DISC 2005 México

Comercio Electrónico

Aspecto Legal

Noviembre 2005

Dr. Alfredo Reyes Krafft

© Derechos Reservados

Que es Comercio Electrónico

- Compra de boletos en mexicana.com
- Compartir inventarios entre Walmart y Procter & Gamble
- Comprar artículos de oficina en officemax.com.mx
- Vender mi viejo celular en mercadolibre.com
- Comprar un libro en gandhi.com
- Ordenar el super en superama.com
- Pedir una hamburguesa en hardrockcafe.com

El comercio electrónico está en todas partes

El comercio no deja de ser comercio...

... aún y cuando éste se realice a través de medios electrónicos...

Comercio Electrónico

- ✓ Firma Electrónica
- ✓ NOM 151
- ✓ Comprobante Fiscal Digital
- ✓ Seguridad

Firma Electrónica

Aspectos Legales

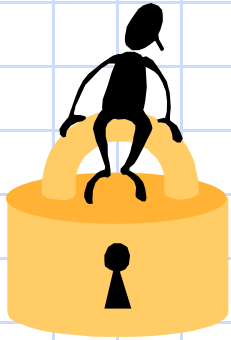
Noviembre 2005

Dr. Alfredo Reyes Krafft

© Derechos Reservados

Conceptos

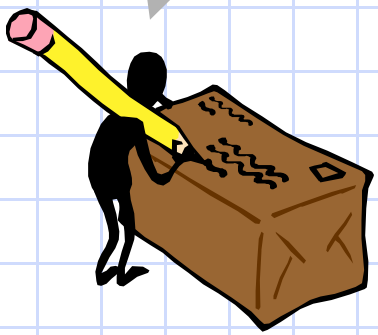
Principios



Criptografía

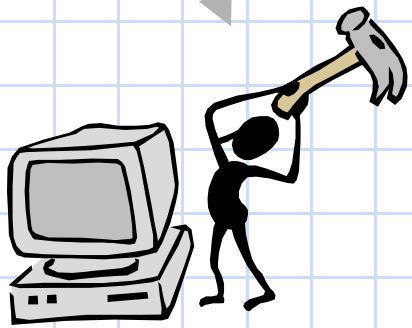
Equivalencia Funcional

Compatibilidad Internacional



Firma

Autonomía de la Voluntad



Tecnología

Neutralidad Tecnológica

Fuente: http://www.notaria77.com/annm.pdf

La Criptografía es el estudio de la escritura oculta. Del griego Kryptos (oculto) y Graphos (escritura).

Julio César

- Utilizaba una sustitución alfabética simple; cada letra del mensaje era sustituída por la tercera letra siguiente en el alfabeto (“hola” = “jqnc”).

Gabriel de Lavinde

- Hizo de la criptografía una ciencia más formal cuando publicó su primer manual sobre Criptología en 1379.

Samuel Morse

- El Código Morse, desarrollado en 1832, aunque no es propiamente un código como los otros, es una forma de cifrar las letras del alfabeto dentro de sonidos largos y cortos.

Fuente: http://www.notaria77.com/annm.pdf

Juan García

10,21,1,14 7,1,18,3,9,1

Juan García

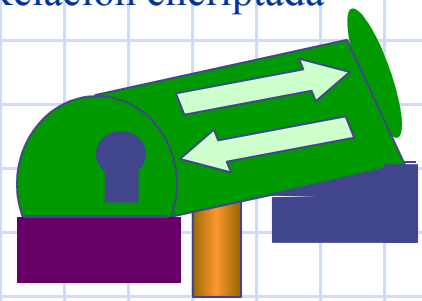
Número ordinal del alfabeto

Encripción Simétrica

Encripción Asimétrica

Relación encriptada

Llave Privada De Alicia



Llave Pública De Alicia

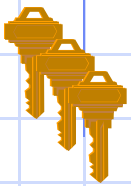
Garantiza integridad

Roberto

Roberto

LLAVE PRIVADA

- Sólo existe **una** llave privada por llave pública
- Para uso único del propietario
- Es secreta
- Se usa para generar firmas digitales



LLAVE PUBLICA

- Un usuario puede tener **N** llaves públicas
- Es puesta a disposición de todos los usuarios
- Se usa para encriptar información

- Las **llaves públicas/privadas** se usan para encriptar,firmar y revisar posibles alteraciones en documentos/transacciones, así como para identificar individuos
- Las funciones realizadas por una parte del par de llaves pueden ser validadas sólo al usar la otra parte del par

Con la invención de las computadoras en el siglo XX, la criptografía se revolucionó.

DES

- IBM creó hace años un código denominado “Data Encryption Standard”, actualmente se usa el 3DES y ya se está implementando el AES (Advanced Encryption Standard). .

TEF

- “...Manera de llevar a cabo transacciones… que importan dinero… que suponen usualmente pago y que pueden operar o no en tiempo real…”, todo por medios electrónicos.

Firma Digital

- Aplicación de disciplina de las matemáticas conocida como “Criptografía de Clave Pública”.

Fuente: http://www.notaria77.com/annm.pdf

Estándares (Criptografía de Clave Pública)

Utilizar estándares abiertos para la generación y utilización de firmas digitales permite:

- ✓ Interoperabilidad internacional y entre diferentes plataformas
- ✓ Menor costo
- ✓ Soluciones probadas y seguras

Fuente: Auditoría de PKI y estándares abiertos
Deloitte & Touche Antonio Pecora M.

A lo largo de la historia, el concepto de firma ha tenido distintas acepciones y modos de manifestarse

Manufirmatio

- En Roma la ceremonia de firma consistía en pasar la mano sobre un documento determinado en actitud de jurar (sin hacerlo).

Sellos

- En la Edad Media, el autor de un documento colocaba sellos personales, marcas y signos para manifestar su voluntad de reconocer el contenido.

Firma Autógrafa

- En la actualidad, la firma no es sino un trazo peculiar mediante el cual un sujeto consigna su nombre, a fin de manifestar la autoría de un documento y el reconocimiento de su contenido.

Fuente: http://www.notaria77.com/annm.pdf

Firma

- Concepto
  - Identificación de la persona
  - Expresión del consentimiento (voluntad de asumir el contenido de un documento en el que se estampa)
  - Medio de prueba
- Consentimiento = Firma
  - Exteriorización de la declaración de voluntad de una persona
- Migrar a medios electrónicos:
  - ✓ Reconocimiento y validez jurídica del contrato celebrado electrónicamente
  - ✓ Exigibilidad judicial
  - ✓ Equivalente funcional a través de la criptografía de clave pública:
    - ✓ ATRIBUCIÓN Y NO REPUDIO
    - ✓ INTEGRIDAD Y AUTENTICIDAD
    - ✓ ACCESIBILIDAD Y CONFIDENCIALIDAD

- Existe y seguirá existiendo la FIRMA ELECTRÓNICA SIMPLE (NIP, CIEC)

- Evolucionamos a una FIRMA ELECTRÓNICA AVANZADA

- Ambos esquemas convivirán en el ámbito fiscal, comercial y bancario y seguirán siendo jurídicamente válidos.

OBJETIVO DE LA FIRMA ELECTRÓNICA AVANZADA

Al actualizarse el Marco Jurídico y las Capacidades Tecnológicas para el uso de los sistemas de intercambio electrónico de información, surge la FIRMA ELECTRÓNICA AVANZADA,

cuyo objetivo es establecer un medio de identificación electrónico que nos permita con toda seguridad técnica y jurídica interactuar electrónicamente.

FIRMA ELECTRÓNICA AVANZADA

Información electrónica que se víncula a la identidad de la persona que la origina, asegurando su integridad y no repudio a través de el uso de un par de claves (pública y privada).

CARACTERÍSTICAS:

- **AUTENTICIDAD.-** Certeza que el mensaje solo proviene del emisor
- **INTEGRIDAD.-** El contenido no puede ser alterado
- **NO REPUDIACIÓN.-** Innegable autoría y recepción del mensaje
- **CONFIDENCIALIDAD.-** Solo el emisor y el receptor pueden leer el mensaje

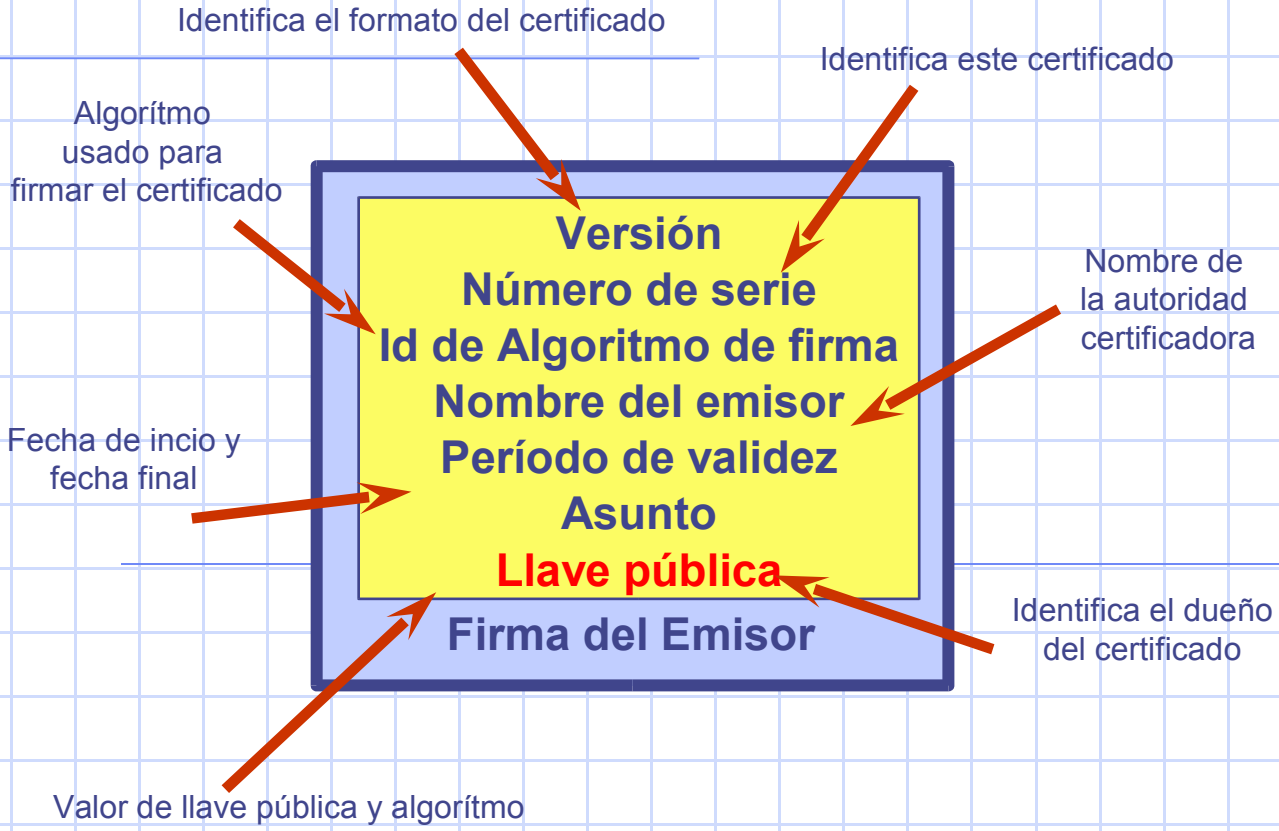
Para el **USO** de la firma electrónica, se requiere:

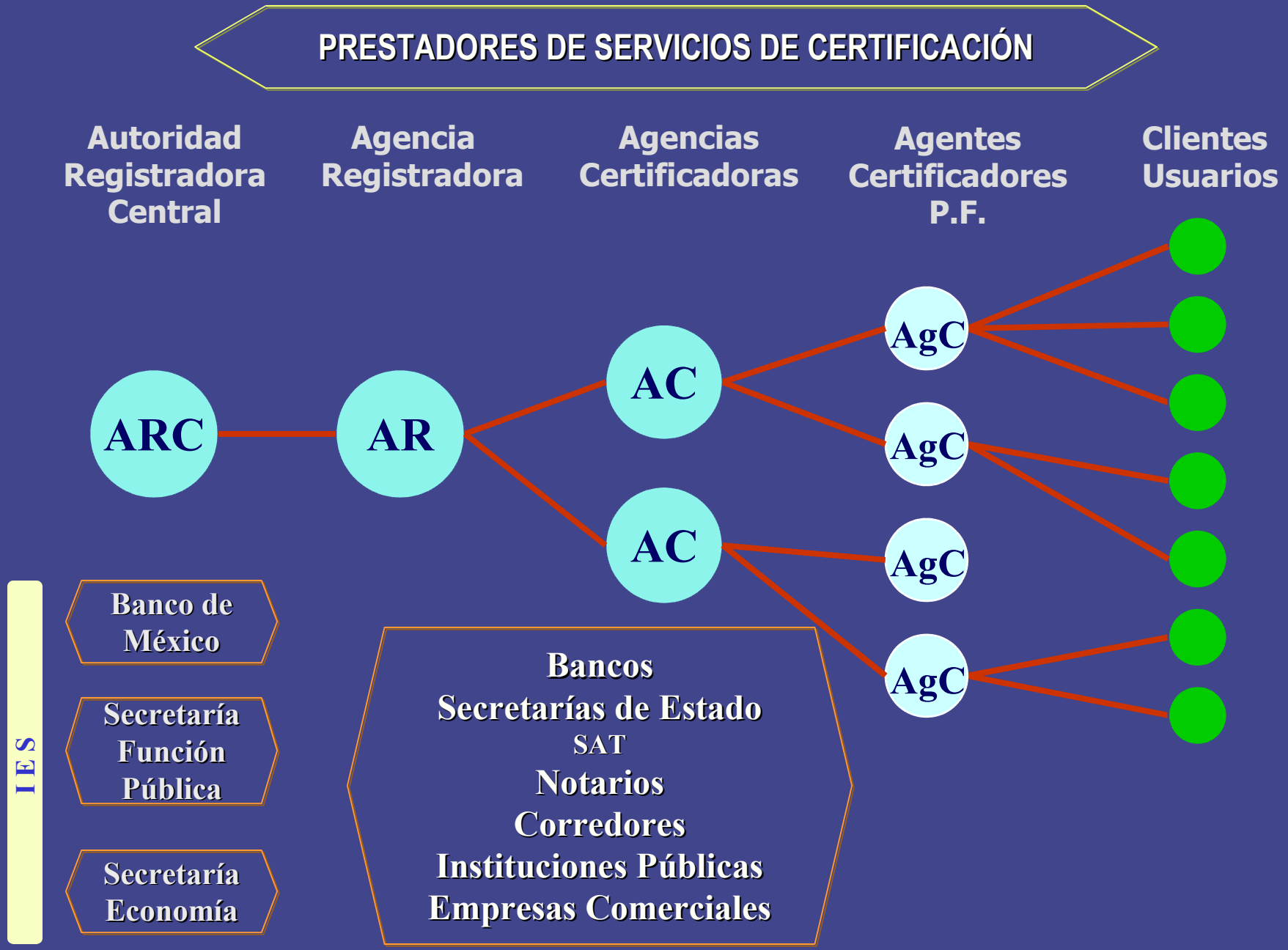
- **Emisión de Certificados Digitales**
  (AGENTE Y AGENCIA CERTIFICADORA)

- **Registro y Administración de los Certificados Digitales**
  (AGENCIA REGISTRADORA Y REGISTRADORA CENTRAL)

CERTIFICADOS DIGITALES

Un certificado digital es un documento electrónico que asegura que una clave pública determinada corresponde a un individuo en específico, el cual está firmado electrónicamente por la agencia que certificó la identidad del individuo.




PRESTADORES DE SERVICIOS DE CERTIFICACIÓN
Autoridad Registradora Central
Agencia Registradora
Agencias Certificadoras
Agentes Certificadores P.F.
Clientes Usuarios
ARC
AR
AC
AC
AgC
AgC
AgC
AgC
I E S
Banco de México
Secretaría Función Pública
Secretaría Economía
Bancos
Secretarías de Estado
SAT
Notarios
Corredores
Instituciones Públicas
Empresas Comerciales

Declaración de Prácticas de Certificación (CPS)

- Las AC tienen un conjunto de políticas operativas que describen la implantación y apoyo a las políticas de seguridad,condensadas en un detallado documento conocido como la **Declaración de Prácticas de Certificación (CPS).** Estas políticas incluyen: Procedimientos Verificación de Identidad, Rango de Usuarios a Certificar, Ciclo de Vida de un certificado, etc. Constituyen la limitación de responsabilidad de la Agencia Certificadora frente a sus usuarios.

- **Lista de Revocación de Certificados (CRL)** determina la validez de un certificado, condensándolo en una lista

SAT → CURP (Clave Única de Registro de Población)

Internet

Usuario

- Requisita su solicitud de certificado electrónicamente y la imprime.
- Genera sus claves (pública y privada) y establece su frase de seguridad (activación y revocación)
- Acude ante el AGENTE CERTIFICADOR, presenta documentos de identificación y firma la solicitud/responsiva de certificado

Agente Certificador

- Certifica la identidad del usuario (coteja documentación vs. RFC)
- Verifica la solicitud/responsiva del certificado.
- Emite precertificado, lo firma electrónicamente y lo envía la AGENCIA CERTIFICADORA

Agencia Registradora

- Registra Certificado
- Valida Unicidad Clave Pública
- Avisa del alta a la Agencia
- Pone a disposición del usuario.

Agencia Certificadora

- Valida la firma electrónica del AgC y los datos del precertificado.
- Emite Certificado Digital y lo firma electrónicamente
- Envía Certificado a la AGENCIA REGISTRADORA

Fuente: ABM-Comité Operaciones 8/03

Dispositivo de almacenamiento	Ventajas	Desventajas
Chip Card	Se almacenan en una tarjeta inteligente	•Se pueden utilizar en cualquier lado •Dispositivo de almacenamiento seguro	•Es caro ya que se requieren lectoras especiales •La tecnología aún no es accesible para todos los usuarios
Browser	Se almacena en la computadora del cliente modificando localmente la configuración del Browser del cliente	•Es el certificado más barato	Únicamente se puede utilizar desde la computadora donde se almacenó el certificado localmente
Servidor	Se almacena en un servidor	El cliente puede accesarla a través de una clave desde cualquier computadora.	•Dependencia total de un solo servidor •Cliente se autentica sin certificado
Dispositivo USB	Se almacena en el dispositivo (que puede ser criptográfico)	Dispositivo seguro. No requiere lectoras (puerto USB)	•El dispositivo criptográfico es caro

...o un diskette ...

PRINCIPALES FUNCIONES

- La **Autoridad Registradora Central** será la encargada de supervisar el funcionamiento de la infraestructura, registrar las claves públicas así como autorizar la operación de las demás entidades que forman parte del esquema. De ella dependerán de manera directa la Agencia Certificadora y la Agencia Registradora (ambas funciones las puede desarrollar una sola empresa).
- Por lo que respecta a la **Agencia Registradora**, ésta tiene como responsabilidad el registro, publicación y, en su caso, revocación de los certificados.
- La **Agencia Certificadora** tendrá a su cargo identificar al agente certificador, corroborar la unicidad de las claves, expedir y registrar el certificado, con base en el precertificado que le presenten los agentes certificadores.
- Los **Agentes Certificadores**, dependerán de la agencia certificadora y tendrán la función de identificar al usuario, verificar la relación entre claves y expedir el precertificado antes mencionado.

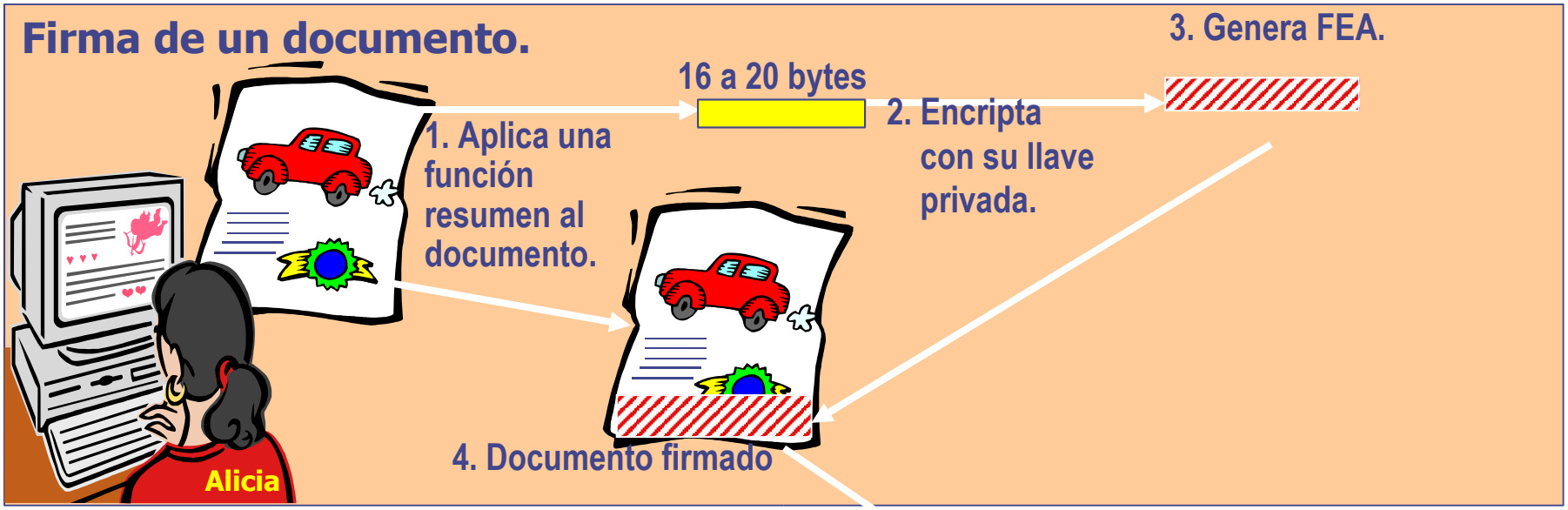
Principales Obligaciones y Responsabilidades

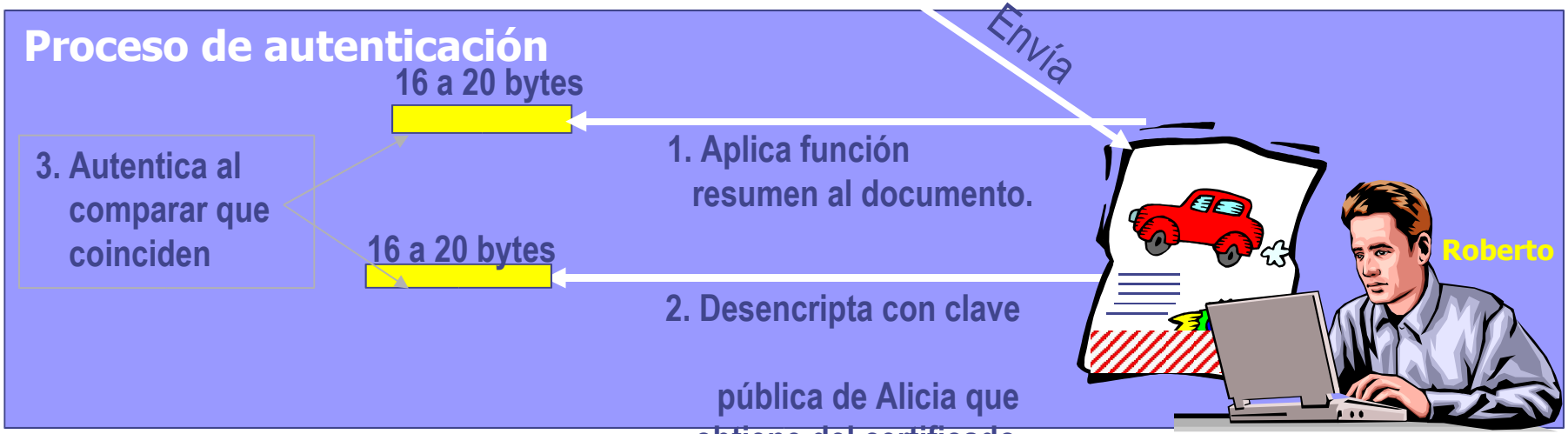
AGENCIA REGISTRADORA
▪ CONTAR CON REGLAS Y PROCEDIMIENTOS DE OPERACIÓN
▪ MANTENER REGISTRO DE CERTIFICADOS DIGITALES (PÚBLICO)
▪ PERMITIR CONSULTAS EN LINEA AL REGISTRO
▪ DIFUNDIR DISPOSICIONES DE BANXICO (SITIO WEB)
▪ REPORTES A BANXICO DE ACTIVIDADES
▪ RESPONDER POR NEGLIGENCIA EN PROCESO DE REGISTRO O REVOCACIÓN
▪ RESPALDO ELECTRÓNICO DE SU BASE DE DATOS

AGENCIA CERTIFICADORA
▪ REGLAS Y PROCEDIMIENTOS SOBRE PRACTICAS DE CERTIFICACIÓN (DE IDENTIDAD) ADOPTADAS
▪ EMITIR Y, EN SU CASO, REVOCAR CERTIFICADOS DIGITALES (REQUISITOS BANXICO)
▪ PROPORCIONAR UN CERTIFICADO DIGITAL Y LOS MEDIOS PARA LA CREACIÓN Y VERIFICACIÓN DE FIRMA ELECTRÓNICA.
▪ REGISTRAR ANTE AR LOS CERTIFICADOS DIGITALES QUE EMITA
▪ CONSERVAR SOLICITUDES POR 10 AÑOS
▪ DIFUNDIR DISPOSICIONES DE BANXICO (SITIO WEB)
▪ REPORTES A BANXICO DE ACTIVIDADES
▪ RESPONDER POR NEGLIGENCIA EN PROCESO DE EMISIÓN O REVOCACIÓN DE CERTIFICADOS
▪ INFORMAR A TITULARES DE REVOCACIÓN DE CERTIFICADOS, EN SU CASO

AGENTE CERTIFICADOR
▪ IDENTIFICAR A TITULARES SOLICITANTES (COMPARESENCIA PERSONAL) CON IDENTIFICACIÓN OFICIAL FIABLE
▪ OBTENER DECLARACIÓN CON FIRMA AUTOGRAFA DEL TITULAR (ATRIBUCIÓN, RESPONSABILIDAD Y CONFORMIDAD CON LIMITES DE RESPONSABILIDAD DE AC)
▪ CONSERVACIÓN DE DOCUMENTACIÓN FÍSICA POR CUANDO MENOS 10 AÑOS (NOM. POSIBLE DIGITALIZACIÓN)
▪ RESPONDER POR DAÑOS Y PERJUICIOS EN CASO DE NEGLIGENCIA EN EL PROCESO DE IDENTIFICACIÓN DEL TITULAR
▪ CONTAR CON RESPALDO DE INFORMACIÓN Y DOCUMENTACIÓN

OPERACIÓN DE LA FIRMA ELECTRÓNICA AVANZADA





ANTECEDENTES LEGISLATIVOS EN MÉXICO

- **Código de Comercio 1889** - Telégrafo
- **Código Civil 1928** - Teléfono
- **Leyes Financieras y Bancarias 1990** - Medios Telemáticos.
- **Ley PROFECO 1992** - Ventas a distancia. Telemarketing.
- **Leyes Fiscales 1998** - Declaraciones y pagos en formato electrónico.
- **Enero 4, 2000 (LAASSP y LOP**)

La legislación existente hasta esa fecha, requería para la validez del acto o contrato del soporte de la forma escrita y la firma autógrafa, para vincular a las partes en forma obligatoria

Disposiciones legales

Reformas en materia de Comercio Electrónico	**29 mayo 2000**
Ley de Procedimiento Administrativo Acuerdo Tramitanet	**30 mayo 2000** 17 enero 2002
NOM 151 SCFI 2002 **FALTA:** AVISO DE INICIO DE VIGENCIA	**4 junio 2002**
Infraestructura Extendida de Seguridad Circular Telefax 1/2002 Circular Telefax 19/2002 y bis Circular Telefax 6/2005	 2 enero 2002 5 julio 2002 y 11 de julio 2003 15 marzo 2005
Reformas en materia de Firma Electrónica Reglamento del Código de Comercio en materia de PSC Reglas Generales en materia de FEA	**29 agosto 2003** 19 julio 2004 10 agosto 2004
Reformas al Código Fiscal de la Federación Miscelánea Fiscal 2004 Miscelanea Fiscal 2005 **FALTA:** ▪ Prestadores de Servicios de Certificación distintos al SAT (Bancos y empresas comerciales) ▪ Representantes de Personas Morales (tanto para FEA como para CFD),	**5 enero 2004**

Consentimiento

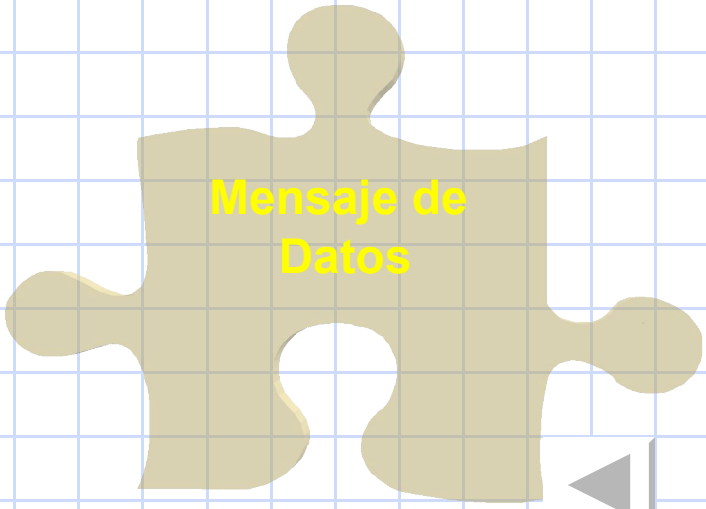
Documento Electrónico

Valor Probatorio

Mayo 29, 2000

Reformas en materia de Comercio Electrónico

Integridad
Atribución
Accesibilidad



Iniciativas Presentadas

- ✓ **Abril 1999 – PAN**
  - Texto Ley Modelo de UNCITRAL.
- ✓ **Diciembre 1999 – PAN**
  - Texto Grupo GILCE.
- ✓ **Marzo 2000 – PRI – Ejecutivo.**
  - Texto incorporando Registro Público y Protección al Consumidor.

Proceso Legislativo

Período de Sesiones Marzo-Abril, 2000.

- **Cámara de Diputados: 26 abril 2000.**
  390 votos a favor
  3 abstenciones
  0 en contra

- **Cámara de Senadores: 29 abril 2000.**
  Unanimidad de 88 votos.

Publicada en el DOF el 29 de mayo del 2000.
Vigente a partir del 7 de junio del 2000.

REFORMAS EN MATERIA DE COMERCIO ELECTRÓNICO

El 29 de mayo del año 2000, se publicó en el Diario Oficial de la Federación el **Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor,** estas reformas constituyen los cimientos del marco legal del Comercio Electrónico en México, tomando como punto de partida las experiencias internacionales y el trabajo de UNCITRAL al respecto

- Las reformas y adiciones al CÓDIGO CIVIL FEDERAL se centraron en el reconocimiento a la **celebración de actos jurídicos a través de medios electrónicos, ópticos o de cualquier otra tecnología**, añadiéndose los "medios tecnológicos" como medio idóneo para expresar el consentimiento. Es importante resaltar que se estableció una equivalencia funcional entre el consentimiento expresado por medios tecnológicos y la firma autógrafa "siempre que la información generada o comunicada en forma **íntegra**, a través de dichos medios sea **atribuible** a las personas obligadas y **accesible** para su ulterior consulta".
- Se reconoce en el CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES como prueba, la información contenida en los medios electrónicos, ópticos o en cualquier otra tecnología, dando una serie de reglas para su valoración por parte del juzgador: **La fiabilidad del método para generar, comunicar, recibir o archivar la información** (que pueda conservarse sin cambio), **su atribución a las personas obligadas y la posibilidad de acceder a ella en ulteriores consultas.** Asimismo y para que la información generada, comunicada, recibida o archivada por medios electrónicos se considere como original (para su conservación o presentación) deberá acreditarse que dicha información se ha mantenido **íntegra e inalterada** a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser **accesible** para su ulterior

1. En el CODIGO DE COMERCIO se define el concepto **“Mensaje de Datos”** como la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología.

Respecto de la obligación a los comerciantes de conservar por un plazo mínimo de 10 años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, en el caso de mensajes de datos se requerirá que el contenido de la información se haya mantenido íntegro e inalterado a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. **La ahora Secretaría de Economía deberá emitir una Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.**

Se establece una presunción en materia mercantil, **salvo pacto en contrario, de que el mensaje proviene del emisor (atribución a la persona obligada) si ha sido enviado: i) Usando medios de identificación, tales como claves o contraseñas de él** (*para lo que se requerirá de un previo acuerdo entre las partes*), **o ii) Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente**.

En materia mercantil, al igual que en la civil, cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea **atribuible a las personas obligadas y accesible para su ulterior consulta.**

Y se reconoce como prueba a los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada la información.

5. Se reformó la **LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR** para reconocer la utilización de medios electrónicos, ópticos o cualquier otra tecnología en la instrumentación de las operaciones que celebren los proveedores con los consumidores, dando las bases sobre las cuales habrán de realizarse dichas operaciones (confidencialidad, certeza, seguridad en la información proporcionada al consumidor, etc.), previendo sanciones administrativas (acaso las mas altas) para el caso de que los proveedores no cumplan con dichas disposiciones.

Para que un mensaje de datos pueda considerarse legalmente válido, es necesario asegurar que reúna las siguientes características:

INTEGRIDAD:

Entendida en dos vertientes, la primera respecto de la fiabilidad del método para generarla, comunicarla, recibirla o archivarla. Y la segunda como la forma de garantizar que la información en él contenida no fue alterada. Al respecto la Secretaría de Economía publicó el 4 de junio del 2002 en el DOF, una NOM que establece los requisitos que deben observarse para la conservación de mensajes de datos.

ATRIBUCIÓN:

La forma en que podemos garantizar que las partes que se obligan en la relación jurídica son quienes dicen ser y expresan su voluntad. Esta atribución a las personas obligadas en la relación jurídica que se pretende formalizar en un mensaje de datos, no es más que una “FIRMA ELECTRÓNICA”, la cual puede ser de dos tipos:

SIMPLE (partiendo del previo acuerdo de las partes en el uso de medios de identificación electrónica como claves o contraseñas por ambas partes conocidas, presunción de atribución establecida en el Código) o

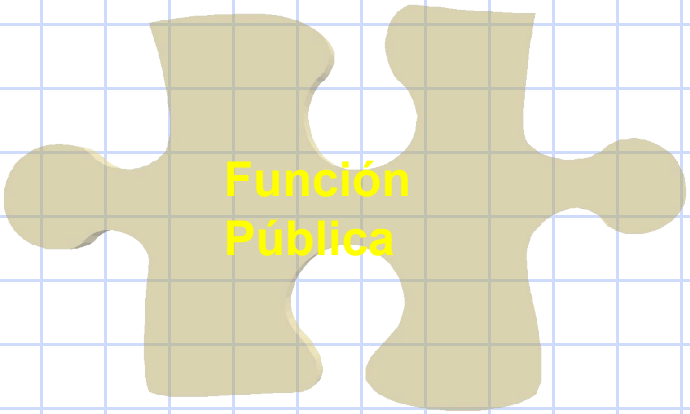
FIABLE o AVANZADA (entendida como proceso electrónico que permite al receptor de un mensaje de datos identificar formalmente a su autor, el cual mantiene bajo su exclusivo control los medios para crear dicha firma, de manera que esté vinculada únicamente a él y a los datos a que se refiere el mensaje, permitiendo detectar cualquier modificación ulterior al contenido del mismo, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento.

ACCESIBILIDAD:

Se refiere a que el contenido de un mensaje de datos pueda estar disponible al usuario (emisor, receptor, juez, auditor, autoridades, etc.) para su ulterior consulta, siempre y cuando reúna las dos características anteriormente anotadas.

Mayo 30, 2000

Reformas a la Ley Federal de Procedimiento Administrativo



LEY FEDERAL DE PROCEDIMIENTO ADMINISTRATIVO

Regula las actuaciones y procedimientos del Poder Ejecutivo Federal (dependencias y organismos descentralizados de la Administración Pública Federal). Reformada el 30 de mayo del 2000, habilita el empleo de medios electrónicos para llevar a cabo algunos procedimientos administrativos de gestión:

- Notificaciones, citatorios, emplazamientos, requerimientos, solicitud de informes, documentos y resoluciones administrativas, entre otros, cuando así lo haya aceptado expresamente el promovente y siempre que pueda comprobarse fehacientemente la recepción de los mismos
- Las promociones o solicitudes que los particulares presenten, en las etapas que las propias dependencias y organismos así lo determinen mediante reglas de carácter general, empleando medios de identificación electrónica tendrán el mismo valor probatorio que los firmados en forma autógrafa

El uso de dichos medios de comunicación electrónica será optativo para cualquier interesado, incluídos los particulares que se encuentren inscritos en el Registro de Personas Acreditadas

La certificación de los medios de identificación electrónica del promovente, así como la verificación de la fecha y hora de recepción de las promociones o solicitudes y de la autenticidad de las manifestaciones vertidas en las mismas, deberán hacerse por las dependencias u organismos descentralizados, bajo su responsabilidad y de conformidad con las disposiciones generales que al efecto emita la Secretaría de Contraloría y Desarrollo Administrativo.

ACUERDO "TRAMITANET"

Publicado en el DOF el 17 de enero del 2002 por la Secretaría de Contraloría y Desarrollo Administrativo.

Objeto: La certificación del medio de identificación electrónica que utilicen los particulares en los trámites electrónicos que realicen; La verificación de la fecha y hora de recepción de las promociones y solicitudes formuladas a través de medios de comunicación electrónica (marca de tiempo o sello digital); La comprobación de la autenticidad de las manifestaciones vertidas en dichas promociones o solicitudes, y las notificaciones, citatorios, emplazamientos, requerimientos, solicitudes de informes o documentos y las resoluciones administrativas que emitan por medios electrónicos, relacionados con el trámite electrónico promovido por el particular.

En el acuerdo se establece también que se utilizará un sistema de encripción de clave pública (PKI) para generar el certificado digital y dos tipos de certificación; básica y de alta seguridad, dependiendo de la necesidad o no de la presencia física del particular o su representante para acreditar identidad, existencia legal y facultades de su representante, en su caso, los cuales podrán ser emitidos por las dependencias u organismos descentralizados de la Administración Pública Federal (Entidad Certificadora), que estuvieren autorizadas para ello por la Secretaria de la Contraloría y Desarrollo Administrativo (Autoridad Certificadora Central) , previa solicitud de los interesados.

Cada dependencia interesada en fungir como Entidad Certificadora, deberá declarar en un documento a disposición de los interesados las prácticas de certificación adoptadas (Tipos de certificación que emitan, trámites en los que podrán ser utilizados los certificados expedidos, métodos para identificar al titular del certificado, mecanismos que permitan al titular verificar su propio certificado, procedimientos para emitir y consultar la lista de certificados revocados, procedimientos de auditoría establecidos, mecanismos de custodia de identificación electrónica e impresa).

Junio 4, 2002

NOM- 151- SCFI-2002.- REQUISITOS QUE DEBEN OBSERVARSE PARA LA CONSERVACIÓN DE MENSAJES DE DATOS

NOM- 151- SCFI-2002.- REQUISITOS QUE DEBEN OBSERVARSE PARA LA CONSERVACIÓN DE MENSAJES DE DATOS

Objetivo: Establecer 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.

Campo de aplicación: Es de observancia general para los comerciantes que deban conservar los mensajes en que se consignen los citados documentos, así como para todas aquellas personas con quienes los comerciantes otorguen o pacten dichos contratos, convenios o compromisos.

Definiciones : Se incluyen definiciones a los conceptos utilizados en la NOM.(DOF. 04/06/2002)

Método a seguir para la conservación de los mensajes de datos: (se describe en el apéndice del proyecto, requiere de la utilización de tecnología PKI y de la existencia y participación de un Prestador de Servicios de Certificación). La información que se desee conservar se podrá almacenar en uno o varios archivos diferentes y/o en una o varias computadoras.

Método para digitalizar archivos soportados en medio físico: La migración deberá ser cotejada por un tercero legalmente autorizado, quien constatará que dicha migración se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva.

Elementos que intervienen en la conservación de mensajes de datos: firma electrónica y/o digital; el prestador de servicios de certificación; La constancia emitida por el prestador de servicios de certificación; equipos y programas informáticos en y con los que se almacenen los mensajes de datos,

Vigilancia: a cargo de la Secretaría de Economía conforme a sus atribuciones y la legislación aplicable.

Entrada en vigor: Se requiere de existencia de infraestructura y publicación de aviso en el DOF

FORMACIÓN DE ARCHIVOS PARCIALES

(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

OBTENCIÓN DE LOS COMPENDIOS O RESUMENES DIGITALES

Se calcula el compendio o resumen digital del *archivo o archivos parciales.*

INTEGRACIÓN DEL EXPEDIENTE ELECTRÓNICO

(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.

OBTENCIÓN DE LA CONSTANCIA DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

(i) el nombre del archivo en donde está almacenada la *constancia*,
(ii) el *expediente* enviado por el sistema de 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.

MÉTODO DE VERIFICACIÓN DE AUTENTICIDAD

(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*.

Modelo

Prestador de Servicios de Certificación
Resguardo de copias de los Expedientes
Generación de Constancias
Sistema de Conservación de Información
Constancias
Constancias
Constancias
Expedientes
Expedientes
Expedientes
Archivos Parciales
Archivos Parciales
Archivos Parciales
Usuarios
Información Contable
Información Legal
Información Comercial

- **INFRAESTRUCTURA EXTENDIDA DE SEGURIDAD** (Circular- Telefax 1/2002 del 2 de enero del 2002).

- Circular-Telefax 19-2002 (5 de julio 2002)
- Circular-Telefax 19-2002 bis (11 de julio 2003)
- CIRCULAR-TELEFAX 6/2005 (15 de marzo del 2005)

REQUERIMIENTOS TÉCNICOS E INFORMÁTICOS MÍNIMOS DE LOS PROGRAMAS Y EQUIPOS DE CÓMPUTO QUE PERMITEN INTERACTUAR DE MANERA ADECUADA EN LA INFRAESTRUCTURA EXTENDIDA DE SEGURIDAD

PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

- La **Asociación de Notariado y la de los Corredores Públicos** firmaron un convenio con **Secretaría de Economía** sobre certificación digital (Octubre 6, 2000), por el que dichas asociaciones se constituyen en entidades certificadoras (previo contrato que estas celebraron con la empresa ACERTIA para su operación) y los notarios y corredores como agentes certificadores.

  Tenía la Secretaría de Economía en esa época facultades para designar certificadoras?

- En el ámbito financiero, el **Banco de México** cuenta con las atribuciones legales suficientes para implementar y regular el uso de medios electrónicos y sistemas de seguridad en los sistemas de pagos, en las transferencias de fondos, y en la celebración de operaciones activas, pasivas y de servicios de los intermediarios financieros.

- Con el objeto de que puedan celebrarse operaciones confiables a través de medios electrónicos entre los intermediarios financieros, el Banco de México diseñó una **infraestructura de seguridad** para el uso de medios de identificación en mensajes electrónicos (circular telefax 1/2002 del 2 de enero del 2002).

PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

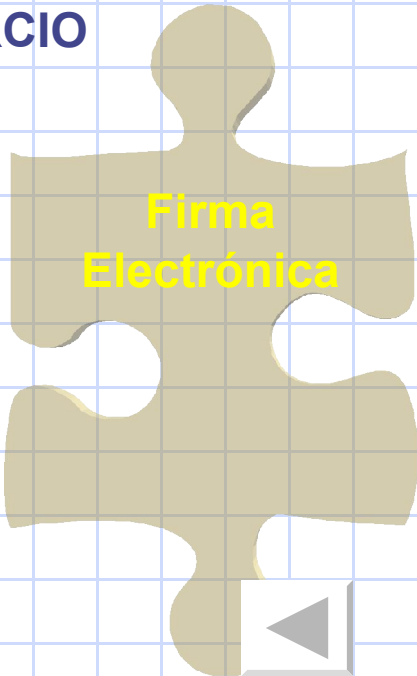
- En cuanto a las operaciones de las instituciones de crédito con su clientela, el Banco de México emitió la Circular-Telefax 19-2002 (5 de julio 2002) por la que, en su carácter de Autoridad Registradora Central (ARC) de la IES, autoriza a las **Instituciones de Crédito** interesadas para actuar como Agencia Registradora (AR) y/o Agencia Certificadora (AC) y por tanto a emitir certificados digitales a sus clientes para celebrar operaciones con ellos y realizar los procesos de registro y distribución de tales certificados, a través de la **IES** (Infraestructura Extendida de Seguridad), previa aprobación de solicitud y firma de convenio con Banco de México.

- Asimismo publicó la Circular-Telefax 19-2002 bis (11 de julio 2003) que contempla expresamente la figura de Agentes Certificadores dentro de la IES que como personas físicas estarán en aptitud de auxiliar en sus funciones de identificación a las Agencias Certificadoras.

- La CIRCULAR-TELEFAX 6/2005 del 15 de marzo del 2005 sustituye a las anteriores

Agosto 29, 2003

DECRETO DE REFORMAS AL CÓDIGO DE COMERCIO EN MATERIA DE FIRMA ELECTRÓNICA



DECRETO DE REFORMAS AL CÓDIGO DE COMERCIO EN MATERIA DE FIRMA ELECTRÓNICA

- Vigente 90 días después de su publicación en el DOF (29 de agosto de 2003).
- Adopta básicamente la ley modelo sobre firmas electrónicas de UNCITRAL e introduce el concepto de **firma electrónica fiable o avanzada** y **complementa la parte relativa a Mensaje de Datos** detallando conceptos como Intermediario, Acuse de Recibo, Copia, Error, etc.
- Establece el uso voluntario y la posibilidad de convenir cualquier método de firma que determinen las partes. Responsabilidad de uso al Firmante.
- Reconoce como ARC a la Secretaría de Economía

- Incorpora la figura del **Prestador de Servicios de Certificación**, quien como tercero confiable estará investido de la facultad de validar, por su probidad y su tecnología (no fé pública), el proceso de emisión, identificación y atribución de firmas electrónicas:
  - ✓ Notarios o Corredores Públicos
  - ✓ Empresas Privadas
  - ✓ Instituciones Públicas
- Reconocimiento y validez de los certificados extranjeros
- Para la prestación de servicios de certificación por parte de las instituciones financieras el **Banco de México**, en el ámbito de su competencia, regulará y coordinará a la autoridad registradora central, registradora y certificadora (**IES**).

REGLAMENTO DEL CÓDIGO DE COMERCIO EN MATERIA DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

- DOF 19 de julio 2004, en vigor 20 de julio.
- Requisitos (elementos humanos, materiales, económicos y tecnológicos)
- Trámite de acreditación (fianza, auditoría)
- Operación (emisión de certificados en territorio nacional, auditorías de verificación de cumplimiento).
- Infracciones y Sanciones (suspensión temporal y definitiva + daños y perjuicios en que incurra).
- Reglas Generales (se publicaron el 10/08/2004)

Firma Electrónica

LEY MODELO UNCITRAL SOBRE FIRMAS ELECTRÓNICAS:

Por "Firma Electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

CÓDIGO DE COMERCIO:

Firma electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

LEY MODELO UNCITRAL SOBRE FIRMAS ELECTRÓNICAS

La firma electrónica se considerará **fiable** …, si:
b) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;
c) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
d) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y
d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

CÓDIGO DE COMERCIO

... Firma Electrónica Avanzada o Fiable: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97. En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica....

Art. 97.- Cuando la Ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte **apropiada para los fines** para los cuales se generó o comunicó ese Mensaje de Datos.

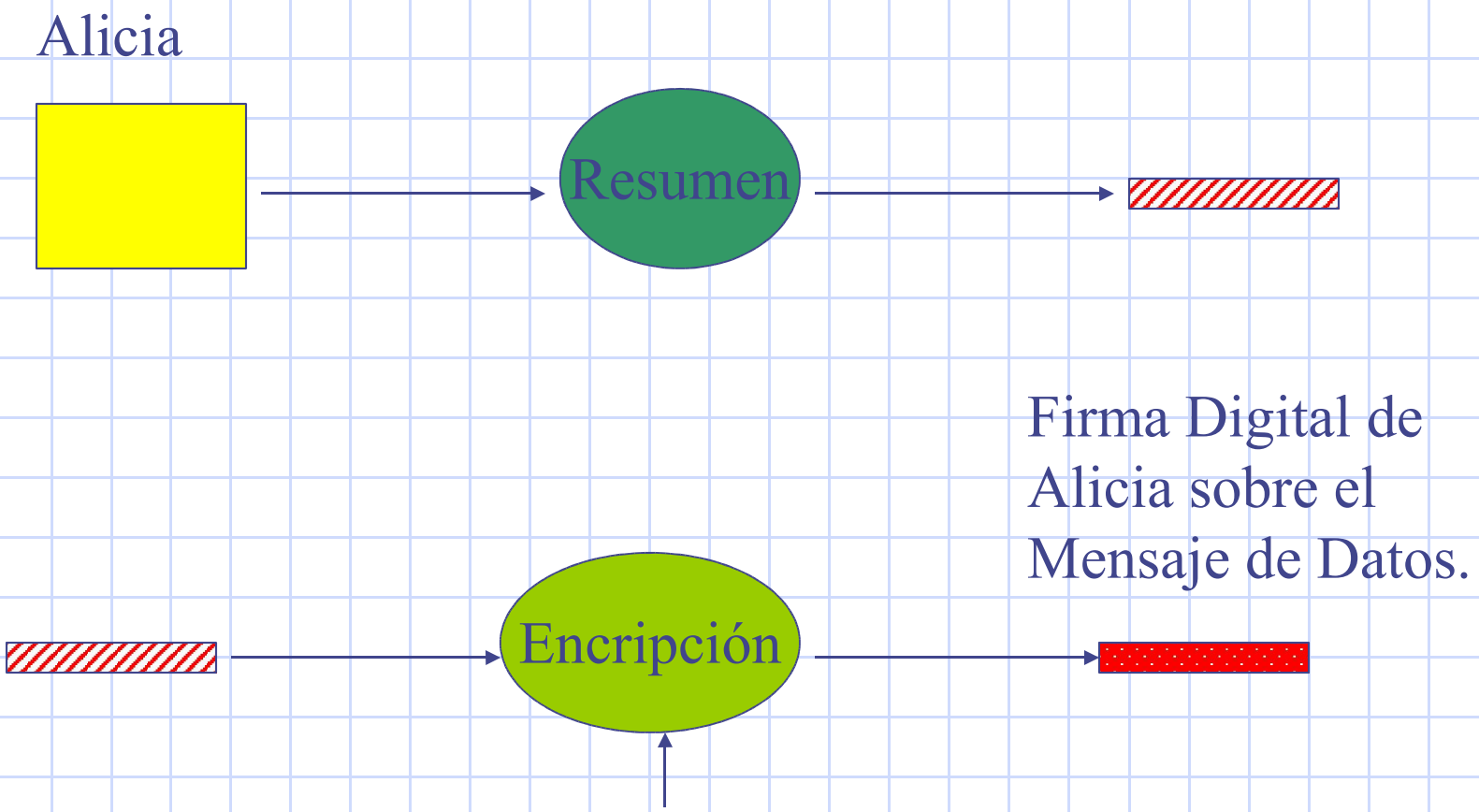
La Firma Electrónica se considerara **Avanzada o Fiable** si cumple por lo menos los siguientes requisitos
I - Los datos de creación de la firma, en el contexto en que son utilizados, **corresponden exclusivamente al firmante;**
II - Los datos de creación de la firma **estaban, en el momento de la firma, bajo el control exclusivo del firmante;**
III - Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma;
IV - Respecto a la integridad de la información de un mensaje de datos es posible detectar cualquier alteración de ésta hecha después del momento de la firma;

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.

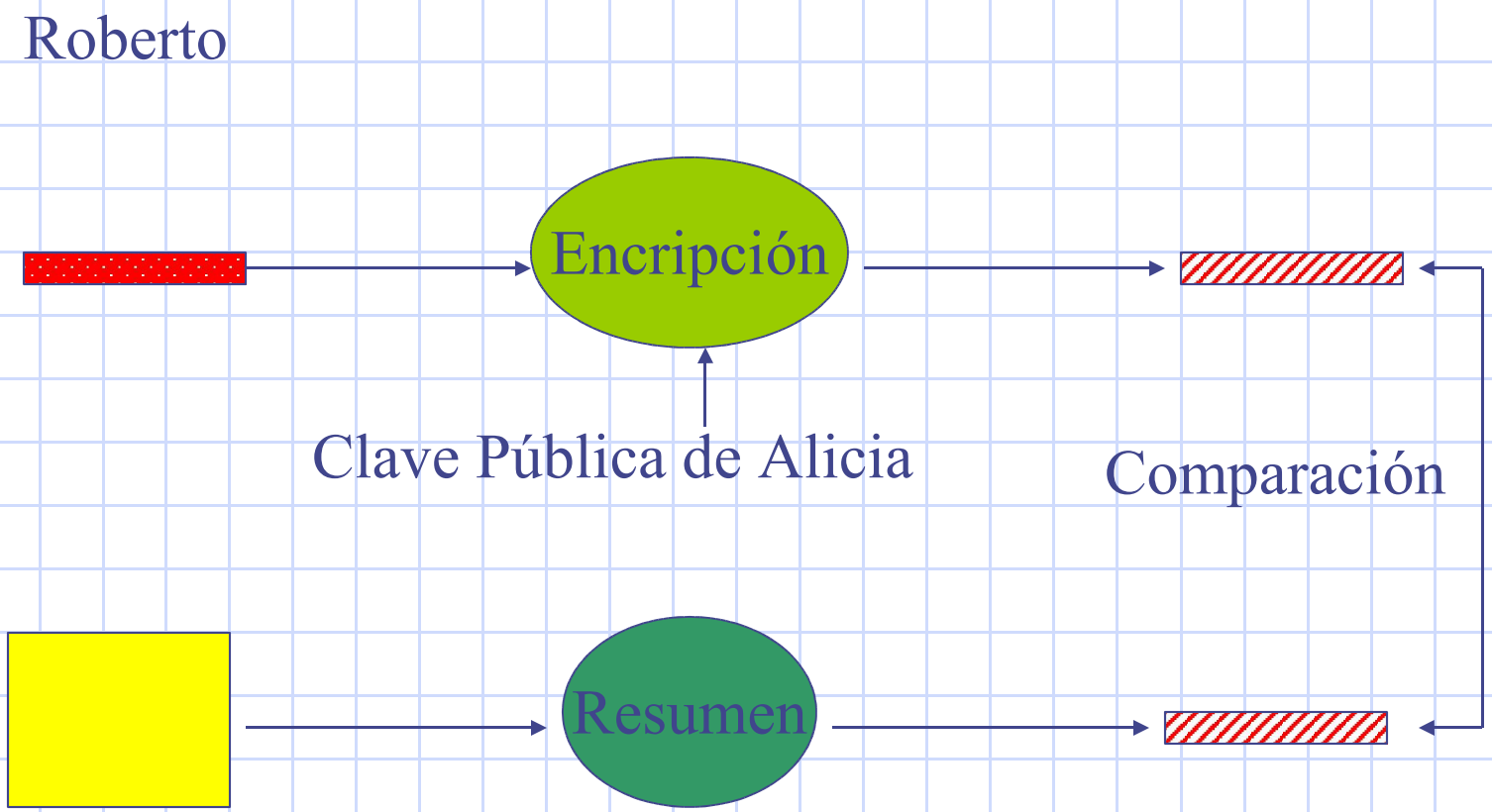
Recapitulando

- Alicia genera, en su computadora, 2 claves: una clave privada y una clave pública.
- Las claves están matemáticamente relacionadas.
- Alicia debe guardar la clave privada, y no darla a conocer a nadie.
- Alicia puede dar a conocer la clave pública a sus socios comerciales, como Roberto.
- No es posible para Roberto que, conociendo la clave pública de Alicia, pueda obtener la clave privada.
- Lo que se encripta con la clave privada sólo puede desencriptarse con la pública.

Integridad y Encripción Asimétrica



Integridad y Encripción Asimétrica



Recordando la Fiabilidad de la Firma

- ✓ Detección de falta de integridad de la firma.
- ✓ Detección de falta de integridad en el mensaje de datos.
- ✓ Control exclusivo del firmante.

Firma Autógrafa y Electrónica

	FIRMA AUTÓGRAFA	FIRMA ELECTRÓNICA FIABLE
ELEMENTOS FORMALES.-		
La firma como signo personal.	X	X
El *animus signandi*, voluntad de asumir el contenido de un documento.	X	X
ELEMENTOS FUNCIONALES		
Función Identificadora, relación jurídica entre el acto firmado y la persona que lo ha firmado.	X	X
Función de Autenticación. El autor del acto expresa su consentimiento y hace propio el mensaje	X	X
INTEGRIDAD		X
ACCESIBILIDAD		X

Enero 5, 2004

DECRETO DE REFORMAS AL CÓDIGO FISCAL DE LA FEDERACIÓN

Evolución de los Servicios Electrónicos en el SAT

Evolución
SAT

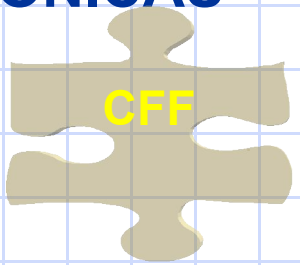
1995-2004

- Internet 1995
- Fedatarios Públicos 2001
- Comprobantes Fiscales 2002
- Esquema de Pagos Electrónicos 2002
- DeclaraSAT 2003
- Dictámenes 2003
- Validación de Ordenes de Fiscalización 2004
- **Firma Electrónica Avanzada 2004**
- **Comprobante Fiscal Digital 2004**

Fuente: SAT

Decreto que reforma, adiciona y deroga diversas disposiciones del Código Fiscal de la Federación (DOF 5 de enero 2004)

- Cuando las disposiciones fiscales obliguen a presentar documentos, éstos **deberán ser digitales y contener la firma electrónica avanzada del autor** (Durante 2004 el uso de la FEA será optativo pero los documentos deberán ser digitales).
- Se deberá contar con un certificado de FEA expedido por el S.A.T. (Personas Morales) o por un **Prestador de Servicios de Certificación autorizado por Banxico** (Personas Físicas).
- Requerimiento de **comparecencia previa ante el SAT** para toma de biométricos (acreditación de identidad).
- Los contribuyentes podrán tramitar ante el SAT por medios electrónicos uno o varios **certificados de Sello Digital** con los que podrán emitir **FACTURAS ELECTRÓNICAS** (Comprobantes Fiscales Electrónicos).



Disposiciones legales en materia Fiscal:

Reconocimiento como AR y AC del Banco de México

Convenio para la utilización de la IES	*Agosto 4, 2004*
Publicación DOF	*Septiembre 21, 2004*

Firma Electrónica Avanzada (*Tu Firm@*)

Art. 17,18, 19, 29,31,32, 38,130,134,140,...	
...141,174,176,177,181 a 183, 185,186 en CFF	*DOF Enero 5, 2004*
Regla 2.22.1 a la 2.22.5 RMF	*DOF Mayo 31, 2004*
Regla 2.11.1 en Materia de Comercio Exterior	*DOF Septiembre 21, 2004*
Facilidades de uso de la FEA	*DOF Diciembre 1, 2004*

Comprobantes Fiscales Digitales (*Factura Electrónica*)

Art. 29 en CFF	*DOF Enero 5, 2004*
Regla 2.22.5 a la 2.22.11 RMF	*DOF Mayo 31, 2004*
Anexo 20	*DOF Mayo 31, 2004*
Regla 2.22.12	*DOF Agosto 31, 2004*
Modificación al Anexo 20	*DOF Septiembre 1, 2004*

Fuente: SAT

Diferencias

Características

Firma Autógrafa

- Grafología – "Sólo yo puedo".
- No pueden robármela, no puedo perderla, pero pueden falsificarla. Es definitiva.
- Lo que veo es lo que firmo.

Firma Electrónica Avanzada

- Clave – "Sólo yo sé".
- Dispositivo – "Solo yo tengo"
  - Sí pueden robármela y puedo perderla. Es temporal.
- Biometría – "Sólo yo puedo"

.cer

.key

Claves de seguridad

****

Fuente: SAT

Definición y características de tu firm@

FE
FIRMA ELECTRONICA (Clave de Identificación Electrónica Confidencial)

tu firma La poderosa

¿Qué es la firma electrónica CIEC?

- La Clave de Identificación Electrónica Confidencial (CIEC) es un sistema de identificación basado en el RFC y el NIP (número de identificación personal).
- Se utiliza para realizar los siguientes trámites:
  - ❖Declaraciones provisionales
  - ❖Declaraciones anuales
- ❖ A partir de Noviembre 2004 otros servicios (Oficina Virtual): Tramites, Declaraciones, Servicios y Consultas

¿Qué es "Tu firma"? (Firma Electrónica Avanzada)

- La firma electrónica que cuente con un certificado digital expedido por el SAT o por un prestador de servicios de certificación autorizada.

Adicionalmente, esta firma tiene las siguientes cualidades:

- ***Reconocimiento*** por el marco legal
- ***Fiabilidad técnica*** basada en infraestructura de llave pública
- Garantías de:
  - ➢***Integridad***
  - ➢***No repudio***
  - ➢***Autenticidad***
  - ➢***Confidencialidad***

Fuente: SAT

Definición y características de tu firm@

¿Qué es el certificado digital?

Para asegurar que una determinada clave pública pertenece a un usuario en concreto se utilizan los **certificados digitales**. Un certificado digital es un documento electrónico que **asocia** una clave pública con la identidad de su propietario.

Art. 17-G, Regla 2.22.3.

- Un certificado digital emitido por el SAT contendrá los siguientes atributos:
  - El código de identificación único del certificado.
  - Mención de que el certificado fue emitido por el SAT
  - Nombre del titular del certificado
  - RFC
  - Periodo de vigencia (2 años)
  - Mención de la tecnología empleada
  - Datos de verificación de firma (Clave pública)

Art. 17-D penúltimo párrafo
Regla 2.22.2.

- Un certificado digital queda sin efecto cuando se pierde o inutilice por daños.

Art. 17-H, Regla 2.22.4.

Fuente: SAT

Normatividad

Código Fiscal de la Federación

Los obligados son Personas Morales y aquellos que no cuentan con Tarjeta Tributaria.

Artículo 31 CFF

Casos de excepción de la obligación (opcional):

- Personas físicas con actividades empresariales con ingresos inferiores a 1,750,000.00.
- Personas físicas que no realicen actividades empresariales con ingresos inferiores a 300,000.00.
- Contribuyentes que exclusivamente se dediquen a actividades agrícolas, ganaderas, pesqueras o silvícolas.

PERSONAS MORALES

- ✓ Comparecencia de apoderado con poder general para actos de dominio o administración ante el SAT, quien debe contar con FEA expedida por un prestador de servicios de certificación autorizado por Banxico, para toma de biométricos (acreditación de identidad). Se pretende en un futuro aprovechar esta base de datos para integrarla a la del CURP. La información forma parte del Registro de Población y no aplica secreto fiscal.
- ✓ Los contribuyentes personas morales podrán presentar "documentos digitales" con su firma electrónica avanzada expedida por el SAT si optan por ello deberán utilizarla en todos sus trámites ante el SAT
- ✓ Se presumirá sin que se admita prueba en contrario, que los documentos digitales que contengan firma electrónica avanzada de las personas morales, fueron presentados por el administrador único, el presidente del consejo de administración...

PERSONAS FÍSICAS

- ✓ Requerimiento de comparecencia personal (menores de edad o incapaces?) previa ante el SAT para toma de biométricos (acreditación de identidad).
- ✓ Prohibición a PSC de emitir certificados (con validez fiscal) sin contar con constancia de acreditación ante el SAT.
- ✓ Obligación de informar al SAT del código de identificación único del certificado
- ✓ El SAT puede actuar también como PSC así como la Secretaría de Función Pública (Ley Federal de Procedimiento Administrativo y Acuerdo Tramitanet) y los PSC autorizados por la Secretaría de Economía (reforma 29 de agosto C. De Com.) previa autorización de Banxico, pues usan su IES.
- ✓ Vigencia 2 años. El SAT mediante reglas de carácter general podrá relevar de la comparecencia para la emisión del segundo y ulteriores certificados.
- ✓ Las personas morales podrán actuar con la firma electrónica avanzada de su representante legal expedida por un PSC autorizado por Banxico, previa inscripción en el registro de representantes legales de las autoridades fiscales (responsabilidad del contribuyente de solicitar la cancelación de el registro citado en los casos en que se revoque el poder correspondiente).

Representante Legal

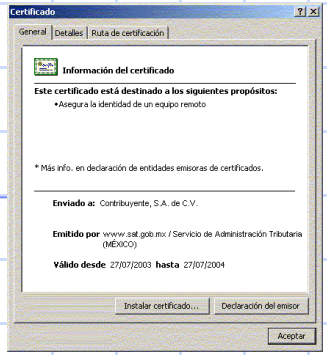
Persona Física

- Certificado propio

Representante Legal

- Tramita el Certificado para Persona Moral con poder general para actos de dominio o de administración

Certificado para Persona Moral



Certificado propio de Representante

Persona Física

- Certificado propio
  - Facultades generales

Persona Física

- Certificado propio
  - Facultades especiales

Persona Física

- Certificado propio
  - Diversos (especial)

SISTEMA DE REGISTRO DE REPRESENTANTES LEGALES

PROCESO GENERAL

CATE

1 El contribuyente pide cita al centro de Atención Telefónica Externo (01 800) 849 93 70

2 Se le asigna cita al contribuyente

El contribuyente Acude a cita 4

SAT

Administración Local

Contribuyente
- Acude a cita
- Entrega documentos
- Entrega archivo .req

ALAC
- Revisa documentos
- Genera certificado de firma electrónica avanzada

3 El contribuyente obtiene aplicación SOLCEDI y genera archivo .key y archivo .req

5 Obtiene certificado de firma electrónica avanzada

CICLO DE GENERACIÓN

SAT.GOB.MX

Fuente: SAT

Facilidades de uso de la FEA (01-12-04)

	DECLARACION PROVISIONAL	DECLARACIÓN ANUAL Y ASALARIADOS
P.F. + 300,000 ceros	**CIEC**	**FEA** **DECLARASAT**
con pago	**VENTANILLA** **TARJ. TRIBUTARIA**	**VENTANILLA** **TARJ. TRIBUTARIA** **DECLARASAT**
P.F.A.E. +1,750,000 ceros	**CIEC**	**FEA** **DECLARASAT**
con pago	**BANCA ELECTRÓNICA**	**DECLARASAT** **BANCA ELECTRÓNICA** **FEA**
P.M. (EXCEPTO ACTIV. PRIMARIAS) ceros	**CIEC**	**FEA** **DEM**
con pago	**BANCA ELECTRÓNICA**	**DEM** **BANCA ELECTRÓNICA** **FEA**

Estas facilidades solo aplican para Declaraciones (provisionales o anuales y sus complementarias o correctivas).

Actualmente están obligados a usar la FEA:

- **Agentes, mandatarios y apoderados aduanales (Regla 2.1.11 de septiembre 21 2004)**
- **Contadores Públicos Registrados y Empresas que dictaminan estados financieros (Regla 2.4.10. de diciembre 1, 2004)**
- **Ademas de los servicios que vaya habilitando paulatinamente el SAT que durante el 2005 publique en la RMF del 2005**

Uso y aplicaciones

Firma Electrónica Avanzada

Comprobante Fiscal Digital (Factura Electrónica)	Enero	Opcional
Expediente Integral del Contribuyente	Marzo	Opcional
DeclaraSAT	Marzo	Opcional
Dictaminados	Junio	Obligatorio
Agentes Aduanales	Mayo	Obligatorio
Contadores Públicos Registrados	Junio	Opcional
Devoluciones de IVA > = a $25,000	Agosto	Obligatorio
Pagos Provisionales	Marzo	Obligatorio

2006

Fuente: SAT

Futuros Servicios Electrónicos del SAT

Firma Electrónica Avanzada

- Notificación
- Avisos al RFC
- Buzón Fiscal
- Estado Fiscal del contribuyente
- Estado de cuenta del contribuyente
- Promociones
- Devoluciones
- Subastas
- Avisos de compensación
- Inscripción al RFC

2004 - 2006

Fuente: SAT

- Los contribuyentes **deberán presentar las solicitudes en materia de RFC, declaraciones, avisos o informes en documentos digitales con FEA a través de los medios y formatos electrónicos que señale el SAT a través de reglas de carácter general, presumiblemente vía Internet a las direcciones de correo electrónico que indique el SAT**. Lo anterior incluye el pago de los impuestos por medio de transferencia electrónica de fondos.

- Para el caso de **notificaciones** por correo electrónico, se requerirá **acuse de recibo** cuando se trate de citatorios, requerimientos o solicitudes de informes o documentos y de actos administrativos que puedan ser requeridos. **El acuse de recibo consistirá en el documento digital con firma electrónica que se transmite al destinatario al abrir el documento digital que le hubiere sido enviado**.

- Para demostrar ante la autoridad / el Tribunal competente, cuando se interponga un medio de defensa, la fecha de la notificación, basta la impresión del mensaje de datos (constancia de recepción).

FUERZA PROBATORIA DE LA INFORMACIÓN TRANSMITIDA A TRAVÉS DE MEDIOS ELECTRÓNICOS

Criterio Judicial

“DECLARACIONES FISCALES PRESENTADAS POR MEDIOS ELECTRONICOS (VIA INTERNET). EL PRIMER ACTO DE APLICACION SE ACREDITA CON ACUSE DE RECEPCION QUE CONTENGA LOS DATOS REFERENTES A LA HORA, FECHA, FOLIO Y TIPO DE OPERACION, TRANSMITIDO POR LA AUTORIDAD CORRESPONDIENTE.-

Para acreditar el primer acto de aplicación y, por ende, el interés jurídico del gobernado para acudir al juicio de amparo a reclamar una ley, basta con la exhibición de la constancia de recepción de la declaración y pago correspondiente, presentada a través de los medios electrónicos, específicamente en la página del Servicio de Administración Tributaria de la red respectiva que contenga los datos relativos a la hora, fecha, folio y tipo de operación, para considerarse acreditado el acto de aplicación de las normas reclamadas en el juicio de garantías, toda vez que las constancias de referencia son el único documento que se puede obtener para demostrar el cumplimiento de las obligaciones fiscales por esa vía, de conformidad con lo dispuesto en el artículo 31, párrafo segundo, del Código Fiscal de la Federación y la regla número 2.10.7. de la miscelánea fiscal vigente para el año dos mil uno. (I.7o.A. 183 A)”.

ORGANISMOS FISCALES AUTÓNOMOS

El artículo 17-C del Código Fiscal de la Federación dispone que:

"Tratándose de contribuciones administradas por organismos fiscales autonómos, las disposiciones de este Código en materia de medios electrponicos sólo serán aplicables cuando así lo establezca la ley de la materia."

Considerando lo anterior, el cuestionamiento que surge es si estos organismos aplicarán los dispuesto por el CFF o establecerán su propia normatividad.

IMSS:

El 3 de marzo de 2004: Publicación en el Diario Oficial de la Federación del acuerdo no. 43/2004 en el cual se establecen los *lineamientos para la asignación del número patronal de identificación electrónica y certificado digital*.

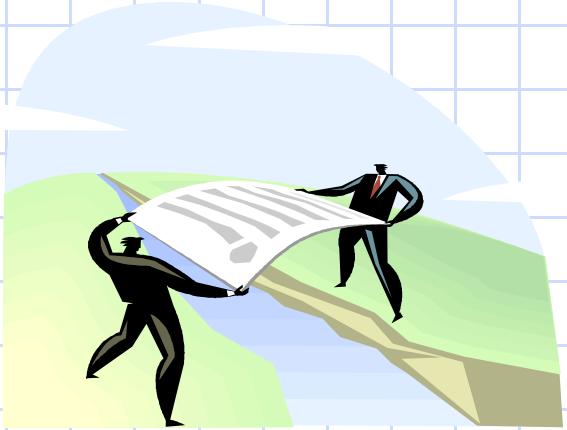
En este acuerdo, se establece que para efectos de la prestación de servicios de certificación se estará a lo dispuesto por el Código de Comercio, ordenamiento que a su vez atribuye su regulación a la Secretaría de Economía. Actuando el IMSS como Agencia Certificadora

El 14 de mayo del 2004 se publicó el Acuerdo 3252003 que adecúa los lineamientos para la asignación del Registro Patronal Único (IDSE)

El 18 de enero del 2005 se publicó el aviso que da a aconocer los formatos relativos a certificación digital

Comprobante Fiscal Digital ¿Factura Electrónica?

La Factura Electrónica es, al igual que una factura en papel, el documento que viene a cerrar el ciclo comercial de las empresas, pero su medio entrega es electrónico.



Factura electrónica es más que la simple presentación de la factura en la pantalla de la PC. Involucra procesos complejos que le dan tanto a la empresa facturadora como a sus clientes beneficios más importantes que la ventaja obvia de la logística de presentación electrónica.

COMPROBANTES FISCALES DIGITALES

Las personas físicas y morales que cuenten con un **certificado de firma electrónica avanzada vigente** y lleven su **contabilidad en sistema electrónico**, podrán emitir los comprobantes de las operaciones que realicen mediante documentos electrónicos que cuenten con sello digital.

- Tramitar (por medios electrónicos ante el SAT) el *certificado para el uso de sellos digitales* (misma regulación que FEA), puede ser uno o varios
- Incorporar en los comprobantes electrónicos que se expidan los datos establecidos en las fracciones I, III, IV, V, VI del artículo 29-A del CFF.
- Asignar un *número de folio* (establecer un sistema electrónico de emisión de folios de acuerdo con Reglas Generales del S.A.T.). Elementos requeridos:
  - Solicitar asignación de folios al SAT
  - Reporte mensual al SAT
- Proporcionar al cliente, si lo solicita, impresión en papel
  - *Registro en contabilidad simultáneo a la emisión*
- Especificaciones técnicas y conservación, sujeto a reglas generales
  - Obligación del contribuyente de comprobación de autenticidad de CFD en la página del SAT

Los contribuyentes que opten por emitir CFD no podrán emitir otro tipo de comprobantes fiscales (en la Resolución Miscelánea Fiscal, cumpliendo ciertos requisitos, se establece la posibilidad de emitir simultanemente CF en papel y digitales))

Esquema de transición

Esquema actual

- Impresores Autorizados
- Autoimpresores

Serie A folio 5,001…

Serie B folio 2,500…

Convivencia

Reporte mensual

Serie	Folio
Serie A	5001
Serie A	5002
Serie AA	

CFD

- Comprobante Electrónico

Serie AA folio 001…

Serie BB folio 001…

- **Contribuyentes que dictaminen o hayan optado por dictaminar**

CFD Únicamente

PROCESO GENERAL DE FACTURA ELECTRÓNICA

Emisor

1) Solicita Certificado de Sello Digital

2) Solicita folios

4) Envía reporte mensual

SAT

3) Envía factura firmada con sello digital y folios autorizados por el SAT

Receptor

Verifica la validez de la factura y la identidad del Emisor

Fuente: SAT

Evolución del comprobante fiscal

Cajas de Cartón S.A. de C.V.

JUAREZ No. 42
COL. CENTRO
DEL. CUAUHTEMOC
MEXICO, D.F. C.P.01423

R.F.C. CAC 940218 UZA

NOTA DE CREDITO
No. 143

CLIENTE: GABRIELA FLORES MARQUEZ
R.F.C.: FOMG 701002 HV3
DOMICILIO: SAN PEDRO No. 28, COL. OLIVARES, DELEGACION CUAJIMALPA MEXICO, D. F., C.P. 53620

LUGAR Y FECHA: México, D.F. a 20 de octubre de 2001
FACTURA No. 120

CANTIDAD	DESCRIPCION	PRECIO UNITARIO	IMPORTE
10	Cajas de cartón de 20 cm. x 50 cm. devolución por defectos de fabricación.	10.00	100.00

CEDULA DE IDENTIFICACION FISCAL CAC 940218 UZA — Cajas de Cartón, S. A. de C. V.

SUBTOTAL 100.00
I. V. A. 15.00
IMPORTE TOTAL 115.00

FIRMA

Importe total en letra:

IMPRESO POR: ROLANDO ORTEGA TEJEDA CALLE 8 DE JULIO No. 23, COL. AJUSCO, C.P. 12200, MEXICO, D.F. R. F. C. OETR 681223 RV2, TEL. 56-95-14-00
AUT. S. H. C. P. 2109/99 LA REPRODUCCION NO AUTORIZADA DE ESTE COMPROBANTE CONSTITUYE UN DELITO EN LOS TERMINOS DE LAS DISPOSICIONES FISCALES. ELABORADO EL 12 DE MARZO DE 2001. VIGENCIA 12 DE MARZO DE 2001 AL 12 DE MARZO DE 2003.
NUMERO DE APROBACION DEL SISTEMA DE CONTROL DE IMPRESORES AUTORIZADOS 425

Cédula de Identificación Fiscal

Cadena original

Sello digital

Comida Gastronómica del Sur

RFC: CGS010302HMG
Domicilio Fiscal: Hidalgo #1254 Tel: 55113456
Domicilio Sucursal: Allende #854 Tel 55667923

Folio: 23456

No. Serie del certificado

Fecha : 3 de Marzo de 2004
Lugar de Expedición: México DF
Cliente: Jesus Eduardo Gonzalez
RFC: GOIJ760714
Dirección: Altavista # 759

Descripción	Importe
Consumo	$200.00
Sub-Total	$200.00
IVA	$30.00
Total	$230.00

Importe con letra: doscientos treinta pesos MN

Cadena Original

CGS010302HMG | 23456 | 03032204 | 200| 30 | 230 | fgt343rfg | .....

Sello digital de la sucursal

Kdkf874374jf87g73lsñskjvmnb873nfiv7ekjvhvb7eifhuf kghfmflkfm.....

Este documento es una impresión de un comprobante fiscal digital

Fuente: SAT

Fundamentos:

Folio
Art. 29 fracción III, Regla 2.22.8.

No. de serie
Art. 29 fracción III, Regla 2.22.8.

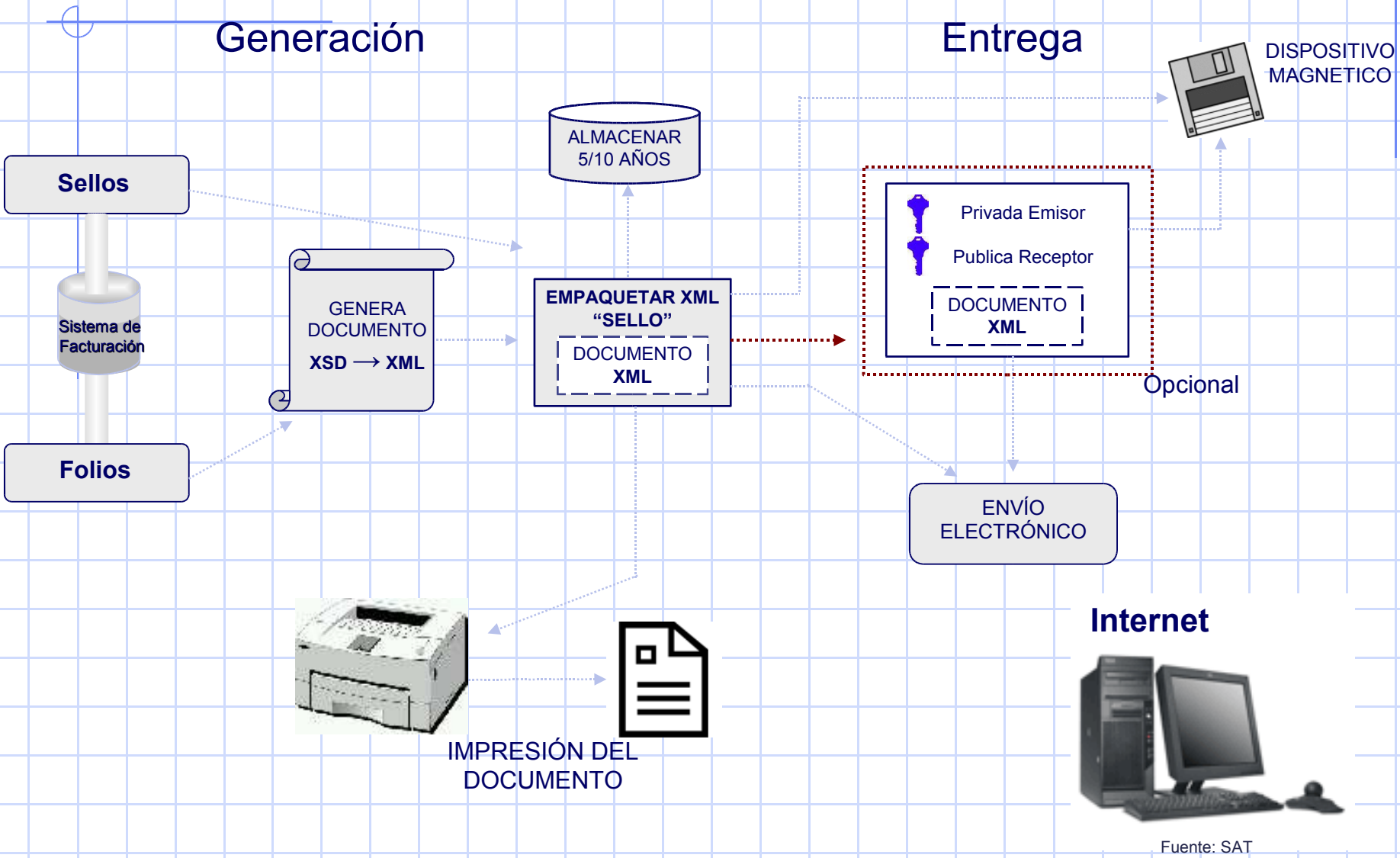
Cadena Original
Art. 29 fracción IV primer párrafo, Regla 2.22.8.

Sello digital
Art. 29 fracción I, Regla 2.22.8.

Leyenda

Fuente: SAT

Esquema de intercambio de Facturas

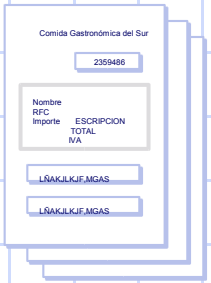


Fuente: SAT

Reportes mensuales al SAT

Empresa
RFC ABC 010101

Facturas generadas por la Empresa



Creación del reporte de folios utilizados

Se enviara un reporte de las facturas utilizadas cada mes al SAT.

Art. 29 fracción II, Regla 2.22.11.

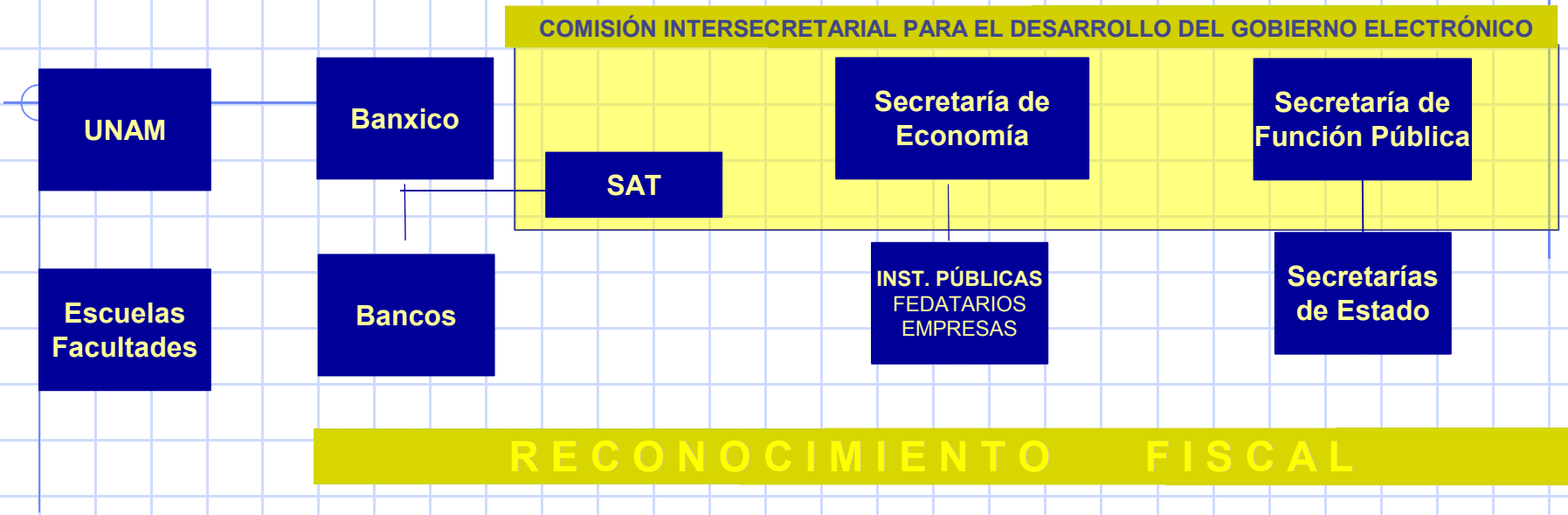
Listado de folios utilizados

RFC del Cliente | Serie | Folio | # de Autorización | Fecha | Monto | IVA | Estado del comprobante |

GOIJ760714 | A | 198485 | 34trgf | 03032004 | $230 | $30 | 1 |
GOIJ760714 | A | 198436 | 34trgf | 03032004 | $460 | $60 | 1 |

Fuente: SAT

MAPA SITUACIÓN ACTUAL



RECONOCIMIENTO FISCAL

Acuerdo del Rector

3 Oct 2005

IES

Circular 6-2005

Reforma CFF

Reglas Generales
(Miscelanea)

Reformas C. Com:
Comercio Electrónico
Firma Electrónica

NOM Conservación (Vigencia)
Reglas Generales / Reglamento

IMSS (acuerdos)

Ley de Procedimiento Administrativo

COMPRANET
TRAMITANET

- **Prestadores de Servicios de Certificación distintos al SAT (Bancos y empresas comerciales)**
- **Representantes de Personas Morales (tanto para FEA como para CFD)**

México online

POR HIROSHI TAKAHASHI
GRÁFICO ALEJANDRO ESPINOSA

Más de 17 millones de habitantes de este país navegan en la red, de acuerdo con la Asociación Mexicana de Internet (Amipci). La edad de los principales usuarios fluctúa entre los 13 y 35 años. Aquí, una aproximación numérica al México en línea, y directa a los mejores sitios de internet nacionales:

10.8 millones de computadoras

46.1 millones de celulares

1.7 millones de agendas electrónicas

3.6 millones de cuentas de acceso a internet

24% escucha música

24% descarga canciones

17% juega en línea

11% busca noticias

Los ganadores del reconocimiento Amipci 2005, una distinción a la calidad de los productos y servicios en internet en México entre más de 850 empresas e instituciones registradas como aspirantes, fueron:

Medios de comunicación: **El Universal Online**

Arte, Cultura y Educación: **Tecnológico de Monterrey**

Asociaciones y Organismos No Gubernamentales: **NIC México**

B2C Tiendas y Comercios Electrónicos: **MercadoLibre**

Construcción e Inmobiliarias: **Metros Cúbicos**

- Entretenimiento: **Cinemex**
- Hardware y Software: **Apple**
- Industria automotriz: **Autocosmos.com**
- Infraestructura y Telecomunicaciones: **Avantel**
- Portales horizontales, Buscadores y Directorios: **Google**
- Presencia corporativa o de marca: **Grupo Bimbo**
- Servicios de gobierno electrónico: **Presidencia de la República**
- Servicios y productos de salud: **Laboratorios Pisa**
- Servicios y productos financieros: **BBVA Bancomer**
- Servicios profesionales: **OCC Mundial**
- Servicios y Productos turísticos: **ClickHoteles.com**

2,384,687,000 pesos las ventas totales del comercio electrónico en México durante 2004.

450,836,000 pesos, ventas de enero a marzo de 2004.

806,150,000 pesos, facturación del primer trimestre de 2005 (81% más que el año anterior).

31% libros

35% de las compras en el último año fueron aparatos electrónicos

28% discos compactos

35% compró software

45% pagó con tarjeta de crédito

25% reservaciones / boletos de avión

10% en efectivo

36% gastó entre 400 y mil pesos

23% de mil a tres mil pesos

34% depósito

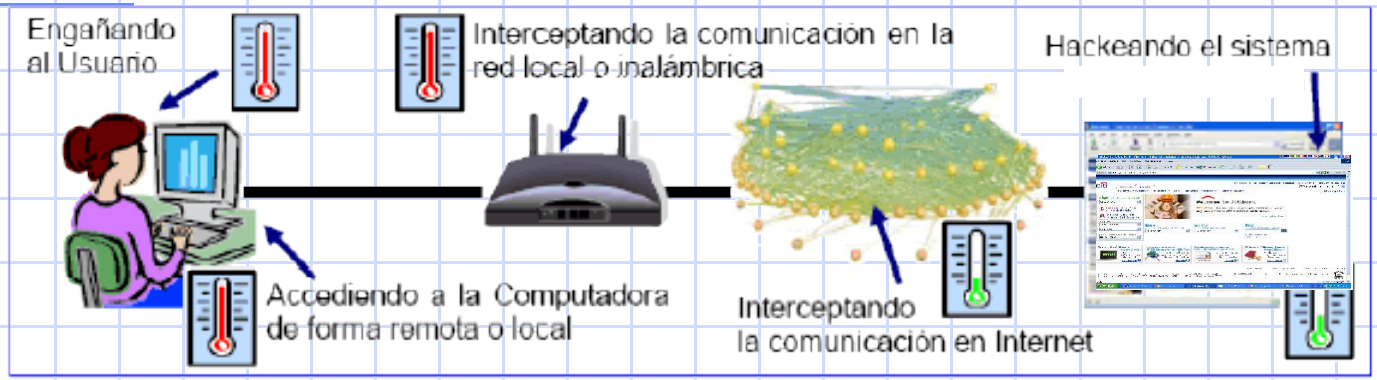
49% no compra en internet por desconfianza

36% tiene miedo de proporcionar información

39% por no contar con tarjeta de crédito

Fuente: Amipci. "Hábitos de los usuarios de internet en México 2005" y el primer estudio de la Asociación Mexicana de Internet sobre el comercio electrónico.

Seguridad en Internet



Actualmente los principales riesgos de fraude se concentran del lado del usuario final.

- Computadoras de uso Público (cafés Internet, universidades, etc.)
- Redes Inalámbricas Públicas (hoteles, aeropuerto, restaurantes, etc)
- Redes Inalámbricas Privadas pero desprotegidas* (casa, oficina, universidad, etc.)
- Redes Privadas Cableadas o Inalámbricas Protegidas (casa u oficina)
- Computadora Personal conectada directo a Internet (con firewall personal) (vía MODEM, ADSL, MMDS)

*Las redes inalámbricas se pueden acceder por medio de antenas, por lo que si no está protegida (cifrando la comunicación), cualquier persona ajena se puede conectar, espiar la transferencia de información o hacer mal uso.

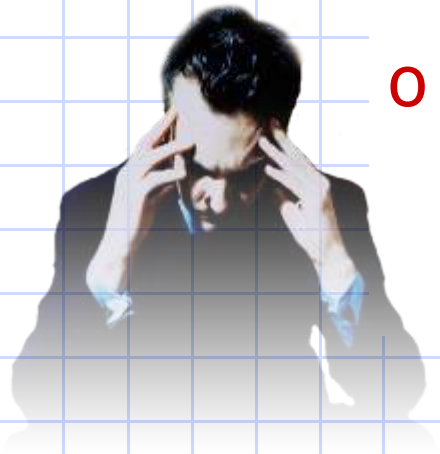
- Alto Riesgo o Muy Frecuente
- Riesgo Medio o Poco Frecuente
- Bajo Riesgo o Muy Poco Frecuente

FUENTE: http://www.amipci.org.mx/contenidos/fraudes_en_internet.html

Percepción vs Realidad

La tecnología no se percibe como segura

- 45% de los usuarios no hacen banca en línea porque no confían en la seguridad de las transacciones (AMPCI Select)
- Solo 4.2**%** de los usuarios de Internet compra en línea (Select, PWC)
- El **58%** de los internautas señala que la peor amenaza hoy en dia es el Spyware, solo el 19% tiene problemas con virus. (Reforma poll)



Navega protegido en Internet

Esto Afecta a la Industria ...

- **La percepción de inseguridad de los usuarios es un inhibidor del uso de Internet (banca en línea, comercio electrónico, inversión en tecnología, etc.)**

Debido a la Inseguridad:

Navega protegido en Internet

De un Mercado Potencial superior a los $38,000 millones de pesos, se realizan operaciones por solo $ 2,384 millones de pesos al año

Más de $ 11,600 millones de pesos no son vendidos al año en Comercio Electrónico porque al usuario '**Le da miedo dar su numero de tarjeta de crédito**'

La Banca Electrónica pierde ahorros hasta por $ 75 millones de pesos mensuales porque los usuarios

'No confían en realizar sus movimientos en línea'

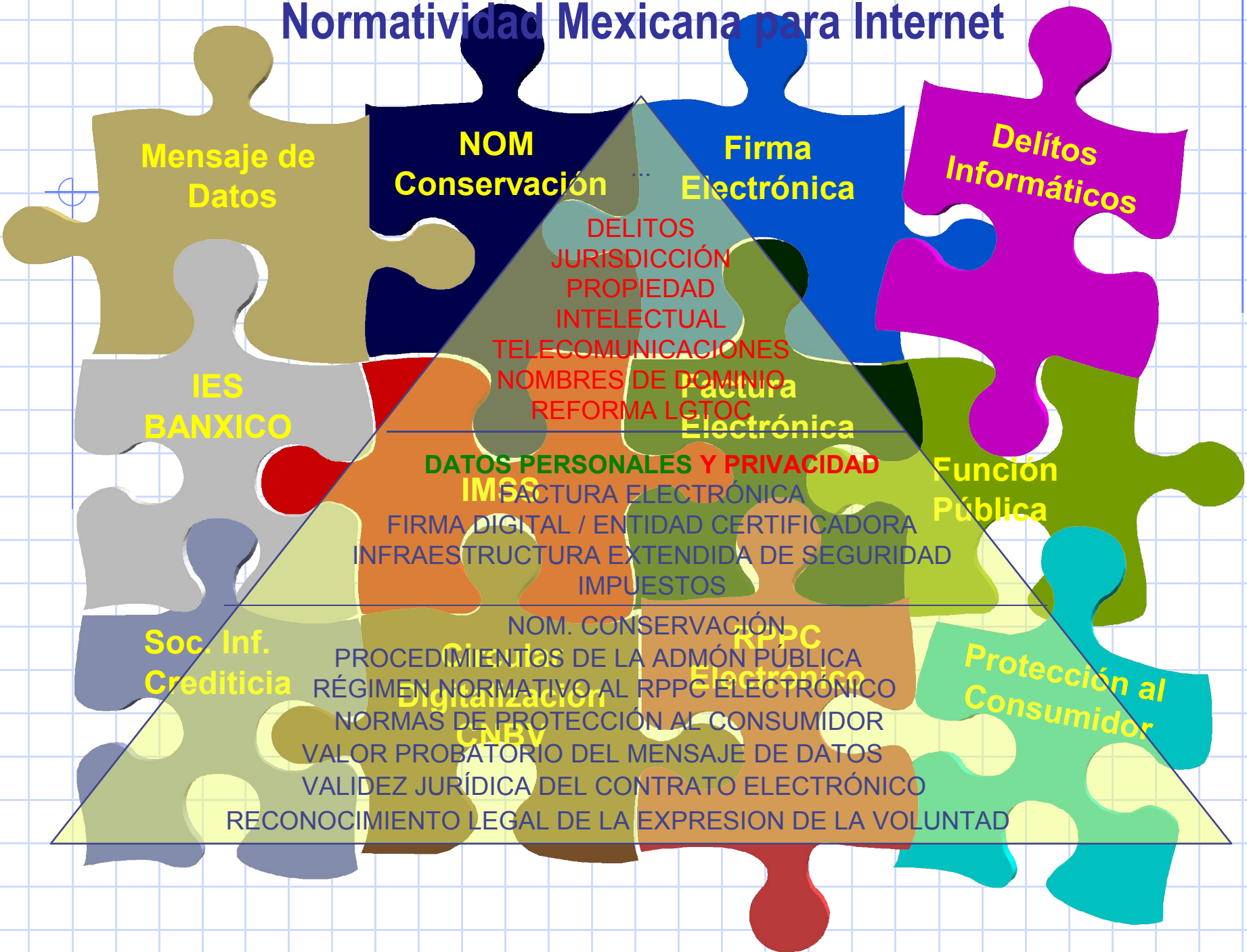
Lo que comunica la prensa:

"En la Red nadie esta a Salvo"
Reforma

"En menos de 4 horas, una computadora conectada a Internet es atacada … aun si no se navega en ella!!."
Reforma

"Mas de 40 millones de tarjetas de crédito expuestas a fraude por fallas de seguridad, informó MasterCard."
NY Times

Dos millones de cuentas bancarias afectadas en EU en los últimos 12 meses
MSNBC

Navega protegido en Internet

Normatividad Mexicana para Internet