en el algoritmo RSA

H.1 Preámbulo

(El preámbulo se deja en blanco a propósito)

H.2 Introducción

Este anexo especifica los mecanismos con los que ofrecer características de seguridad basadas en el sistema criptográfico RSA. El esquema de codificación del documento transmitido como característica de seguridad puede ser de cualquiera de los tipos definidos en las Recomendaciones T.4 y T.30 [Huffmann modificado, Read modificado (MR) y Read modificado modificado (MMR), modo carácter definido en el anexo D/T.4, transferencia de ficheros binarios (BFT, *binary file transfer*), otros modos de transferencia de ficheros definidos en el anexo C/T.4.].

H.3 Referencias

– ISO/CEI 9796:1991, *Information technology – Security techniques – Digital signature scheme giving message recovery*.

  Anexo A: RSA: R.L. Rivest, A. Shamir, L. Adleman: Método de obtener firmas digitales y criptosistemas de claves públicas, *CACM (Comunicaciones del ACM)*, vol. 21, N.º 2, páginas 120-126, 1978.

– ISO/CEI 10118-3[1], *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*.

  Número de referencia: N1108 de JTC 1/SC27 de ISO/CEI:

  SHA-1 [Secure Hash Algorithm (algoritmo de troceado seguro)], descrito en *Secure Hash Standard*, FIPS (Federal Information Processing Standard) PUB 180-1, abril de 1995, un algoritmo procedente del NIST (National Institute of Standardization) de los Estados Unidos.

– MD-5 (RFC 1321): *Message digest algorithm*.

  ISO/CEI 9979:1991, *Data cryptographic techniques – Procedures for the registration of cryptographic algorithms*.

H.4 Mecanismos de seguridad

H.4.1 Mecanismo de firma digital y gestión de claves

El algoritmo básico utilizado para la firma digital (servicios de autenticación y tipo de integridad) es el **RSA**.

El par de claves utilizadas al fin es el de "clave pública"/"clave secreta".

Cuando se ofrece el servicio de confidencialidad facultativo, el testigo que contiene la clave de sesión "Ks", utilizada para cifrar el documento, se encripta también mediante el algoritmo RSA. El par de claves utilizada a tal fin, llamado ("clave pública de cifrado"/"clave secreta de cifrado"), no es el mismo que el utilizado por los servicios de autenticación y tipo de integridad. Con ello se pretende desvincular las dos formas de utilización.

La realización del algoritmo RSA utilizado en este anexo se describe en ISO/CEI 9796 relativa al esquema de firma digital que restablece el mensaje.

---

[1] Actualmente en estado de proyecto.

Para el cifrado del testigo que contiene la clave de sesión, las reglas de redundancia cuando se procesa el algoritmo RSA son las mismas que se especifican en ISO/CEI 9796.

NOTA – Algunas administraciones quizá exijan que, además del RSA, (que es el mecanismo básico en el contexto de este anexo) se implemente un mecanismo facultativo: el DSA.

Referencias

– ISO/CEI CD 14888-3: 1995.

  Número de referencia: N1113 de JTC 1/SC27 de ISO/CEI.

– FIPS PUB 186-1: Digital Signature Standard, *NIST de los Estados Unidos*, 1 de febrero de 1993.

H.4.2 Longitud de las claves públicas, las claves secretas y las firmas digitales

Las claves públicas, las claves secretas y las firmas digitales tienen, como característica básica, una longitud de **512 bits**. Se pueden utilizar longitudes mayores como opciones reconocidas; se negocia en el protocolo (véase más adelante).

H.4.3 Longitud del exponente público del RSA

Para firmas digitales, el exponente público tiene un valor fijo de 3.

Para el cifrado del testigo que incluye la clave de sesión "Ks", el exponente público tiene un valor fijo igual a: $2^{16} + 1$. La clave de sesión se utiliza en caso de cifrado del documento. Véase más adelante.

H.4.4 Autoridades de certificación

No se utilizan autoridades de certificación por defecto.

Como opción, se pueden utilizar autoridades de certificación que garanticen la validez de la clave pública del emisor del mensaje facsímil. En tal caso, la clave pública se puede certificar tal como se especifica en la Recomendación X.509.

La manera de transmitir el certificado de la clave pública del emisor se describe en el presente anexo, pero el formato preciso del certificado queda en estudio (en versiones posteriores de este anexo).

La transmisión efectiva del certificado se negocia en el protocolo.

H.4.5 Modo registro

Como característica **obligatoria** se proporciona un *modo registro*. Dicho modo, permite al emisor y al receptor registrar y almacenar las claves públicas de la otra parte de manera confidencial, antes de que tenga lugar cualquier comunicación facsímil segura entre las dos partes.

Con el modo registro se evita que el usuario introduzca manualmente en el terminal las claves públicas de sus correspondientes (las claves públicas son bastante largas, de 64 octetos o más).

Puesto que el modo registro permite intercambiar las claves públicas y almacenarlas en los terminales, no es necesario transmitirlas durante las comunicaciones facsímil.

El esquema del modo registro se detalla más adelante en el presente anexo.

H.4.6 Función de troceado

Tal como se describe en este anexo, algunas firmas se aplican en base al resultado de una "función troceado".

La función troceado que se utiliza es el algoritmo de troceado asegurado (SHA-1, *secured hash algorithm*), del NIST de los Estados Unidos o bien el MD-5 (RFC 1321).

Para el SHA-1, la longitud del resultado del proceso de troceado es de **160 bits**.

Para el MD-5, la longitud del resultado del proceso de troceado es de **128 bits**.

Un terminal puede realizar el SHA-1 o el MD-5 o bien ambos.

La utilización de uno u otro algoritmo se negocia en el protocolo (véase más adelante).

En el futuro, se pueden añadir a este anexo otras funciones troceado facultativas.

H.4.7 Cifrado

H.4.7.1 Generalidades

El cifrado de los datos para la prestación del servicio de confidencialidad es facultativo.

En el marco de este anexo están registrados cinco esquemas de cifrado facultativos:

FEAL-32, SAFER K-64, RC5, IDEA y HFX40 (descritos en la Recomendación T.36). En algunos países, su utilización puede estar sujeta a la reglamentación nacional.

En el futuro podrían registrarse otros algoritmos facultativos, cuya utilización también es posible.

Se seleccionan de conformidad con ISO/CEI 9979 (sobre procedimiento de registro de algoritmos criptográficos).

La capacidad del terminal de tratar esos algoritmo, y la utilización efectiva de uno en concreto durante la comunicación, se negocia en el protocolo.

Para cifrado se emplea una clave de sesión llamada "**Ks**".

La longitud básica de Ks es 40 bits.

– Para algoritmos que utilizan una clave de sesión de 40 bits (por ejemplo HFX40), la clave de sesión Ks es la clave utilizada realmente en el algoritmo de cifrado.

– Para algoritmos que requieren claves de más de 40 bits (por ejemplo, FEAL-32, IDEA, SAFER K-64, que requieren respectivamente: 64 bits, 128 bits y 64 bits), se emplea un mecanismo de redundancia para obtener la longitud necesaria. La clave resultante se denomina “clave de sesión redundante”. La “clave de sesión redundante” es la clave que se utiliza realmente en el algoritmo de cifrado.

El mecanismo de redundancia se describe en la subcláusula siguiente.

El testigo "BE", que incluye la clave Ks (véase más adelante), se cifra mediante la "clave pública de cifrado" del receptor, al que se lo envía el emisor.

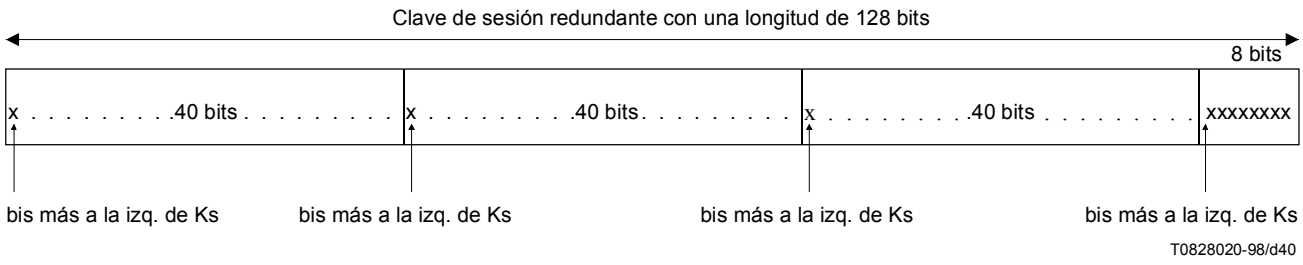
Cuando se necesita una clave con redundancia, el terminal receptor la regenera a partir del testigo “BE” recibido del terminal emisor.

H.4.7.2 Mecanismo de redundancia para obtener la clave de sesión redundante cuando sea necesario

Cuando se necesita una “clave de sesión redundante” (el algoritmo de cifrado necesita una clave de más de 40 bits), esta entidad se genera como sigue:

El patrón de bits Ks se repite tantas veces cuantas sean necesarias para obtener la longitud requerida por el algoritmo. Si es necesario, una parte del patrón (comenzando por el bit más a la izquierda) se añade al final para adaptarse a la longitud correcta.

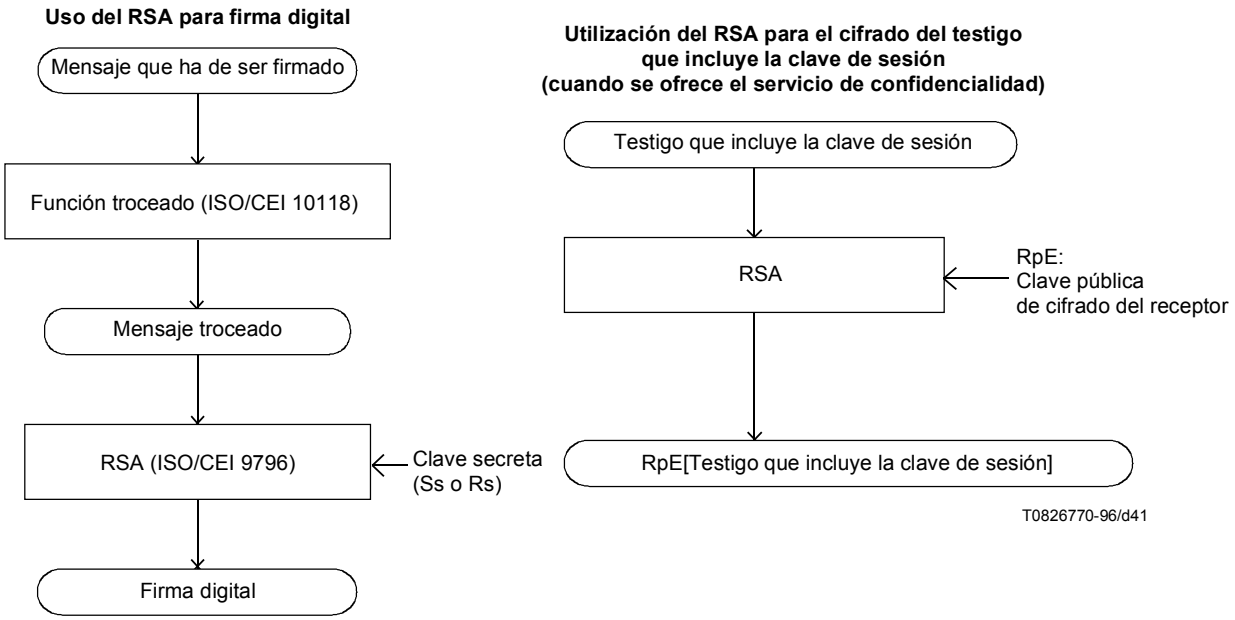
Este principio se ilustra en el siguiente ejemplo en que el algoritmo requiere 128 bits (por ejemplo, IDEA).



H.4.8 Utilización de la función troceado y del algoritmo RSA

H.4.8.1 Esquema general

Véase la figura H.1/T.30.



NOTA – La Norma ISO/CEI 9796 se ha concebido para la firma RSA de una información breve, que puede ser el mensaje que se ha de firmar (si es corto) o el código de troceado del mensaje que se ha de firmar (si el mensaje es demasiado largo). Véase ISO/CEI 9796.

Figura H.1/T.30

H.4.8.2 Orden de los bits para la transmisión

A lo largo de este anexo:

1) Todas las secuencias de octetos se transmiten de modo que el octeto situado más a la izquierda (tal como se representa en este anexo) sea el primer octeto transmitido.

   La regla respecto al orden de transmisión de los bits dentro de cada octeto es como se indica a continuación.

2) Salvo por lo que se refiere al contenido del campo de información facsímil (**FIF**) de la señal ampliada digital (DES) y las señales de instrucción ampliada digital (DEC), petición ampliada digital (DER) y petición de inversión digital (DTR), definido más abajo, el orden en que se transmiten los bits de cada octeto representado en este anexo es de izquierda a derecha según se escribe. Tal es el caso, por ejemplo, para los códigos del campo de control facsímil (FCF).

3) Para el contenido del **FIF** de las señales DES, DEC, DER y DTR:

   3a) Hay una "regla general":

   Consiste en que, en cada octeto, el bit menos significativo es el que se transmite primero.

   Cuando los bits están numerados en cuadros, el bit menos significativo se numera como "`bit N.° 0`".

   Por ejemplo, el octeto `"1 0 1 1 0 0 1 1"`

   numerado (si lo está) como sigue:

```
bit N.° 7 6 5 4 3 2 1 0
        1 0 1 1 0 0 1 1
```

   se transmitirá de la siguiente manera:

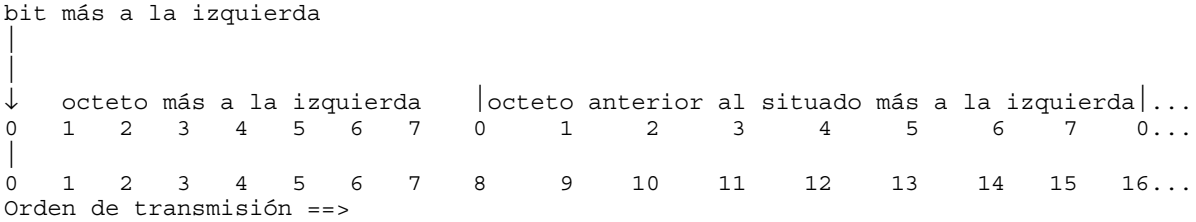
   Orden de transmisión ==>

   1 1 0 0 1 1 0 1

   3b) Cuando el contenido del FIF de las señales de la Recomendación/T.30 se encapsula dentro de una estructura de rótulos codificados (véase el H.6.1.4.7 "supergrupo de tramas encapsuladas"), se mantiene la coherencia con el orden de transmisión de los octetos y bits del FIF, tal como se ha definido anteriormente para esas señales (véanse los 5.3 y 5.3.6.2).

3c) Dentro del FIF de las señales DES, DEC, DER y DTR, hay una excepción a la regla general para los parámetros identificados como de "codificación binaria" en el cuadro H.1/T.30. Con estos parámetros se aplica la regla.

El primer bit transmitido por la línea es el bit situado más a la izquierda del octeto situado más a la izquierda:



H.4.8.3 Orden de los bits en los procesos de troceado y RSA

Las normas relativas a la función troceado (SHA-1 y MD-5) definen una cadena de bits sobre la que se aplica el proceso de troceado y una cadena de bits que es el resultado del troceado.

El primer bit de estas cadenas de bits es el situado más a la izquierda (según se representan las figuras de estas normas).

En el presente anexo, se especifican diversos parámetros a los que se aplica la función troceado. Algunos resultados del troceado se transmiten por la línea. Las reglas respecto al orden de los bits por la línea y al orden de los bits para el procesamiento en la función troceado son las mismas:

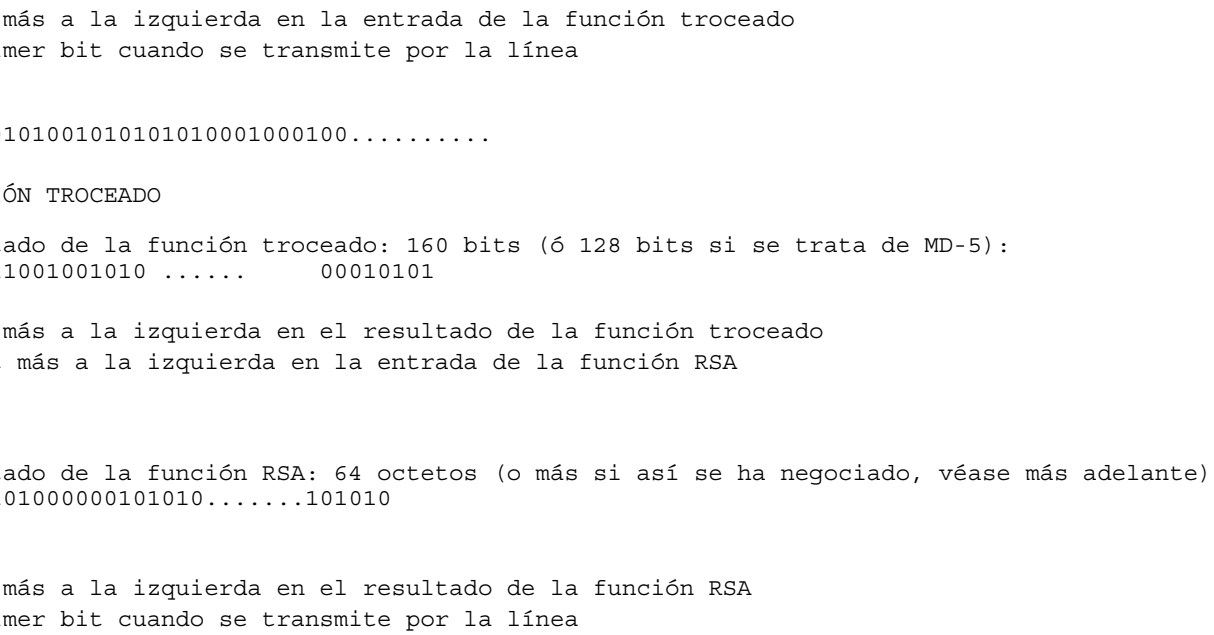
– el primer bit que pasa por la función troceado es el bit situado más a la izquierda del octeto situado más a la izquierda.

Si la función troceado se aplica a varias entidades concatenadas, por ejemplo h(a,b,c,...), la cadena de bits que se ha de trocear es la cadena de bits [a] seguida inmediatamente por la cadena de bits [b], etc.

En el caso de la función RSA se aplica el mismo principio:

el primer bit que pasa por la función RSA es el bit situado más a la izquierda del octeto situado más a la izquierda.

El orden de los bits a través de la función troceado y de la función RSA es tal como se ilustra a continuación (las cadenas de bits representadas son sólo un ejemplo).



Este principio es válido también para los parámetros que pasan directamente a la función RSA sin troceado (por ejemplo, el testigo que incluye la clave de sesión "Ks").

Si la función RSA se aplica a varias entidades concatenadas, por ejemplo (a,b,c,…), la cadena de bits que ha de ser procesada por la función RSA es la cadena de bits [a] seguida inmediatamente por la cadena de bits [b], etc.

H.5 Parámetros de seguridad

El cuadro H.1/T.30 define diversos parámetros de seguridad, algunos de los cuales se intercambian.

Para todos los parámetros de seguridad se define una longitud básica. El soporte de esta longitud básica es obligatorio.

Además, algunos parámetros permiten longitudes mayores facultativas, que pueden ser negociadas en el protocolo.

El cuadro H.1/T.30 indica también el tipo de codificación de los parámetros (binaria, ASCII, …).

La manera de transmitir estos parámetros en las señales DES, DEC, DER y DTR se especifica más adelante en el presente anexo.

Cuadro H.1/T.30 – Parámetros de seguridad

Abreviatura	Descripción	Longitud básica	Longitudes mayores facultativas	Codificación del campo
S	Identidad del emisor	20 octetos	Queda en estudio	IA5 (Nota 1)
Sp	Clave pública del emisor	64 octetos	Es posible	Binaria (Nota 2)
Ss	Clave secreta del emisor	64 octetos	Lo mismo que Sp	Binaria (Nota 2)
SpE	Clave pública de cifrado del emisor (para la criptación de un testigo que contiene la clave de sesión)	64 octetos	Es posible	Binaria (Nota 2)
SsE	Clave secreta de cifrado del emisor (para la descriptación de un testigo encriptado que contiene la clave de sesión)	64 octetos	Lo mismo que SpE	Binaria (Nota 2)
Sra	Número aleatorio creado por el emisor para la autenticación del receptor	8 octetos	Es posible	Binaria (Nota 2)
Srd	Número aleatorio creado por el emisor para la firma digital	8 octetos	Es posible	Binaria (Nota 2)
R	Identidad del receptor	20 octetos	Queda en estudio	IA5 (Nota 1)
Rp	Clave pública del receptor	64 octetos	Es posible	Binaria (Nota 2)
Rs	Clave secreta del receptor	64 octetos	Lo mismo que Rp	Binaria (Nota 2)
RpE	Clave pública de cifrado del receptor (para la criptación de un testigo que contiene la clave de sesión)	64 octetos	Es posible	Binaria (Nota 2)
RsE	Clave secreta de cifrado del receptor (para la descriptación de un testigo encriptado que contiene la clave de sesión)	64 octetos	Lo mismo que RpE	Binaria (Nota 2)
Rra	Número aleatorio creado por el receptor para la autenticación del emisor	8 octetos	Es posible	Binaria (Nota 2)
Ks	Clave de sesión	40 bits	Queda en estudio	Binaria (Nota 2)
BE	BE = RpE[S, Ks] = Identidad del emisor y clave de sesión concatenadas y encriptadas por RpE	64 octetos	Lo mismo que RpE	Binaria (Nota 2)
UTCd	Fecha/hora elegida por el emisor (fecha/hora de la generación/firma del documento)	8 octetos	Queda en estudio	YY MM DD HH MM SS con respecto al GMT, decimal codificado en binario (BCD) (Nota 3)
UTCr	Fecha/hora elegida por el receptor (fecha/hora de la confirmación de la recepción del mensaje)	8 octetos	Queda en estudio	YY MM DD HH MM SS con respecto al GMT, decimal codificado en binario (BCD) (Nota 3)
Lm	Longitud del documento	4 octetos	Queda en estudio	Corresponde al número de octetos del documento completo transmitido (octetos de datos + bits de justificación, véase H.6.5/T.30) decimal codificado en binario (BCD) (Nota 4)

Cuadro H.1/T.30 – Parámetros de seguridad *(fin)*

Abreviatura	Descripción	Longitud básica	Longitudes mayores facultativas	Codificación del campo
h(…)	Resultado troceado de la entidad escrita entre paréntesis	160 bits o 128 bits, dependiendo de la función troceado	Queda en estudio	Binaria (Nota 2)
Rs[h(…)]	Resultado troceado de la entidad escrita entre paréntesis, firmado por el receptor	64 octetos	Lo mismo que Rp	Binaria (Nota 2)
Ss[h(…)]	Resultado troceado de la entidad escrita entre paréntesis, firmado por el emisor	64 octetos	Lo mismo que Sp	Binaria (Nota 2)
Sia	Indicador en el testigo utilizado para la autenticación del emisor	1 octeto	Ninguna	Octeto igual a: "00000000" (Nota 5)
Ria	Indicador en el testigo utilizado para la autenticación del receptor	1 octeto	Ninguna	Octeto igual a: "00000001" (Nota 5)
Sis	Indicador en el testigo utilizado para la firma digital	1 octeto	Ninguna	Octeto igual a: "00000010" (Nota 5)
Ris	Indicador en el testigo utilizado para la confirmación de la recepción del mensaje	1 octeto	Ninguna	Octeto igual a: "00000011" (Nota 5)
document	El documento enviado durante el modo transmisión facsímil segura	Variable	Es irrelevante	Es irrelevante
enc.document	El documento criptado enviado durante el modo transmisión facsímil segura cuando se invoca el servicio de confidencialidad. La criptación del documento se hace con la clave de sesión Ks (o con la clave de sesión redundante si el algoritmo, para que funcione, requiere más bits que Ks	Variable	Es irrelevante	Es irrelevante

NOTA 1 – Se aplica la regla general del FIF de las señales DES/DEC/DER/DTR: el bit menos significativo de cada octeto es el bit que se transmite primero.

NOTA 2 – La regla para la transmisión de elementos codificados en binario se definen en H.4.8.2/T.30.

NOTA 3 – Ejemplo: para el 24 de marzo de 1995. 8H25 05s PM. Respecto GMT: 3H:

```
" 1    9     9    5     0    3     2    4     2    0     2    5     0    5     0    3 "

0001 1001  1001 0101  0000 0011  0010 0100  0010 0000  0010 0101  0000 0101  0000 0011
```

Se aplica la regla general del FIF de las señales DES/DEC/DER/DTR: el bit situado más a la derecha de cada octeto es el bit que se transmite primero.

NOTA 4 – Ejemplo: para un documento de 123456 octetos de longitud:

```
" 0    0      1    2      3    4      5    6 "

0000 0000   0001 0010   0011 0100   0101 0110
```

Se aplica la regla general del FIF de las señales DES/DEC/DER/DTR: el bit situado más a la derecha de cada octeto es el bit que se transmite primero.

NOTA 5 – Se aplica la regla general del FIF de las señales DES/DEC/DER/DTR: el bit situado más a la derecha de cada octeto es el bit que se transmite primero.

H.6 Intercambios de parámetros de seguridad

Se necesita el modo con corrección de errores (ECM, *error correction mode*) descrito en el anexo A/T.30 para ofrecer los servicios de seguridad basados en la función RSA.

Durante la comunicación facsímil se han de transmitir algunos parámetros de seguridad específicos al nivel del protocolo (fases B y D del protocolo de la Recomendación T.30). Facultativamente (véase más adelante "página de seguridad") se transmiten algunos parámetros de seguridad al nivel del mensaje (fase C del protocolo de la Recomendación T.30).

H.6.1 Intercambio de parámetros de seguridad al nivel del protocolo

Las ocho nuevas señales utilizadas son las siguientes:

– DER: Petición ampliada digital (*digital extended request*)

Esta instrucción la envía el terminal emisor. Puede fijar los parámetros de seguridad de la sesión y además pide otros detalles sobre las capacidades de seguridad de la máquina receptora.

– DES: Señal ampliada digital (*digital extended signal*)

Enviada por el dispositivo receptor; contiene las capacidades de seguridad de la máquina receptora.

– DEC: Instrucción ampliada digital (*digital extended command*)

Enviada por el terminal emisor en respuesta a la DES o DTR.

La DEC contiene todos los valores de ajuste para la comunicación en curso y sustituye a la señal de instrucción digital (DCS, *digital command signal*) que no se envía. La información que figura normalmente en el FIF de la DCS está contenida en la DEC. La DEC contiene también los diversos parámetros de seguridad enviados desde el terminal emisor al terminal receptor.

– DTR: Petición de inversión digital (*digital turnaround request*)

Puede ser enviada por el terminal llamante en respuesta a una señal de identificación digital DIS o una DES y se utiliza cuando se desea interrogación secuencial o inversión.

La DTR sustituye a la instrucción de transmitir digital (DTC) que no se envía. La información que figura normalmente en el FIF de la DTC está contenida en la DTR. La DTR contiene también los diversos parámetros de seguridad enviados desde el terminal receptor al terminal emisor.

– DNK: Acuse de recibo incorrecto digital (*digital not acknowledge*)

Las señales DER, DES, DEC o DTR están estructuradas en tramas de control para enlace de datos de alto nivel (HDLC).

La señal DNK indica que la instrucción anterior (DER, DES, DEC o DTR) no ha sido recibida de manera satisfactoria y que las tramas especificadas en el FIF de la propia DNK han de ser transmitidas de nuevo. La DNK puede ser emitida por el terminal emisor o por el terminal receptor (al contrario que la petición de página parcial (PPR) del anexo A/T.30, que sólo puede ser enviada por el terminal receptor).

La DNK se utiliza también para rechazar la verificación del acondicionamiento (TCF).

– TNR: Transmisor no preparado (*transmitter not ready*)

Esta señal se utiliza para indicar que el transmisor todavía no está preparado para transmitir.

Formato:

FCF: X101 0111 (X es el bit definido en 5.3.6.1/T.30).

– TR: ¿Transmisor preparado? (*transmitter ready?*)

Esta señal se utiliza para preguntar cuál es la situación del transmisor.

Formato:

FCF: X101 0110 (X es el bit definido en 5.3.6.1/T.30).

– PPS-PSS: Señal de página parcial-Señal de firma presente (*partial page signal-present signature signal*)

Esta señal se utiliza para indicar el final del documento y que sigue una señal de firma digital.

Formato:

FCF1: X111 1101 (X es el bit definido en 5.3.6.1/T.30).

FCF2: 1111 1000.

La codificación particular de DER, DES, DEC, DTR y DNK se detalla más adelante en el presente anexo.

H.6.1.1 Estructura de DER, DES, DEC y DTR

H.6.1.1.1 Generalidades

Las señales DER, DES, DEC y DTR están estructuradas en tramas HDLC.

La estructura de la secuencia de tramas sigue las mismas reglas que las de las instrucciones multitramas ya especificadas en la Recomendación T.30 (por ejemplo, NSF-CSI-DIS). Dichas reglas se describen en 5.3.1, 5.3.3, 5.3.4 y 5.3.5 de la Recomendación T.30.

H.6.1.1.2 FCF (campo de control facsímil)

El FCF de las tramas es como sigue:

– tramas DES: 0000 0101

– tramas DEC: 1100 1001

– tramas DER: 1100 1010

– tramas DTR: 1000 1000

H.6.1.1.3 Campo de información facsímil (FIF)

Las especificaciones para el FIF de DES, DEC, DER y DTR en el ámbito de aplicación del anexo H son como sigue:

La longitud máxima del FIF de una trama es de 65 octetos. Si la trama es una trama intermedia (no la última), su FIF debe tener una longitud de 65 octetos, **excepto cuando el contenido de la trama es "FIF de DCS"** (véase más adelante). En este caso, la trama es tan larga como haga falta para contener los octetos del FIF de la DCS, pero no más (no se permiten octetos de justificación).

Si se trata de la última trama, la longitud del FIF puede ser inferior a 65 octetos, dependiendo del número de octetos de datos que haya que llevar. No se permiten octetos de justificación.

El primer octeto del FIF de cada trama contiene el número de trama, a lo que sigue el campo de datos. El número de trama es un número binario de ocho bits. Se aplica la regla general del FIF de las señales DES/DEC/DER/DTR: el bit menos significativo del número de trama (bit situado más a la derecha) es el que se transmite primero.

La trama cuyo número es "0" se transmite en primer lugar.

La figura H.2/T.30 ilustra estos principios.

NOTA – El uso de tramas con FIF de longitud superior a los 65 octetos queda en estudio.

Preámbulo	Dirección HDLC	Campo de control	Campo de control facsímil	FIF		FCS	Bandera(s)	Dirección HDLC	Campo de control	Campo de control facsímil	FIF		FCS	Bandera(s)
Banderas	1111 1111	1100 X000 X = 0 (no trama final)	DEC = 1100 1001	Número de trama 0000 0000	Campo de datos de 64 octets	FCS	Al menos una bandera	1111 1111	1100 X000 X = 1 (trama final)	DEC = 1100 1001	Número de trama 0000 0001	Campo de datos ≤ 64 octets	FCS	Al menos una bandera

NOTA 1 – El FCF se transmite de tal modo que el bit situado más a la izquierda (según se muestra en la figura) es el bit que se transmite primero.

NOTA 2 – El número de trama se transmite de tal modo que el bit situado más a la derecha (según se muestra en la figura) es el bit que se transmite primero.

Por ejemplo, para el número de trama de la segunda trama:

1000 0000

Orden de transmisión ===>

NOTA 3 – **El campo de datos de la trama "0" puede ser de menos de 64 octetos si contiene el "FIF de DCS".**

Figura H.2/T.30 – Ejemplo para una DEC que consta de dos tramas

H.6.1.2 Utilización y estructura de la señal DNK

H.6.1.2.1 Estructura de la señal DNK

Definición

En el resto del presente anexo, los términos "señal X" o "X" designan cualquiera de las señales DER, DES, DEC o DTR.

Cuando algunas tramas de la "señal X" recibidas son defectuosas, la señal DNK permite pedir la retransmisión de esas tramas específicas.

La señal DNK se utiliza también para rechazar la TCF. Véase más adelante.

NOTA – Cuando todas las tramas de una señal X han sido recibidas correctamente, se utiliza la respuesta normal (especificada en este anexo) como un acuse de recibo implícito, excepto si se ha de rechazar la TCF (para este rechazo se utiliza la señal DNK).

La señal DNK consta de una trama HDLC cuya estructura sigue las mismas reglas que para las demás señales de la Recomendación T.30 (reglas descritas en 5.3.1, 5.3.3, 5.3.4 y 5.3.5 de la Recomendación T.30).

H.6.1.2.2 FCF de DNK

El FCF es como sigue: X101 1001

La definición del bit X figura en 5.3.6.1/T.30.

H.6.1.2.3 FIF de DNK

H.6.1.2.3.1 Generalidades

El FIF consta de un número entero de octetos.

En cada octeto del FIF de la señal DNK, el bit situado más a la izquierda (según se escribe) es el bit que se transmite primero. Su número de bit es el "0".

El orden de transmisión correspondiente a la numeración de los bits es como sigue:

Bit N.º 01234567 01234567 01234567 …

orden de transmisión ========>

El primer octeto de la señal DNK se utiliza para rechazar la TCF cuando sea necesario (la TCF recibida está degradada).

Los demás octetos se utilizan para pedir tramas recibidas con error.

H.6.1.2.3.2 Petición de tramas recibidas con error

Empezando con el segundo octeto del FIF, cada bit corresponde a una trama de la instrucción o respuesta enviada previamente, es decir, el primer bit transmitido corresponde a la primera trama, etc. Para tramas recibidas correctamente, el bit correspondiente se pondrá a "0"; el bit de las tramas recibidas incorrectamente se pondrá a "1". Se añadirán bits de justificación de valor "1", según se requiera, para alinear con el límite del último octeto.

Al igual que en el modo ECM descrito en el anexo A/T.30 (pero aquí a la velocidad de modulación del protocolo), si se transmite más de una señal DNK (tras varios intentos fallidos de transmitir las tramas X), el bit correspondiente a una trama X que ya ha sido recibida correctamente se debe poner siempre a "0".

NOTA 1 – Puede ocurrir que la señal DNK sea reenviada con un FIF de tamaño diferente.

Por ejemplo: la señal X se recibe con muchos errores y se observa que sólo tiene siete tramas de longitud, mientras que su longitud real es de nueve tramas. En este caso, el FIF de la señal DNK sólo contendrá dos octetos (el primero es el que se utiliza para rechazar la TCF – véase más adelante – y con el segundo basta para indicar las tramas detectadas con error). Una vez reemitidas las tramas de la señal X, el aparato receptor comprueba que la señal X tiene una longitud de nueve tramas. Si ocurre de nuevo que algunas tramas están degradadas, se envía una nueva señal DNK con tres octetos en su FIF. Este ejemplo se ilustra más abajo.

NOTA 2 – Hay que señalar que el terminal que recibe la señal X puede localizar la última trama con el bit "x" del campo de control HDLC (puesto a "1").

Ejemplo con una DEC recibida defectuosa (el mismo ejemplo es aplicable a una señal DES, DER o DTR degradada)

---------->

DEC

9 tramas <----------

DNK con FIF de 2 octetos de longitud:

```
Bit N.º  0123   4567   01234567
         xxxx   xxx0   10101111
```

primer octeto para rechazo de TCF
(véase la explicación más adelante)
tramas 0, 2, 4, 5 y 6 recibidas defectuosas
tramas 7 y 8 no recibidas
(el último bit "1" es sólo para alineación de octetos)

---------->

DEC

tramas 0, 2, 4, 5, 7 y 8 <----------

DNK con FIF de 3 octetos de longitud:

```
Bit N.º  0123   4567   01234567  01234567
         xxxx   xxx0   10000000  01111111
```

sólo la trama 0 se recibe defectuosa

---------->

DEC

trama 0 <----------

trama recibida correctamente
respuesta normal = acuse de recibo implícito
(depende del contexto)

H.6.1.2.3.3 Tiempo máximo para la retransmisión de la señal X tras la ocurrencia de los DNK

En relación con la retransmisión de la señal X tras la ocurrencia de varios DNK (acuses de recibo incorrecto digitales), se define el temporizador "prevención de fallos" llamado Tx.

– El temporizador Tx de prevención de fallos tiene la siguiente temporización:

  Tx = 60 s ± 5 s.

– En el transmisor de la señal X, el temporizador Tx se arranca en el momento del reconocimiento del primer DNK y se detiene en el momento del reconocimiento de la respuesta normal o de FNV.

– Si expira el temporizador Tx, el transmisor de la señal X envía una instrucción de desconectar (DCN) para la liberación de la llamada.

H.6.1.2.3.4 Rechazo especifico mediante una señal DNK

El bit situado más a la izquierda del primer octeto del FIF de una señal DNK (numerado "N.º 0" en el cuadro H.2/T.30) se utiliza para el rechazo de la TCF (TCF degradada); su cometido es equivalente al de la señal de fallo de acondicionamiento (FTT) en modo normal de la Recomendación T.30.

El rechazo de la TCF definido en el cuadro H.2/T.30 no se puede combinar con la indicación de las tramas X recibidas con error, a las que se refiere en H.6.1.2.3.2/T.30.

El proceso de rechazo es secuencial y se efectúa como sigue:

1) Primeramente, todas las tramas degradadas de la DEC (o DES, o DER, o DTR) son solicitadas por la señal DNK. El bit N.º 7 y el bit N.º 0 del primer octeto de la DNK se ponen a "0" (el bit N.º 0 no tiene significado en esta etapa).

2) Una vez corregidas todas las tramas, el contenido de la DEC (o DES, o DER, o DTR) puede ser rechazado por FNV si es necesario (véase más adelante);

   o si el contenido de la DEC es correcto y en el case de que la TCF que sigue a la DEC está degradada, la TCF es rechazada por el primer octeto de la DNK.

Cuadro H.2/T.30 – Rechazo específico mediante el primer octeto del FIF de la señal DNK

Rechazo específico	Codificación del primer octeto del FIF de la señal DNK
TCF degradada (equivalente a la FTT en modo normal)	Bit N.º 0 1 2 3 4 5 6 7 1 x x x x x x x
Los bits 1 a 6 se reservan para uso futuro	Bit N.º 0 1 2 3 4 5 6 7 x x x x x x x x
El bit N.º 7 se debe poner a "1" si todas las tramas se han recibido correctamente y la señal DNK se envía solamente para rechazar la TCF. Si el bit N.º 7 se pone a "1", los octetos que siguen al primero no son enviados.	Bit N.º 0 1 2 3 4 5 6 7 x x x x x x x 1

Precisiones:

– Como se ha precisado en este anexo, los bits del FIF de DCS están colocados en la primera trama HDLC de la DEC.

– En cuanto a las otras tramas, la trama N.º 0 de una DEC que contiene el FIF de DCS sólo vuelve a emitirse cuando lo solicite la DNK (si esta trama se ha recibido incorrectamente). Esta regla tiene una excepción cuando se rechaza la TCF: en tal caso, la trama N.º 0 deberá enviarse siempre junto con la TCF, véase ejemplo más adelante.

Ejemplo con una DEC seguida de una TCF

---------->

DEC de 3 tramas

————————>

TCF <----------

DNK con FIF de 2 octetos de longitud:

Bit N.º 01234567 01234567

00000000 01011111

trama 1 recibida incorrectamente,
tramas 0 y 2 recibidas correctamente

---------->

DEC de 1 trama:
trama 1

————————>

TCF <----------

DNK con FIF de longitud de 1 octeto:

Bit N.º 01234567

10000001

trama 1 recibida correctamente
Rechazo de TCF

---------->

DEC de una trama:

trama 0 (contiene FIF de DCS)

————————>

TCF <----------

trama 0 recibida correctamente y TCF correcta
respuesta normal = acuse de recibo implícito
(depende del contexto)

H.6.1.3 Precisiones para la utilización de la señal FNV en el presente anexo H

La señal de campo no válida (FNV, *field not valid*) definida en 5.3.6.2.12/T.30 sólo se utiliza cuando se satisface la siguiente condición:

– No hay ninguna trama de una señal X pendiente de corrección.

Ejemplo

---------->

DEC de 3 tramas

————————>

TCF <----------

DNK con FIF de 2 octetos de longitud:

```
Bit N.º  01234567  01234567
         00000000  01011111
```

trama 1 recibida incorrectamente,
tramas 0 y 2 recibidas correctamente

---------->

DEC de 1 trama:
trama 1

————————>

TCF <----------

trama 1 recibida correctamente
FNV (porque hay un error en el contenido de parámetro)

H.6.1.4 Codificación de datos dentro de los FIF de las DER, DES, DEC y DTR

H.6.1.4.1 Supergrupos y grupos

La secuencia de los campos de información facsímil de las señales DER, DES, DEC y DTR se estructura en grupos y supergrupos.

Los grupos son conjuntos de atributos de terminal o sesión, similares o conexos, que a menudo será preciso negociar al mismo tiempo.

Los supergrupos proporcionan una jerarquía adicional, de tal modo que los grupos de atributos conexos pueden mantenerse juntos.

La secuencia general de los supergrupos y grupos que pueden ser presentados en la secuencia de los campos de información facsímil de las señales DER, DES, DEC y DTR es como sigue:

SG1[G1..G2...G3...]SG2[G1..G2..G3...]...SGN[G1..G2..G3...]

donde SG indica supergrupos y G indica grupos.

Los supergrupos se identifican mediante rótulos de supergrupo, llamados también en este anexo "superrótulos".

Los supergrupos contienen grupos identificados mediante rótulos de grupo, a los que en el presente anexo se denomina simplemente "rótulos".

Un superrótulo va seguido por la longitud del supergrupo que identifica y, a continuación, por la secuencia de los grupos y supergrupos.

El rótulo que identifica cada grupo va seguido por la longitud de ese grupo y, a continuación, por el contenido del mismo.

Notaciones:

– En este anexo, el contenido del grupo se llama "parámetro".

– La longitud del grupo se llama "longitud del valor de parámetro".

– El valor del contenido del grupo se llama "valor de parámetro".

H.6.1.4.2 Asignación de rótulo

1) Los superrótulos tienen una longitud de 8 bits

   Un valor de rótulo inicial de FF en hexadecimal indica una extensión de 8 bits adicionales (puede ser utilizada en futuras versiones de este anexo).

2) Los rótulos tienen una longitud de 8 bits. El principio de extensión aplicado es el mismo que se utiliza para los superrótulos.

H.6.1.4.3 Longitud de los supergrupos y longitud de los grupos

La cuenta se hace en unidades de octetos. El primer octeto después del superrótulo o rótulo contiene el número de octetos que siguen. Si el octeto de cuenta inicial es 0, los dos octetos después del de cuenta indican el número de octetos que siguen.

Ejemplo: para un valor de parámetro con una longitud de 20 octetos, el octeto de longitud será: "00010100".

Ejemplo: para un valor de parámetro con una longitud de 257 octetos, los octetos de longitud serán: "0000 0000 0000 0001 0000 0001".

Se aplica la regla general del FIF de las señales DES/DEC/DER/DTR: el bit situado más a la derecha de cada octeto según se representa por escrito (el bit menos significativo) es el bit que se transmite primero.

H.6.1.4.4 Reglas de codificación:

A continuación se hace una descripción formal de las reglas de codificación para codificar los campos de información facsímil de las señales DER, DES, DEC y DTR, en forma Backus-Naur (BNF):

REGLAS DE CODIFICACIÓN PARA SINTAXIS DE CODIFICACIÓN DE RÓTULOS FACSÍMIL

<bit>	::=	<0> | <1>
<octet>	::=	<bit><bit><bit><bit><bit><bit><bit><bit>
<8_bit_tag>	::=	<octet>
<extend_octet>	::=	{< 1><1><1><1><1><1><1><1>}
<tag>	::=	<8_bit_tag> | <extend_octet> | <8_bit_tag><8_bit_tag>
<parameter_value>	::=	<octet>{<octet>}
<count_extend_octet>	::=	<0><0><0><0><0><0><0><0>
<parameter_length>	::=	<octet> | <count_extend_octet> <octet> <octet>
<Group>	::=	<tag><parameter_length><parameter_value>
<frame_number>	::=	<octet>
<Supergroup_tag>	::=	<tag>
<Supergroup_length>	::=	<parameter_length>
<Supergroup>	::=	<Supergroup_tag> <Supergroup_length><Group>{<Group>}
<Tag_Encoded_Data>	::=	<Supergroup>{<Supergroup>}
<FIF>	::=	<frame_number>< Tag_Encoded_Data>

NOTA – Los Tag_Encoded_Data pueden extenderse a lo largo de múltiples tramas. Véase H.6.1.4.6/T.30.

H.6.1.4.5 Descripción de la forma Backus-Naur

Lo que sigue es una descripción de la sintaxis del estilo Backus-Naur que se utiliza en el apartado anterior.

Símbolo	Descripción de su utilización
literal	Un testigo (o componente) se indica mediante un literal.
::=	Operador de asignación de producción.
|	Símbolo utilizado para separar testigos alternativos o grupos de testigos.
< >	Un testigo no terminal se indica mediante un literal encerrado entre los caracteres "<" y ">".
[ ]	Un testigo o grupo de testigos facultativo se encierra entre los caracteres "[" y "]".
{ }	Un grupo de testigos encerrado entre "{" y "}" se puede repetir 0, 1 o más veces.

H.6.1.4.6 Relación entre la codificación de los FIF y la estructura de las tramas HDLC

La formatación de los superrótulos, rótulos y parámetros descritos más arriba es independiente de la estructura de las tramas HDLC descritas en H.6.1.1/T.30. La serie de octetos que constituye la secuencia de superrótulos, rótulos y parámetros correspondientes se inserta ordenadamente en el FIF de las tramas HDLC: primero se rellena el FIF de la primera trama (trama "0"), a continuación se rellena el FIF de la segunda trama "1", etc.

H.6.1.4.7 Supergrupo de tramas encapsuladas

Se crea un supergrupo que reúne todos los grupos que contienen el FIF de las siguientes tramas usuales de la Recomendación T.30: DCS, TSI, SUB, SID, DTC, CIG, SEP y PWD, PSA.

Este supergrupo se denomina "Supergrupo de tramas encapsuladas".

El superrótulo que identifica a este supergrupo es: 0000 0001.

H.6.1.4.8 Los dos supergrupos de seguridad

Se crean dos supergrupos de seguridad:

– uno para el modo registro;

– otro para el modo transmisión segura.

H.6.1.4.9 Lista de superrótulos

Véase el cuadro H.3/T.30.

Cuadro H.3/T.30 – Lista de superrótulos

Código del superrótulo	Nombre del superrótulo	Descripción
0000 0001	Trama encapsulada (abreviatura: "E-F")	Este superrótulo es el del supergrupo de tramas encapsuladas que reúne todos los grupos que contienen el FIF de las tramas usuales de la Recomendación T.30.
0000 0010	Modo registro	Este superrótulo es el del supergrupo que reúne todos los grupos transmitidos en el modo registro.
0000 0011	Modo transmisión segura	Este superrótulo es el del supergrupo que reúne todos los grupos transmitidos en la comunicación facsímil segura.

H.6.1.4.10 Lista de los rótulos dentro del supergrupo de tramas encapsuladas

Véase el cuadro H.4/T.30.

H.6.1.4.11 Lista de rótulos para características de seguridad

Los rótulos siguientes pueden ser introducidos por:

- los superrótulos de seguridad "modo registro"; o
- "modo transmisión segura".

Algunos de los parámetros se utilizan sólo al nivel de mensaje ("página de seguridad", véase más adelante); se indican mediante un "*" en el cuadro H.5/T.30.

H.6.1.4.12 Orden de superrótulos y rótulos

En la secuencia de superrótulos, rótulos y valores de parámetros, el orden es como sigue:

– el supergrupo de tramas encapsulada se transmite antes que los supergrupos de seguridad;

– dentro de cada supergrupo, el orden de los rótulos no está fijado, con la salvedad de que:

  - dentro del supergrupo de tramas encapsuladas, el rótulo "**FIF de DCS" debe ser transmitido el primero** (si está presente); esto es así para mayor facilidad en caso de reemisión después de una TCF rechazada [el campo de datos de la primera de trama DEC que contiene (y contiene solamente) "FIF de DCS" **es de longitud inferior a 64 octetos**];

– dentro de cada secuencia de rótulos (y valores de parámetros) introducida por los superrótulos de seguridad, el orden de los rótulos no está fijado.

Cuadro H.4/T.30 – Lista de los rótulos dentro del supergrupo de tramas encapsuladas

Código del rótulo	Nombre del rótulo	Descripción
1000 0011	FIF de DCS	Este rótulo delimita la zona en la que están situados los bits correspondientes a la FIF de la DCS (bits del cuadro 2/T.30).
0100 0011	FIF de TSI	Este rótulo delimita la zona en la que están situados los bits correspondientes a la FIF de la TSI (cuando se utiliza).
1100 0011	FIF de SUB	Este rótulo delimita la zona en la que están situados los bits correspondientes a la FIF de la SUB (cuando se utiliza).
1010 0011	FIF de SID	Este rótulo delimita la zona en la que están situados los bits correspondientes a la FIF de la SID (cuando se utiliza).
1000 0001	FIF de DTC	Este rótulo delimita la zona en la que están situados los bits correspondientes a la FIF de la DTC (cuando se utiliza).
0100 0001	FIF de CIG	Este rótulo delimita la zona en la que están situados los bits correspondientes a la FIF de la CIG (cuando se utiliza).
1100 0001	FIF de PWD	Este rótulo delimita la zona en la que están situados los bits correspondientes a la FIF de la PWD (cuando se utiliza).
1010 0001	FIF de SEP	Este rótulo delimita la zona en la que están situados los bits correspondientes a la FIF de la SEP (cuando se utiliza).
0110 0001	FIF de PSA	Este rótulo delimita la zona en la que están situados los bits correspondientes a la FIF de la PSA (cuando se utiliza).

H.6.1.4.13 Codificación del parámetro "servicios de seguridad"

El cuadro H.6/T.30 da la codificación del valor de parámetro que sigue al rótulo "servicios de seguridad" y el octeto de longitud pertinente.

El octeto de longitud es "0000 0001" (la longitud del parámetro es de sólo un octeto). En próximas versiones de este anexo, el parámetro podrá ser más largo.

Cuadro H.5/T.30 – Lista de rótulos para características de seguridad

Código del rótulo		Nombre del rótulo	Descripción
0001 0001		S	Identidad del emisor
0001 0010		Sp	Clave pública del emisor
0001 0011		Ss	Clave secreta del emisor
0001 0100		SpE	Clave pública de cifrado del emisor
0001 0101		SsE	Clave secreta de cifrado del emisor
0001 0110		R	Identidad del receptor
0001 0111		Rp	Clave pública del receptor
0001 1000		Rs	Clave secreta del receptor
0001 1001		RpE	Clave pública de cifrado del receptor
0001 1010		RsE	Clave secreta de cifrado del receptor
0001 1011		Srd/Rra	Número aleatorio creado respectivamente por el emisor para la firma digital y por el receptor para la autenticación del emisor
0001 1100		BE = RpE[S, Ks]	Identidad del emisor y clave de sesión cifrada por RpE
0001 1101		UTCd	Fecha/hora elegida por el emisor (fecha/hora de la generación/firma del documento)
0001 1110		UTCr	Fecha/hora elegida por el receptor (fecha/hora de la confirmación de recepción del mensaje)
0001 1111		Lm	Longitud del documento
0010 0000		Testigo 2 = Ss[h(Sra, Rra, R), Sia]	Testigo utilizado para la autenticación del emisor cuando no se ha invocado el servicio [confidencialidad del mensaje + establecimiento de clave de sesión]
0010 0001		Testigo 2-enc. = Ss[h(Sra, Rra, R, BE), Sia]	Testigo utilizado para la autenticación del emisor cuando se ha invocado el servicio [confidencialidad del mensaje + establecimiento de clave de sesión]
0010 0010		Testigo 3 = Rs[h(Rra, Sra, S), Ria]	Testigo utilizado para la autenticación del receptor
0010 0011		Testigo 4 = Ss[h(Srd, UTCd, Lm, R, h(document)), Sis]	Testigo utilizado para facilitar la integridad del mensaje cuando no se ha invocado el servicio [confidencialidad del mensaje + establecimiento de clave de sesión]
0010 0100		Testigo 4-enc. = Ss[h(Srd, UTCd, Lm, R, BE, h(enc.document)), Sis]	Testigo utilizado para facilitar la integridad del mensaje cuando se ha invocado el servicio [confidencialidad del mensaje + establecimiento de clave de sesión]
0010 0101		Testigo 5 = Rs[h(Srd, UTCr, Lm, S, h(document)), Ris]	Testigo utilizado para confirmar la recepción del mensaje cuando no se ha invocado el servicio [confidencialidad del mensaje + establecimiento de clave de sesión]
0010 0110		Testigo 5-enc. = Rs[h(Srd, UTCr, Lm, S, BE, h(enc.document)), Ris]	Testigo utilizado para confirmar la recepción del mensaje cuando se ha invocado el servicio [confidencialidad del mensaje + establecimiento de clave de sesión]
0010 0111		Servicios de seguridad	Servicios de seguridad
0010 1000		Mecanismos de seguridad	Mecanismo de gestión de claves, funciones troceado y algoritmos de cifrado
0010 1001		Capacidad de longitudes facultativas	Capacidad de longitudes facultativas
0010 1010		Petición de capacidades de seguridad	Al utilizar este rótulo (y el parámetro pertinente), el terminal pide al terminal distante que le indique sus capacidades de seguridad
0010 1011		Acuse de recibo	Acuse de recibo utilizado en el modo registro
0010 1100	*	Indicador de página de seguridad	Indica que la página es la página de seguridad
0010 1101	*	Identificación del tipo de página de seguridad	Indica el número de la versión de la página de seguridad En las próximas versiones del presente anexo puede haber otros tipos de página de seguridad a los que se les dará otros números de versión
0010 1110	*	Trayecto de certificación	Trayecto de certificación
0010 1111		Características no normalizadas	Características no normalizadas
NOTA – El rótulo facultativo "características no normalizadas" puede utilizarse sobre la base del reconocimiento de códigos de identificación en la NSF. La información contenida en los octetos iniciales del valor de parámetro "características no normalizadas" será coherente con las reglas de identificación definidas en 5.3.6.2.7/T.30 (Capacidades no normalizadas NSF, NSC, NSS).			

Cuadro H.6/T.30 – Parámetro "Servicios de seguridad"

Servicios de seguridad	Clasificación	Codificación del campo
Autenticación mutua	Obligatorio	Bit N.º 7 6 5 4 3 2 1 0 x x x x x x x x No es necesaria la asignación de bits porque es obligatorio
Servicio de seguridad que incluye: • Autenticación mutua • Integridad del mensaje • Confirmación de la recepción del mensaje	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x x x x x x x 1
Servicio de seguridad que incluye: • Autenticación mutua • Confidencialidad del mensaje (criptación) • Establecimiento de clave de sesión	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x x x x x x 1 x
Servicio de seguridad que incluye: • Autenticación mutua • Integridad del mensaje • Confirmación de la recepción del mensaje • Confidencialidad del mensaje (criptación) • Establecimiento de clave de sesión	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x x x x x x 1 1
NOTA 1 – El servicio de registro no necesita asignación de bits porque es obligatorio. NOTA 2 – Si no hay servicio facultativo, la asignación de bits es "0000 0000". NOTA 3 – Si el servicio de seguridad "autenticación mutua" sólo lo selecciona el emisor (para el modo transmisión facsímil segura), no se envía el parámetro "servicios de seguridad" (porque el servicio básico es "autenticación mutua").		

Los cuatro conjuntos de servicios descritos en el cuadro H.6/T.30 se muestran en el cuadro H.7/T.30 en el que se identifican cuatro perfiles de servicio:

Cuadro H.7/T.30 – Perfiles de seguridad en el presente anexo H

Servicios de seguridad	Perfiles de servicio			
	1	2	3	4
Autenticación mutua	X	X	X	X
• Integridad del mensaje • Confirmación de la recepción del mensaje		X		X
• Confidencialidad del mensaje (criptación) • Establecimiento de clave de sesión			X	X

H.6.1.4.14 Codificación del parámetro "mecanismos de seguridad"

El cuadro H.8/T.30 da la codificación del valor de parámetro que sigue al rótulo "mecanismos de seguridad" y el octeto de longitud pertinente.

El octeto de longitud depende del número de algoritmos de cifrado facultativos que se indican (véase el cuadro H.8/T.30).

Para la negociación:

– si lo solicita el terminal emisor, el terminal receptor indica el mecanismo de seguridad que admite enviando el parámetro "mecanismo de seguridad";

– el terminal emisor selecciona el mecanismo de seguridad para la sesión: una función troceado, un (o ningún) algoritmo de cifrado.

En la "página de seguridad" (véase más adelante), el parámetro "mecanismos de seguridad" indica también los mecanismos de seguridad que han sido seleccionados para la sesión.

Cuadro H.8/T.30 – Parámetro "Medidas de seguridad"

Mecanismos	Clasificación	Codificación del campo
Versión del sistema de seguridad	Obligatorio	Bit N.º 7 6 5 4 3 2 1 0 x x x x x x 0 0 (Nota)
SHA-1 (función troceado)	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x x x x x 1 x x
MD-5 (función troceado)	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x x x x 1 x x x
Página de seguridad	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x x x 1 x x x x
SAFER K-64 (algoritmo de cifrado)	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x x 1 x x x x x
FEAL-32 (algoritmo de cifrado)	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x 1 x x x x x x
RC5 (algoritmo de cifrado)	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 1 x x x x x x x
Segundo octeto	Facultativo	
IDEA (algoritmo de cifrado)	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x x x x x x x 1
HFX40	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x x x x x x 1 x
DSA (gestión de claves)	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x x x x x 1 x x
Los bits 3 a 7 se reservan para uso futuro (puestos a "0")		Bit N.º 7 6 5 4 3 2 1 0 x x x x x x x x
.....	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x x x x x x x x
Último octeto	Facultativo	Bit N.º 7 6 5 4 3 2 1 0 x x x x x x x x

NOTA – Cuando aparezcan nuevas versiones del sistema de seguridad del anexo H/T.30, se deberá mantener la retrocompatibilidad.

El segundo octeto es facultativo.

Los octetos del tercero al último también, que también son facultativos, pueden estar ausentes.

Cada uno de estos octetos codifica un algoritmo de cifrado facultativo disponible en el terminal receptor. El octeto es el número de un algoritmo de cifrado registrado en el índice de entradas del anexo 2 a ISO/CEI 9979 (sobre "procedimiento de registro de algoritmos criptográficos"); dicho número está codificado en binario, (por ejemplo, "0000 0000" para la entrada N.º 00).

Cuando el terminal emisor selecciona los mecanismos, el parámetro "mecanismos de seguridad" suele tener una longitud de sólo uno o dos octetos. El tercer octeto sólo se necesita en caso de que se seleccione un algoritmo de cifrado registrado en ISO/CEI 9979 y que no sea ninguno de los siguientes: SAFER K-64, FEAL-32, RC5, IDEA y HFX40 (el tercer octeto indica el algoritmo seleccionado).

H.6.1.4.15 Codificación del parámetro "capacidad de longitudes facultativas"

H.6.1.4.15.1 Principo

Para indicar las capacidades de longitudes facultativas se envía el rótulo "capacidad de longitudes facultativas", el octeto de longitud y el valor de parámetro correspondiente.

H.6.1.4.15.2 Codificación del parámetro "Capacidad de longitudes facultativas"

Para codificar el parámetro se definen los principios que se indican a continuación:

– Mediante los desplazamientos se indican las longitudes máximas que pueden ser procesadas por el terminal.

  Los desplazamientos se codifican en binario, en 4 bits u 8 bits, dependiendo del parámetro de que se trate.

– La utilización de los desplazamientos se hace siguiendo un orden específico:

Octeto N.° 0							
Bit N.°	7	6	5	4	3	2	1	0
desplazamiento a				desplazamiento b			
Octeto N.° 1							
Bit N.°	7	6	5	4	3	2	1	0
desplazamiento c				reservado			

En primer lugar, el octeto N.º 0, que contiene:

– primero, el desplazamiento "a" (4 bits) para indicar la longitud máxima de las claves pública y secreta aceptadas;

– después, el desplazamiento "b" (4 bits) para indicar la longitud de los números aleatorios aceptados (Sra, Srd, Rra).

Seguidamente, el octeto N.º 1 (facultativo) que contiene:

– el desplazamiento "c" (4 bits) para indicar la longitud máxima de las claves pública y secreta de cifrado aceptadas.

Así pues, el octeto de longitud del parámetro "capacidad de longitudes facultativas" es "0000 00001" (1 octeto de longitud si no se ofrece el servicio [confidencialidad del mensaje + establecimiento de clave de sesión]) ó "0000 0001" (2 octetos si se ofrece el servicio [confidencialidad del mensaje + establecimiento de clave de sesión]). En las próximas versiones de este anexo, el parámetro podrá ser más largo.

H.6.1.4.15.3 Reglas para la utilización de los desplazamientos

Longitud máxima (en octetos) de las claves pública y secreta =

$$64 \text{ (longitud básica)} + ([\text{desplazamiento a}] \times 16) \quad \text{octetos}$$

$$\text{con } 0 \leq \text{desplazamiento a} \leq 4 \quad \text{octetos}$$

El terminal debe ser capaz de tratar todas las longitudes comprendidas entre la longitud básica y la longitud máxima, por incrementos de 16 octetos.

Longitud máxima (en octetos) de números aleatorios =

$$8 \text{ (longitud básica)} + [\text{desplazamiento b}] \quad \text{octetos}$$

$$\text{con } 0 \leq \text{desplazamiento b} \leq 8 \quad \text{octetos}$$

El terminal debe ser capaz de tratar todas las longitudes comprendidas entre la longitud básica y la longitud máxima.

Longitud máxima (en octetos) de las claves pública y secreta de cifrado =

$$64 \text{ (longitud básica)} + ([\text{desplazamiento c}] \times 16) \quad \text{octetos}$$

$$\text{con } 0 \leq \text{desplazamiento c} \leq 4 \quad \text{octetos}$$

El terminal debe ser capaz de tratar todas las longitudes comprendidas entre la longitud básica y la longitud máxima, por incrementos de 16 octetos.

H.6.1.4.15.4 Ejemplos

Ejemplo 1

Octeto N.° 0								
Bit N.°	7	6	5	4	3	2	1	0
	0	0	0	1	0	0	0	0
Octeto N.° 1								
Bit N.°	7	6	5	4	3	2	1	0
	0	0	0	1	0	0	0	0

En este ejemplo:

– Longitud máxima de las claves pública y secreta = 64 + 16 × 1 = 80 octetos

– Longitud máxima de los números aleatorios = 8 + 0 = 8 octetos (no se admite longitudes facultativas)

– Longitud máxima de las claves pública y secreta de cifrado = 64 + 16 × 1 = 80 octetos

Ejemplo 2

Octeto N.° 0								
Bit N.°	7	6	5	4	3	2	1	0
	0	0	0	0	0	0	0	0

En este ejempl, el terminal indica las capacidades básicas solamente.

H.6.1.4.16 Codificación del parámetro "Petición de capacidades de seguridad"

Utilizando este rótulo (y el parámetro pertinente), el terminal pide al terminal distante que indique sus capacidades de seguridad. Véase el cuadro H.9/T.30.

El octeto de longitud es "0000 0001" (el parámetro tiene una longitud de sólo un octeto). En las próximas versiones de este anexo, el parámetro podrá ser más largo.

Cuadro H.9/T.30 – Parámetro "Petición de capacidades de seguridad"

Indicación de capacidades pedidas	Clasificación	Codificación del campo
Petición de "servicios de seguridad"	Facultativo	Bit N.° 7 6 5 4 3 2 1 0 x x x x x x x 1
Petición de "mecanismos de seguridad"	Facultativo	Bit N.° 7 6 5 4 3 2 1 0 x x x x x x 1 x
Petición de "capacidad de longitudes facultativas"	Facultativo	Bit N.° 7 6 5 4 3 2 1 0 x x x x x 1 x x
Petición de "características no normalizadas"	Facultativo	Bit N.° 7 6 5 4 3 2 1 0 x x x x 1 x x x
NOTA – Si se utiliza el parámetro "petición de capacidades de seguridad", al menos un bit se debe poner a "1" (si no es así, no existe la intención de utilizar este parámetro para la sesión).		

H.6.2 Modo registro

H.6.2.1 Esquema

El esquema se describe en la figura H.3/T.30. Comprende dos pasos:

– *Primer paso:*

  [La identidad del emisor y su clave pública son troceadas por el terminal emisor. La identidad del receptor y su clave pública son troceadas por el terminal receptor.]

  O/Y

  [(La identidad del emisor y su clave pública de cifrado son troceadas por el terminal emisor.)

  O/Y

  (La identidad del receptor y su clave pública de cifrado son troceadas por el terminal de receptor)].

  Los resultados del troceado se intercambian fuera de banda (de mano a mano directamente, por correo, por teléfono, etc.) y se almacenan en los terminales.

– *Segundo paso:*

  Intercambio, mediante el protocolo T.30, de las identidades y de las claves públicas entre las dos partes. Almacenamiento en los terminales.

El orden de los dos pasos no está fijado.

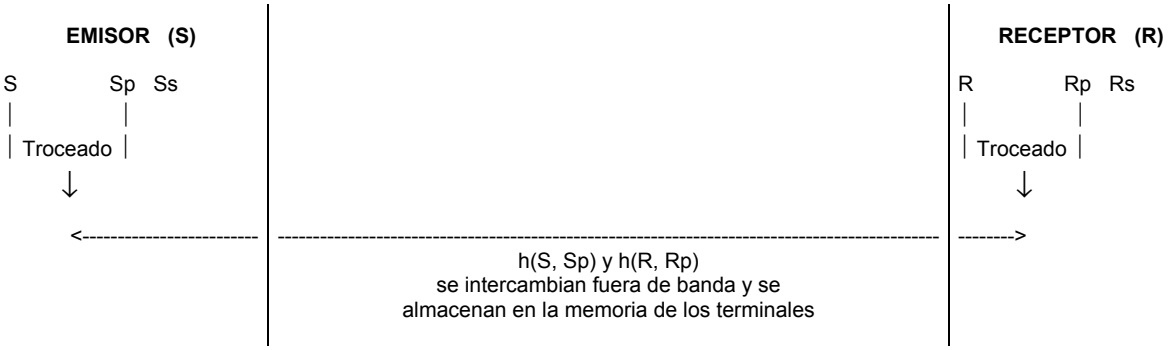
La validez de la identidad y de la clave o claves públicas de la otra parte se estima comparando el resultado del troceado intercambiado fuera de banda con el resultado del troceado de la identidad y de la clave o las claves públicas recibidas mediante el protocolo.

Una vez validados, estos valores (identidad y clave o claves públicas de la parte distante) se almacenan en los terminales y se utilizan para otras comunicaciones facsímil seguras con esa parte.

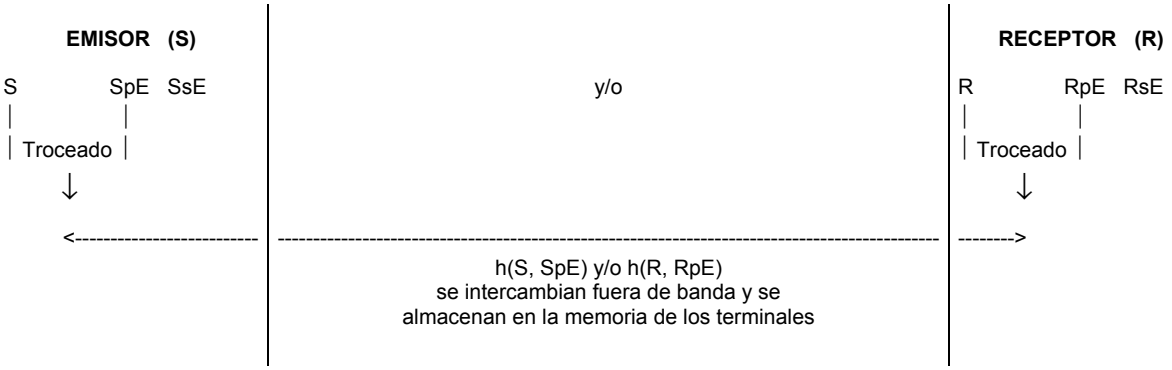
El registro de las claves públicas o de las claves públicas de cifrado o de unas y otras se fija mediante acuerdo entre los usuarios de los dos terminales. Para el cifrado de las claves públicas, el registro puede concernir solamente a uno de los usuarios o bien a ambos.

Los ajustes de los terminales para los registros pertinentes es un asunto local.

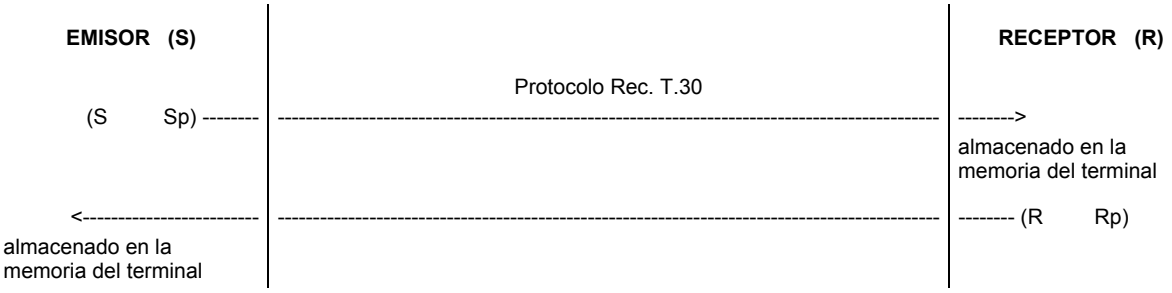
Intercambio de los resultados del troceado fuera de banda y su almacenamiento en los terminales.



En vez de, o además de a [S, Sp, h(S, Sp)] y [R, Rp, h(R, Rp)], la operación anterior puede concernir a [S, SpE, h(S, SpE)] y/o [R, RpE, h(R, RpE)]:



Establecimiento de la comunicación e intercambio de identidades y claves públicas mediante el protocolo de la Recomendación T.30.



En vez de, o además de, a [S, Sp] y [R, Rp], la operación anterior puede concernir a [S, SpE] y/o [R, RpE]:

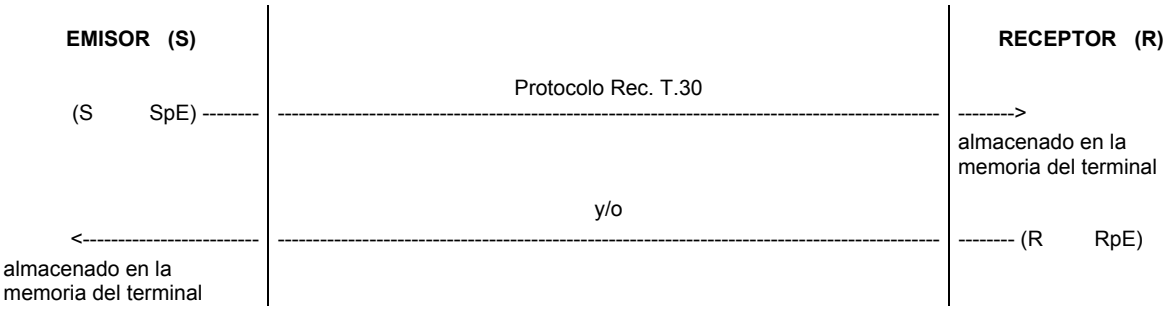
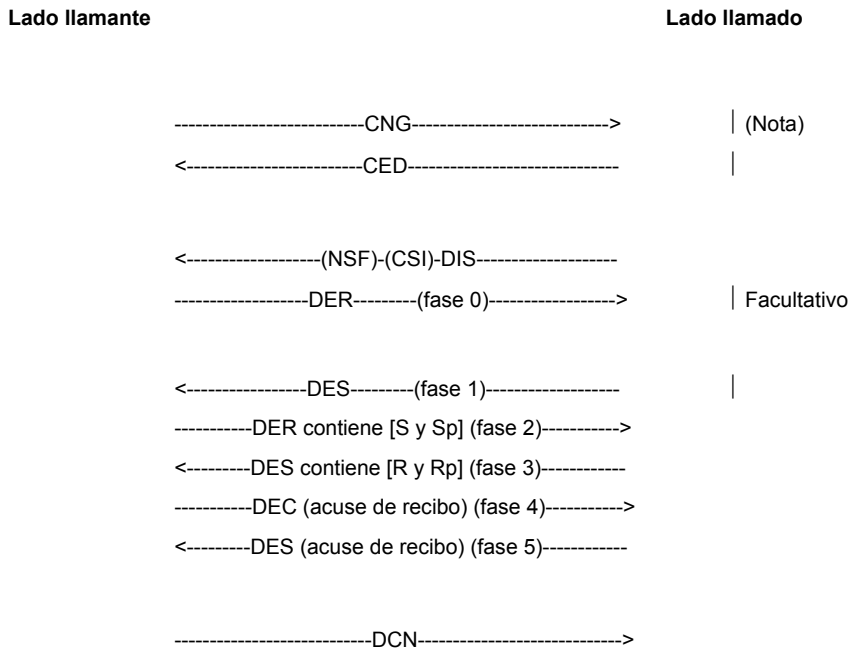


Figura H.3/T.30 – Esquema del modo registro

H.6.2.2 Utilización de DER, DES y DEC en el modo registro

En el segundo paso del modo registro, las señales DER, DES, DEC se utilizan en la figura H.4/T.30 como sigue:



NOTA – El establecimiento de la comunicación CNG/CED (tono de llamada/identificación de la estación llamada) que se muestra en la figura se da a título de ejemplo.

También pueden tener lugar los otros métodos de explotación definidos en 3.1.

En vez de, o además de, a Sp y Rp respectivamente, el método de explotación anterior puede concernir a SpE y/o RpE.

Los temporizadores utilizados en el anterior intercambio de señales son los mismos que los del protocolo T.30 normalizado (T1, T2, T4, …). Si no hay respuesta una vez transcurrida la temporización del T4, la instrucción del lado emisor (DER, DEC o DNK) es reenviada (para DER y DEC, solo las tramas de las que todavía no se ha acusado recibo).

Figura H.4/T.30 – Intercambio de señales para el modo registro

H.6.2.3 Asignación de bits en la DIS

En el cuadro 2/T.30 se muestra la asignación de bits en el FIF de la DIS para indicar las capacidades de seguridad en base al algoritmo RSA. Se utiliza el bit N.° 82.

H.6.2.4 Formato de los campos de información facsímil de las DER, DES y DEC para modo registro

Convenio

En las figuras del presente anexo, cuando el rótulo (y el octeto de longitud pertinente y el valor de parámetro) se representa en casillas sombreadas, su utilización es facultativa.

Cuando se representa en casillas en blanco, su utilización es obligatoria.

H.6.2.4.1 Fase 0 FACULTATIVA

Si el lado llamante no desea utilizar las capacidades facultativas, la fase 0 es facultativa; el modo registro sigue adelante con las características básicas (Sp y Rp tienen una longitud de 64 octetos, no hay intercambio de claves públicas de cifrado).

La secuencia contenida en el(los) FIF de la DER es:

Superrótulo "E-F"	Longitud de Supergrupo	Rótulo "FIF de SUB"	Longitud + contenido de "FIF de SUB"	Rótulo "FIF de SID"	Longitud + contenido de "FIF de SID"	Rótulo "FIF de TSI"	Longitud + contenido de "FIF de TSI"

Superrótulo "modo registro"	Longitud de supergrupo	Rótulo "petición de capacidades de seguridad"	Longitud + contenido de "petición de capacidades de seguridad"

Rótulo "características no normalizadas"	Longitud + contenido de "características no normalizadas"

Convenios

Por simplicidad, las representaciones de secuencias [superrótulos, rótulos, octetos de longitud y valores de parámetros] no describen la estructura HDLC interna de la señal [preámbulo, banderas, dirección, control, ..., secuencias de verificación de trama (FCS, *frame checking sequences*), banderas].

Una secuencia se puede representar mediante casillas en varias filas, para mayor comodidad; la secuencia es continua.

Las observaciones anteriores son aplicables al resto del anexo en donde figuren esas representaciones.

H.6.2.4.2 Fase 1 FACULTATIVA

La fase 1 tiene lugar sólo si existe la fase 0.

La secuencia contenida en el(los) FIF de la DES es:

Superrótulo "modo registro"	Longitud de supergrupo	Rótulo "servicios de seguridad"	Longitud + contenido de "servicios de seguridad"

Rótulo "mecanismos de seguridad"	Longitud + contenido de "mecanismos de seguridad"	Rótulo "capacidad de longitudes facultativas"	Longitud + contenido de "capacidad de longitudes facultativas"	Rótulo "características no normalizadas"	Longitud + contenido de "características no normalizadas"

La presencia de los grupos facultativos [rótulo, octeto de longitud y valor de parámetro] depende de las peticiones en la fase 0 (bits en el parámetro "petición de capacidades de seguridad").

H.6.2.4.3 Fase 2

La secuencia contenida en el(los) FIF de la DER es:

Superrótulo "E-F"	Longitud de supergrupo	Rótulo "FIF de SUB"	Longitud + contenido de "FIF de SUB"	Rótulo "FIF de SID"	Longitud + contenido de "FIF de SID"	Rótulo "FIF de TSI"	Longitud + contenido de "FIF de TSI"

Superrótulo "modo registro"	Longitud de supergrupo	Rótulo "S"	Longitud + contenido de "S"	Rótulo "Sp"	Longitud + contenido de "Sp"

Rótulo "SpE"	Octeto de longitud + contenido de "SpE"	Rótulo "mecanismos de seguridad"	Octeto de longitud + contenido de "mecanismos de seguridad	Rótulo "características no normalizadas"	Longitud + contenido de "características no normalizadas"

El anterior es un ejemplo de registro de Sp y SpE al mismo tiempo.

También es posible que se registre solamente Sp o SpE. S está presente en todos los casos.

Los ajustes de los terminales para los registros pertinentes es un asunto local.

El parámetro "mecanismos de seguridad" es obligatorio porque indica la función troceado seleccionada y/o el algoritmo de cifrado seleccionado (en caso de que se intercambien SpE y/o RpE).

H.6.2.4.4 Fase 3

La secuencia contenida en el(los) FIS de la DES es:

Superrótulo "modo registro"	Longitud de supergrupo	Rótulo "R"	Longitud + contenido de "R"	Rótulo "Rp"	Longitud + contenido de "Rp"

Rótulo "RpE"	Longitud + contenido de "RpE"

El anterior es un ejemplo de registro de Rp y RpE al mismo tiempo.

También es posible que se registre solamente Rp o RpE. R está presente en todos los casos.

Los ajustes de los terminales para los registros pertinentes es un asunto local.

Si cabe la posibilidad de que el terminal llamado encuentre que los parámetros S y Sp (y/o [S, SpE]) no están conformes con el valor resultante del troceado almacenado (en caso de que el intercambio de valores resultantes del troceado fuera de banda ya se haya realizado, véase H.6.2.1/T.30), puede rechazarlos mediante la señal FNV.

El motivo del error en FNV es "error de registro de clave pública" o "error de registro de clave pública de cifrado". Véase el cuadro H.10/T.30.

La utilización de la señal FNV para esa indicación de error se explica en H.6.7/T.30.

H.6.2.4.5 Fase 4

La secuencia contenida en el FIF de la DEC es:

Superrótulo "modo registro"	Longitud de supergrupo	Rótulo "Acuse de recibo"	Octeto de longitud "0000 0000"

Si cabe la posibilidad de que el terminal llamante encuentre que los parámetros R y Rp (y/o [R, RpE]) no están conformes con el valor resultante del troceado almacenado (en caso de que el intercambio de valores resultantes del troceado fuera de banda ya se haya realizado, véase H.6.2.1/T.30), puede rechazarlos mediante la señal FNV.

El motivo del error en la señal FNV es "error de registro de clave pública" o "error de registro de clave pública de cifrado". Véase el cuadro H.10/T.30.

La utilización de la señal FNV para esa indicación de error se explica en H.6.7/T.30.

H.6.2.4.6 Fase 5

La secuencia contenida en el FIF de la DES es:

Superrótulo "modo registro"	Longitud de supergrupo	Rótulo "Acuse de recibo"	Octeto de longitud "0000 0000"

H.6.3 Modo transmisión facsímil segura

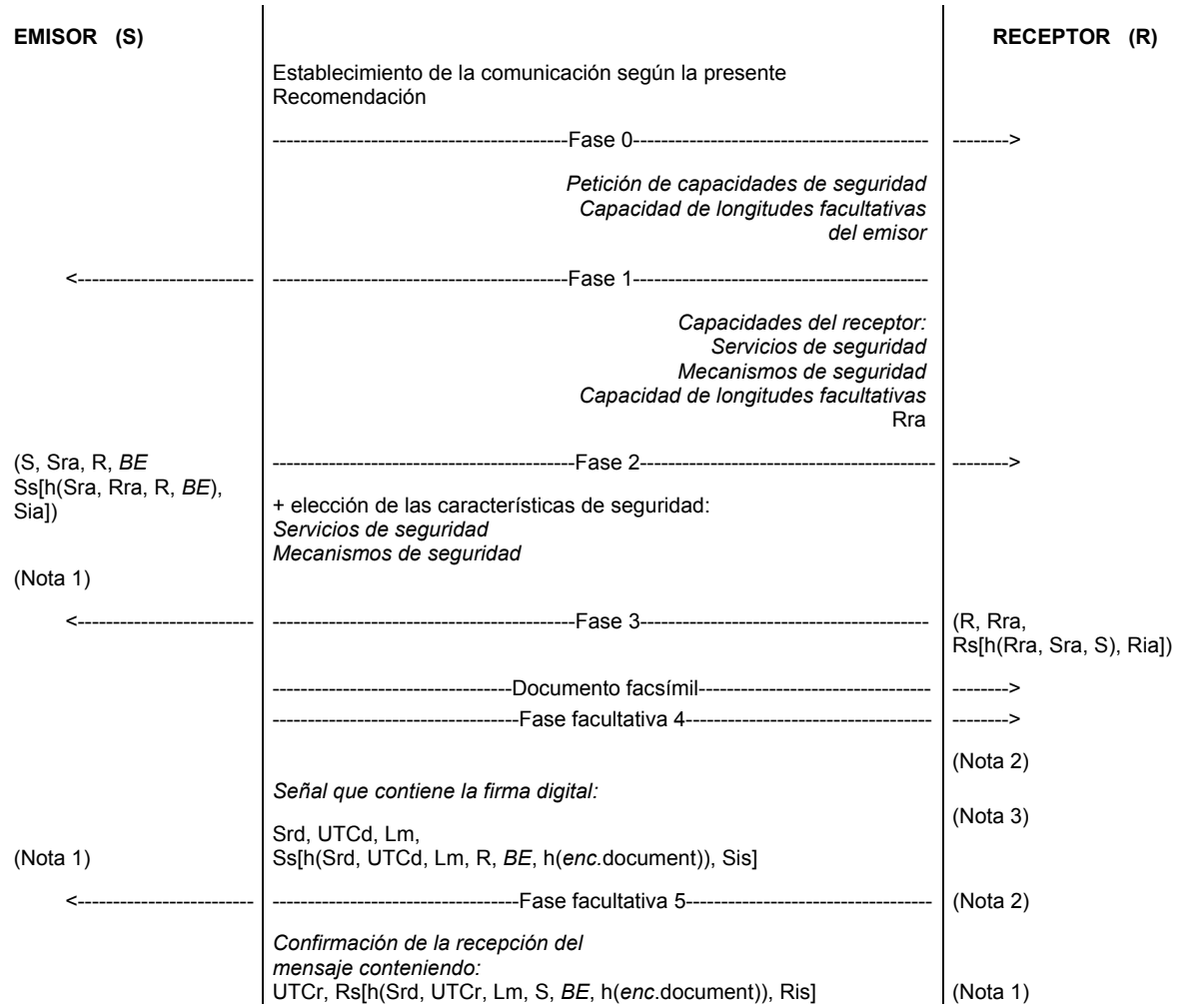
Este modo consiste en la transmisión del documento facsímil con características de seguridad.

Los parámetros de seguridad se transmiten dentro de los elementos del protocolo (fases B y D del protocolo T.30).

Facultativamente, algunos de los parámetros de seguridad se transmiten al nivel de mensaje (a la velocidad del mensaje, fase C del protocolo T.30): dentro de una página especial llamada "**página de seguridad**".

H.6.3.1 Esquema

Véase la figura H.5/T.30.



Las características indicadas con caracteres en cursiva son facultativas.

NOTA 1 – BE (= RpE[S, Ks]) existe en los diferentes testigos solamente si el servicio [confidencialidad del mensaje + establecimiento de clave de sesión] ha sido negociado entre las dos partes (con el parámetro "servicios de seguridad").

NOTA 2 – Las fases 4 y 5 existen solamente si el servicio [integridad del mensaje + confirmación de la recepción del mensaje] ha sido negociado entre las dos partes (con el parámetro "servicios de seguridad").

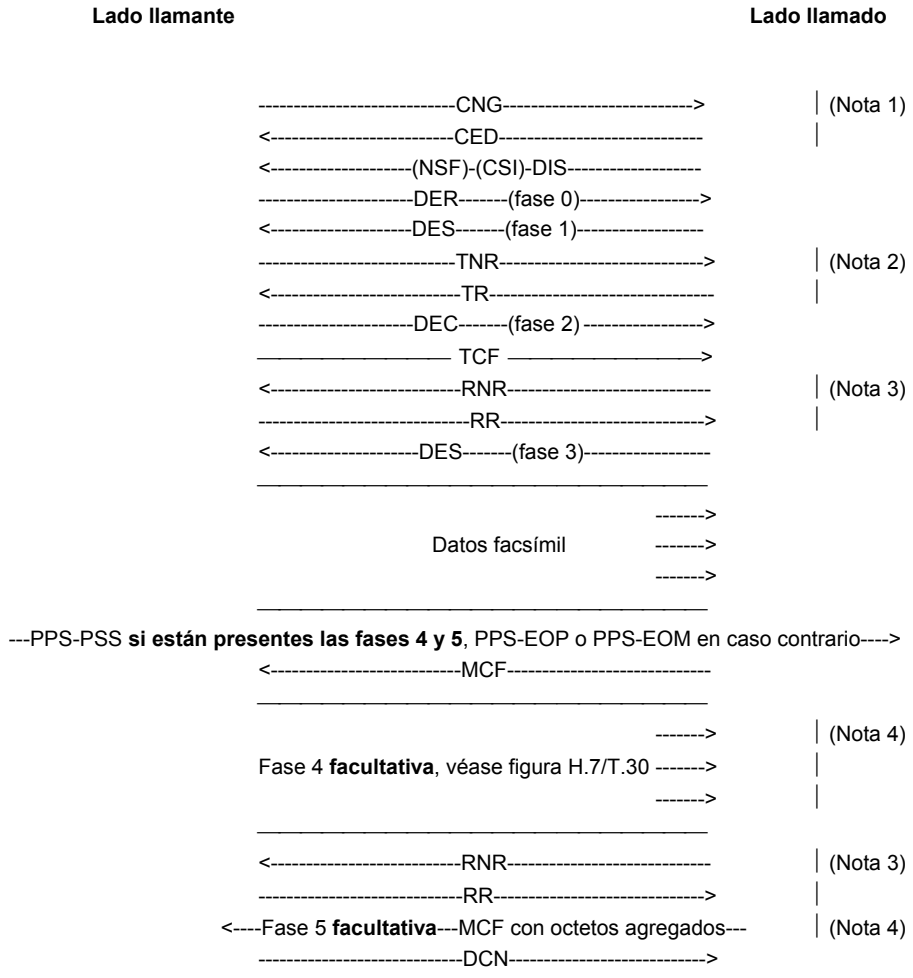
NOTA 3 – Si en la fase 4 se utiliza una página de seguridad, están presentes más parámetros.

Figura H.5/T.30 – Esquema del modo transmisión facsímil segura

H.6.3.2 Utilización de DER, DES y DEC en el modo transmisión facsímil segura

H.6.3.2.1 Esquema general del modo transmisión facsímil segura

Las señales DER, DES y DEC se utilizan en el modo transmisión facsímil segura. Véase la figura H.6/T.30:



Los temporizadores utilizados en el anterior intercambio de señales son los mismos que los del protocolo T.30 normalizado y del anexo A/T.30 a la presente Recomendación (T1, T2, T4, T5, …). Si no hay respuesta una vez transcurrida la temporización de T4, la instrucción del lado emisor (DER, DEC o DNK) es reenviada (para DER y DEC, sólo las tramas de las que todavía no se ha acusado recibo).

NOTA 1 – El establecimiento de la comunicación CNG/CED (tono de llamada/identificación de la estación llamada) que se muestra en la figura se da a título de ejemplo. También pueden tener lugar los otros procedimientos de explotación definidos en 3.1.

NOTA 2 – La utilización de TNR y TR es exactamente la misma que la de RNR/RR, pero concierne al terminal emisor en vez de al terminal receptor. Algunas ocurrencias facultativas del intercambio TNR-TR pueden permitir al terminal emisor retener el terminal receptor mientras dura la temporización de T5 como máximo (véase el anexo A/T.30).

NOTA 3 – Algunas ocurrencias facultativas del intercambio RNR-RR (ya definido en el anexo A/T.30) pueden permitir al terminal receptor retener el terminal emisor mientras dura la temporización de T5 como máximo (véase el anexo A/T.30).

NOTA 4 – Las fases 4 y 5 existen solamente si el servicio [integridad del mensaje + confirmación de la recepción del mensaje] ha sido negociado entre las dos partes (con el parámetro "servicios de seguridad").

Figura H.6/T.30 – Intercambio de señales en el modo transmisión facsímil segura
Ejemplo para un documento de una página facsímil

H.6.3.2.2 Fase 4

Cuando está presente la fase 4 (y a continuación la fase 5), existen dos casos que dependen de si se ha negociado o no la capacidad de página de seguridad entre las dos partes:

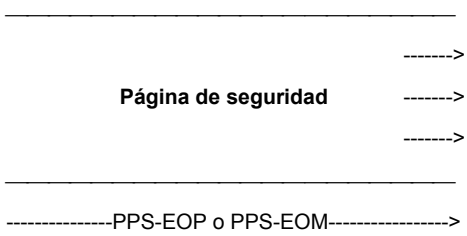
Caso 1 – Cuando ambos aparatos (emisor y receptor) proporcionan la capacidad de página de seguridad y se invoca el servicio [integridad del mensaje + confirmación de la recepción del mensaje], debe utilizarse la solución página de seguridad (caso 1).

Caso 2 – Cuando uno de los dos aparatos no proporciona la capacidad de página de seguridad y se invoca el servicio [integridad del mensaje + confirmación de la recepción del mensaje], debe utilizarse la solución de PPS-EOP o PPS-EOM agregado (caso 2).

PPS-EOM (no agregado en el caso 1, agregado en el caso 2) se utiliza si la comunicación se va a continuar con otro documento.

PPS-EOP (no agregado en el caso 1, agregado en el caso 2) se utiliza en el caso común, con sólo un documento facsímil durante la comunicación.

Caso 1: El servicio [integridad del mensaje + confirmación de la recepción del mensaje] ha sido invocado y se utiliza la página de seguridad



Caso 2: El servicio [integridad del mensaje + confirmación de la recepción del mensaje] ha sido invocado y no se utiliza la página de seguridad

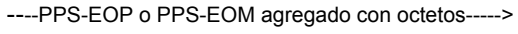


Figura H.7/T.30 – Intercambio de señales en la fase 4

H.6.3.3 Asignación de bits en la DIS

En el cuadro 2/T.30 se muestra la asignación de bits en el FIF de la DIS para indicar las capacidades de seguridad en base al algoritmo RSA. Se utiliza el bit N.° 82.

En el contexto del presente anexo H/T.30 no se emite la DCS; el FIF de la DCS se incluye dentro de la nueva señal "DEC" en la que el bit correspondiente N.° 82 se debe poner a "1".

H.6.3.4 Formato de los campos de información facsímil de las DER, DES y DEC para modo transmisión facsímil segura

H.6.3.4.1 Fase 0

La secuencia contenida en el(los) FIF de la DER es:

Superrótulo "E-F"	Longitud de supergrupo	Rótulo "FIF de SUB"	Longitud + contenido de "FIF de SUB"	Rótulo "FIF de SID"	Longitud + contenido de "FIF de SID"	Rótulo "FIF de TSI"	Longitud + contenido de "FIF de TSI"

Superrótulo "modo transmisión segura"	Longitud de supergrupo	Rótulo "capacidad de longitudes facultativas"	Longitud + contenido de "capacidad de longitudes facultativas"	Rótulo "petición de capacidades de seguridad"	Longitud + contenido de "petición de capacidades de seguridad"

Rótulo "características no normalizadas"	Longitud + contenido de "características no normalizadas"

Si el lado llamante no desea utilizar los servicios facultativos ni las capacidades facultativas, no se envía el parámetro "petición de capacidades de seguridad". El modo transmisión facsímil segura sigue adelante con las características básicas (Sp, Rp de 64 octetos de longitud, etc. ...), invocándose solamente el servicio de autenticación mutua.

Además, si el lado llamante no puede tratar números aleatorios de longitudes facultativas (mayores que la básica), no hay que enviar el parámetro "capacidad de longitudes facultativas".

H.6.3.4.2 Fase 1

La secuencia contenida en el(los) FIF de la DES es:

Superrótulo "modo transmisión segura"	Longitud de supergrupo	Rótulo "Rra"	Longitud + contenido de "Rra"	Rótulo "servicios de seguridad"	Longitud + "servicios de seguridad"

Rótulo "mecanismos de seguridad"	Longitud + contenido de "mecanismos de seguridad"	Rótulo "capacidad de longitudes facultativas"	Longitud + contenido de "capacidad de longitudes facultativas"	Rótulo "características no normalizadas"	Longitud + contenido de "características no normalizadas'

La presencia de los grupos facultativos [rótulo, octeto de longitud y valor de parámetro] depende de las peticiones en la fase 0 (bits en el parámetro "petición de capacidades de seguridad").

H.6.3.4.3 Fase 2

La secuencia contenida en el(los) FIF de la DEC es:

Super-rótulo "E-F"	Longitud de supergrupo	Rótulo "FIF de DCS"	Longitud + contenido de "FIF de DCS"	Rótulo "FIF de SUB"	Longitud + contenido de "FIF de SUB"	Rótulo "FIF de SID"	Longitud + contenido de "FIF de SID"	Rótulo "FIF de TSI"	Longitud + contenido de "FIF de TSI

Superrótulo "modo transmisión seguro"	Longitud de supergrupo	Rótulo "S"	Longitud + contenido de "S"	Rótulo "Sra"	Longitud + contenido de "Sra"	Rótulo "R"	Longitud + contenido de "R"

Rótulo "BE"	Longitud + contenido de "BE"	Rótulo "testigo 2" o "testigo 2-enc."	Longitud + contenido de "testigo 2" o "testigo 2-enc."

Rótulo "servicios de seguridad"	Longitud + contenido de "servicios de seguridad"	Rótulo "mecanismos de seguridad"	Longitud + contenido de "mecanismos de seguridad"	Rótulo "características no normalizadas"	Longitud + contenido de "características no normalizadas"

– El rótulo BE sólo está presente si se invoca el servicio [confidencialidad del mensaje + establecimiento de clave de sesión]. En tal caso, se envía el testigo 2-enc.

– El rótulo "servicios de seguridad" no está presente si la transmisión ha de tener lugar solamente con el servicio de autenticación mutua.

– El parámetro "mecanismos de seguridad" es obligatorio ya que indica la función troceado seleccionada.

H.6.3.4.4 Fase 3

La secuencia contenida en el(los), FIF de la DES es:

Superrótulo "modo transmisión segura"	Longitud de supergrupo	Rótulo "R"	Longitud + contenido de "R"	Rótulo "Rra"	Longitud + contenido de "Rra"	Rótulo "testigo 3"	Longitud + contenido de "testigo 3"

H.6.3.4.5 Fase 4

Las fases 4 y 5 existen solamente si el servicio [integridad del mensaje + confirmación de la recepción del mensaje] ha sido negociado entre las dos partes.

La señal enviada en la fase 4 es la señal PPS-EOP (o PPS-EOM) con octetos agregados (caso 2 expuesto en la figura H.7/T.30) o la página de seguridad (caso 1 expuesto en la figura H.7/T.30).

Cuando ambos aparatos (emisor y receptor) proporcionan la capacidad de página de seguridad y se invoca el servicio [integridad del mensaje + confirmación de la recepción del mensaje], debe utilizarse la solución página de seguridad.

El contenido de la página de seguridad se define en H.6.4/T.30.

En el caso 2, la estructura de la señal PPS-EOP (o PPS-EOM) con octetos agregados es la misma que la de las señales DER, DES, DEC y DTR (definidas en H.6.1.1/T.30): multitramas, bit X = 1 para la trama final, FIF de 65 octetos, números de tramas, ...

El FCF es el ya definido en el anexo A/T.30 (en A.4.3/T.30).

La secuencia contenida en el(los) FIF de la señal PPS-EOP (o PPS-EOM) agregada es:

Superrótulo "modo transmisión segura"	Longitud de supergrupo	Rótulo "Srd"	Longitud + contenido de "Srd"	Rótulo "UTCd"	Longitud + contenido de " UTCd"	Rótulo "Lm"	Longitud + contenido de "Lm"

Rótulo "testigo 4" o "testigo 4-enc."	Longitud + contenido de "testigo 4" o "testigo 4-enc."	Rótulo "características no normalizadas"	Longitud + contenido de "características no normalizadas"

Se envía "testigo 4" o "testigo 4-enc." según que se haya invocado o no, en la fase 2, el servicio [confidencialidad del mensaje + establecimiento de clave de sesión].

H.6.3.4.6 Fase 5

Las fases 4 y 5 existen solamente si el servicio [integridad del mensaje + confirmación de la recepción del mensaje] ha sido negociado entre las dos partes.

La señal enviada en la fase 5 es la señal MCF agregada con octetos.

La estructura de la señal MCF agregada con octetos es la misma que la de las señales DER, DES, DEC y DTR (definidas en H.6.1.1/T.30): multitramas, bit X = 1 para la trama final, FIF de 65 octetos, números de trama, etc.

La FCF es la ya definida para el protocolo T.30 del modo normal (en 5.3.6.1.7/T.30).

La secuencia contenida en el(los) FIF de la MCF agregada es:

Superrótulo "modo transmisión segura"	Longitud de supergrupo	Rótulo "UTCr"	Longitud + contenido de "UTCr"	Rótulo "testigo 5" o "testigo 5-enc."	Longitud + contenido de "testigo 5" o "testigo 5-enc."

Se envía "testigo 5" o "testigo 5-enc." según que se haya invocado o no, en la fase 2, el servicio [confidencialidad del mensaje + establecimiento de clave de sesión].

H.6.3.4.7 Mensajes error

Si se detectan errores en la fase 1, 2, 3, 4 ó 5, el emisor o el receptor (dependiendo de la fase) indica el error con la señal FNV.

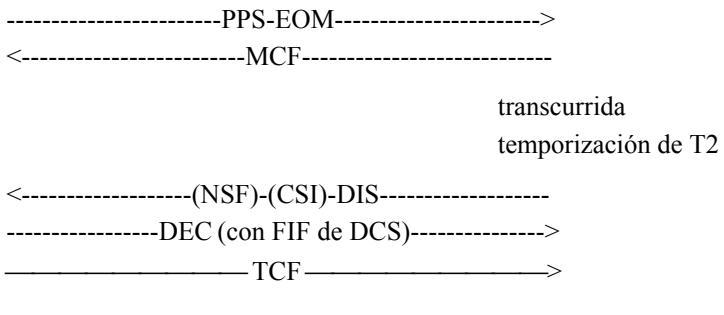
El motivo del error se codifica en la señal FNV.

El cuadro H.10/T.30 da la codificación del valor de error.

El uso de FNV para indicación de error se explica en H.6.7/T.30.

H.6.3.5 Precisiones para la utilización de PPS-EOM en un documento seguro

Dentro de la secuencia de páginas parciales que constituyen un documento seguro se permite la utilización de PPS-EOM (por ejemplo, para cambiar la resolución de la imagen). El procedimiento después de PPS-EOM es muy similar al del anexo A/T.30:



En este caso, para fijar la transmisión de las páginas restantes del documento, la DEC debe contener el FIF de la DCS (con el bit o bits de seguridad pertinentes puestos a "1", como en la fase 2). Los parámetros de seguridad enviados en la fase 2 no se incluyen en la DEC en esta etapa; son válidos durante la transmisión del documento.

H.6.4 A nivel del mensaje: página de seguridad

La utilización de la página de seguridad se define en el caso 1 de la figura H.7/T.30.

Cuando ambos aparatos (emisor y receptor) proporcionan la capacidad de página de seguridad y se invoca el mensaje [integridad del mensaje + confirmación de la recepción del mensaje], debe utilizarse la solución página de seguridad.

H.6.4.1 Contenido de la página de seguridad

La "página de seguridad" contiene los siguientes parámetros de seguridad definidos en los cuadros H.1/T.30 y H.5/T.30:

Indicador de página de seguridad	:	Indica el bloque que contiene la página de seguridad.
S	:	Identidad del emisor.
Sp	:	Clave pública del emisor.
R	:	Identidad del receptor.
Srd	:	Número aleatorio creado por el emisor para la firma digital.
UTCd	:	Fecha/hora elegida por el emisor (fecha/hora de la generación/firma del documento).
Lm	:	Longitud del documento.
Parámetro "servicios de seguridad"	:	Véase la definición en el cuadro H.6/T.30.
Parámetro "mecanismos de seguridad"	:	Véase la definición en el cuadro H.8/T.30.
BE	:	RpE[S, Ks].
Testigo 4 o Testigo 4-enc.	:	Véase la definición en el cuadro H.5/T.30.
Identificación del tipo de página de seguridad	:	Indica el número de la versión de la página de seguridad. En las próximas versiones del presente anexo puede haber otros tipos de página de seguridad a los que se les dará otros números de versión.
Trayecto de certificación	:	Certifica la clave pública del emisor. La definición precisa del trayecto de certificación queda en estudio.
Características no normalizadas	:	Características no normalizadas.

El orden de transmisión de los bits dentro de la página de seguridad sigue las mismas reglas definidas para el FIF de las DES/DEC/DER/DTR en H.4.8.3/T.30 y precisadas en el cuadro H.1/T.30.

H.6.4.1.1 Codificación del parámetro "indicador de página de seguridad"

Este rótulo (y el parámetro pertinente) indica el bloque que contiene la página de seguridad.

El octeto de longitud es "0000 1000" (8 octetos).

El contenido es (en hexadecimal):

0x01 0x23 0x45 0x67 0x89 0xAB 0xCD 0xEF

H.6.4.1.2 Codificación del parámetro "identificación del tipo de página de seguridad"

Este parámetro es facultativo en la página de seguridad.

El octeto de longitud es "0000 0001" (1 octeto).

El contenido es el número de versión de la página de seguridad. En la presente versión de este anexo, sólo existe una versión de página de seguridad, el número de versión es: 0x00.

H.6.4.2 Formato de la página de seguridad

La página de seguridad tiene exactamente la misma clase de formato que las secuencias dentro de las señales DER, DES, DEC y DTR (superrótulos, rótulos y valores de parámetros), excepto que, este caso, la secuencia no está situada en la serie de FIF de DER, DES, DEC o DTR sino en las tramas ECM.

Dentro de la secuencia de rótulos introducidos por el superrótulo, **el orden no está fijado**, salvo para el indicador de página de seguridad que es el primero.

La secuencia es como sigue:

Superrótulo "modo transmisión segura"	Longitud de superrótulo	Rótulo "indicador de página de seguridad"	Longitud + contenido de "indicador de página de seguridad"	Rótulo "S"	Longitud + contenido de "S"	Rótulo "Sp"	Longitud + contenido de "Sp"

Rótulo "R"	Longitud + contenido de "R"	Rótulo "Srd"	Longitud + contenido "Srd"	Rótulo "UTCd"	Longitud + contenido de "UTCd"	Rótulo "Lm"	Longitud + contenido de "Lm"

Rótulo "servicios de seguridad"	Longitud + contenido de "servicios de seguridad"	Rótulo "mecanismos de seguridad"	Longitud + contenido de "mecanismos de seguridad"

Rótulo "BE"	Octeto de longitud + contenido de "BE"

Rótulo "testigo 4" o "testigo 4-enc."	Longitud + contenido de "testigo 4" o "testigo 4-enc."	Rótulo "identificación de tipo de página de seguridad"	Longitud + contenido de "identificación del tipo de página de seguridad"

Rótulo "trayecto de certificación"	Longitud + contenido de "trayecto de certificación"	Rótulo "características no normalizadas"	Longitud + contenido de "características no normalizadas"

NOTA 1 – Los bits de los parámetros "servicios de seguridad" y "mecanismos de seguridad" se ponen de conformidad con el cuadro H.6/T.30 y el cuadro H.8/T.30, respectivamente, [versión del sistema de seguridad, bit indicador de la función troceado utilizada, bit indicador del algoritmo de cifrado utilizado (si hay documento cifrado)].

NOTA 2 – El parámetro BE sólo está presente si se ha invocado el servicio [confidencialidad del mensaje + establecimiento de clave de sesión].

NOTA 3 – El formato del trayecto de certificación queda en estudio.

H.6.5 Reglas para trocear el documento, reglas para cifrar el documento

H.6.5.1 Reglas para trocear el documento

Los datos del documento que forman parte de la cadena de bits que se trocea son todos los octetos contenidos en la FIF de todas las tramas de datos ECM, excepto el primer octeto de cada trama (que es el número de trama). Por consiguiente, todos los bits de relleno y de justificación (descritos en A.3.6.2/T.4 y en 2.4.1.2/T.6) forman parte de los datos que pasan a través de la función troceado.

El tren de bits que entra en el proceso de troceado para producir h(document) o h(enc.document) (en caso de cifrado) se puede representar como la cadena de bits contenida en el rectángulo mostrado en la figura H.8/T.30.

En cada octeto, esa cadena de bits tiene el mismo orden de bits en el proceso de troceado que los bits de datos de cada uno de los octetos cuando se transmiten por la línea.

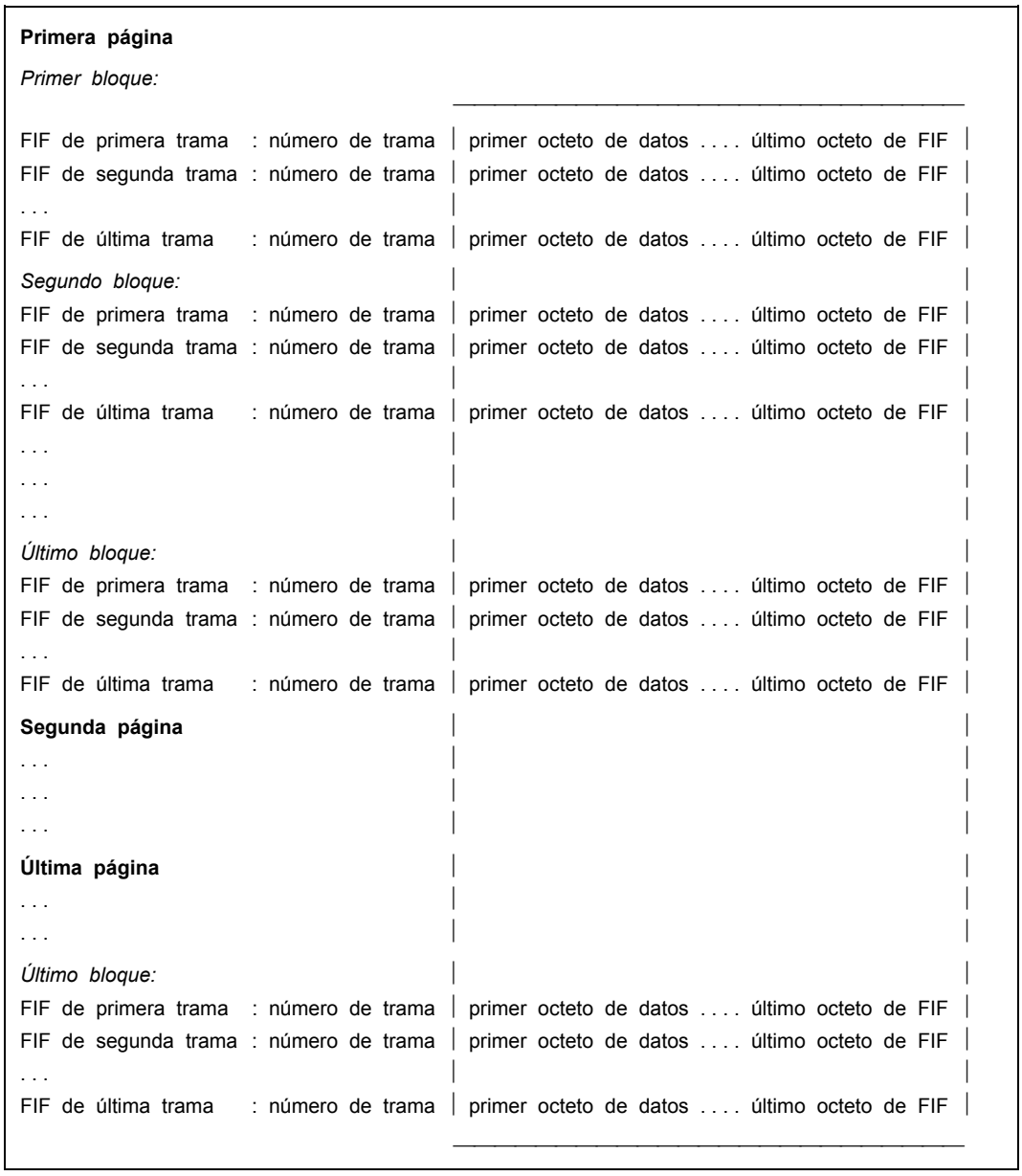


Figura H.8/T.30 – Reglas para trocear el documento

H.6.5.2 Reglas para cifrar el documento

Los datos del documento que serán encriptados son los octetos contenidos en la FIF de las tramas de datos ECM, excepto el primer octeto de cada trama (que es el número de trama).

El orden de entrada de los bits a la función de encripción es el mismo que cuando los datos facsímil se transmiten por la línea sin criptación.

NOTA – Para FEAL-32, estos datos se alinean cada 64 bits en orden de izquierda a derecha y se introducen en la función FEAL-32.

Cada 64 bits de los datos encriptados procedentes de la función FEAL-32 se alinean en orden de izquierda a derecha y el bit situado más a la izquierda es el que se transmite primero.

H.6.6 Modo interrogación secuencial segura

H.6.6.1 Interrogación secuencial simple

El uso y la codificación de las señales en el modo interrogación secuencial segura sigue las mismas reglas que para el modo transmisión facsímil segura.

En la figura H.9/T.30 se muestra el intercambio de señales.

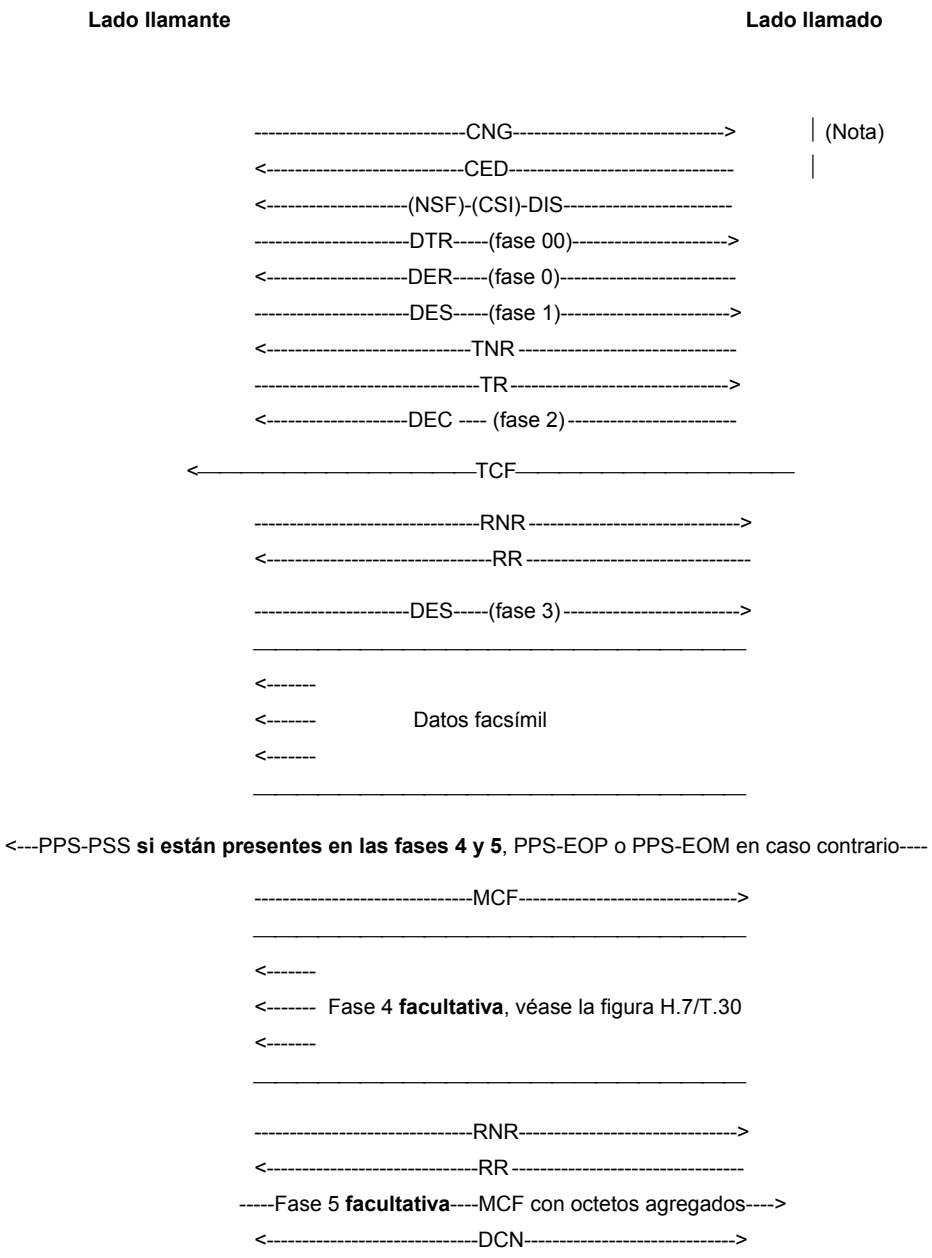


Figura H.9/T.30 – Intercambio de señales en el modo interrogación secuencial segura
Ejemplo para un documento de una página facsímil

NOTA – El establecimiento de la comunicación CNG/CED (tono de llamada/identificación de la estación llamada) que se muestra en la figura, se da a título de ejemplo. También pueden tener lugar los otros métodos de explotación definidos en 3.1/T.30.

Las fases 0, 1, 2, 3 y 4 son las mismas que en el modo transmisión facsímil segura.

Para la fase 00, la secuencia contenida en el(los) FIF de la DTR es:

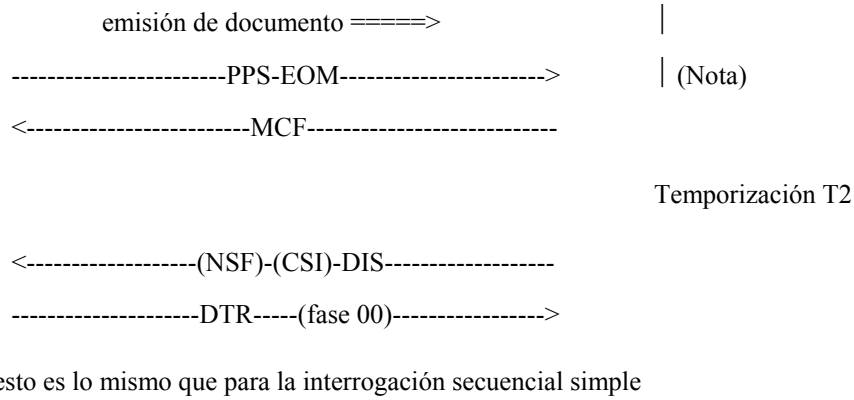
Superrótulo "E-F"	Longitud de supergrupo	Rótulo "FIF de PWD"	Longitud + contenido de "FIF de PWD"	Rótulo "FIF de PSA"	Longitud + contenido de "FIF de PSA"	Rótulo "FIF de SEP"	Longitud + contenido de "FIF de SEP"

Rótulo "FIF de CIG"	Longitud + contenido de "FIF de CIG"	Rótulo "FIF de DTC"	Longitud + contenido de "FIF de DTC"

Superrótulo "modo transmisión segura"	Longitud de supergrupo	Rótulo "características no normalizadas"	Longitud + contenido de "características no normalizadas"

H.6.6.2 Interrogación secuencial con inversión

En caso de interrogación secuencial con inversión, una vez recibido la DIS, tiene lugar la secuencia de fases (00, 0, 1, 2, 3 y 4) exactamente igual que en el caso de interrogación secuencial simple.



NOTA – Si el documento enviado antes de la interrogación secuencial con inversión se envía según el modo transmisión facsímil segura, las reglas aplicables son las del H.6.3.2/T.30: si están presentes las fases 4 y 5, se envía la página de seguridad o PPS-EOM con octetos agregados y a la respuesta MCF se le agregan octetos.

H.6.7 Mensajes error

H.6.7.1 Mensajes de error

Cuando se tenga que indicar un mensaje de error, el bit N.º 5 del octeto motivo de la señal FNV (bit que indica "error de facsímil seguro") se debe poner a "1".

La FNV se define en 5.3.6.2.12/T.30.

El motivo del error está contenido en los octetos de información de diagnóstico de la señal FNV.

El octeto tipo para mensajes de error es "error de facsímil seguro", definido en 5.3.6.2.12/T.30.

El cuadro H.10/T.30 especifica los octetos contenidos en el campo valor de "error de facsímil seguro".

Cuadro H.10/T.30 – Motivos de error codificados en el campo de valor de error de facsímil seguro de la señal FNV

Codificación de los octetos de valor de la señal FNV	Motivos del error
	Primer octeto
Bit N.º 7 6 5 4 3 2 1 0 x x x x x x x 1	Error de registro de clave pública
Bit N.º 7 6 5 4 3 2 1 0 x x x x x x 1 x	Error de registro de clave pública de cifrado
Bit N.º 7 6 5 4 3 2 1 0 x x x x x 1 x x	Servicio no soportado
Bit N.º 7 6 5 4 3 2 1 0 x x x x 1 x x x	Parte no registrada
Bit N.º 7 6 5 4 3 2 1 0 x x x 1 x x x x	Fallo de autenticación
Bit N.º 7 6 5 4 3 2 1 0 x x 1 x x x x x	Recepción no confirmada (Srd no válido) El número aleatorio recibido es rechazado por el receptor (por ejemplo, en caso de reproducción detectada)
Bit N.º 7 6 5 4 3 2 1 0 x 1 x x x x x x	Recepción no confirmada (UTCd no válido) El receptor no acepta el UTCd recibido del emisor (los criterios dependen de la realización)
Bit N.º 7 6 5 4 3 2 1 0 1 x x x x x x x	Recepción no confirmada (Lm no válido) La longitud indicada por el emisor no corresponde a la longitud real del documento recibido
	Segundo octeto
Bit N.º 7 6 5 4 3 2 1 0 x x x x x x x 1	Recepción no confirmada (testigo 4 o testigo 4-enc. no válido) El receptor detecta que la firma digital del emisor no es correcta
Bit N.º 7 6 5 4 3 2 1 0 x x x x x x 1 x	Recepción no válida (testigo 5 o testigo 5-enc. no válido)
NOTA 1 – Se pueden indicar varios motivos al mismo tiempo (varios bits puestos a "1"). NOTA 2 – En próximas versiones de este anexo se pueden definir más octetos para codificar otros motivos de error. NOTA 3 – Para cada octeto, el bit menos significativo (el bit situado más a la derecha) es el que se transmite primero.	

H.6.7.2 Utilización de la señal FNV para indicación de error

Una vez enviada la señal FNV que indica error de fax seguro, el terminal que la recibe "acusa recibo" de la misma enviando DCN y desconecta la línea.

A continuación se da un ejemplo en el que falla la autenticación del receptor en la fase 3 de la transmisión facsímil segura.

Lado llamante **Lado llamado**

<----------DES-----(fase 3)----------

fallo de autenticación

----------FNV---------->

indicación de fallo de autenticación por la FNV

<----------DCN----------

desconexión

(el documento no se envía)

4 Sección 4

Introducción del nuevo anexo I:

Anexo I

Procedimiento para la transmisión de documentos por facsímil grupo 3 con imágenes en escala de grises y en color mediante la utilización del esquema de la Recomendación T.43

I.1 Introducción

Este anexo describe las adiciones a la Recomendación T.30 para permitir la transmisión de imágenes en escala de grises y en color utilizando el método de codificación sin pérdidas definido en la Recomendación T.43 para el modo de funcionamiento facsímil grupo 3.

Esta Recomendación es un modo facultativo de escala de grises y color que sólo se realizará si también se han realizado los modos de base de escala de grises y color definidos en el anexo E/T.4. La realización del modo escala de grises de la Recomendación T.43 requiere la realización del modo asociado escala de grises del anexo E/T.4. De manera similar, la realización del modo color de la Recomendación T.43 requiere la realización del modo color asociado del anexo E/T.4.

El objetivo es permitir la transmisión eficaz de una gran variedad de imágenes, desde un simple documento que contiene caracteres en rojo o en azul hasta imágenes de alta calidad en escala de grises o en colores por la red telefónica general conmutada y por otras redes. Las imágenes se obtienen normalmente explorando las fuentes originales con exploraciones de 200 pels/25,4 mm o superiores. Las fuentes originales suelen ser documentos comerciales subrayados con diversos colores, gráficos comerciales generados por computador, imágenes con paleta de colores e imágenes en escala de grises y en color de tonos continuos.

En este anexo, se admiten tres tipos de imágenes: imagen de un bit por color CMY(K)/RGB, imagen con paleta de colores e imagen en escala de grises y en color de tonos continuos. La imagen de un bit por color CMY(K)/RGB se representa también utilizando la tabla de paleta de colores, y es un caso especial de la imagen con paleta de colores en la cual cada color está representado por información de un bit de color imprimible original. La representación de datos de imágenes en color se basa en las Recomendaciones T.42 y T.43. El modo básico es una representación del espacio cromático independiente del dispositivo, el espacio CIELAB, que permite el intercambio inequívoco de información de color. La descomposición de los planos de bits y la codificación mediante la Recomendación T.82 se describe también en la Recomendación T.43.

Este anexo describe el procedimiento para negociar las capacidades de transmisión de imágenes en color y en escala de grises. Especifica las definiciones y las especificaciones de nuevas entradas al campo de información facsímil de las tramas DIS/DTC y DCS de la Recomendación T.30.

La información relativa a la capacidad del receptor, capacidad de modo de color, precisión de amplitud de imagen en digitalización (bits/componente), método de entrelazado, iluminación y gama de colores habituales está sujeta a negociación en la fase previa al mensaje del protocolo de la Recomendación T.30.

Este anexo no trata de la semántica ni de la sintaxis de la codificación real de las imágenes en escala de grises y en color mediante codificación sin pérdidas. Esta información figura en la Recomendación T.43.

La utilización del modo con corrección de errores (ECM, *error correction mode*) para una transmisión sin errores es obligatoria en el procedimiento descrito por este anexo. En el modo de transmisión con corrección de errores, la secuencia de datos de imágenes codificados está incrustada en la parte datos codificados facsímil (FCD, *facsimile coded data*) de las tramas de transmisión del control de enlace de datos de alto nivel (HDLC, *high-level data link control*) que se especifica en el anexo A/T.30.

I.2 Definiciones

I.2.1 espacio CIE (L* a* b*) (CIELAB): Un espacio cromático definido por la comisión internacional del alumbrado (CIE, *commission internationale de l'éclairage*) que tiene una diferencia visualmente perceptible aproximadamente igual entre puntos separados igualmente en el espacio. Los tres componentes son L* (en luminosidad), a* y b* (ambos en crominancia).

I.2.2 grupo mixto de expertos en imágenes binivel (JBIG, *joint bi-level image experts group*) y también abreviatura para el método de codificación, descrito en la Recomendación T.82, definido por dicho grupo.

I.3 Referencias normativas

– Recomendación UIT-T T.4 (1996), *Normalización de los aparatos facsímil del grupo 3 para la transmisión de documentos.*

– Recomendación UIT-T T.82 (1993) | ISO/CEI 11544:1993, *Tecnología de la información – Representación codificada de la información de imagen y de audio – Compresión de imagen binivel progresiva. (Denominada también Norma JBIG.)*

– Recomendación UIT-T T.42 (1996), *Método de representación de los colores en tonos continuos para facsímil.*

– Recomendación UIT-T T.43 (1997), *Representaciones imágenes en escala de grises y en color que utilizan el esquema de codificación sin pérdidas para facsímil.*

I.4 Procedimiento de negociación

La negociación para transmitir y recibir imágenes en escala de grises y en color codificadas con la codificación de planos de bits sin pérdidas en el protocolo facsímil del grupo 3 se invoca mediante la fijación de los bits en las tramas DIS/DTC y DCS durante el procedimiento previo a la transmisión del mensaje (fase B) del protocolo T.30.

Los tres tipos de imágenes mencionados se dividen además en 7 clases de submodos de codificación especificados en el cuadro G.1/T.4. La relación de las 4 clases de modos de codificación y las 7 clases de submodos de codificación que se han de admitir se muestra en los cuadros G.2/T.4.

La relación de las 7 clases de submodos de codificación y las 4 clases de modos de codificación que vienen dadas por la combinación de los bits X a través de X + 2, se indica en el cuadro I.1/T.30.

En el cuadro I.1/T.30, se describen explícitamente la capacidad de la codificación de la escala de grises/color sin pérdidas, el número de índices de la paleta de colores y el número de precisión de bits. Los parámetros que se han de negociar figuran en el cuadro I.2/T.30.

Cuadro I.1/T.30 – Correspondencia de las clases de submodos de codificación con los bits DIS/DTC/DCS

Clase de submodo de codificación		**Espacio cromático**	**Bit 36 codificación de la Rec. T.43**	**Bit 69 modo de color**	**Bit 71 modo de 12 bits**	
Tipo de imagen	**# de plano de bits**					
Un bit por imagen de color	(3,4)		1	1	0	(Nota)
Imagen con paleta de colores	Básico (1-12) x 1 precisión de 8 bits	Lab	1	1	0	
	Ampliado (1-12) x 1 Precisión de 12 bits o (13-16) x 1 precisión de 8 ó 12 bits	Lab	1	1	1	
Imagen de tonos continuos	Escala de grises 2-8 9-12	 L L	 1 1	 0 0	 0 1	
	Color (2-8) x 3 (9-12) x 3	 Lab Lab	 1 1	 1 1	 0 1	
NOTA – Este submodo de codificación es un caso especial del submodo de paleta de colores, en el cual cada plano de bit corresponde con los colores primarios CMY(K) o RGB. El número de planos (3 ó 4) será distinguido por la entrada G3FAX0.						

Cuadro I.2/T.30 – Capacidades obligatorias y facultativas

Obligatoria	Facultativa
Escala de grises de la Recomendación T.43	Color de la Recomendación T.43
Modo de 8 bits	Modo de 12 bits
Entrelazado de rayas	Entrelazado de planos
Iluminante D50 de CEI	Iluminante habitual
Gama de colores por defecto	Gama de colores habitual

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Transmisiones de señales radiofónicas, de televisión y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	**Terminales para servicios de telemática**
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Z	Lenguajes de programación

12814

Impreso en Suiza
Ginebra, 1998