

**NORMA Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos.**

---

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de Economía.

La Secretaría de Economía, por conducto de la Dirección General de Normas, con fundamento en los artículos 34 fracciones XIII y XXX de la Ley Orgánica de la Administración Pública Federal; 39 fracción V, 40 fracciones III y XVIII, 47 fracción IV de la Ley Federal sobre Metrología y Normalización, y 23 fracciones I y XV del Reglamento Interior de esta Secretaría, y

**CONSIDERANDO**

Que es responsabilidad del Gobierno Federal procurar las medidas que sean necesarias para garantizar que los servicios que se comercialicen en territorio nacional contengan los requisitos necesarios, con el fin de garantizar los aspectos de información para lograr una efectiva protección del consumidor;

Que con fecha 28 de septiembre de 2001 el Comité Consultivo Nacional de Normalización de Seguridad al Usuario, Información Comercial y Prácticas de Comercio aprobó la publicación del proyecto de Norma Oficial Mexicana PROY-NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos, lo cual se realizó en el **Diario Oficial de la Federación** el 16 de noviembre del mismo año, con objeto de que los interesados presentaran sus comentarios;

Que durante el plazo de 60 días naturales contados a partir de la fecha de publicación de dicho proyecto de Norma Oficial Mexicana, la Manifestación de Impacto Regulatorio a que se refiere el artículo 45 de la Ley Federal sobre Metrología y Normalización estuvo a disposición del público en general para su consulta; y que dentro del mismo plazo, los interesados presentaron sus comentarios al proyecto de norma, los cuales fueron analizados por el citado Comité Consultivo, realizándose las modificaciones procedentes;

Que con fecha 20 de marzo de 2002 el Comité Consultivo Nacional de Normalización de Seguridad al Usuario, Información Comercial y Prácticas de Comercio, aprobó por unanimidad la norma referida;

Que la Ley Federal sobre Metrología y Normalización establece que las Normas Oficiales Mexicanas se constituyen como el instrumento idóneo para la protección de los intereses del consumidor, se expide la siguiente Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos.

México, D.F., a 20 de marzo de 2002.- El Director General, **Miguel Aguilar Romo**.- Rúbrica.

**NORMA OFICIAL MEXICANA NOM-151-SCFI-2002, PRACTICAS COMERCIALES-REQUISITOS QUE DEBEN OBSERVARSE PARA LA CONSERVACION DE MENSAJES DE DATOS**

**PREFACIO**

En la elaboración de la presente Norma Oficial Mexicana participaron las siguientes empresas e instituciones:

- ACERTIA NETWORKS, S.A. DE C.V.
- ALESTRA, S. DE R.L. DE C.V.
- ASOCIACION MEXICANA DE ESTANDARES PARA EL COMERCIO ELECTRONICO, A.C.
- ASOCIACION MEXICANA DE LA INDUSTRIA DE TECNOLOGIAS DE INFORMACION, A.C.
- ASOCIACION NACIONAL DE TIENDAS DE AUTOSERVICIO Y DEPARTAMENTALES, A.C.
- BANCO DE MEXICO.
- BANCO INTERNACIONAL, S.A.
- BANCO NACIONAL DE MEXICO, S.A.
- BBVA BANCOMER, S.A.
- CAMARA NACIONAL DE COMERCIO DE LA CIUDAD DE MEXICO.
- CAMARA NACIONAL DE LA INDUSTRIA ELECTRONICA, DE TELECOMUNICACIONES E INFORMATICA.
- CECOBAN, S.A. DE C.V.
- CONSEJO MEXICANO DE LA INDUSTRIA DE PRODUCTOS DE CONSUMO, A.C.

- COMISION FEDERAL DE TELECOMUNICACIONES.
- COMPAÑIA PROCTER & GAMBLE MEXICO, S. DE R.L. DE C.V.
- HEWLETT PACKARD DE MEXICO, S.A. DE C.V.
- IBM DE MEXICO, S.A. DE C.V.
- INSTITUTO NACIONAL DE ESTADISTICA, GEOGRAFIA E INFORMATICA.  
Dirección General de Políticas y Normas en Informática.
- KPMG CARDENAS DOSAL, S.C.
- PEGASO COMUNICACIONES Y SISTEMAS, S.A. DE C.V.
- PETROLEOS MEXICANOS.  
Gerencia de Informática y Sistemas Financieros.
- PODER JUDICIAL FEDERAL.  
Instituto Federal de Especialistas de Concursos Mercantiles.
- PROMOCION Y OPERACION, S.A. DE C.V.
- SECRETARIA DE ECONOMIA.  
-Dirección General de Normas.  
-Dirección General de Fomento al Comercio Interior.  
-Dirección General de Política de Comercio Interior y Abasto.
- SEGURIDATA PRIVADA, S.A. DE C.V.
- SERVICIO DE ADMINISTRACION TRIBUTARIA.  
Administración General de Grandes Contribuyentes.  
Administración General de Tecnología de la Información.
- SOFTWARE AG, S.A. DE C.V.
- VERA ABOGADOS, S.C.
- WAL-MART DE MEXICO, S.A. DE C.V.
- XEROX MEXICANA, S.A. DE C.V.
- X WEB ADOBE, S.A. DE C.V.

## INDICE

- 0. Introducción**
- 1. Objetivo**
- 2. Campo de aplicación**
- 3. Definiciones**
- 4. Disposiciones generales**
- 5. Elementos que intervienen en la conservación de mensajes de datos**
- 6. Vigilancia**
- 7. Apéndice normativo**
- 8. Bibliografía**
- 9. Concordancia con normas internacionales**

Transitorio

### **0. Introducción**

De conformidad con lo dispuesto por los artículos 40 de la Ley Federal sobre Metrología y Normalización en relación con el 49 del Código de Comercio, la Secretaría de Economía deberá emitir una Norma Oficial Mexicana que permita el cumplimiento de la obligación, a cargo de los comerciantes que utilicen mensajes de

datos para realizar actos de comercio, de conservar por el plazo establecido en dicho Código, el contenido de los mensajes de datos en que se hayan consignado contratos, convenios o compromisos que den nacimiento a derechos y obligaciones; y cuyo contenido debe mantenerse íntegro e inalterado a partir del momento en que se generó por primera vez en su forma definitiva, debiendo ser accesible para su ulterior consulta.

### **1. Objetivo**

La presente Norma Oficial Mexicana establece los requisitos que deben observarse para la conservación del contenido de mensajes de datos que consignen contratos, convenios o compromisos y que en consecuencia originen el surgimiento de derechos y obligaciones.

### **2. Campo de aplicación**

La presente Norma Oficial Mexicana es de observancia general para los comerciantes que deban conservar los mensajes de datos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, así como para todas aquellas personas con quienes los comerciantes otorguen o pacten dichos contratos, convenios o compromisos.

### **3. Definiciones**

#### **3.1 Aceptación de autoría**

A la propiedad de un algoritmo de firma digital que permite atribuir a una persona física o moral la autoría de un mensaje de datos inequívocamente.

#### **3.2 Acto de comercio**

A todo acto que la legislación vigente considera como tal.

#### **3.3 Autenticación**

Al proceso en virtud del cual se constata que una entidad es la que dice ser y que tal situación es demostrable ante terceros.

#### **3.4 Archivo parcial**

Al mensaje de datos representado en formato ASN.1, conforme al apéndice de la presente Norma Oficial Mexicana.

#### **3.5 ASN.1**

A la versión 1 de Abstracts Syntax Notation (Notación Abstracta de Sintaxis).

#### **3.6 Bits**

A la unidad mínima de información que puede ser procesada por una computadora.

#### **3.7 Bytes**

A la secuencia de 8 bits.

#### **3.8 Clave pública**

A la cadena de bits perteneciente a una entidad particular y susceptible de ser conocida públicamente, que se usa para verificar las firmas electrónicas de la entidad, la cual está matemáticamente asociada a su clave privada.

#### **3.9 Clave privada**

A la cadena de bits conocida únicamente por una entidad, que se usa en conjunto con un mensaje de datos para la creación de la firma digital, relacionada con ambos elementos.

#### **3.10 Certificado digital**

Al mensaje de datos firmado electrónicamente que vincula a una entidad con una clave pública.

#### **3.11 Código**

Al Código de Comercio.

#### **3.12 Código de error**

A la clave indicativa de un suceso incorrecto.

### **3.13 Comerciantes**

A las personas físicas o morales a los que la legislación les otorga tal carácter.

### **3.14 Compromiso**

A cualquier acto jurídico diferente del contrato o del convenio, que genere derechos y obligaciones.

### **3.15 Confidencialidad**

Al estado que existe cuando la información permanece controlada y es protegida de su acceso y distribución no autorizada.

### **3.16 Contrato**

Al acuerdo de voluntades que crea o transfiere derechos y obligaciones.

### **3.17 Convenio**

Al acuerdo de voluntades que crea, transfiere, modifica o extingue derechos y obligaciones.

### **3.18 Constancia del prestador de servicios de certificación**

Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente Norma Oficial Mexicana.

### **3.19 Criptografía**

Al conjunto de técnicas matemáticas para cifrar información.

### **3.20 Destinatario**

A aquella entidad a quien va dirigido un mensaje de datos.

### **3.21 Emisor**

A aquella entidad que genera y transmite un mensaje de datos.

### **3.22 Entidad**

A las personas físicas o morales.

### **3.23 Expediente electrónico**

Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente norma oficial mexicana.

### **3.24 Firma digital**

A la firma electrónica que está vinculada al firmante de manera única, permitiendo así su identificación, creada utilizando medios que aquél pueda mantener bajo su exclusivo control, estando vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable. La firma digital es una especie de firma electrónica que garantiza la autenticidad e integridad y la posibilidad de detectar cualquier cambio ulterior.

### **3.25 Firma electrónica**

A los datos en forma electrónica consignados en un mensaje de datos, o adjuntados, o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que dicho firmante aprueba la información recogida en el mensaje de datos. La firma electrónica establece la relación entre los datos y la identidad del firmante.

### **3.26 Formato**

A la secuencia claramente definida de caracteres, usada en el intercambio o generación de información.

### **3.27 Legislación**

A las normas jurídicas generales y abstractas emanadas del Congreso de la Unión, así como la normatividad emanada del Poder Ejecutivo.

### **3.28 Mensaje de datos**

A la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología.

### **3.29** Objetos

A las definiciones del lenguaje ASN.1

### **3.30** Original

A la información contenida en un mensaje de datos que se ha mantenido íntegra e inalterada desde el momento en que se generó por primera vez en su forma definitiva.

### **3.31** Prestador de servicios de certificación

A la entidad que presta los servicios de certificación a que se refiere la presente Norma Oficial Mexicana.

### **3.32** Red

Al sistema de telecomunicaciones entre computadoras.

### **3.33** Resumen o compendio

Al resultado de aplicarle a un mensaje de datos una función de criptografía del tipo *hash*.

### **3.34** Sello del prestador de servicios de certificación

Al mensaje de datos representado en formato ASN.1, conforme al Apéndice de la presente Norma Oficial Mexicana.

### **3.35** Secretaría

A la Secretaría de Economía.

## **4. Disposiciones generales**

**4.1** Los comerciantes deberán conservar los mensajes de datos de acuerdo al método que se describe en el Apéndice de la presente Norma Oficial Mexicana.

**4.2** La información que se desee conservar se podrá almacenar en uno o varios archivos diferentes y/o en una o varias computadoras.

**4.3** Sin perjuicio de lo que dispongan otros ordenamientos jurídicos aplicables, cuando se pretenda conservar en un medio electrónico, óptico o de cualquier otra tecnología, información derivada de un acto de comercio, que se encuentre soportada en un medio físico similar o distinto a aquéllos, los comerciantes podrán optar por migrar dicha información a una forma digital y, observar para su conservación en forma digital, las disposiciones a que se refiere la presente Norma Oficial Mexicana. La migración de la información deberá ser cotejada por un tercero legalmente autorizado, que constatará que dicha migración se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva. El tercero legalmente autorizado deberá ser una persona física o moral que cuente con la capacidad tecnológica suficiente y cumpla con los requisitos legales aplicables.

**4.4** Los programas de cómputo (*software*) para la conservación de los mensajes de datos deberán dar cumplimiento a lo establecido por la presente Norma Oficial Mexicana.

## **5. Elementos que intervienen en la conservación de mensajes de datos**

**5.1** Para la emisión de la firma electrónica y/o digital, así como el prestador de servicios de certificación, deberán observar los requisitos que la normatividad aplicable señale para su operación.

**5.2** La constancia emitida por el prestador de servicios de certificación deberá observar los términos establecidos en el Apéndice de la presente Norma Oficial Mexicana.

**5.3** Los programas informáticos en y con los que se almacenen los mensajes de datos a los que se refiere la presente Norma Oficial Mexicana, utilizarán los formatos para mensajes de datos en los términos establecidos en el Apéndice del mismo.

## **6. Vigilancia**

La vigilancia de la Norma Oficial Mexicana estará a cargo de la Secretaría conforme a sus atribuciones y la legislación aplicable.

## **7. Apéndice Normativo**

# **INTRODUCCION**

En este Apéndice normativo se presentan los elementos necesarios para la implantación de la presente Norma Oficial Mexicana; la descripción del algoritmo de conservación de información y la definición ASN.1 de los objetos usados.

Se describe brevemente el algoritmo y se muestran dos archivos de texto que serán usados para construir los objetos ASN.1 resultantes de aplicar la presente Norma Oficial Mexicana a estos dos archivos. Los objetos ASN.1 creados son mostrados a través de un vaciado hexadecimal de su contenido en formato BER. Se incluyen las claves de criptografía que se usaron en la creación de los ejemplos con el propósito de que se pueda verificar la implantación de la presente Norma Oficial Mexicana.

El contenido de los archivos, las definiciones pertenecientes al lenguaje ASN.1 y los archivos ASN.1 aparecen con el tipo Courier New. Cuando se use el nombre de un objeto ASN.1 dentro del texto, éste aparecerá en *itálicas*. Como referencia se presenta el juego de caracteres ISO 8859-1 (Latín 1).

### FORMACION DE ARCHIVOS PARCIALES

Para formar un *archivo parcial* se crea un mensaje en formato ASN.1 que contiene (i) el nombre del archivo del sistema de información en el que está o estuvo almacenado el contenido del archivo, (ii) el tipo del archivo, y (iii) el contenido del mismo; con el objetivo de guardar la relación lógica que existe entre estos tres elementos.

### OBTENCION DE LOS COMPENDIOS O RESUMENES DIGITALES

Se calcula el compendio o resumen digital del *archivo o archivos parciales* resultado del proceso anterior, usando el algoritmo MD5.

### INTEGRACION DEL EXPEDIENTE ELECTRONICO

Para conformar un *expediente electrónico* se creará un mensaje ASN.1 que contiene (i) el nombre del *expediente*, que debe de coincidir con el nombre con el que se identifica en el sistema de información en donde está o estuvo almacenado, (ii) un índice, que contiene el nombre y el compendio de cada *archivo parcial* que integra el *expediente*, (iii) la identificación del operador del sistema de conservación, y (iv) su firma digital de acuerdo a la definición correspondiente en la presente Norma Oficial Mexicana.

### OBTENCION DE LA CONSTANCIA DEL PRESTADOR DE SERVICIOS DE CERTIFICACION

Para la obtención de la *constancia* el sistema de conservación deberá usar el protocolo de aplicación descrito en este apéndice para enviar el *expediente* al prestador de servicios de certificación, quien emitirá una *constancia* en formato ASN.1 y la regresará al sistema de conservación, haciendo uso del mismo protocolo.

El expediente opcionalmente podrá enviarse como un anexo de correo electrónico, siendo aplicables en este caso los protocolos Internet correspondientes.

También podrá usarse la transmisión vía Web siempre que el expediente se reciba como un archivo y siempre que se utilice un directorio protegido por nombre de usuario y contraseña. Para ello, la forma en que lo envíe deberá ser como la siguiente:

```
<form action="url del programa generador de constancias " method="post"
  enctype="multipart/form-data">
  Expediente: <input type="file" name="expediente">
  <input type="submit" value="Obtener Constancia">
</form>
```

La constancia deberá regresar al cliente como un archivo de tipo mime application/octet-stream<sup>1</sup>.

El prestador de servicios de certificación podrá recibir, si así lo acuerda con sus clientes, medios físicos conteniendo los archivos correspondientes a los expedientes.

### FORMACION DE LA CONSTANCIA

El prestador de servicios de certificación formará una *constancia* en formato ASN.1 que contendrá (i) el nombre del archivo en donde está almacenada la *constancia*, (ii) el *expediente* enviado por el sistema de

---

<sup>1</sup> Los MIME Types (Multipurpose Internet Mail Extensions) son la manera estándar de mandar contenido a través de la red. Los tipos MIME especifican tipos de datos, como por ejemplo texto, imagen, audio, etc.

conservación, (iii) fecha y hora del momento en que se crea la *constancia*, (iv) la identificación del prestador de servicios de certificación y (v) su firma digital de acuerdo a la definición correspondiente de esta Norma Oficial Mexicana.

#### METODO DE VERIFICACION DE AUTENTICIDAD

La verificación de la autenticidad de una *constancia* se realizará por medio del uso de un sistema de verificación que lleve a cabo los pasos siguientes:

- i) verificar la firma digital del prestador de servicios de certificación en la *constancia*;
- ii) verificar la firma digital del operador del sistema de conservación en el *expediente* contenido en la *constancia*, y
- iii) recalcular el compendio de él o los *archivos parciales* y verificar que coincidan con los compendios asentados en el *expediente*.

#### Definición ASN.1

```
=====
NCI-NOM-000-SECOFI DEFINITIONS ::=
BEGIN

NombreOP ::= PrintableString

TipoOP ::= OBJECT IDENTIFIER

EmisorOP ::= IdentificadorUsuario

IdUsuarioOP ::= IdentificadorUsuario

md5                OBJECT IDENTIFIER ::= { 1 2 840 113549 2 5}
rsaEncryption      OBJECT IDENTIFIER ::= { 1 2 840 113549 1 1 1}
md5WithRSAEncryption OBJECT IDENTIFIER ::= { 1 2 840 113549 1 1 4}

--
-- Identificador de objeto a utilizar para las Normas Oficiales Mexicanas
--

mex OBJECT IDENTIFIER ::= { 2 37 137 }

nom OBJECT IDENTIFIER ::= { mex 179 }

--
-- Identificadores de objeto a utilizar para tipos de archivos
--

nomArchivos OBJECT IDENTIFIER ::= {nom 197}

nomABinario OBJECT IDENTIFIER ::= {nomArchivos 1}
nomATexto    OBJECT IDENTIFIER ::= {nomArchivos 2} -- Extensiones
nomAT-TXT    OBJECT IDENTIFIER ::= {nomATexto 1}   -- .txt
nomAT-TEX    OBJECT IDENTIFIER ::= {nomATexto 2}   -- .tex
nomAT-PS     OBJECT IDENTIFIER ::= {nomATexto 3}   -- .ps
nomAT-HTML   OBJECT IDENTIFIER ::= {nomATexto 4}   -- .htm .html

nomAAudio    OBJECT IDENTIFIER ::= {nomArchivos 3} -- Extensiones
nomAA-AU     OBJECT IDENTIFIER ::= {nomAAudio 1}   -- .au
nomAA-WAV    OBJECT IDENTIFIER ::= {nomAAudio 2}   -- .wav
nomAA-MP3    OBJECT IDENTIFIER ::= {nomAAudio 3}   -- .mp3
nomAA-RAM    OBJECT IDENTIFIER ::= {nomAAudio 4}   -- .ram
```

```

nomAVideo OBJECT IDENTIFIER ::= {nomArchivos 4} -- Extensiones
nomAV-MPEG OBJECT IDENTIFIER ::= {nomAVideo 1} -- .mpg .mpeg
nomAV-DVD OBJECT IDENTIFIER ::= {nomAVideo 2} -- PENDIENTE
nomAV-MOV OBJECT IDENTIFIER ::= {nomAVideo 3} -- .mov .qt .movie .moov

nomAImagen OBJECT IDENTIFIER ::= {nomArchivos 5} -- Extensiones
nomAI-JPEG OBJECT IDENTIFIER ::= {nomAImagen 1} -- .jpeg .jpg
nomAI-GIF OBJECT IDENTIFIER ::= {nomAImagen 2} -- .gif
nomAI-BMP OBJECT IDENTIFIER ::= {nomAImagen 3} -- .bmp

nomAMicrosoft OBJECT IDENTIFIER ::= {nomArchivos 6} -- Extensiones
nomAM-WORD OBJECT IDENTIFIER ::= {nomAMicrosoft 1} -- .doc
nomAM-W6 OBJECT IDENTIFIER ::= {nomAM-WORD 1}
nomAM-W97 OBJECT IDENTIFIER ::= {nomAM-WORD 2}
nomAM-W2000 OBJECT IDENTIFIER ::= {nomAM-WORD 3}
nomAM-PPT OBJECT IDENTIFIER ::= {nomAMicrosoft 2} -- .ppt
nomAM-EXCEL OBJECT IDENTIFIER ::= {nomAMicrosoft 3} -- .xls
nomAM-OUTLOOK OBJECT IDENTIFIER ::= {nomAMicrosoft 4} -- .pst
nomAM-ACCESS OBJECT IDENTIFIER ::= {nomAMicrosoft 5} -- .mdb
--
-- Identificadores de objeto a utilizar para identificacion de usuarios
--
nomIdentificacion OBJECT IDENTIFIER ::= {nom 373}

nomIPersonaFisica OBJECT IDENTIFIER ::= {nomIdentificacion 1}
nomIF-NOMBRE OBJECT IDENTIFIER ::= {nomIPersonaFisica 1}
nomIF-IFE OBJECT IDENTIFIER ::= {nomIPersonaFisica 2}
nomIF-CURP OBJECT IDENTIFIER ::= {nomIPersonaFisica 3}
nomIF-PASAPORTE OBJECT IDENTIFIER ::= {nomIPersonaFisica 4}
nomIF-CEDULAFISCAL OBJECT IDENTIFIER ::= {nomIPersonaFisica 5}

nomIPersonaMoral OBJECT IDENTIFIER ::= {nomIdentificacion 2}
nomIM-NOMBRE OBJECT IDENTIFIER ::= {nomIPersonaMoral 1}
nomIM-CURP OBJECT IDENTIFIER ::= {nomIPersonaMoral 2}
nomIM-CEDULAFISCAL OBJECT IDENTIFIER ::= {nomIPersonaMoral 3}

NombrePersonaFisica ::= SEQUENCE {
    nombreIdP PrintableString,
    apellido1IdP PrintableString,
    apellido2IdP PrintableString
}

IdentificadorPersona ::= SEQUENCE {
    nombreIdP NombrePersonaFisica,
    tipoIdP OBJECT IDENTIFIER,
    contenidoIdP PrintableString
}

NumeroCertificado ::= PrintableString

IdentificadorUsuario ::= SEQUENCE {
    personaFisicaMoral OBJECT IDENTIFIER,
    nombreRazonSocialIdU CHOICE {NombrePersonaFisica, PrintableString},
    tipoIdU OBJECT IDENTIFIER,
    contenidoIdU PrintableString,
    numeroCertificadoU NumeroCertificado,
    representanteIdU IdentificadorPersona OPTIONAL -- Este campo es para el
                                                    -- representante legal
}

AlgorithmIdentifier ::= SEQUENCE {
    algorithm OBJECT IDENTIFIER,
    NULL
}

NombreConstanciaOP ::= PrintableString

FirmaUsuarioOP ::= SEQUENCE {
    algoritmoFirma AlgorithmIdentifier,
    firma BIT STRING
}

```



```

}
FirmaConstanciaOP ::= SEQUENCE {
    algoritmoFirma      AlgorithmIdentifier,
    firma               BIT STRING
}
ResumenOP ::= SEQUENCE {
    algoritmoResumen   AlgorithmIdentifier,
    resumen            BIT STRING
}
Folio-UsuarioOP ::= INTEGER
ArchivoParcial ::= SEQUENCE {
    titulo             NombreOP,
    tipo               TipoOP,
    contenido          BIT STRING
}
Entrada-al-Indice ::= SEQUENCE {
    titulo             NombreOP,
    resumen            ResumenOP
}
Expediente ::= SEQUENCE {
    nombre-expediente PrintableString,
    indice             SET OF Entrada-al-Indice,
    id-usuario         IdUsuarioOP,
    firma-usuario      FirmaUsuarioOP
}
Sello ::= SEQUENCE {
    estampa-de-tiempo UTCTime,
    emisor             EmisorOP,
    folio-usuario      Folio-UsuarioOP
}
Constancia ::= SEQUENCE {
    nombre-de-la-constancia NombreConstanciaOP,
    expediente              Expediente,
    marca-de-tiempo         Sello,
    firma-constancia        FirmaConstanciaOP
}
END
=====

```

En el programa ASN.1 se definen primeramente los identificadores de objeto necesarios para identificar los tipos de archivo que se podrán almacenar observando la presente Norma Oficial Mexicana; estas definiciones podrían ser objeto de revisiones periódicas para incluir nuevos formatos, luego los objetos necesarios para almacenar los archivos o mensajes de datos que serán conservados.

A lo largo del programa se definen diferentes objetos ASN.1 cuyo uso dentro del programa aclara su función.

El campo *firma-usuario* del objeto *expediente* es la firma digital de los campos *nombre-expediente*, *indice* e *id-usuario* concatenados en ese orden, vistos como una secuencia de bytes.

En el objeto *sello*, el campo *estampa-de-tiempo* es la fecha y hora en formato GMT o IMT con la cual se creó el *sello*, *emisor* es el representante del prestador de servicios de certificación que está creando el *sello* y *folio-usuario* es un número secuencial ascendente para cada usuario registrado del prestador de servicios de certificación. Es decir, cada usuario llevará un registro numerado consecutivamente de cada operación que registra el prestador de servicios de certificación.

El objeto *Constancia* contiene un campo *nombre-de-la-constancia* que almacena el nombre del archivo de computadora donde se guardará dicha *constancia* en el sistema de información del prestador de servicios de certificación, *expediente* que es de tipo *Expediente* y es la información que se registra con el prestador de servicios de certificación con un *sello* emitido por ella, este *sello* contiene la fecha y la hora del momento en que se crea la *Constancia*. El campo *firma-constancia* es la firma digital de los campos *nombre-de-la-constancia*, *expediente*, *marca-de-tiempo* concatenados en ese orden y vistos como una secuencia de bytes.

El ejemplo de codificación está organizado de la siguiente forma: primero se presentan dos archivos que se desea conservar, a continuación se construyen cada uno de los objetos ASN.1 correspondientes, (i) los *archivos parciales*, (ii) el *expediente* que está almacenado en un archivo de nombre "docusuario.ber" y (iii) la *Constancia* que está en el archivo "recibo.ber". Los nombres de los archivos que almacenan al *expediente*, *constancia* y *archivos parciales* están almacenados en los campos nombre-expediente, nombre-de-la-constancia y título respectivamente (ver Definición ASN.1).

Enseguida se presenta el contenido de los objetos ASN.1 correspondientes. La línea "======" representa el principio y el fin del archivo respectivamente y no forma parte del archivo.

Los objetos ASN.1 que se presentan están en formato BER y se muestra un vaciado hexadecimal comentado.

Archivo "mensaje.txt"

```
=====  
Archivo de texto utilizado para ejemplificar la creacion de documentos de  
usuario y constancias de la Oficialia de Partes. Este es uno de dos archivos  
que se utilizaran en dicho ejemplo.  
=====
```

Archivo "mensaje1.txt"

```
=====  
Segundo archivo de texto que se utilizara en la creacion de un ejemplos  
para mostrar un documento usuario y una constancia de la oficialia de partes.  
=====
```

Archivo parcial "arpl.ber"

```
=====
30 81 d7 /*ArchivoParcial*/
  13 0b 6d 65 6e 73 61 6a 65 2e 74 78 74 /*titulo:mensaje.txt*/
  06 09 75 81 09 81 33 81 45 02 01 /*tipo:nomAT-TXT*/
  03 81 bc /*contenido*/
    00 41 72 63 68 69 76 6f 20 64 65 20 74 65 78 74 6f 20 75 74 69 6c 69
7a 61 64 6f 20 70 61 72 61 20 65 6a 65 6d 70 6c 69 66 69 63 61 72 20 6c 61
20 63 72 65 61 63 69 6f 6e 20 64 65 20 64 6f 63 75 6d 65 6e 74 6f 73 20 64
65 0a 75 73 75 61 72 69 6f 20 79 20 63 6f 6e 73 74 61 6e 63 69 61 73 20 64
65 20 6c 61 20 4f 66 69 63 69 61 6c 69 61 20 64 65 20 50 61 72 74 65 73 2e
20 45 73 74 65 20 65 73 20 75 6e 6f 20 64 65 20 64 6f 73 20 61 72 63 68 69
76 6f 73 0a 71 75 65 20 73 65 20 75 74 69 6c 69 7a 61 72 61 6e 20 65 6e 20
64 69 63 68 6f 20 65 6a 65 6d 70 6c 6f 2e 0a
=====
```

Archivo parcial "arp2.ber"

```
=====
30 81 b3 /*ArchivoParcial*/
  13 0c 6d 65 6e 73 61 6a 65 31 2e 74 78 74 /*titulo:mensaje1.txt*/
  06 09 75 81 09 81 33 81 45 04 01 /*tipo:nomAV-MPEG*/
  03 81 97 /*contenido*/
    00 53 65 67 75 6e 64 6f 20 61 72 63 68 69 76 6f 20 64 65 20 74 65 78
74 6f 20 71 75 65 20 73 65 20 75 74 69 6c 69 7a 61 72 61 20 65 6e 20 6c 61
20 63 72 65 61 63 69 6f 6e 20 64 65 20 75 6e 20 65 6a 65 70 6d 6c 6f 73 0a
70 61 72 61 20 6d 6f 73 74 72 61 72 20 75 6e 20 64 6f 63 75 6d 65 6e 74 6f
20 75 73 75 61 72 69 6f 20 79 20 75 6e 61 20 63 6f 6e 73 74 61 6e 63 69 61
20 64 65 20 6c 61 20 6f 66 69 63 69 61 6c 69 61 20 64 65 20 70 61 72 74 65
73 2e 0a
=====
```

Expediente "docusuario.ber"

El expediente en formato BER correspondiente a los *archivos parciales* que aparecen arriba es:

```
=====
30 82 01 4b /*expediente electrónico-usuario:*/
  13 0f 64 6f 63 75 6d 65 6e 74 6f 20 23 20 34 35 36 /*nombre-expediente
electrónico:documento # 456*/
  31 5e /*indice:*/
    30 2d /*Entrada-al-Indice:*/
      13 08 61 72 70 31 2e 62 65 72 /*titulo:arpl.ber*/
      30 21 /*resumen:*/
        30 0c /*algoritmo resumen:*/
          06 08 2a 86 48 86 f7 0d 02 05 /*Identificador de Objeto: md5*/
          05 00 /*NULL*/
          03 11 00 23 e7 4a 8a be d5 60 dd ec 07 5c 66 44 29 71 c2 /*resumen*/
        30 2d /*Entrada-al-Indice:*/
```

```
13 08 61 72 70 32 2e 62 65 72 /*titulo:arp2.ber*/
30 21 /*resumen:*/
    30 0c /*algoritmo resumen:*/
        06 08 2a 86 48 86 f7 0d 02 05 /*Identificador de Objeto: md5*/
        05 00 /*NULL*/
    03 11 00 8c c0 81 b0 ce 66 e9 b7 90 5a 96 05 e8 38 13 20 /*resumen*/
30 64 /*id-usuario*/
    06 08 75 81 09 81 33 82 75 01 /*peronaMoralFisica: nomIPersonaFisica*/
    30 1c /*nombreRazonSocialIdU:*/
        13 08 52 61 79 6d 75 6e 64 6f /*Raymundo*/
        13 07 50 65 72 61 6c 74 61 /*Peralta*/
        13 07 48 65 72 72 65 72 61 /*Herrera*/
    06 09 75 81 09 81 33 82 75 01 03 /*tipopIdU: nomIF-CURP*/
    13 2f 41 71 75 69 20 76 61 20 6c 61 20 43 6c 61 76 65 20 55 6e 69
63 61 20 64 65 20 52 65 67 69 73 74 72 6f 20 64 65 20 50 6f 62 6c 61 63 69
6f 6e /*contenidoIdU:Aqui va la Clave Unica de Registro de Poblacion*/
    30 72 /*firma-usuario:*/
    30 0d /*algoritmoFirma:*/
        06 09 2a 86 48 86 f7 0d 01 01 04 /*Identificador de Objeto:
md5WithRSAEncryption*/
        05 00 /*NULL*/
    03 61 /*firma:*/
        00 6f 06 26 71 0e 7a 2a 55 33 f2 e1 cc 1b 44 de 3a 40 e9 b3
0d 87 ee 32 5d 90 5b 7c b2 29 72 56 d8 57 88 6d e4 37 c2 7b 95 2f 32 f8 72
15 87 ce 95 71 39 66 3c b2 d7 25 76 08 15 49 07 cf 2c 87 04 87 f5 f3 d6 31
c3 d0 13 16 1b 26 fc f2 6b 73 63 2c 37 e1 ce d6 0a a7 b4 30 57 df 96 c5 6d
30 98
=====
```

Constancia "recibo.ber"

Finalmente la *constancia* del prestador de servicios de certificación contiene una copia del *expediente* más la *estampa de tiempo* y la identificación del prestador de servicios de certificación que la generó.

```
=====
30 82 02 f0 /*Constancia de la Oficialia de Partes*/
    13 0a 72 65 63 69 62 6f 2e 62 65 72 /*nombre-de-la-constancia:recibo.ber*/
    30 82 01 4b /*expediente electrónico-usuario:*/
        13 0f 64 6f 63 75 6d 65 6e 74 6f 20 23 20 34 35 36 /*nombre-expediente
electrónico:documento # 456*/
    31 5e /*indice:*/
        30 2d /*Entrada-al-Indice:*/
            13 08 61 72 70 31 2e 62 65 72 /*titulo:arpl.ber*/
            30 21 /*resumen:*/
                30 0c /*algoritmo resumen:*/
                    06 08 2a 86 48 86 f7 0d 02 05 /*Identificador de Objeto: md5*/
                    05 00 /*NULL*/
                03 11 00 23 e7 4a 8a be d5 60 dd ec 07 5c 66 44 29 71 c2
/*resumen*/
            30 2d /*Entrada-al-Indice:*/
                13 08 61 72 70 32 2e 62 65 72 /*titulo:arp2.ber*/
                30 21 /*resumen:*/
                    30 0c /*algoritmo resumen:*/
                        06 08 2a 86 48 86 f7 0d 02 05 /*Identificador de Objeto: md5*/
                        05 00 /*NULL*/
```

```
03 11 00 8c c0 81 b0 ce 66 e9 b7 90 5a 96 05 e8 38 13 20
/*resumen*/
 30 64 /*id-usuario*/
06 08 75 81 09 81 33 82 75 01 /*peronaMoralFisica: nomIPersonaFisica*/
 30 1c /*nombreRazonSocialIdU:*/
13 08 52 61 79 6d 75 6e 64 6f /*Raymundo*/
13 07 50 65 72 61 6c 74 61 /*Peralta*/
13 07 48 65 72 72 65 72 61 /*Herrera*/
06 09 75 81 09 81 33 82 75 01 03 /*tipopIdU: nomIF-CURP*/
13 2f 41 71 75 69 20 76 61 20 6c 61 20 43 6c 61 76 65 20 55 6e 69
63 61 20 64 65 20 52 65 67 69 73 74 72 6f 20 64 65 20 50 6f 62 6c 61 63 69
6f 6e /*contenidoIdU:Aqui va la Clave Unica de Registro de Poblacion*/
 30 72 /*firma-usuario:*/
 30 0d /*algoritmoFirma:*/
06 09 2a 86 48 86 f7 0d 01 01 04 /*Identificador de Objeto:
md5WithRSAEncryption*/
05 00 /*NULL*/
03 61 /*firma:*/
00 6f 06 26 71 0e 7a 2a 55 33 f2 e1 cc 1b 44 de 3a 40 e9 b3
0d 87 ee 32 5d 90 5b 7c b2 29 72 56 d8 57 88 6d e4 37 c2 7b 95 2f 32 f8 72
15 87 ce 95 71 39 66 3c b2 d7 25 76 08 15 49 07 cf 2c 87 04 87 f5 f3 d6 31
c3 d0 13 16 1b 26 fc f2 6b 73 63 2c 37 e1 ce d6 0a a7 b4 30 57 df 96 c5 6d
30 98
 30 81 fc /*marca-de-tiempo:*/
17 0d 30 31 30 34 33 30 31 33 32 33 32 32 5a /*estampa-de-
tiempo:010430132322Z */
 30 81 e7 /*emisor:*/
06 08 75 81 09 81 33 82 75 02 /*personaMoralFisica:
nomIPersonaMoral*/
13 1c 4f 66 69 63 69 61 6c 69 61 20 64 65 20 50 61 72 74 65 73
20 4e 75 6d 65 72 6f 20 31 /*nombreRazonSocialIdU:Oficialia de Partes Numero 1*/
06 09 75 81 09 81 33 82 75 02 03 /*tipoIdU: nomIM-CEDULAFISCAL*/
13 2a 41 71 75 69 20 76 61 20 6c 61 20 63 65 64 75 6c 61 20 64
65 20 69 64 65 6e 74 69 66 69 63 61 63 69 6f 6e 20 66 69 73 63 61 6c
/*contenidoIdU:
Aqui va la cedula de identificacion fiscal*/
 30 81 85 /*representanteIdU:*/
 30 4c /*nombreIdP:*/
13 11 4e 6f 6d 62 72 65 20 64 65 6c 20 65 6d 69 73 6f 72
/*nombreIdP:
Nombre del emisor*/
13 1a 50 72 69 6d 65 72 20 41 70 65 6c 6c 69 64 6f 20 64
65 6c 20 65 6d 69 73 6f 72 /*apellido1IdP:Primer Apellido del emisor*/
13 1b 53 65 67 75 6e 64 6f 20 41 70 65 6c 6c 69 64 6f 20
64 65 6c 20 65 6d 69 73 6f 72 /*apellido2IdP:Segundo Apellido del emisor*/
06 09 75 81 09 81 33 82 75 01 02 /*tipoIdP: nomIF-IFE*/
13 2a 4e 75 6d 65 72 6f 20 64 65 20 6c 61 20 43 72 65 64 65
6e 63 69 61 6c 20 64 65 20 45 6c 65 63 74 6f 72 20 64 65 6c 20 49 46 45
/*contenidoIdP:
Numero de la Credencial de Elector del IFE*/
02 01 01 /*folio-usuario:1*/
 30 81 93 /*firma-constancia:*/
 30 0d /*algoritmoFirma:*/
06 09 2a 86 48 86 f7 0d 01 01 04 /*Identificador de Objeto
md5WithRSAEncryption*/
05 00 /*NULL*/
```

```
03 81 81 /*firma:*/  
00 94 c1 94 4a 8c 32 59 5d 5f b8 2c f8 6c fc f4 d7 b0 1f 24 81  
b9 ad ba 2d db 7e c8 43 f4 25 5e cf d6 40 a9 2e f8 d0 02 59 1a b2 99 95 76  
5e 56 ee f6 e8 4b ee 0b 45 3d 3f 50 86 12 f4 74 f4 17 59 2f e5 45 d2 d9 d6  
d6 ec f7 e6 58 54 f8 da c2 8e a8 6b 9f d3 0f e1 cd 87 de 2d 38 85 ee 56 cd  
03 53 c9 c6 49 f3 36 b3 a6 d9 03 3a d6 e7 16 db 6d 82 89 54 93 8d 92 f9 2b  
5f 63 10 1e e6 bb 94 78  
=====
```

### Claves privadas usadas para firmar

Con el propósito de poder verificar los objetos ASN.1 definidos en este documento se incluyen las claves privadas que fueron usadas para generar las firmas de los documentos mencionados. Durante el proceso de generación de claves no se generó la clave pública y ya se ha perdido la información de generación de dichas claves. Las claves y los resultados presentados pueden ser usadas únicamente para verificar los formatos de este ejemplo.

### Clave privada de usuario

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-CBC, 4DE1D2C3EC19A11A

BmLA5XLigZn3knYyUQSrxeeUI+p7gRqB5bIP8ONUp4SAgELue0mlx1sGYAKuSbuX
lZo5ytQTzq33AKd/e4MfTHLVDwDK3mhtG9vRpOevJLOejxDhT11kN9kbbS+MGoxC
ht2OSH19vjrXGbUfnaO2Z7oBb3fTbE4XRtQq+ZcuuQa4KAyikTVr/IFKsxvc8Y1N
FYyXLSM6jBxS4cnBQe9GGFC+38relyfnK26HYTiQeVhzXZmer2ybxhQLadD3CgY7
k1UWvyUCGxOayMY01ZdgQrly78H7AbbLKucdWNOt5vrTy0vKn2+6FslAuGT8PcvT
ehRGixMG7IsAWobYKbncYDGk7NV8MRRmdioQR7FFhTfPWRUdd7dPQgwMbnMxlz/
wTXcPgrlqV2/RhA8r+AuboV6/et5tfc+8vBvodwzTSgZasGdeDhctdN6QvtmUv1v
W1tx1lNOXZU/ebjDn2FR00aUnLhEqt7h3FBdaT3pzn7g6N7jcyAnDD3h81N76E8H
UK1xCACgIr6gQ30muZfwtO2aDRT75j7obUvzdlxbmcN4GCF62/5eIDt8djeLDhH7
PZVrb8qpF6fQ8BJZ/j1Ptr7tilguRzXNmhl8YBO7QyA=
-----END RSA PRIVATE KEY-----
```

### Clave privada del prestador de servicios de certificación

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-CBC, 74C87323189C03C7

AgINEuo+G75BpZkiQ2juE2j/etkKgve0zsU0TYagcQNjFZsb35MaY0IjUzMG0f2h
72OxJALQEt9RgW+xQX24v7QSAmporEFkUs7D1hqtRrRtv5H+2Ob8i+uoFLePZtjt
LfdVebJgCHxRDjW9tvW11qEBgsjyQQiwYq7BKcqhKP6CnpGyid5QOIYJUb8dE4W
x7r33oltUuVA8djR4A9UX34w0fnNoicqGh30/xpKEF4znguwk3uAck7pskb8KFJ
ieOGh4fbpozKNYARh+YRYZc827YehT54bRu+bUauABRomFCBH8A0dcvHA47pO2/n
mYpU0R34d50uBuONZQGPTuDZXiEa448X1B4kkhcljAndfJ30SnAunCFYFcJ0iJFq
oP4cJ2/5OWq1gQPpw639P3+to0FbgyargutRFFv005efq000HKx7MzM+eGc5v1Z/
jf2W41C7OZzbT8sw1ho7T9C9vqC9H60UZnqzeLpwUOxyF2LzBVU9hI3LBxvJya+J
cN7jX5cBG20wZl6GOSrXSAiAhW7bEgzvuGXFEf3x0EYwq3gWIk6wqrB9Ki9h57N
WSz8b9e1IvoFwxSV79N05MZ0szT5oGjxqbsIb1xJlvalPmk5VL96gzCb5sXiDS6P
fE1/KGzJ7SsKmZ2jgDSYifwFrL7qTX4efsDdXOEgQnshlLaUNp8gf1nDvftWMrF/
WrA0VM8paAXr6QByrcAy5lgIn3vpaX5AaG+jGM5RFR1hzmazf21yKYFqn1j25+zsM
YzQN5vhH5pDkWBtXkQ/JxgLAB5LKEIoMyTlL3DR2gtqPgeZBwcJoYg==
-----END RSA PRIVATE KEY-----
```

## **Front End de Comunicaciones (FEC, referencia de implantación para el prestador de servicios de certificación)**

### Introducción

El FEC es un programa desarrollado para manejar las comunicaciones en aplicaciones con arquitectura cliente/servidor, fue diseñado pensando en aplicaciones que requieran intercambiar mensajes en tiempo real. Se puede usar la definición de este sistema para especificar el protocolo de comunicación entre los clientes del prestador de servicios de certificación y los sistemas que se indican en la presente Norma Oficial Mexicana. La Secretaría de Economía deberá contar con un sistema de referencia para que el o los

prestadores de servicios de certificación tengan un estándar contra el cual verificar que la implantación de la norma es correcta.

Los objetivos del FEC son:

Simplificar la programación de los sistemas con arquitectura cliente/servidor, de tal manera que al desarrollar un sistema se dejen a un lado los detalles relacionados al manejo de las comunicaciones y el esfuerzo se centre en los detalles propios del sistema.

Lograr un ambiente de operación flexible que permita la interacción de programas desarrollados en distintas plataformas, sistemas operativos y lenguajes.

Optimar el uso de los recursos y permitir que los sistemas que lo usen operen en tiempo real.

El FEC se encarga de realizar algunas tareas que, en la arquitectura cliente/servidor tradicional, serían realizadas por el servidor, por ejemplo:

Autenticar a los clientes que desean establecer comunicación con algún servidor.

Notificar la conexión o desconexión de un cliente al servidor adecuado.

Notificar a los clientes si un servidor está o no en servicio.

Verificar continuamente el estado de los clientes y servidores conectados.

Es por ello que su uso proporciona las siguientes ventajas:

Provee de transparencia en la localización de clientes y servidores.

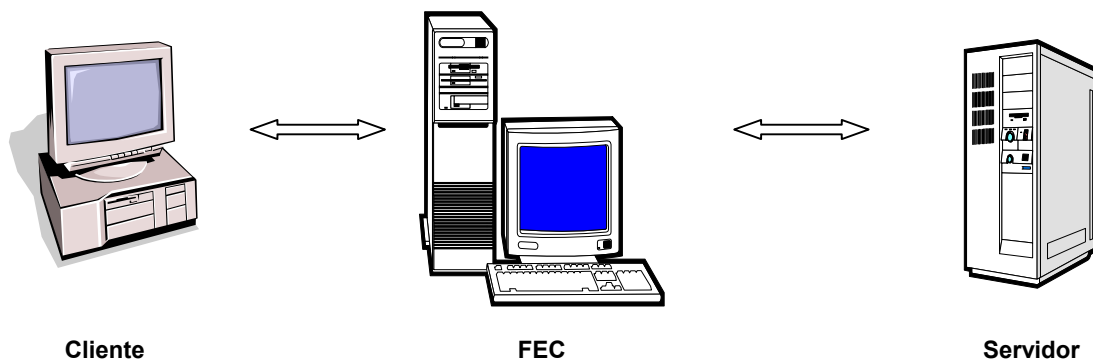
Simplifica la programación de servidores.

Permite la interacción de programas desarrollados en distintas plataformas.

Minimiza el uso de recursos de la red de comunicaciones.

### Esquema de operación

El modelo básico de operación del FEC se muestra en la figura 1, en ella se esquematiza un programa cliente, el FEC y un programa servidor. El esquema de operación es simple: el FEC se encarga de aceptar las conexiones de los clientes, autenticar y, en caso de que el servicio al que se deseen conectar se encuentre en operación, avisar a este último de la conexión del cliente.



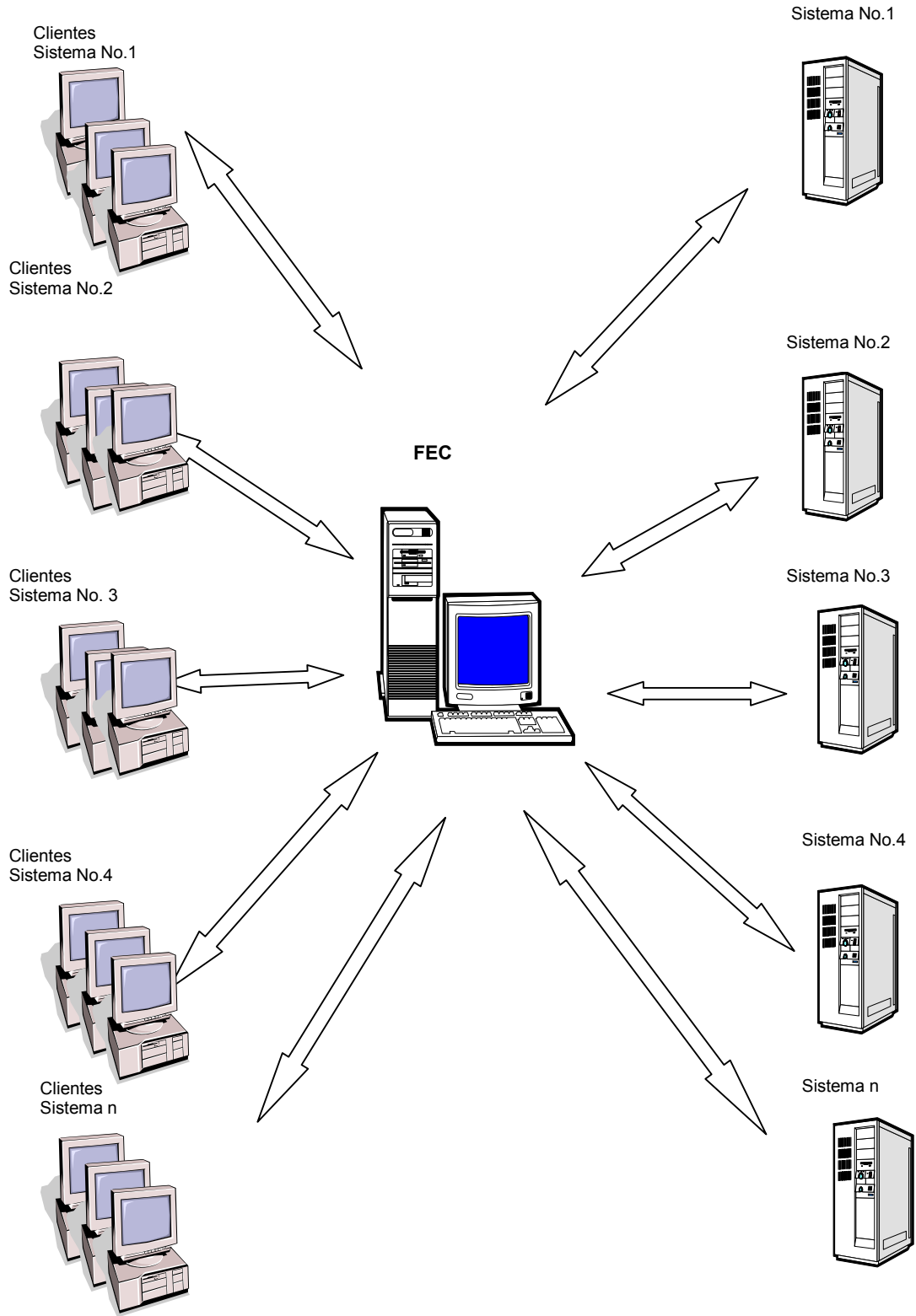
**Figura 1. Esquema básico de operación del FEC**

En este esquema los clientes no establecen comunicación directa con el servidor, en lugar de ello envían sus mensajes a través del FEC, éste los toma y los entrega al servidor adecuado.



Del mismo modo, el FEC recibe los mensajes del servidor y los entrega al cliente indicado por éste.

Visto a grandes rasgos, una vez realizada la autenticación de clientes y servidores, la labor del FEC se limita a registrar y transmitir los mensajes de los clientes al servidor adecuado y viceversa, es decir, el FEC es únicamente un mecanismo de enlace entre clientes y servidores.



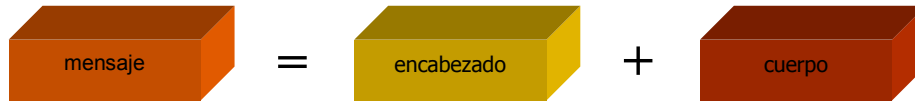
En la figura 2 se muestra un esquema de la operación del FEC

## Comunicaciones en el FEC

### Manejo de Comunicaciones en el FEC

A fin de minimizar el tráfico en la red de comunicaciones y permitir el intercambio de información entre programas desarrollados en distintos lenguajes y sistemas operativos, el FEC utiliza un protocolo de comunicación abierto.

En este protocolo todos los mensajes constan de dos partes: encabezado y cuerpo, como se muestra en la figura 3.



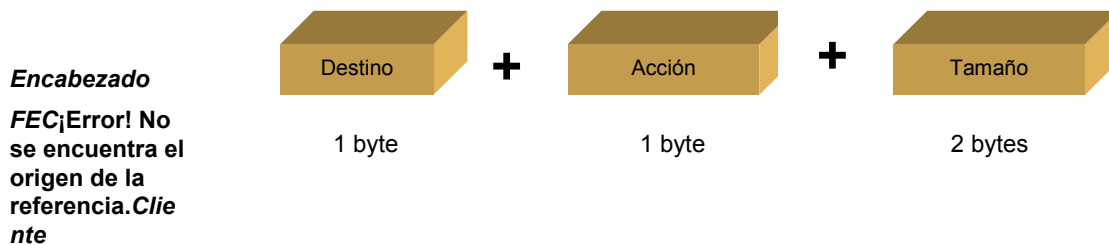
**Figura 3. Todos los mensajes están formados por encabezado y cuerpo**

Tanto el encabezado como el cuerpo de los mensajes se construyen con los tipos de datos básicos de todos los lenguajes de programación: char, int, short, string.

Es importante mencionar que el protocolo utilizado permite, a partir de los tipos de datos mencionados y respetando ciertas reglas (similares a las de las expresiones regulares), construir cualquier tipo de mensaje. La única restricción para que los programas intercambien información es que acuerden de antemano el "formato" de los mensajes que se enviarán durante la operación.

### Encabezado de los Mensajes

En el protocolo del FEC, la longitud del encabezado de un mensaje depende del destinatario, por ejemplo, en los mensajes que envían los clientes y servidores hacia el FEC, así como los mensajes que envía el FEC a los clientes, el encabezado tiene una longitud de 4 bytes con la estructura que se muestra en la figura 4.



**Figura 4. Encabezado de un mensaje FEC Cliente**

A continuación se explican los campos que lo forman:

*Destino.* Servidor o Cliente a quien se desea enviar el mensaje (1 byte).

*Acción.* Instrucción o procesamiento que se desea realizar (1 byte).

*Tamaño.* Longitud en bytes del cuerpo del mensaje, sin incluir el encabezado (2 bytes).

Por otra parte, el encabezado de los mensajes que el FEC envía a los servidores tiene una longitud de 12 bytes y la estructura que se muestra en la figura 5.

Los elementos que conforman este encabezado son:

*Origen.* Cliente que envía el mensaje (1 byte).

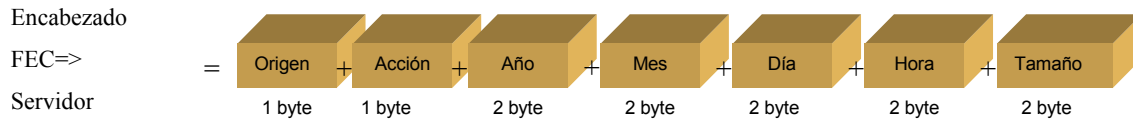
*Acción.* Instrucción o procesamiento que se desea realizar (1 byte).

*Año, Mes, Día.* Fecha en que el FEC recibió el mensaje (2 bytes cada campo).

*Hora.* Hora en que el FEC recibió el mensaje.

*Tamaño.* Longitud en bytes del cuerpo del mensaje, sin incluir el encabezado (2 bytes).

La existencia de estos dos tipos de encabezado se debe a la necesidad de llevar un registro detallado de los mensajes que se transfieren a los servidores a través del FEC, además de proveer un cierto grado de seguridad. Es por ello que antes de transferir un mensaje a un servidor, el FEC debe colocarle una estampa de tiempo que certifique la fecha y hora en que se recibió.



**Figura 5. Encabezado de un mensaje FEC => Servidor**

### Cuerpo de los mensajes

Esta parte del mensaje es de longitud variable y puede construirse como una expresión regular a partir de los tipos de datos mencionados anteriormente.

El elemento *Acción* en el encabezado de un mensaje indica la solicitud de que se ejecute una determinada instrucción o procesamiento. En algunos casos, para realizar dicha *Acción* se requiere de información adicional. El contenido e interpretación del cuerpo de un mensaje depende de la *Acción* indicada en su encabezado, es decir, el cuerpo de un mensaje debe respetar un “formato” previamente establecido entre quien lo envía y quien debe ejecutar la acción solicitada.

Como este “formato” se establece de antemano entre los interesados, cuando se recibe un mensaje basta conocer la *Acción* del encabezado para deducir la forma en que debe interpretarse el cuerpo, es decir, su “formato”.

El “formato” de un mensaje es una secuencia de tipos de datos básicos que describe su contenido. Para facilitar la lectura e interpretación de estas secuencias, a cada tipo de dato se le ha asignado un símbolo, el cual se muestra a continuación<sup>2</sup> :

Tipo de dato	Símbolo	Tamaño en bytes
Char	%c	1
Int	%l	4
Short	%d	2
String	%s	Libre
N	n	4

**Nota:** Dado que el protocolo de comunicación del FEC es abierto, toda la información viaja en formato de red.

### Interpretación del formato de un mensaje

Para reafirmar la idea de “formato”, a continuación se muestra el “formato” del encabezado y cuerpo de algunos mensajes utilizados por el protocolo del FEC.

Formato del encabezado de 4 bytes: “%c%c%d”. En una trama de bytes con este formato viajan tres datos. El primer y segundo dato vienen en el primer y segundo bytes de la trama respectivamente. El valor del tercer dato debe obtenerse de los dos últimos bytes de la trama. Lo anterior puede deducirse de la tabla donde se muestra la longitud de los elementos que conforman los mensajes<sup>3</sup> .

Formato del encabezado de 12 bytes: “%c%c%d%d%d%d%d”. En una trama de bytes con este formato contiene siete datos. Los dos primeros tienen una longitud de un byte y los restantes 5 de dos bytes cada uno.

Formato del mensaje Greeting “%s %l”. Este mensaje se utiliza para avisar a un servidor de la conexión de un cliente. Contiene dos datos: el nombre del cliente en una cadena de longitud indefinida, pero terminada con el carácter de fin de cadena, y a continuación su clave en un valor de 4 bytes.

Formato del mensaje Login: “%s”. Se utiliza cuando un cliente envía su login a un servidor, contiene una cadena con la información.

<sup>2</sup> El tipo de dato string que se maneja en el protocolo no tiene una longitud fija e incluye el carácter de fin de cadena. Es muy importante que se considere la longitud de cada tipo de dato al desarrollar su software, sobretodo si utiliza un sistema operativo diferente a Linux.

<sup>3</sup> Tome en cuenta las longitudes de los tipos de datos mostrados en la tabla de la sección anterior y además recuerde que los datos viajan en formato de red, es decir, una vez obtenidos deberán transformarse al formato de la computadora receptora.

Formato cualquiera: "%c %d %l %s n(%c %d %l %s)". Este formato contiene un número variable de datos. Podemos deducir que primero viene un dato que ocupa un byte (es decir un valor entre 0 y 255), después un dato que ocupa 2 bytes, luego uno que ocupa 4 bytes, a continuación una cadena cuya longitud se desconoce y después una serie de "n" elementos, este número "n" es un valor de 4 bytes. A continuación vienen "n" elementos de un byte, "n" elementos de 2 bytes, "n" elementos de 4 bytes y finalmente "n" cadenas.

Este último formato muestra el potencial del protocolo de comunicación, el cual permite construir mensajes de longitud y contenido variable.

### Construcción de mensajes

Dado que el campo Acción en el encabezado de un mensaje tiene una longitud de 1 byte, existen únicamente 255 acciones válidas en la operación de un sistema.

Aunque cada aplicación es la encargada de determinar el número de acciones que requiere y la información que debería incluirse en el cuerpo de los mensajes a enviar, resulta evidente que existe un conjunto de acciones comunes a todos los sistemas que interactúen con el FEC (por ejemplo los mensajes para establecer o terminar la conexión con el FEC); es por ello que algunos de los 255 posibles mensajes están reservados a estas acciones comunes a todos los sistemas. En esta sección se indican cuáles son estos mensajes reservados y se dan ejemplos de su construcción.

### Mensajes reservados

En esta sección se muestran los mensajes que deben usar los programas que se desee establecer comunicación con el FEC y el formato de éstos el hecho de que no aparezca un formato asociado a un tipo de mensaje indica que no se requiere información adicional para realizar la acción solicitada, es decir, este tipo de mensajes tienen un cuerpo nulo. En la siguiente sección se muestra la manera de construirlos.

#### Mensajes reservados para el FEC

Acción	Nombre	Formato	Descripción
236	CONFPASSWD		Confirma a un cliente que su contraseña fue cambiada exitosamente
243	DEADSRVR		Avisa a un cliente que el servidor ha dejado de operar
244	BYE		Avisa a un servidor que un cliente se desconectó
245	AREYOUALIVE		Pregunta a un cliente/servidor si opera correctamente
247	GREETING	%s%l	Avisa a un servidor de la conexión de un cliente. Incluye nombre y clave del cliente
249	CHPSWDFAIL		Avisa a un cliente que su contraseña no pudo ser cambiada
251	LOGINFAIL		Avisa a un cliente que su conexión fue rechazada
252	NOSERVICE		El servidor al que desea conectarse está fuera de servicio
253	LOGGED	%d	Avisa a un cliente que su conexión fue aceptada
254	LOGINREQ		Solicita a un cliente su clave de usuario para autenticarlo
255	PASSWREQ		Solicita a un cliente su contraseña para autenticarla

#### Mensajes comunes a todos los clientes

Acción	Nombre	Formato	Descripción
0	LOGOUT		Avisa al FEC del fin de la conexión
1	LOGIN	%s	Envía clave de usuario al FEC
2	PASSWD	%s	Envía contraseña al FEC
7	IAMALIVE		Avisa al FEC que opera sin problemas

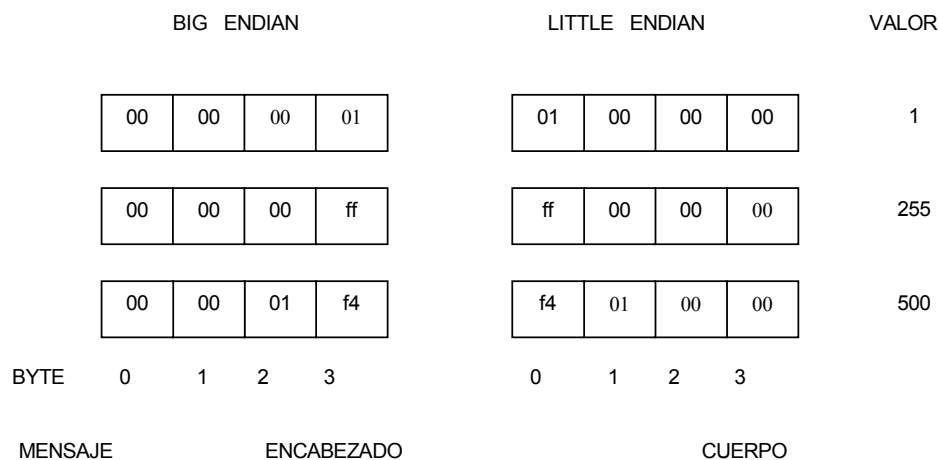
16	CONEXION		Solicita conexión al FEC
212	CHANGEPASS	%s	Solicita cambio de contraseña, envía nueva contraseña al FEC

### Ejemplos de construcción de mensajes

Para lograr que nuestro protocolo sea abierto debemos enviar los datos en una forma tal que cualquier computadora pueda interpretarlos adecuadamente. Por ejemplo, cuando una computadora envía un entero de 32 bits a otra. El hardware se encarga de transportar los bits desde la primer computadora a la segunda sin cambiar el orden, sin embargo, no todas las computadoras almacenan los enteros de 32 bits de la misma manera.

En algunos casos la dirección más baja de memoria contiene el byte menos significativo del entero (formato Little Endian). En otros, la dirección más baja de memoria contiene el byte más significativo del entero (Formato Big Endian). Estas dos maneras de almacenar datos se ilustran en la figura 6<sup>4</sup>.

Internet resuelve el problema del orden de los bytes al definir un estándar de red que debe utilizarse para intercambiar datos. Las computadoras que intercambian información deben convertir sus datos de la representación local a la representación estándar de red antes de enviarlos. Al recibir datos deben convertirlos de la representación estándar de red a la representación local.



**Figura 6. Diferentes Representaciones de Datos**

El estándar de red de Internet indica que primero debe enviarse el byte más significativo de un entero, es decir, si uno considera los bytes sucesivos de un paquete viajando de una computadora a otra, los enteros en ese paquete tienen su byte más significativo cerca del inicio y el byte menos significativo cerca del final del paquete.

Nuestro protocolo utiliza el estándar de red de Internet para intercambiar información. En la figura 7 representamos los mensajes necesarios para que un cliente establezca comunicación con el FEC siguiendo el estándar antes mencionado<sup>5</sup>. No olvide que los valores deben enviarse en formato de red.

<sup>4</sup> En la figura 6 el contenido de cada byte se ha representado en formato hexadecimal únicamente con fines ilustrativos, **esto no significa que en el protocolo los valores deban enviarse en formato hexadecimal.**

<sup>5</sup> Observe que en el campo Destino se ha colocado el valor "1", esto indica que se quiere establecer comunicación con un servidor cuya clave de identificación es "1". Todos los servidores conectados al FEC tienen asignada una clave de identificación.

	Destino	Acción	Tamaño										
CONEXION	1	16	0										
LOGIN	1	1	8	m	i	l	o	g	i	n	\0		
PASSWD	1	2	7	m	i	p	a	s	s	\0			
IMALIVE	1	7	0										
Byte	0	1	2, 3	...									

**Figura 7. Construcción de Mensajes para Conectarse al FEC**

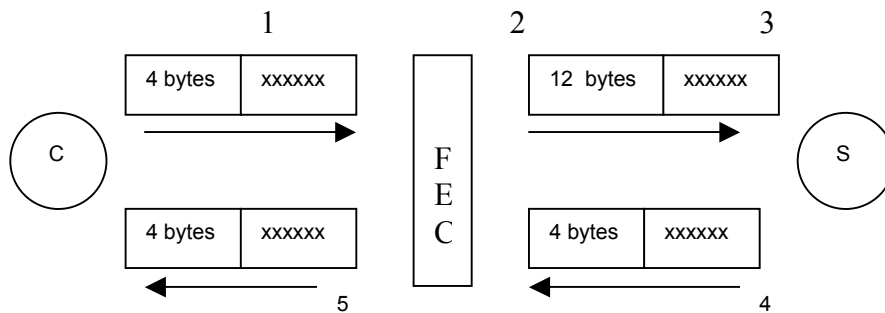
**Secuencia de Conexión**

**Recepción y transmisión de mensajes en el FEC**

La secuencia de recepción y transmisión de mensajes en el FEC se muestra en la figura 8.

El mecanismo es el siguiente:

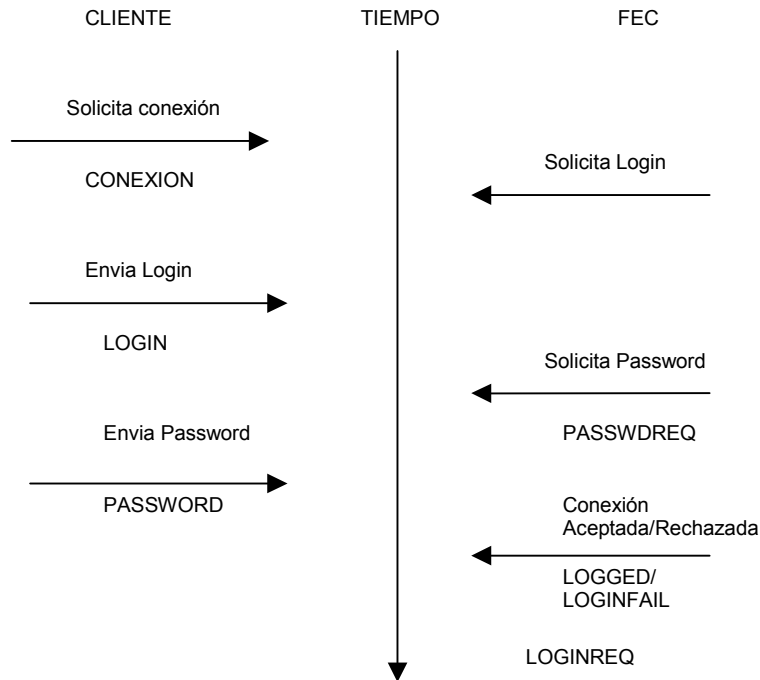
1. El cliente C envía al FEC un mensaje destinado al servidor S, este mensaje tiene un encabezado de 4 bytes.
2. El FEC recibe el mensaje y analiza el encabezado para determinar a quién debe transferirlo, incluye en el encabezado original una estampa de tiempo y lo envía al destinatario adecuado.
3. El servidor S recibe un mensaje del FEC cuyo encabezado es de 12 bytes, en él se indica quien lo originó y a que hora se recibió en el FEC.
4. El servidor S envía un mensaje dirigido al cliente C, este mensaje tiene un encabezado de 4 bytes.
5. El FEC recibe el mensaje del Servidor S, analiza el encabezado, determina a quién debe transferirlo y lo envía.



**Figura 8. Secuencia de transmisión y recepción de Mensajes en el FEC**

**Conexión entre un Cliente y el FEC**

El intercambio de mensajes que debe llevarse a cabo para que un cliente establezca conexión con el FEC se esquematiza en la figura 9.



MENSAJES PARTICULARES DE LA APLICACION

**Figura 9. Esquema de conexión de un cliente con el FEC**

**Protocolo de comunicación entre el software de almacenamiento y el prestador de servicios de certificación**

Se define el protocolo para solicitar una constancia como el procedimiento siguiente:

1. El usuario genera, a partir de sus mensajes de datos los *archivos parciales* necesarios para hacer con ellos un *expediente* el cual enviará al prestador de servicios de certificación. Solicitud de conexión por parte del usuario ante el prestador de servicios de certificación e identificación entre ellos usando un esquema seguro de identificación con certificados digitales (este proceso puede darse mediante un esquema de clave de usuario y contraseña en una primera etapa).
2. El prestador de servicios de certificación genera una *Constancia* a partir del *Expediente* recibido, dicha constancia se registra en las bases de datos del prestador de servicios de certificación y se envía una copia de ese mensaje ASN.1 al usuario.
3. El usuario almacena su *Constancia* como considere conveniente.

**MENSAJES TIPO FEC**

Mensajes del usuario al prestador de servicios de certificación.

Nombre	Acción	Formato	Descripción	Posible respuesta
--------	--------	---------	-------------	-------------------



SolConsta	12	%l %d n(%c)	<p>Envío de un <i>Expediente</i> a la OP.</p> <p>El campo %l contiene un identificador del documento (por sesión) para la transmisión.</p> <p>El campo %d puede tener los siguientes valores:</p> <p>0 - Primer y único envío</p> <p>1 - Primero de varios envíos</p> <p>2 - Envío intermedio</p> <p>3 - Ultimo envío</p> <p>El campo n(%c) representa el <i>Expediente</i> como una secuencia de caracteres, en formato ASN.1</p>	ConstaOP/ DocNoVal
-----------	----	-------------	--	-----------------------

Mensajes del prestador de servicios de certificación al usuario

Nombre	Acción	Formato	Descripción
ConstaOP	22	%l %d n(%c)	<p>La OP envía una <i>Constancia</i> al usuario.</p> <p>El campo %l contiene un identificador del documento (por sesión) para la transmisión, éste es el mismo valor que el enviado por el usuario en el mensaje SolConsta.</p> <p>El campo %d puede tener los siguientes valores:</p> <p>0 - Primer y único envío</p> <p>1 - Primero de varios envíos</p> <p>2 - Envío intermedio</p> <p>3 - Ultimo envío</p> <p>El campo n(%c) representa el <i>Constancia</i> como una secuencia de caracteres, en formato ASN.1</p>
DocNoVal	23	%d	<p>Contiene un código de error que indica el motivo por el cual no se llevó a cabo la creación de la constancia solicitada.</p> <p>Los posibles valores son:</p> <p>-1 Error en los tipos de datos básicos</p> <p>-2 Expediente electrónico de usuario incompleto</p> <p>-3 Algoritmo de resumen o compendio de firma desconocido</p> <p>-4 Identificador de usuario inválido</p> <p>-5 Firma de usuario inválida</p>

Juego de caracteres ISO 8859-1 (Latín 1)

Char	Code (código) (en decimal)	Name (nombre)	Description (descripción)
	32	-	Normal space
!	33	-	Exclamation
"	34	quot	Double quote
#	35	-	Hash or pound
\$	36	-	Dollar
%	37	-	Percent
&	38	-	Ampersand
'	39	-	Apostrophe
(	40	-	Open bracket
)	41	-	Close bracket
*	42	-	Asterik

+	43	-	Plus sign
,	44	-	Comma
-	45	-	Minus sign
.	46	-	Period
/	47	-	Forward slash
0	48	-	Digit 0
1	49	-	Digit 1
2	50	-	Digit 2
3	51	-	Digit 3
4	52	-	Digit 4
5	53	-	Digit 5
6	54	-	Digit 6
7	55	-	Digit 7
8	56	-	Digit 8
9	57	-	Digit 9
:	58	-	Colon
;	59	-	Semicolon
<	60	lt	Less than
=	61	-	Equals
>	62	gt	Greather than
?	63	-	Question mark
@	64	-	At sign
A	65	-	A
B	66	-	B
C	67	-	C
D	68	-	D
E	69	-	E
F	70	-	F
G	71	-	G
H	72	-	H
I	73	-	I
J	74	-	J
K	75	-	K
L	76	-	L
M	77	-	M
N	78	-	N
O	79	-	O
P	80	-	P
Q	81	-	Q
R	82	-	R
S	83	-	S
T	84	-	T
U	85	-	U
V	86	-	V
W	87	-	W
X	88	-	X
Y	89	-	Y
Z	90	-	Z
[	91	-	Open square bracket
\	92	-	Backslash
]	93	-	Close square bracket
^	94	-	Pointer
_	95	-	Underscore

`	96	-	Grave accent
a	97	-	a
b	98	-	b
c	99	-	c
d	100	-	d
e	101	-	e
f	102	-	f
g	103	-	g
h	104	-	h
i	105	-	i
j	106	-	j
k	107	-	k
l	108	-	l
m	109	-	m
n	110	-	n
o	111	-	o
p	112	-	p
q	113	-	q
r	114	-	r
s	115	-	s
t	116	-	t
u	117	-	u
v	118	-	v
w	119	-	w
x	120	-	x
y	121	-	y
z	122	-	z
{	123	-	Left brace
	124	-	Vertical bar
}	125	-	Right brace
~	126	-	Tilde
	160	nbsp	Non-breaking space
¡	161	ixcl	Inverted exclamation
¢	162	cent	Cent sign
£	163	pound	Pound sign
¤	164	curren	Currency sign
¥	165	yen	Yen sign
	166	brvbar	Broken bar
§	167	sect	Section sign
¨	168	uml	Umlaut or diaeresis
©	169	copy	Copyright sign
ª	170	ordf	Feminine ordinal
«	171	laquo	Left angle quotes
¬	172	not	Logical not sign
-	173	shy	Soft hyphen
®	174	reg	Registered trademark
—	175	macr	Spacing macron
°	176	deg	Degree sign
±	177	plusmn	Plus-minus sign
²	178	sup2	Superscript 2
³	179	sup3	Superscript 3
´	180	acute	Spacing acute
µ	181	micro	Micro sign

¶	182	para	Paragraph sign
	183	middot	Middle dot
¸	184	cedil	Spacing cedilla
<sup>1</sup>	185	sup1	Superscript 1
º	186	ordm	Masculine ordinal
»	187	raquo	Right angle quotes
¼	188	frac14	One quarter
½	189	frac12	One half
¾	190	frac34	Three quarters
¿	191	iquest	Inverted question mark
À	192	Agrave	A grave
Á	193	Aacute	A acute
Â	194	Acirc	A circumflex
Ã	195	Atilde	A tilde
Ä	196	Auml	A umlaut
Å	197	Aring	A ring
Æ	198	AElig	AE ligature
Ç	199	Ccedil	C cedilla
È	200	Egrave	E grave
É	201	Eacute	E acute
Ê	202	Ecirc	E circumflex
Ë	203	Euml	E umlaut
Ì	204	Igrave	I grave
Í	205	Iacute	I acute
Î	206	Icirc	I circumflex
Ï	207	Iuml	I umlaut
Ð	208	ETH	ETH
Ñ	209	Ntilde	N tilde
Ò	210	Ograve	O grave
Ó	211	Oacute	O acute
Ô	212	Ocirc	O circumflex
Õ	213	Otilde	O tilde
Ö	214	Ouml	O umlaut
×	215	times	Multiplication sign
Ø	216	Oslash	O slash
Ù	217	Ugrave	U grave
Ú	218	Uacute	U acute
Û	219	Ucirc	U circumflex
Ü	220	Uuml	U umlaut
Ý	221	Yacute	Y acute
Þ	222	THORN	THORN
ß	223	szlig	sharp s
à	224	agrave	a grave
á	225	aacute	a acute
â	226	acirc	a circumflex
ã	227	atilde	a tilde
ä	228	auml	a umlaut
å	229	aring	a ring
æ	230	aelig	ae ligature
ç	231	ccedil	c cedilla
è	232	egrave	e grave
é	233	eacute	e acute
ê	234	ecirc	e circumflex

ë	235	euml	e umlaut
ì	236	igrave	i grave
í	237	iacute	i acute
î	238	icirc	i circumflex
ï	239	iuml	i umlaut
ø	240	eth	eth
ñ	241	ntilde	n tilde
ò	242	ograve	o grave
ó	243	oacute	o acute
ô	244	ocirc	o circumflex
õ	245	otilde	o tilde
ö	246	ouml	o umlaut
÷	247	divide	division sign
ø	248	oslash	o slash
ù	249	ugrave	u grave
ú	250	uacute	u acute
û	251	ucirc	U circumflex
ü	252	uuml	u umlaut
ý	253	yacute	y acute
þ	254	thorn	thorn
ÿ	255	yuml	y umlaut

## 7. Bibliografía

- Código de Comercio.
- Ley Federal sobre Metrología y Normalización.
- Reglamento de la Ley Federal sobre Metrología y Normalización.
- NMX-Z-13-1997, Guía para la redacción, estructuración y presentación de las normas oficiales mexicanas.
- Schneier, Bruce. Applied Cryptography.
- Leyes Modelo de la CNUDMI sobre las Firmas Electrónicas y sobre Comercio Electrónico en General.
- ISO/IEC 8859-1:1998 Information technology-8bit single-byte coded graphic character sets-Part 1: Latin alphabet No. 1.

## 8. Concordancia con normas internacionales

- La presente Norma Oficial Mexicana no tiene concordancia con norma internacional por no existir referencia alguna al momento de su elaboración.

## TRANSITORIO

**UNICO.-** La presente Norma Oficial Mexicana entrará en vigor una vez que la Secretaría de Economía por conducto de la Dirección General de Normas, publique en el **Diario Oficial de la Federación** el aviso mediante el cual dé a conocer la existencia de infraestructura para llevar a cabo la evaluación de la conformidad en los términos de la Ley Federal sobre Metrología y Normalización y su Reglamento.

México, D.F., a 20 de marzo de 2002.- El Director General, **Miguel Aguilar Romo**.- Rúbrica.

DECLARATORIA