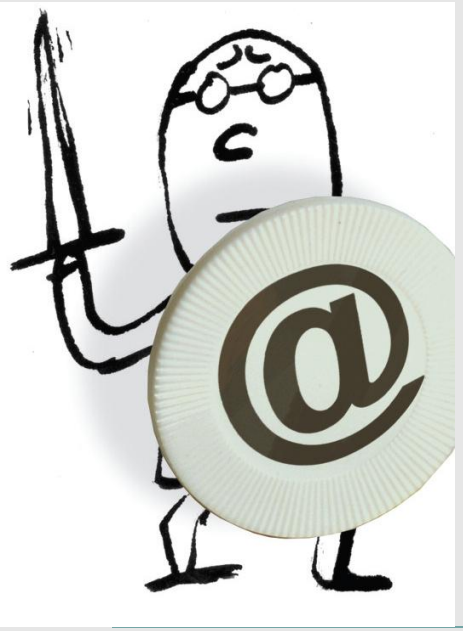
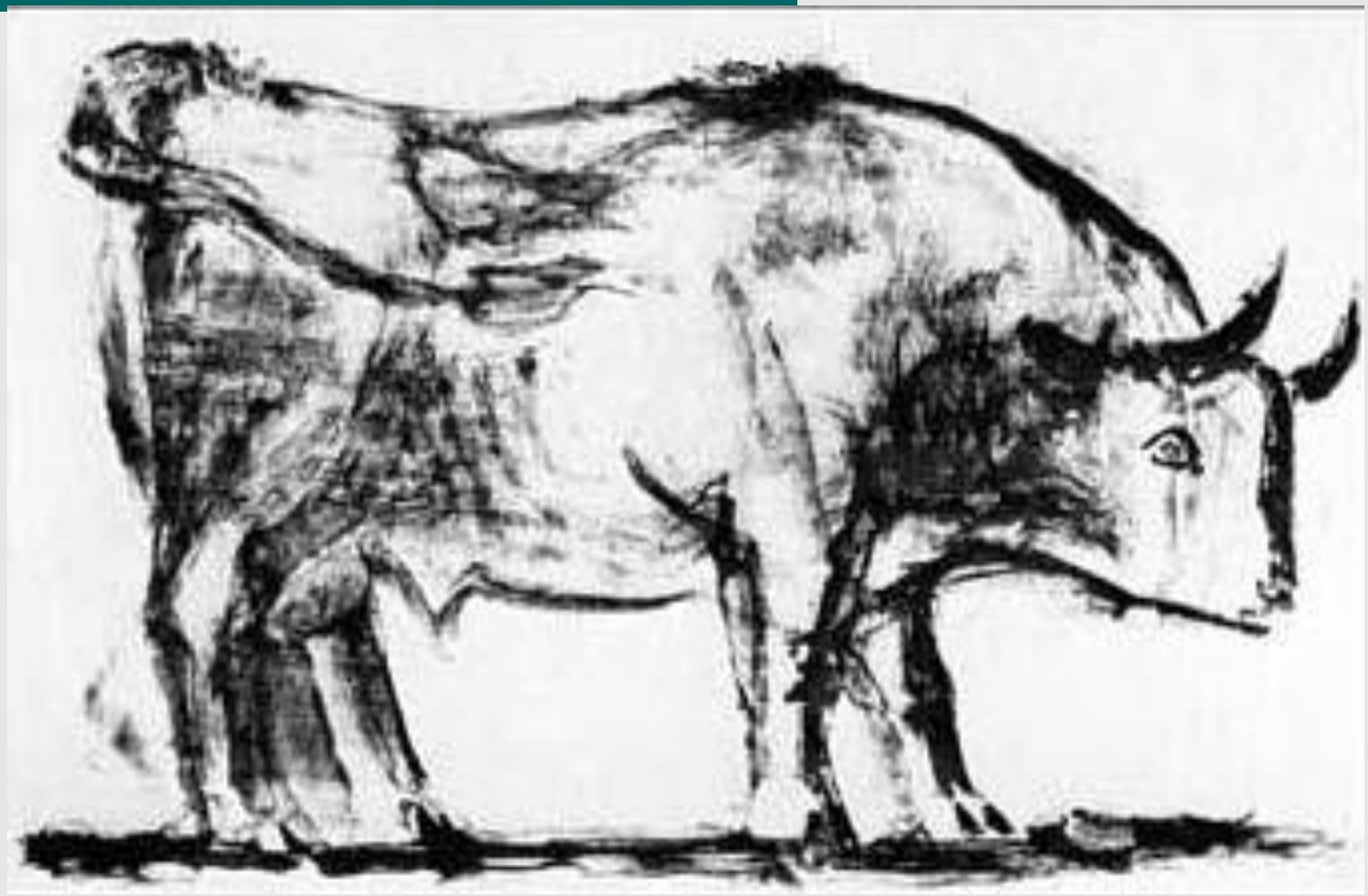
Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México



Presentado por Francisco Rodríguez-Henríquez
CINVESTAV-IPN

Conceptos básicos y antecedentes



Modelo de Capas para Sistemas de Seguridad

Aplicaciones: correo electrónico seguro, facturas digitales, elecciones electrónicas, cortafuegos, etc.

Protocolos de Comunicación: SSL/TLS/WTLS, IPSEC, IEEE 802.11, etc.

Servicios de Seguridad: Confidencialidad, Integridad de Datos, Autenticación, No-Repudio

Funciones Criptográficas: Cifrar/Descifrar, Firmar/Verificar

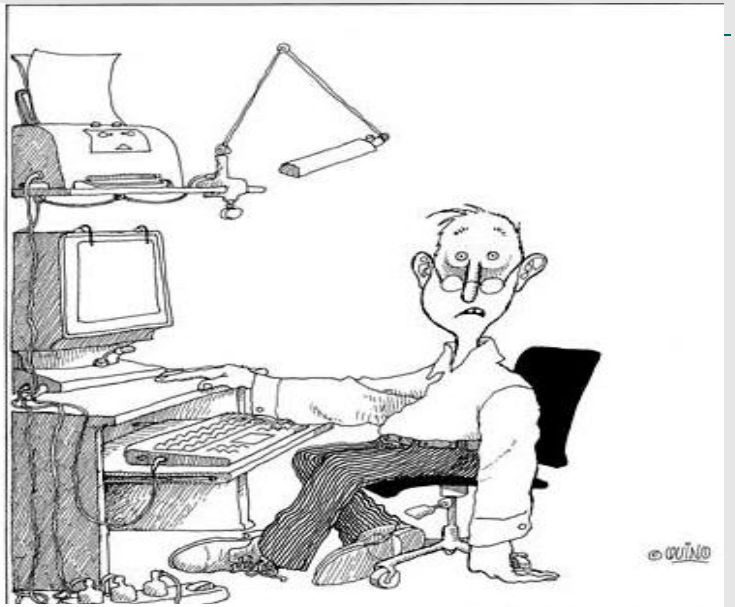
Algoritmos de Llave Pública: RSA, ECC
Algoritmos de llave Simétrica: AES, DES, RC4, etc..

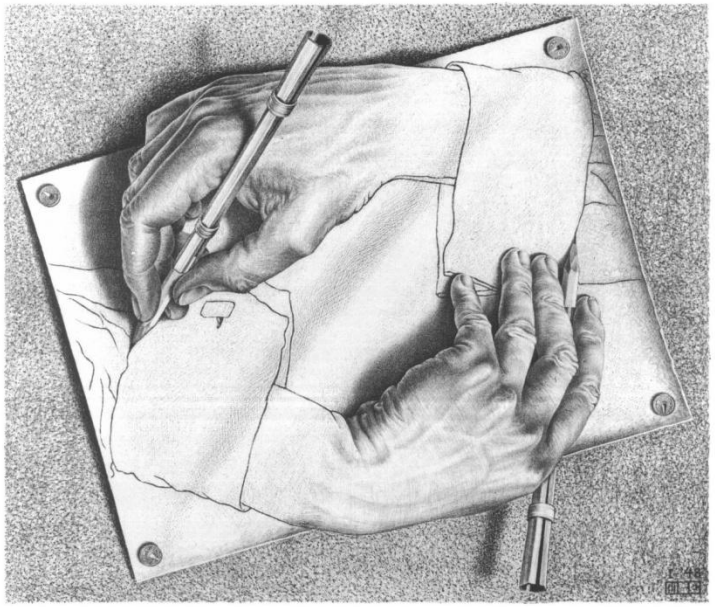
Aritmética Computacional : Suma, Elevar al cuadrado, multiplicación, inversión y Exponenciación

Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México

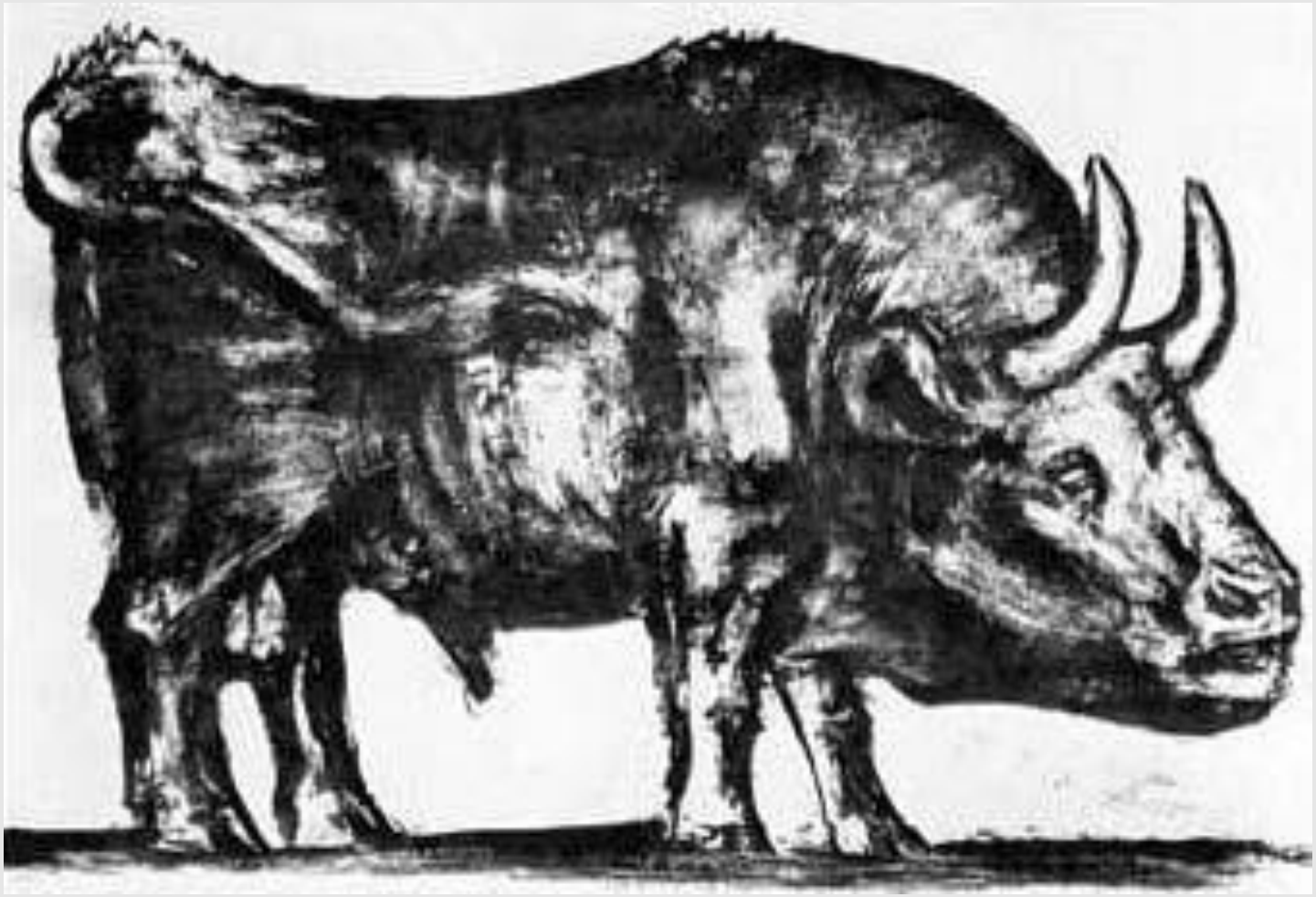
Áreas de las ciencias de la computación involucradas

- autenticación biométrica
- bases de datos
- criptografía
- minería de datos
- procesamiento digital de señales
- reconocimiento de patrones
- reconocimiento de voz
- recuperación de la información
- seguridad informática
- sistemas distribuidos
- …



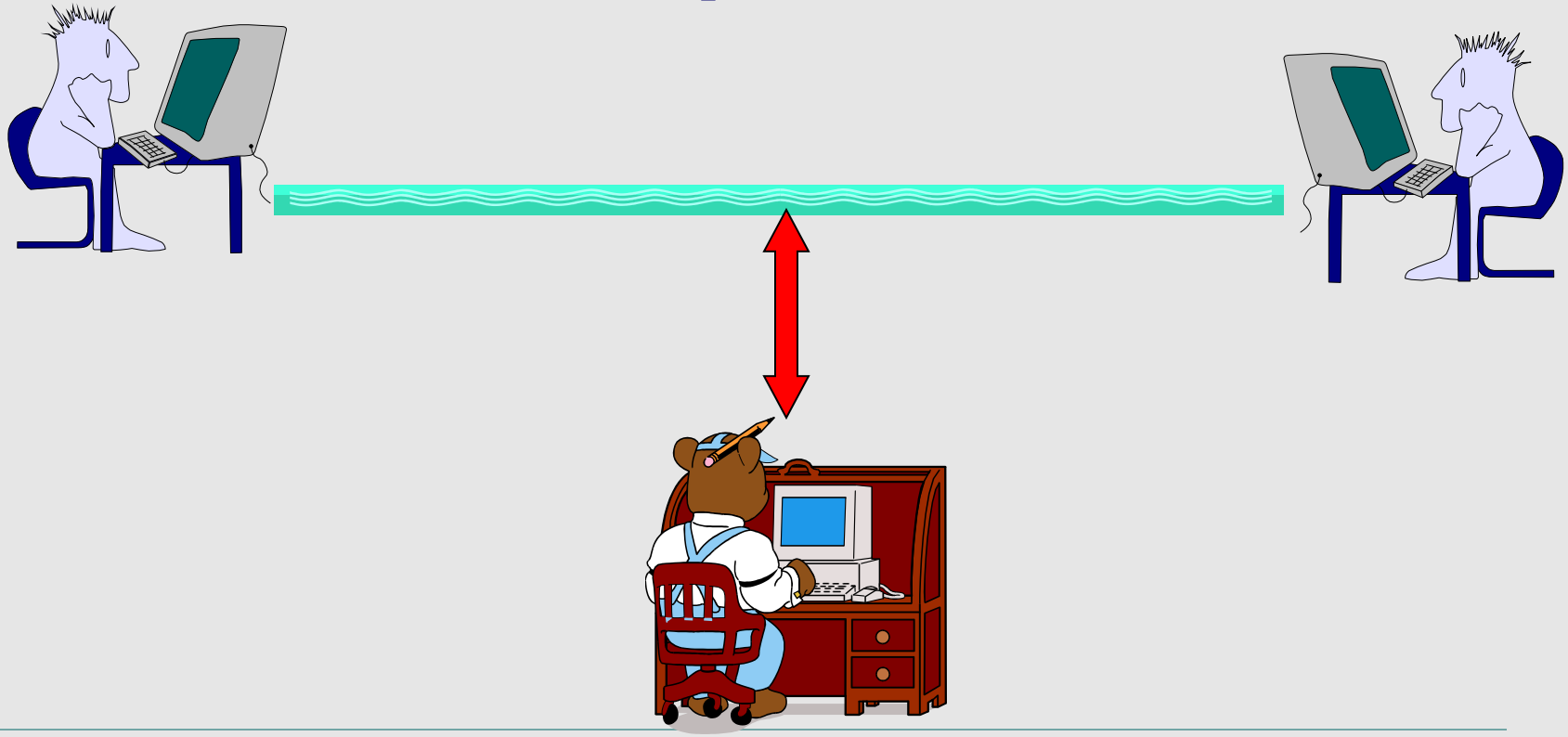


Ataques



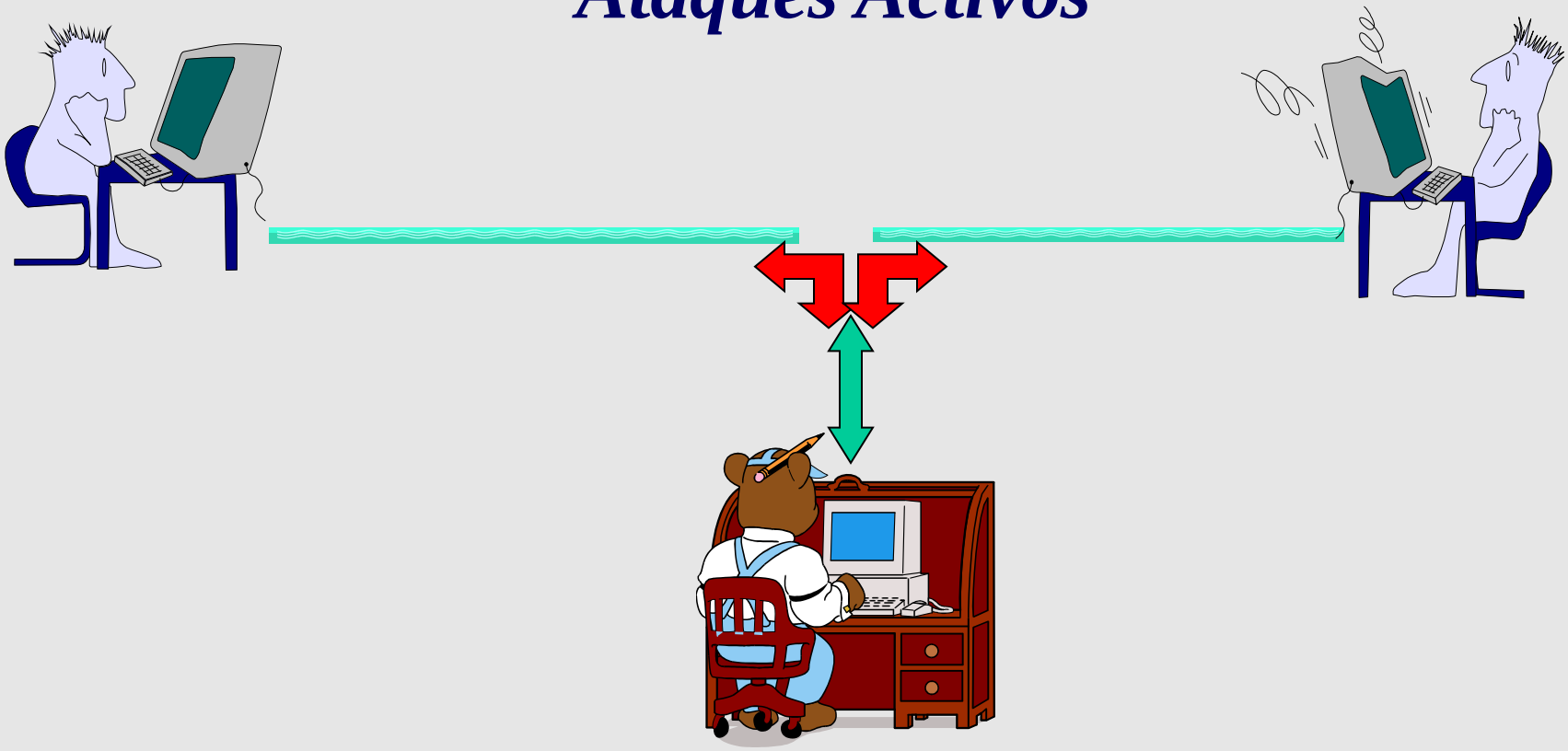
Ataques a la Seguridad

Ataques Pasivos



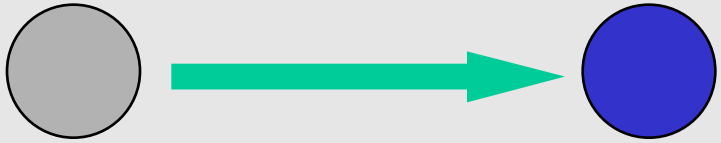
Ataques a la Seguridad

Ataques Activos



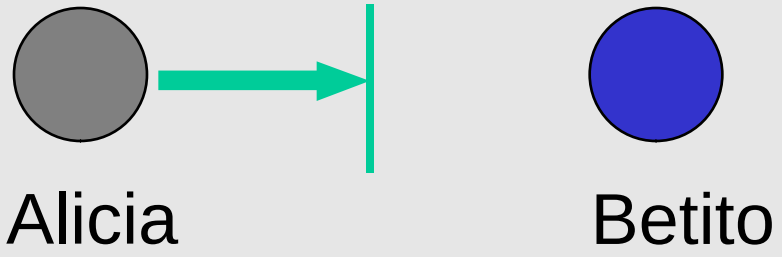
Clases de Ataques a la Seguridad

- Interrupción
- Intercepción
- Modificación
- Fabricación



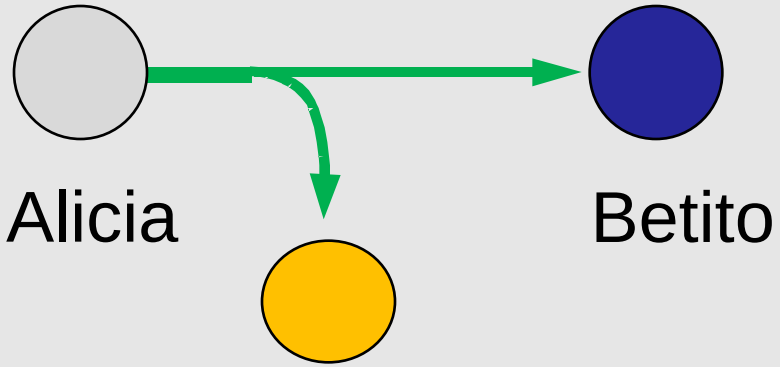
Clases de Ataques a la Seguridad: Interrupción

- Interrupción
  - Disponibilidad
- Intercepción
- Modificación
- Fabricación



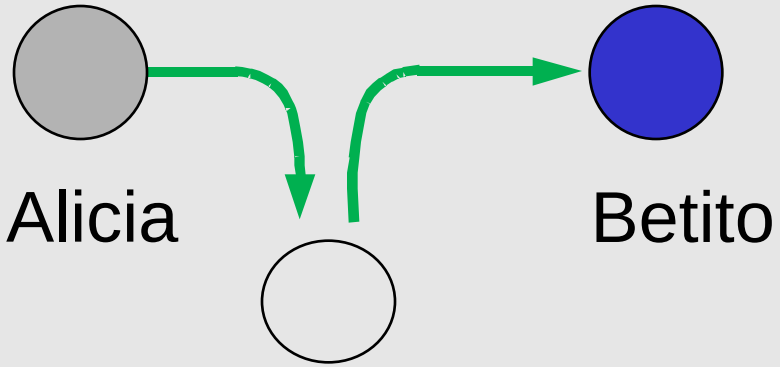
Clases de Ataques a la Seguridad: Intercepción

- Interrupción
- Intercepción
  - Confidencialidad
- Modificación
- Fabricación



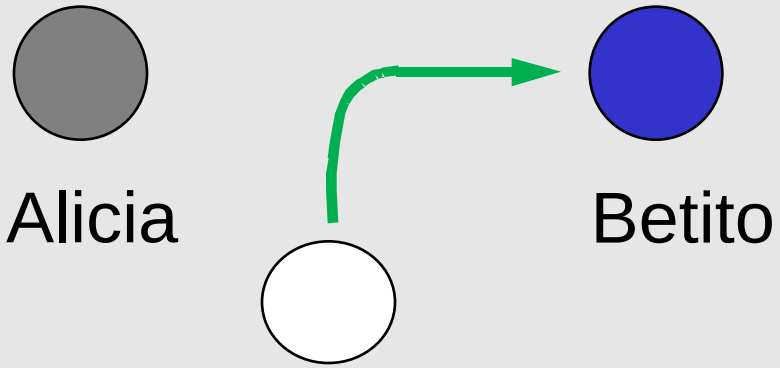
Clases de Ataques a la Seguridad: Modificación

- Interrupción
- Intercepción
- Modificación
  - Integridad
- Fabricación

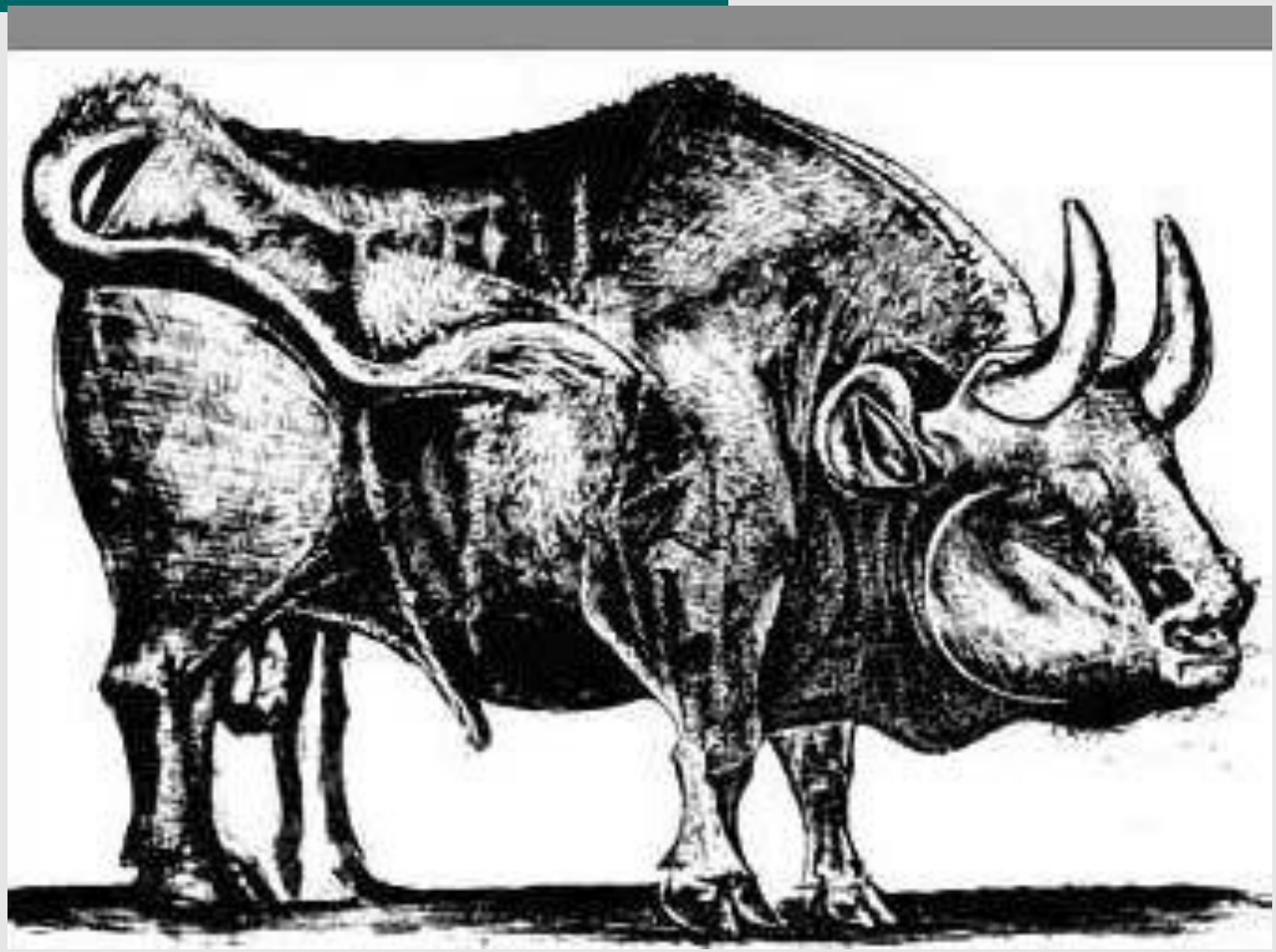


Clases de Ataques a la Seguridad: Fabricación

- Interrupción
- Intercepción
- Modificación
- Fabricación
  - Autenticidad



¿Cuáles son los desafíos de la seguridad informática?



Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México

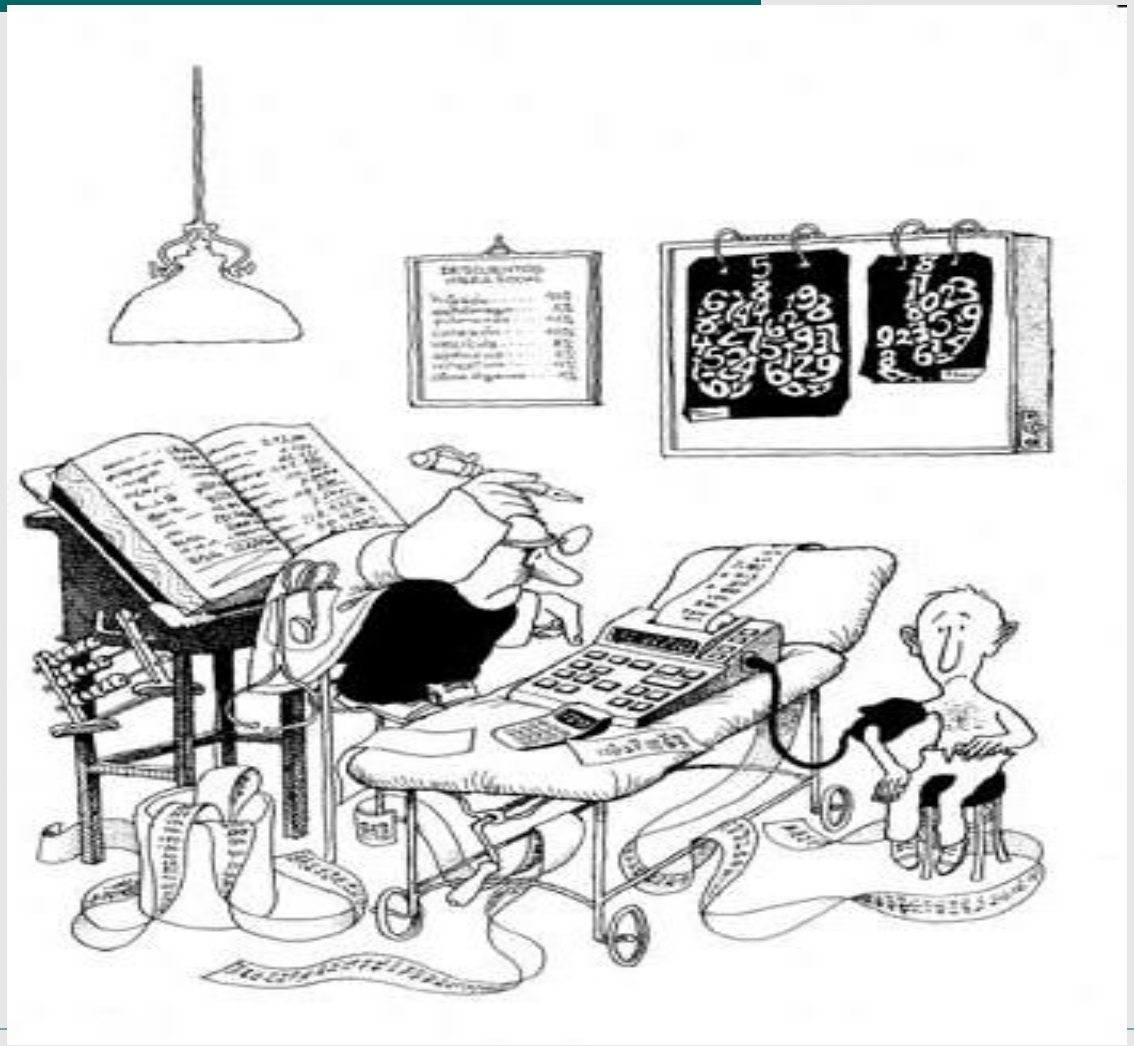
Dilema de la seguridad informática y la economía

- Los usuarios no está dispuestos a pagar por la seguridad informática *per se*
- Los usuarios no comprarán productos inseguros

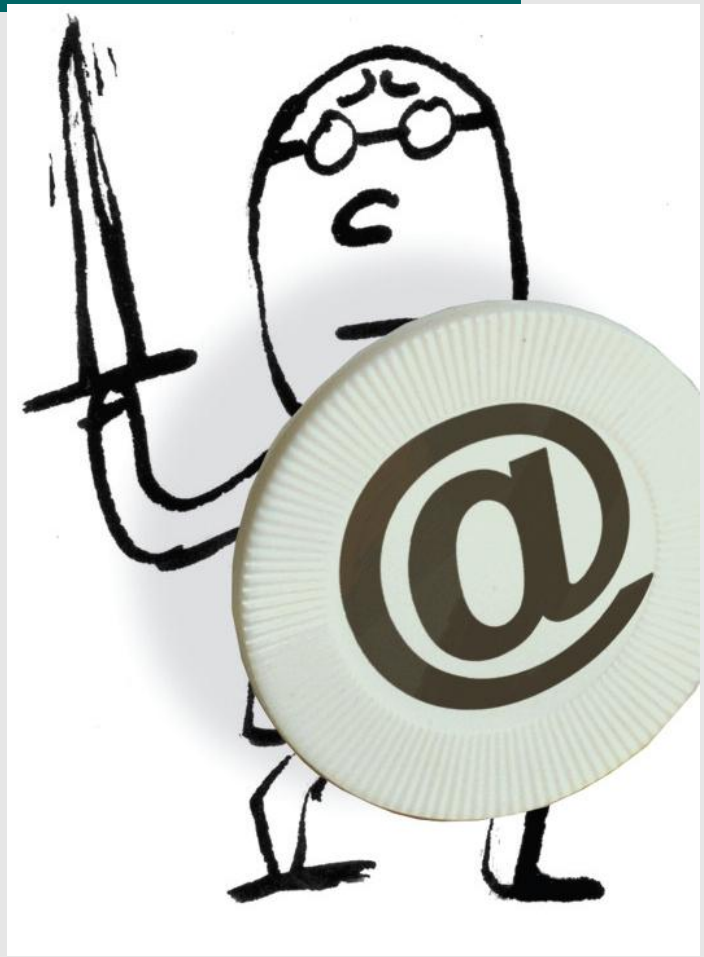
Las tres leyes de la seguridad:

1. No existen sistemas absolutamente seguros

Las tres leyes de la seguridad:
2. Reducir las vulnerabilidades a la mitad implica duplicar los gastos de seguridad

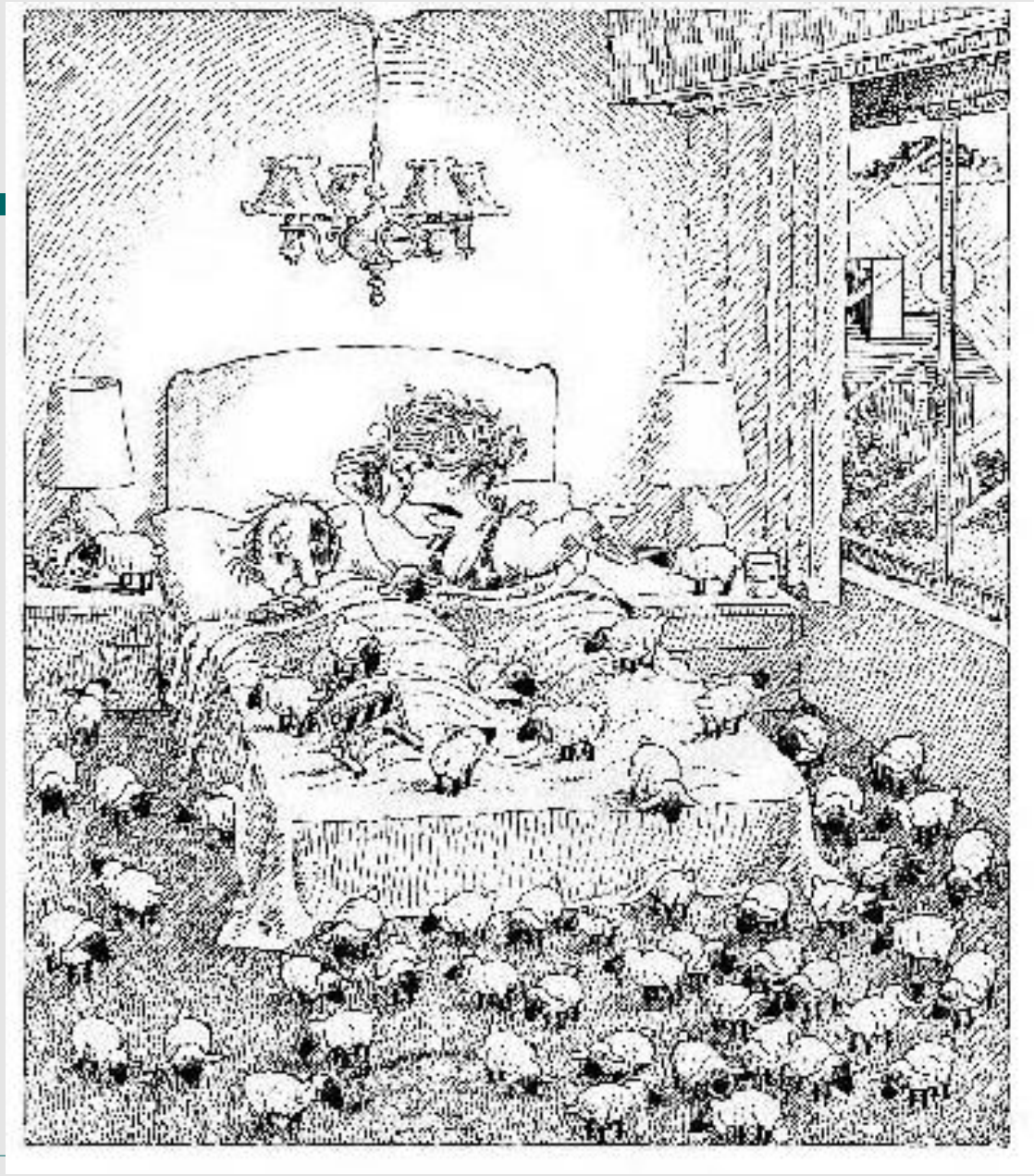


Las tres leyes de la seguridad:
3. Típicamente la criptografía no es vulnerada sino más bien brincada



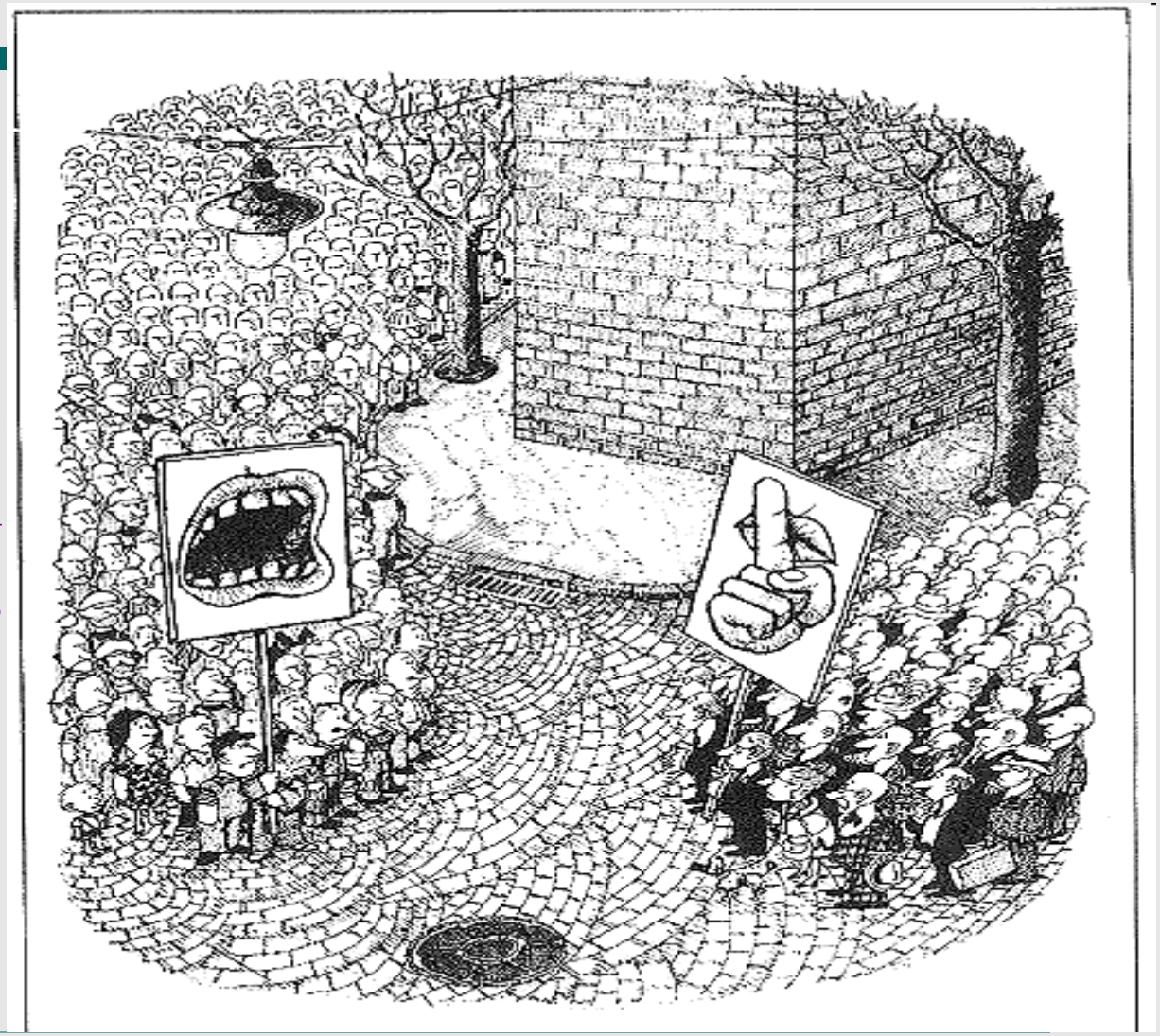
Privacidad

- ¿Cómo podemos estar seguros que nuestros datos personales no serán difundidos ni redirigidos a otras entidades?

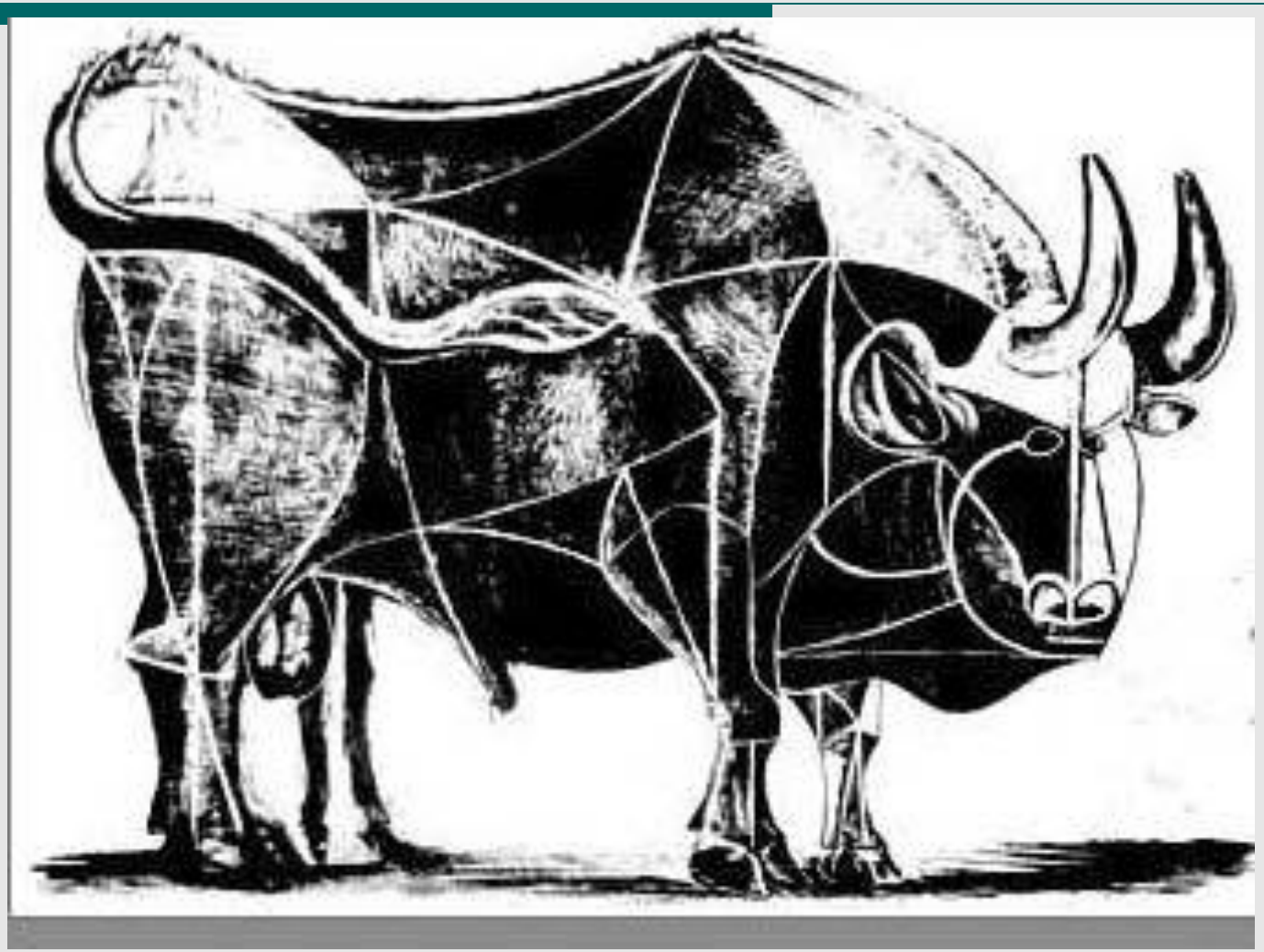


Confianza

- ¿Debo confiar mis datos confidenciales a las bases de datos gubernamentales?



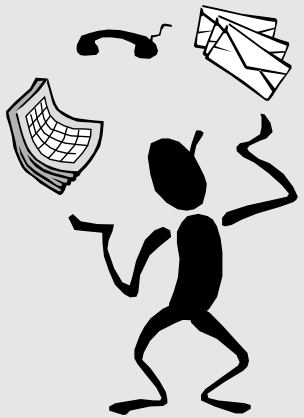
Servicios de Seguridad

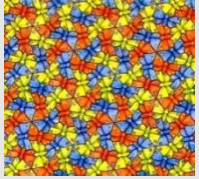


Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México

Servicios de Seguridad

- Confidencialidad
- Autenticación
- Identificación
- Integridad
- No-repudio
- Control de acceso
- Disponibilidad





Servicios de Seguridad (1/2)

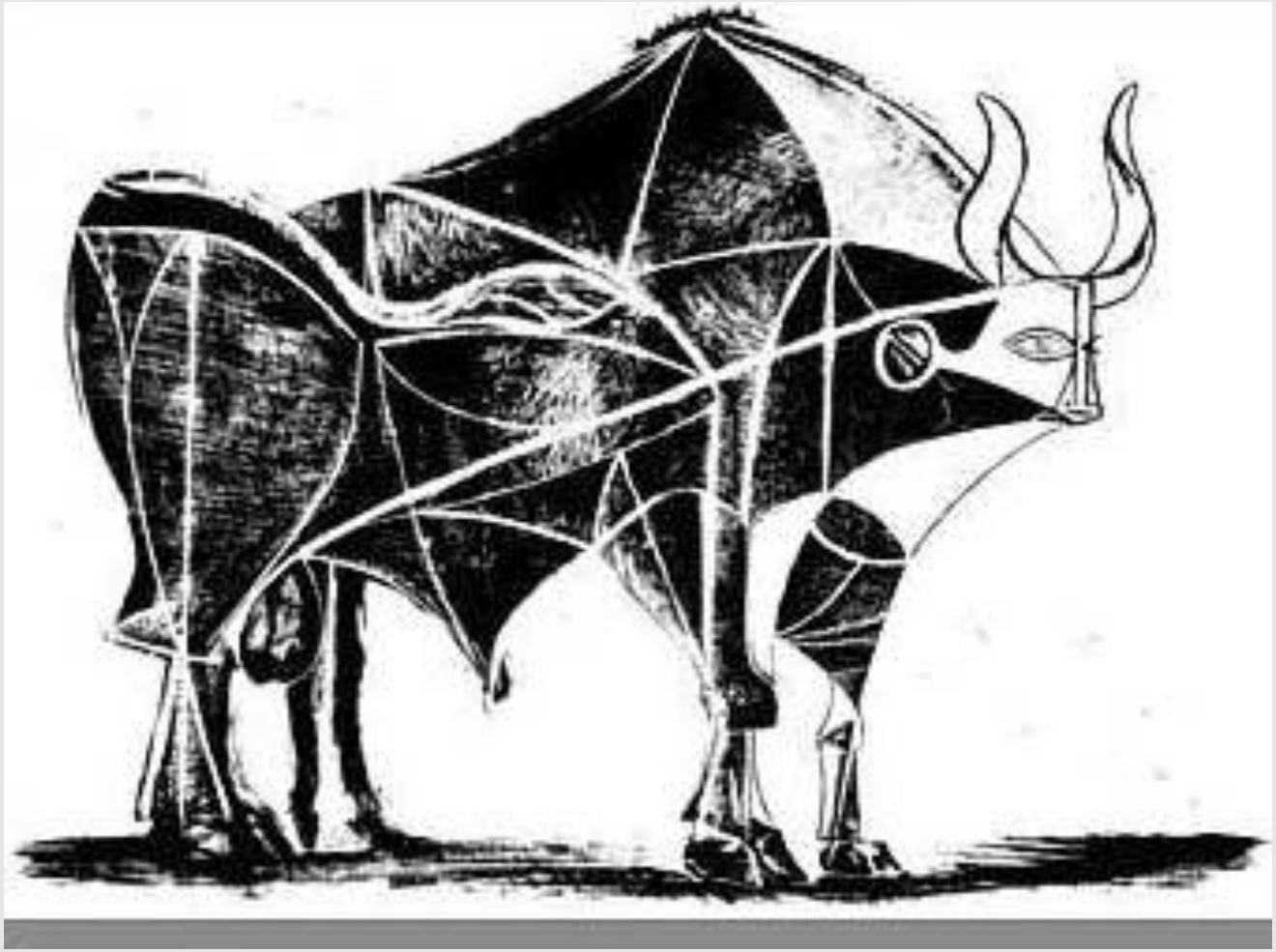
1. *Confidencialidad*. La confidencialidad asegura que la información sensible sólo podrá ser consultada o manipulada por usuarios, entidades o procesos autorizados.
2. *Integridad*. La integridad da la certeza de que la información no ha sido modificada por entidades no autorizadas para hacerlo.

Servicios de Seguridad (2/2)

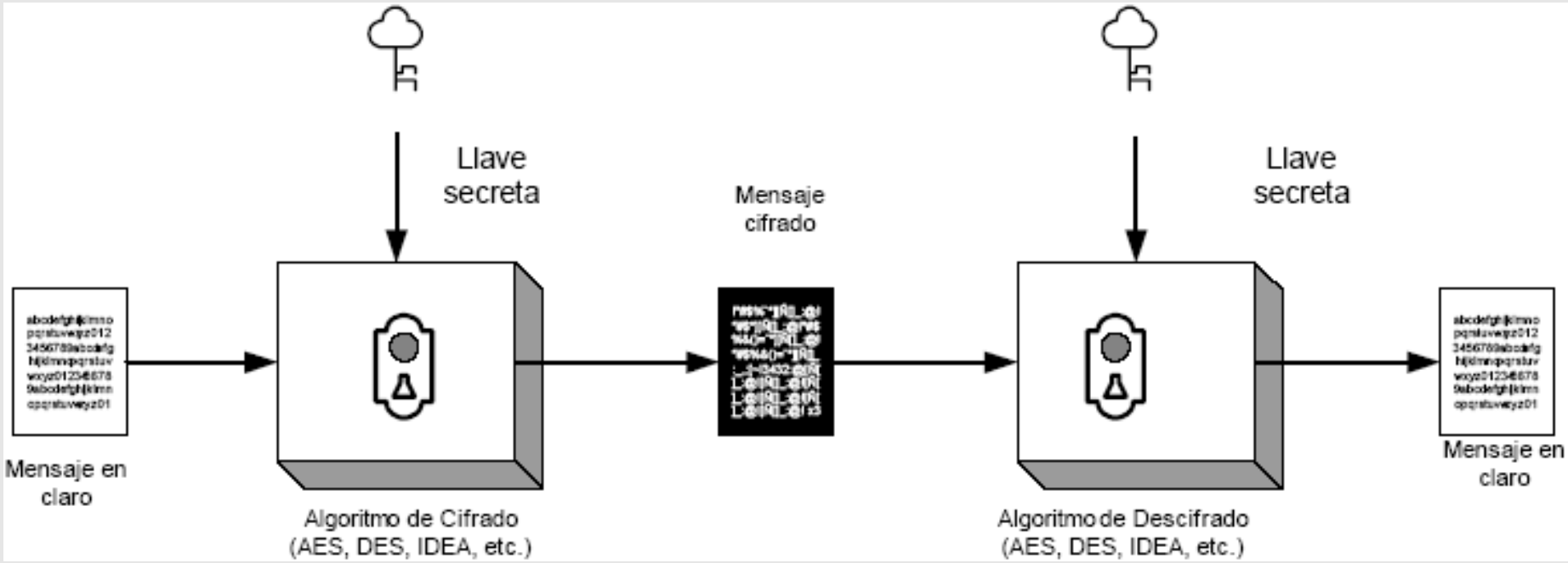
3. *Autenticación*. La autenticación asegura que la identidad de los participantes es verdadera.

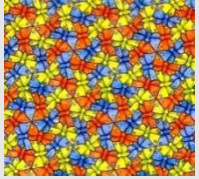
4. *No repudio*. El no repudio ofrece protección a un usuario o entidad frente a la situación en la cual otro usuario niega que cierta transacción alguna vez ocurrió.

Bloques Básicos



Modelo simplificado de Cifrado simétrico





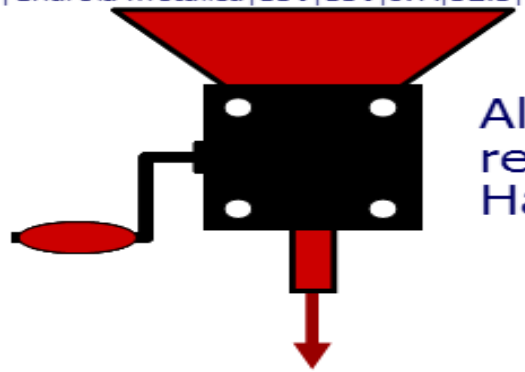
Criptografía Simétrica

- Algoritmos altamente eficientes. Ambas partes convienen en compartir el mismo secreto
- Desventajas: un problema importante es la distribución de las llaves. En un sistema con *n* usuarios se necesita generar *n*(*n*-1)/2 llaves.
- La administración de llaves también tiende a ser problemática
- Algoritmos utilizados:
  - DES - 56 bit key
  - 3DES usa tres llaves DES
  - IDEA 128 bits
  - AES fue escogido como el nuevo estándar de cifrado en el 2000.

Esquema convencional de una función picadillo

Cadena Original

||A|1|2005-09-02T16:30:00|1|ISP900909Q88|Industrias del Sur Poniente, S.A. de C.V.|Alvaro Obregón|37|3|Col. Roma Norte|México|Cuauhtémoc|Distrito Federal|México|06700|Pino Suarez|23|Centro|Monterrey|Monterrey|NuevoLéon|México|95460|CAUR390312S87|Rosa María Calderó|Uriegas|Topochico|52|Jardines del Valle|Monterrey|Monterrey|Nuevo León|México|95465|10|Caja|Vasos decorados|20|200|1|pieza|Charola metálica|150|150|IVA|52.5||

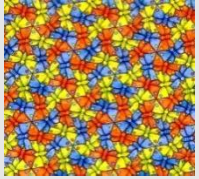


Algoritmo de resumen o Hash

8a a2 b6 17
94 44 27 35
36 97 e6 94
a2 e3 5a 07

Resumen o Hashing

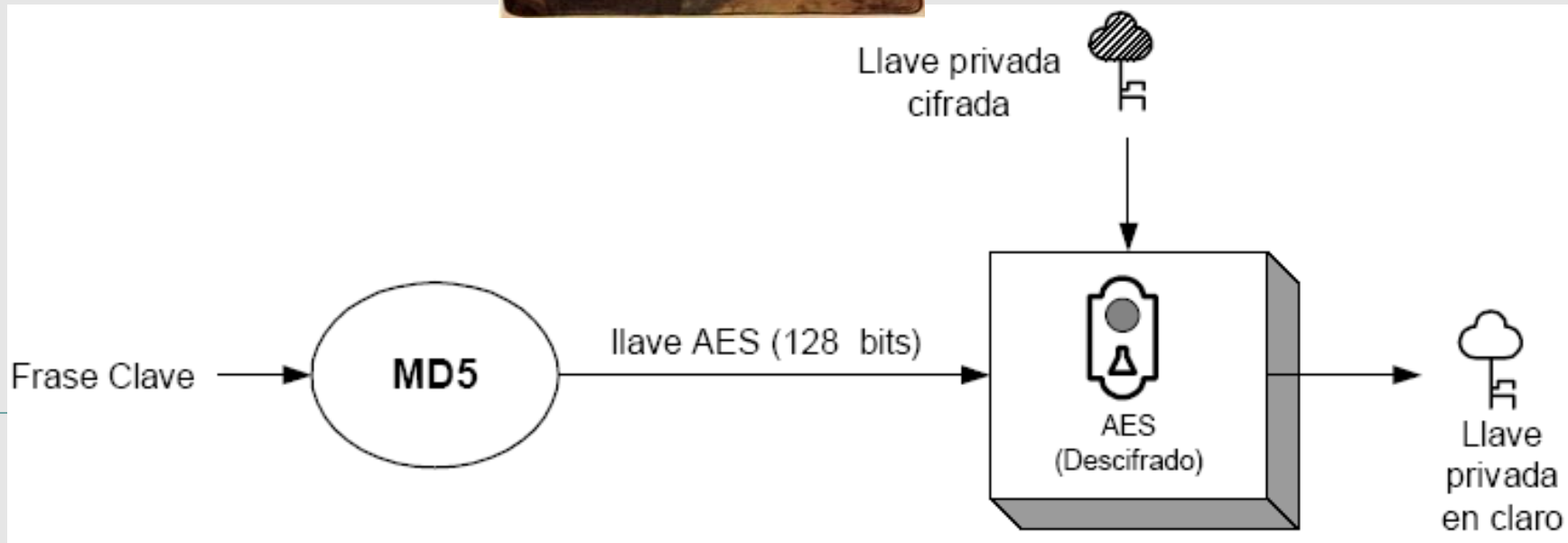
Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México



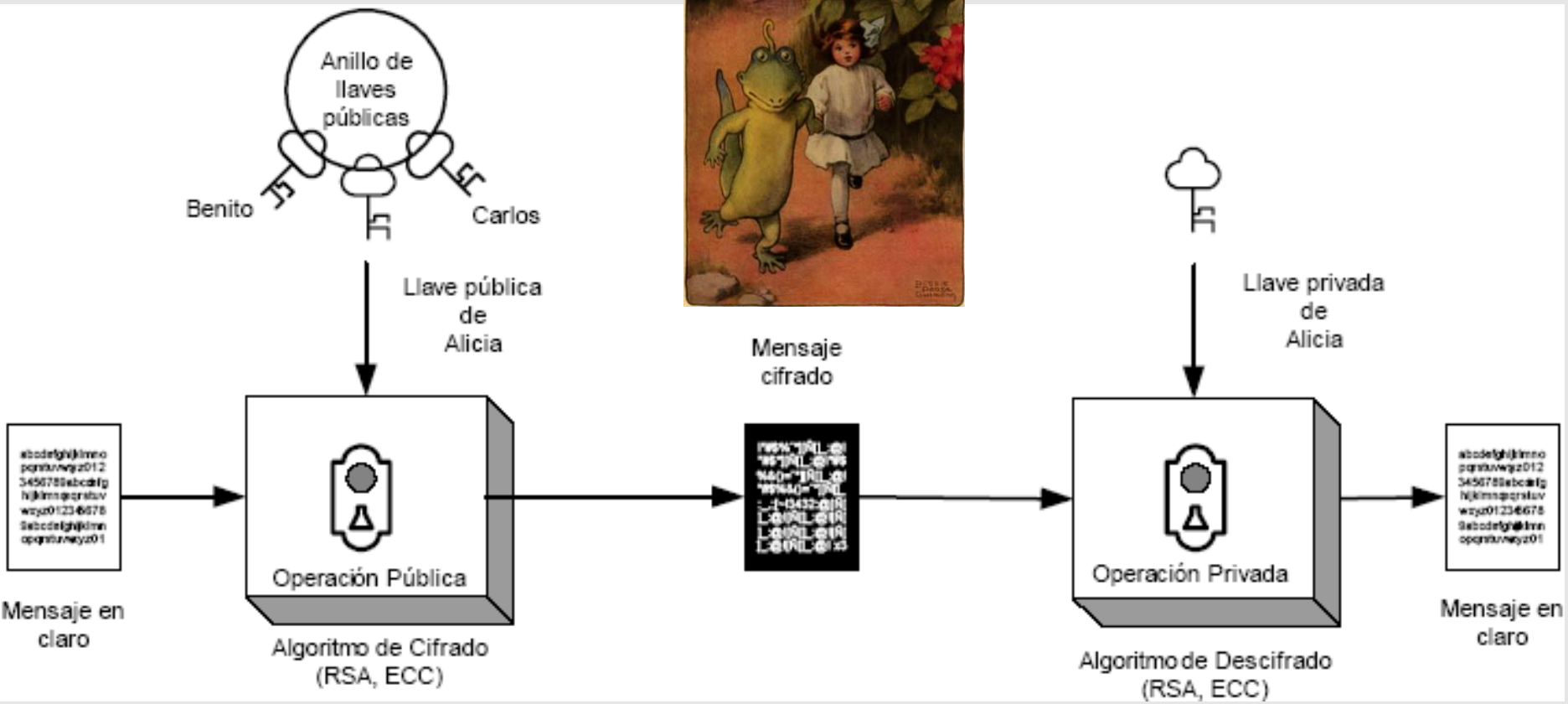
Funciones picadillo

- Usadas para
  - Producir huellas digitales de longitud fija para documentos de longitud arbitraria
  - Producir información útil para detectar modificaciones maliciosas
  - Traducir contraseñas a salidas de longitud fija.

Obtención de llave privada

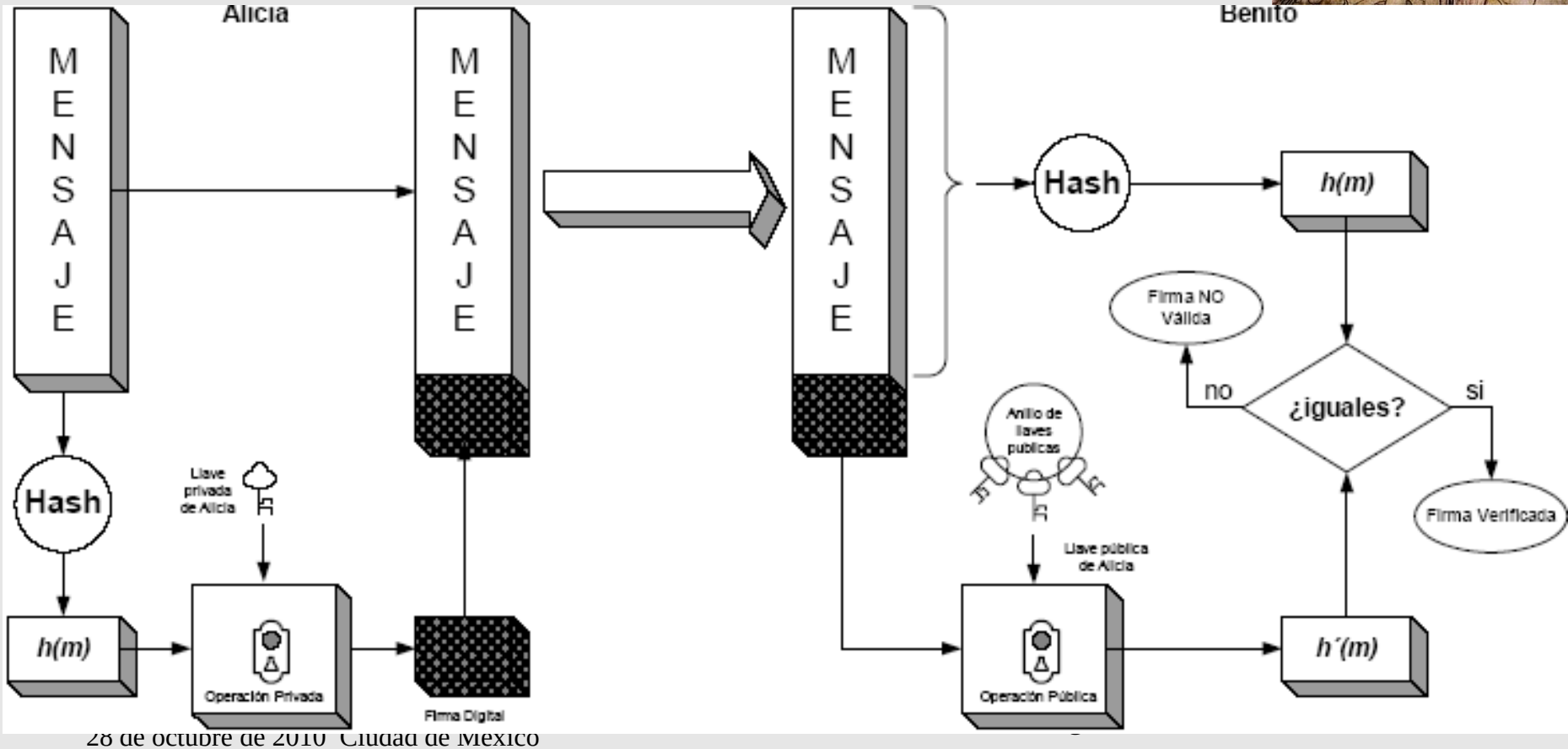


Criptografía de llave pública: confidencialidad

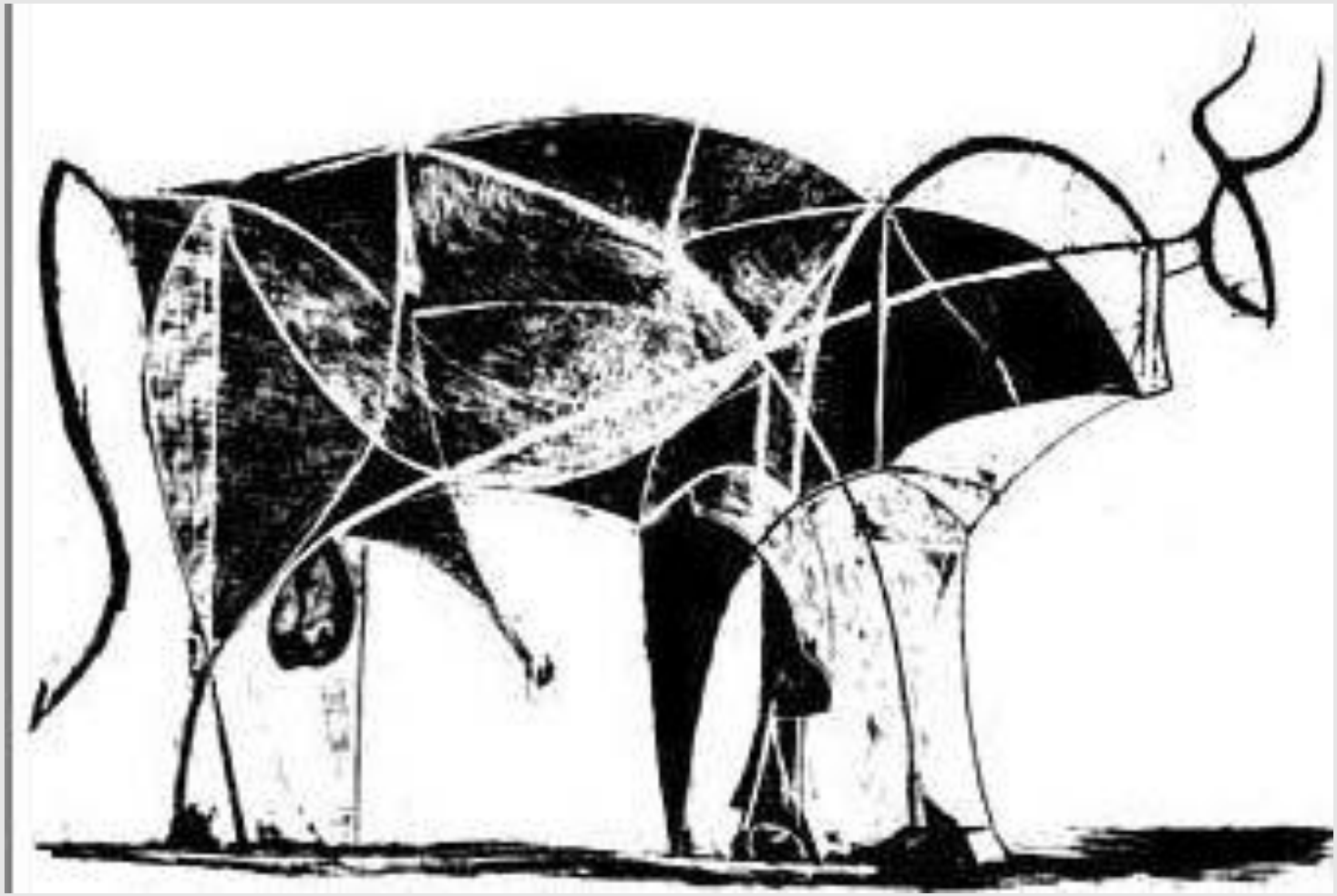


Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México

Criptografía de llave pública: Firma Digital



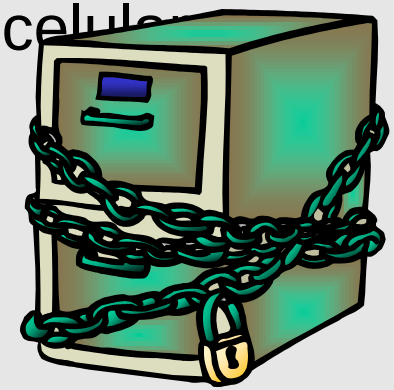
Aplicaciones y Servicios



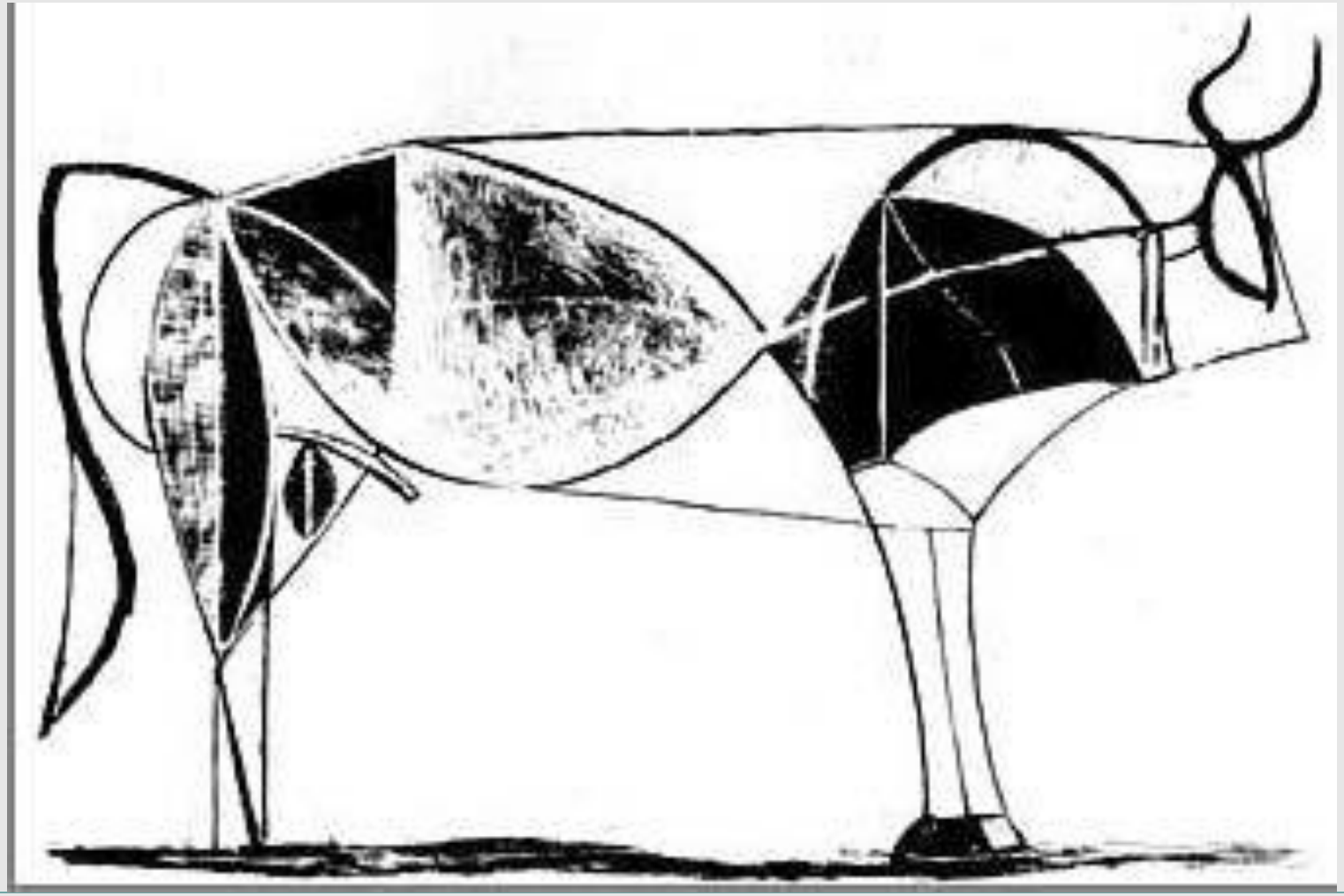
Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México

Aplicaciones de seguridad informática mexicana

- Comprobantes digitales fiscales
- elecciones electrónicas
- Urnas electrónicas
- Programa de Resultados Electorales Preliminares del IFE
- base de datos de usuarios en telefonía celular
- distribución de datos
- notaría digital

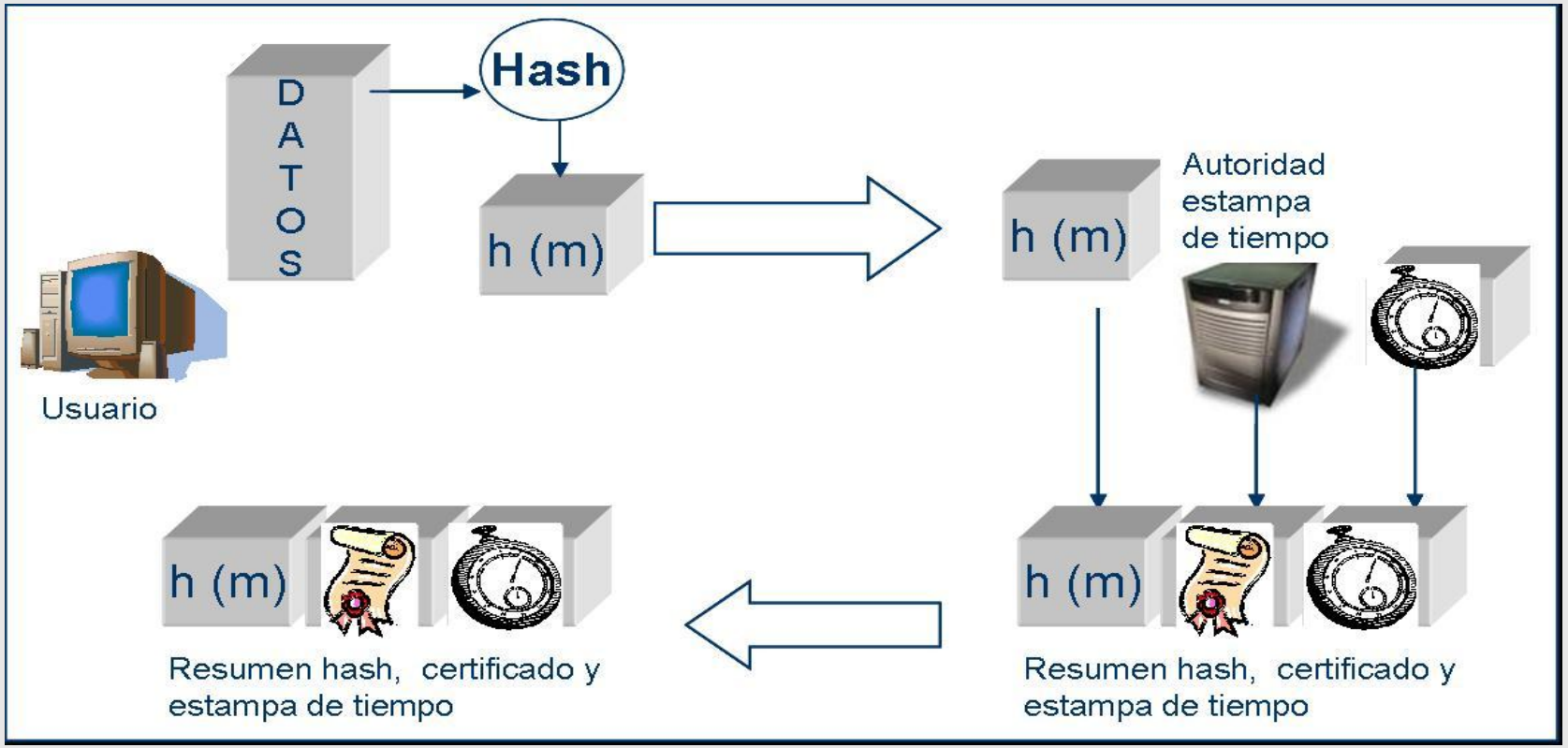


Notaría digital y almacenamiento seguro

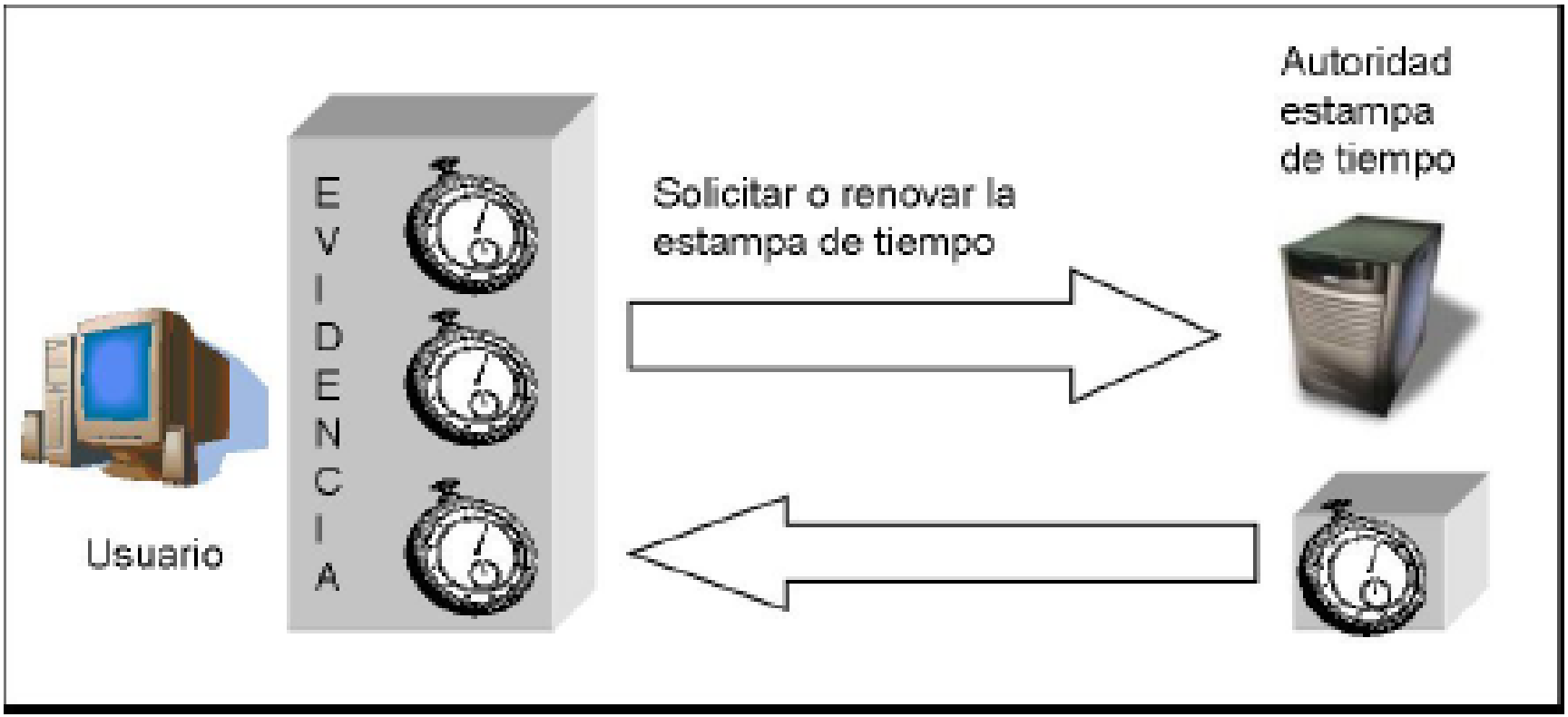


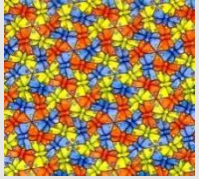
Notaría Digital

Estampa de tiempo



Notaría Digital





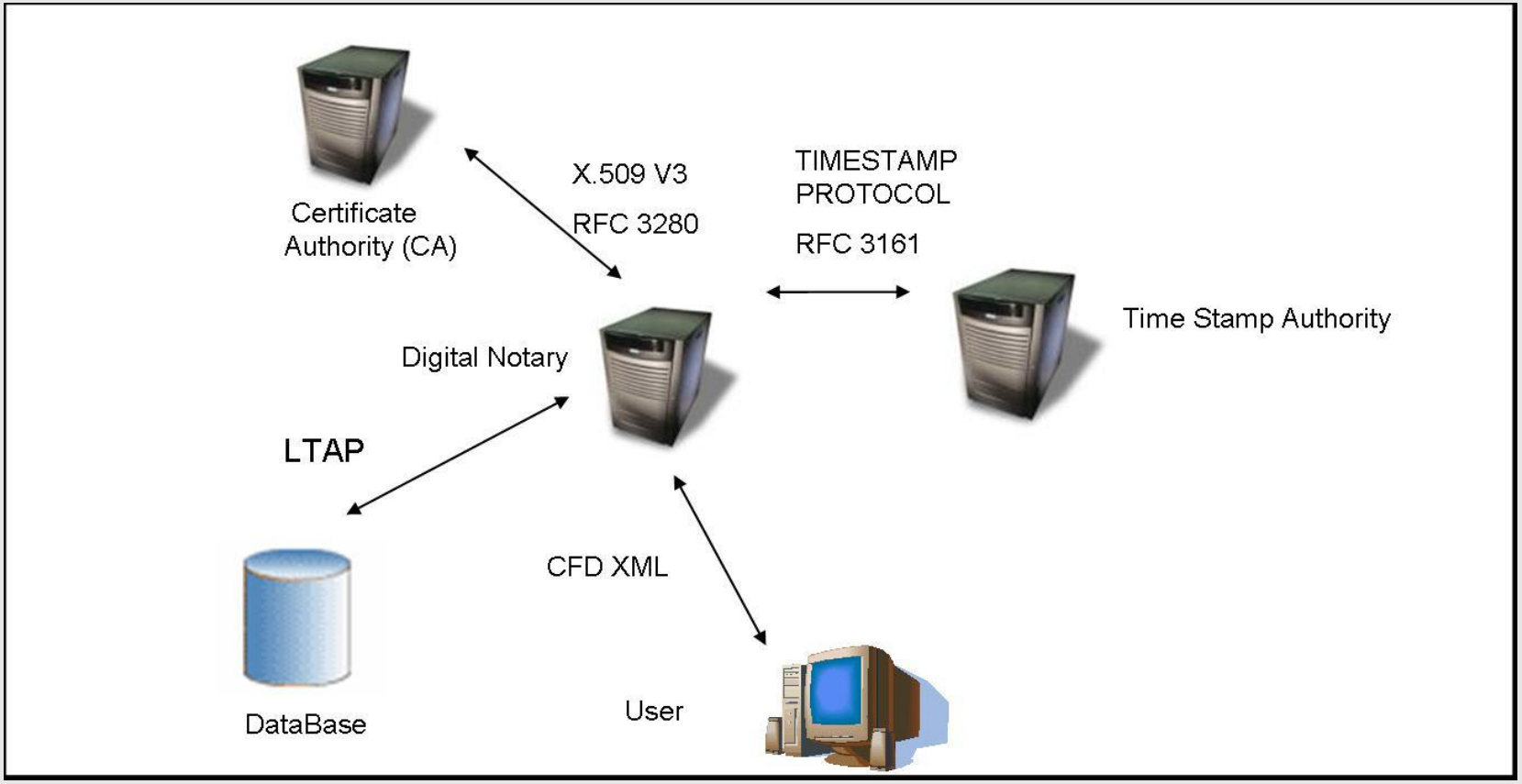
Notaría Digital

Servicios de protocolo *Long Term Archive Notary Service* (LTANS)

- ALMACENAMIENTO
- ESTADO
- VERIFICACIÓN
- EXPORTACIÓN
- BORRADO

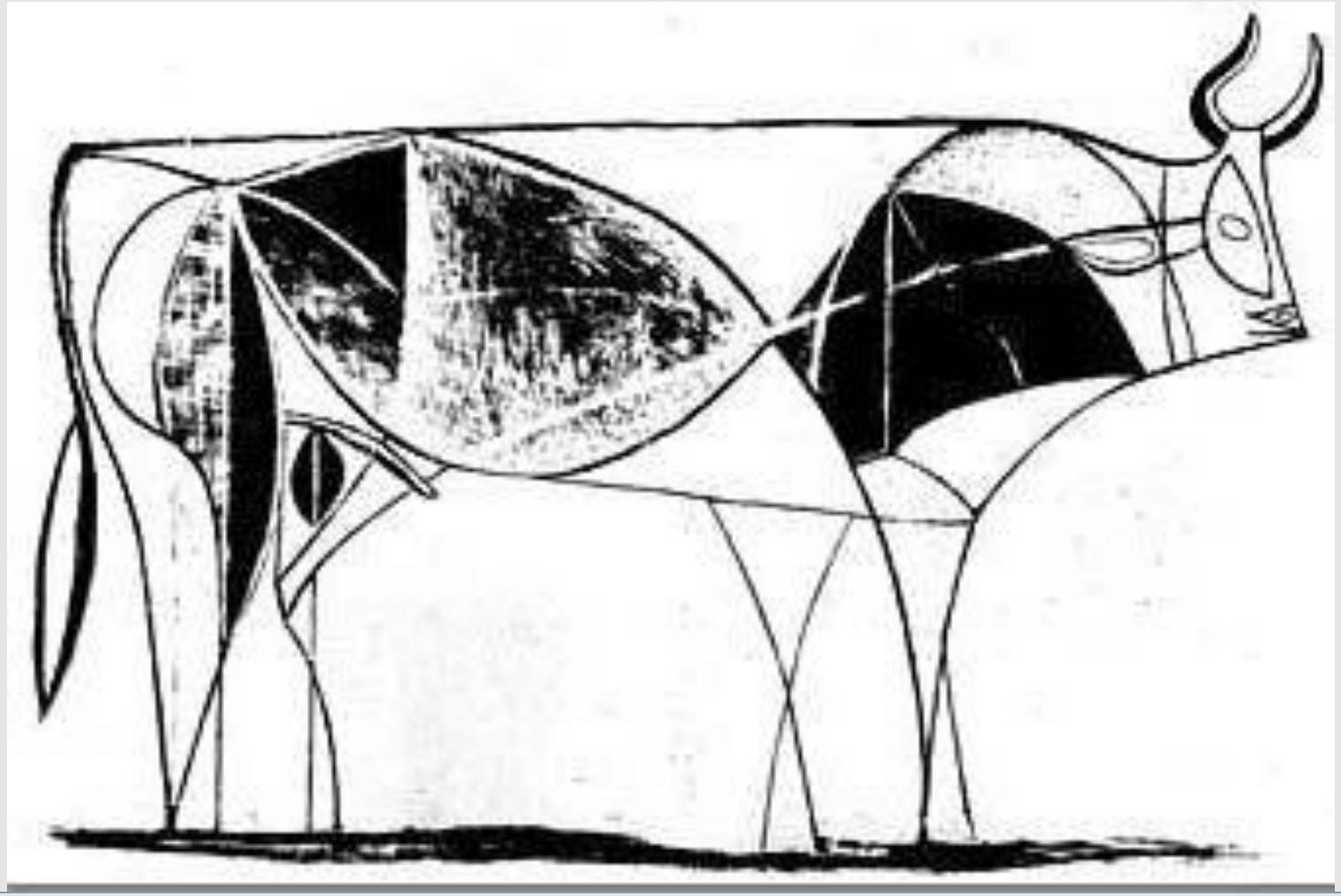
Notaría Digital

Arquitectura de **Notaría Digital**



Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México

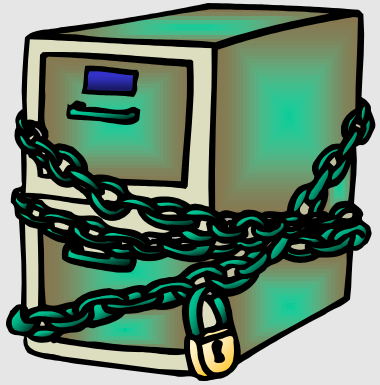
Factura Electrónica

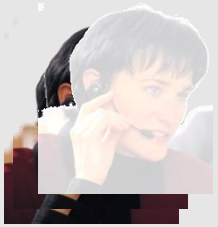


Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México

Factura Electrónica

- Escenarios
  - Notario Electrónico
  - Factura Electrónica
- Objetivos
  - Comprobar que los documentos son copias legítimas de los originales
  - Autenticación de las partes involucradas
- Herramientas
  - Criptografía de llave pública
  - Certificados Digitales
  - Autoridades Certificadoras





CATE

1 El contribuyente pide <u>cita</u> al centro de Atención Telefónica Externo *(01 800) 849 93 70*

2 Se le asigna cita al contribuyente

Administración Local

<u>Contribuyente</u>
- Acude a cita
- Entrega documentos
- Entrega archivo .req

El contribuyente Acude a cita **4**

<u>ALAC</u>
- Revisa documentos
- Genera certificado de firma electrónica avanzada

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

SAT.GOB.MX

5 Obtiene certificado de firma electrónica avanzada

CICLO DE GENERACIÓN

Seguridad

- Los estándares de Seguridad empleados en la Firma Electrónica Avanzada y el Comprobante Fiscal Digital están basadas en la tecnología de Llaves Publicas.

- Llaves de 1024 bits RSA (Llave Privada y Publica)
  - Se estima que se requieren de más de 70 años con las computadoras más potentes y un presupuesto de mas de 100 millones de dólares para poder 'quebrar' este algoritmo.
  - Los certificados de Firma Electrónica Avanzada y de Sellos Digitales tienen una validez de 2 años lo cual elimina la posibilidad de que alguien quiebre esta llave.
- Encriptación 3 DES (Encriptación de Seguridad en la Llave Privada)
  - Si con un hardware especial se pudiera desencriptar algo encriptado con DES en 1 segundo, se requerirían 2,285 billones de años para 'quebrar' un encriptamiento con Triple DES con el mismo hardware.
  - Se requirieron 22 horas y 100,000 computadoras para 'quebrar' el algoritmo DES en su ultima prueba.

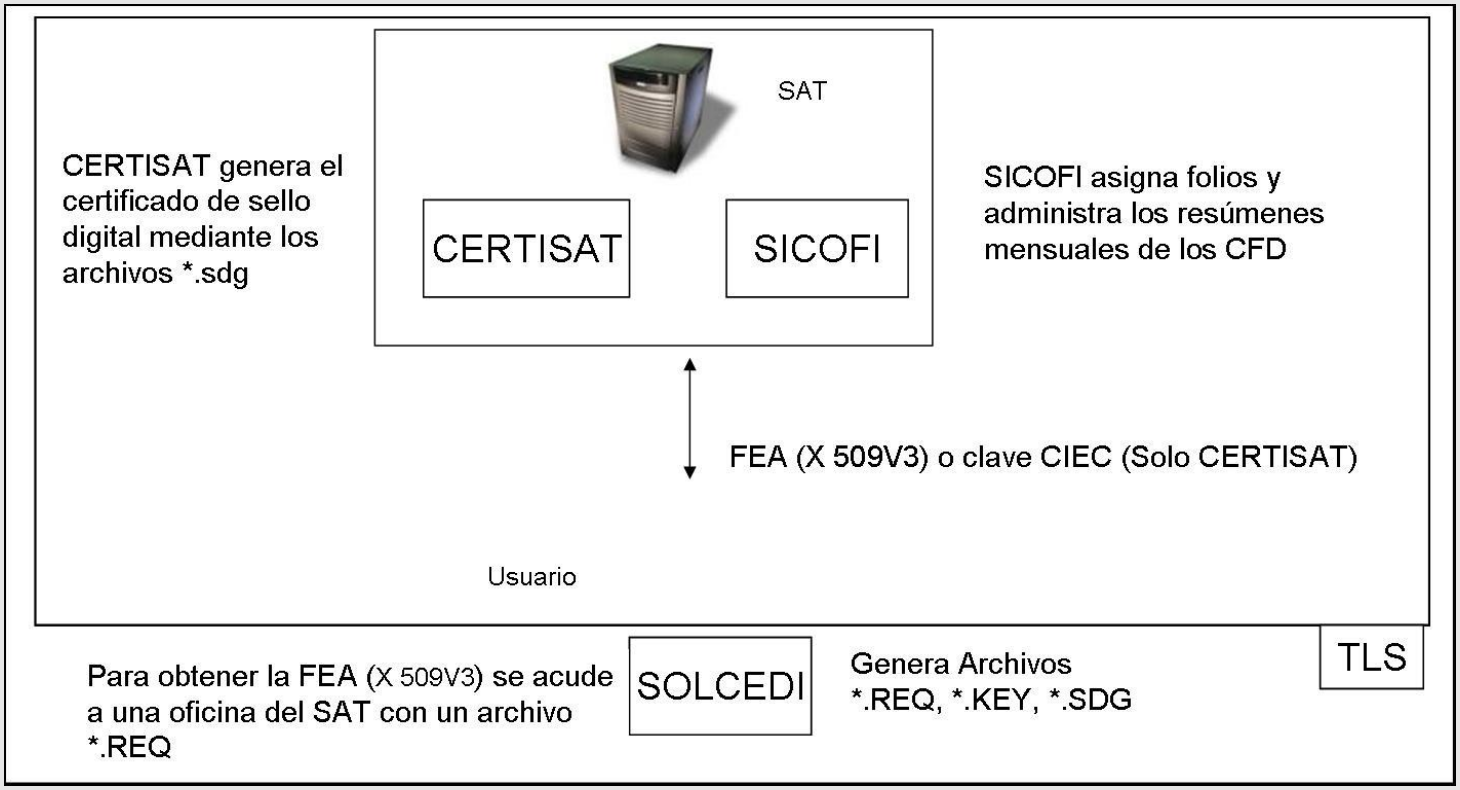
*** Number 13 - April 2000* - Bulletin**
A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths
Robert D. Silverman, RSA Laboratories

**** Data Encryption Standard" FIPS 46**
Extracting a 3DES key from an IBM 4758
***** FIPS 180-1 / 180-2**

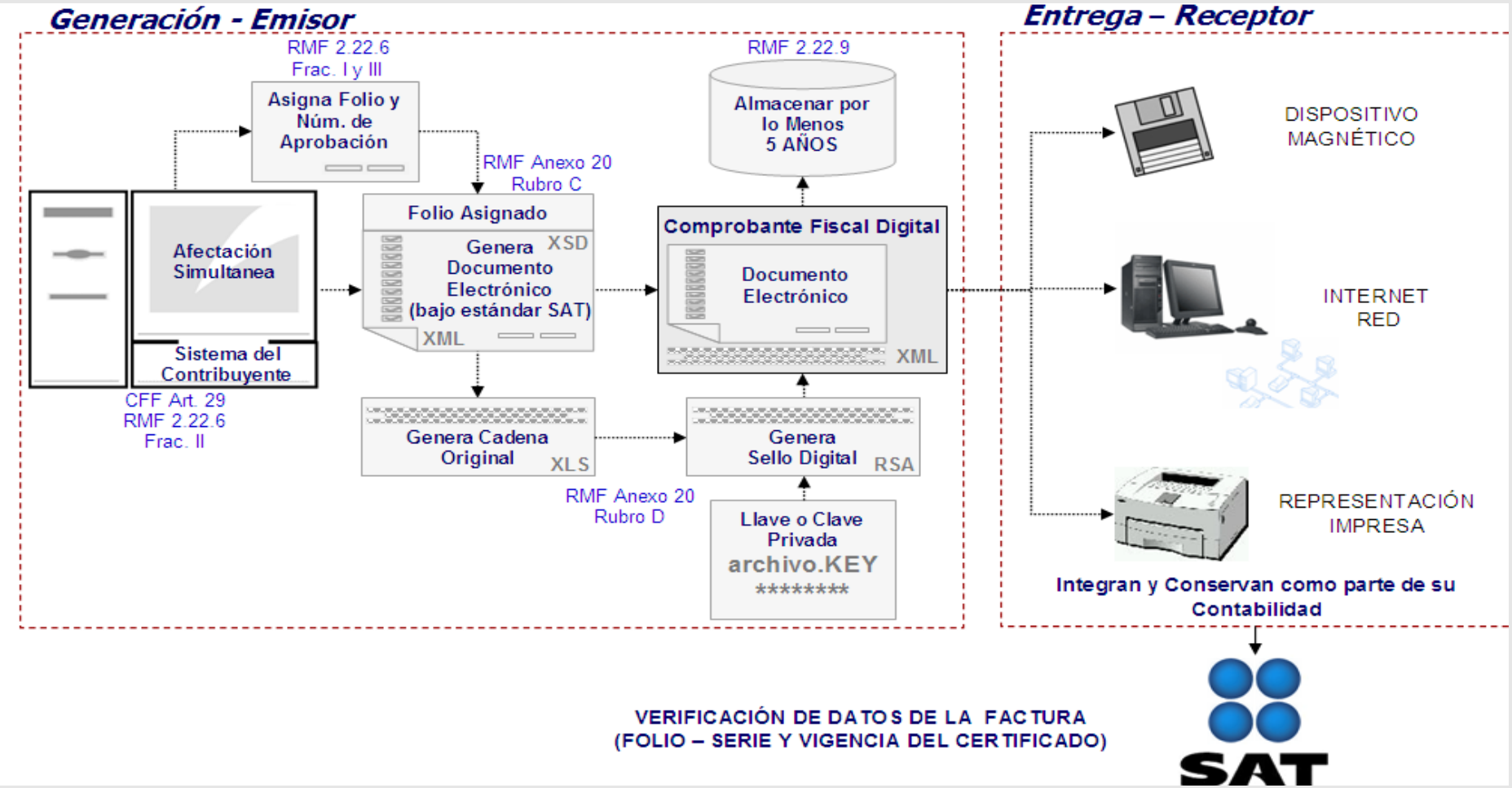
Aplicaciones de muy alto impacto y muy alto

Comprobantes Fiscales Digitales del SAT

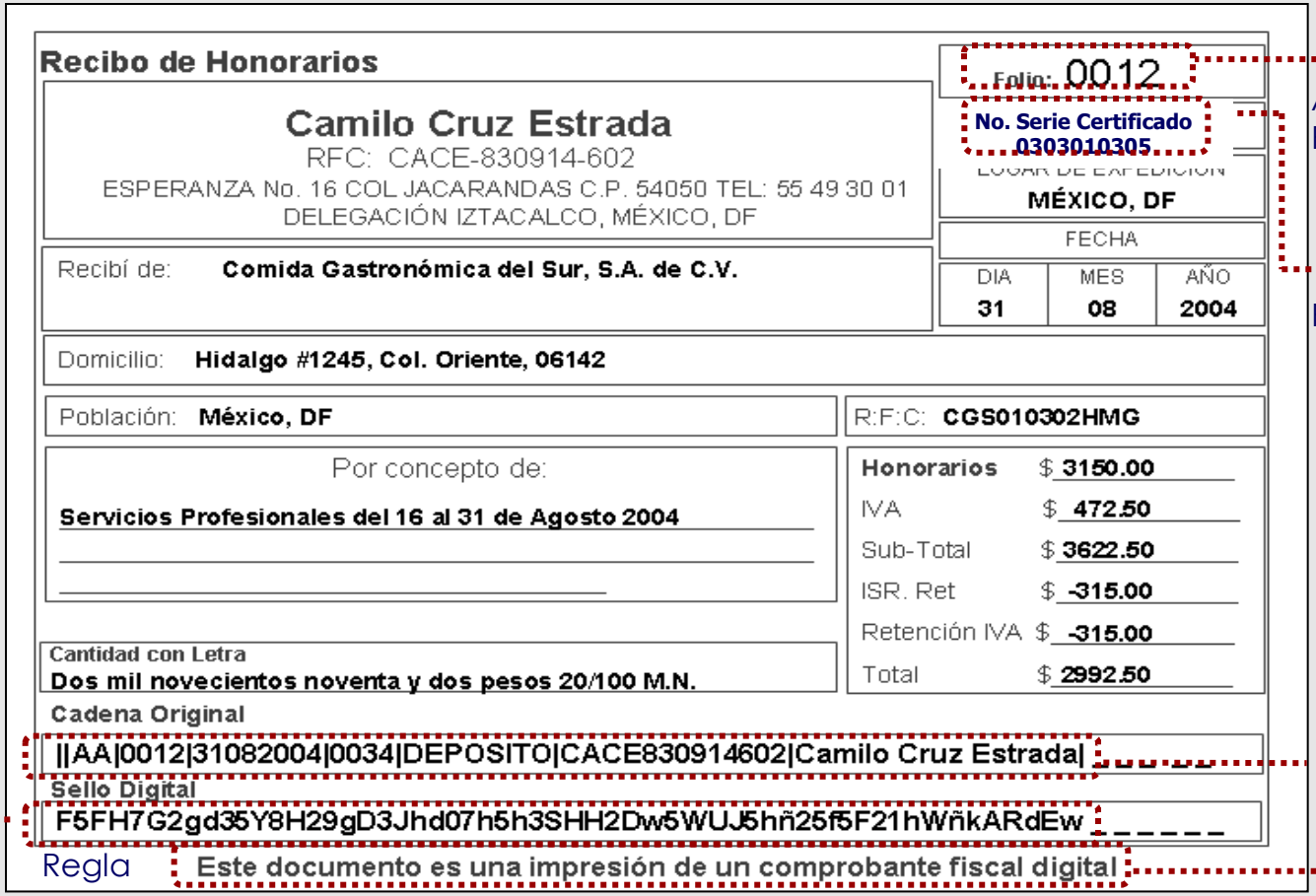
Sistema de Comprobantes Fiscales Digitales del SAT



Comprobantes Fiscales Digitales del SAT



Comprobantes Fiscales Digitales del SAT



Recibo de Honorarios

Folio: 0012

No. Serie Certificado 0303010305

Camilo Cruz Estrada
RFC: CACE-830914-602
ESPERANZA No. 16 COL JACARANDAS C.P. 54050 TEL: 55 49 30 01
DELEGACIÓN IZTACALCO, MÉXICO, DF

LUGAR DE EXPEDICION
MÉXICO, DF

Recibí de: **Comida Gastronómica del Sur, S.A. de C.V.**

FECHA

DIA	MES	AÑO
31	08	2004

Domicilio: **Hidalgo #1245, Col. Oriente, 06142**

Población: **México, DF**

R.F.C: **CGS010302HMG**

Por concepto de:
Servicios Profesionales del 16 al 31 de Agosto 2004

Honorarios	$ **3150.00**
IVA	$ **472.50**
Sub-Total	$ **3622.50**
ISR. Ret	$ **-315.00**
Retención IVA	$ **-315.00**
Total	$ **2992.50**

Cantidad con Letra
Dos mil novecientos noventa y dos pesos 20/100 M.N.

Cadena Original

||AA|0012|31082004|0034|DEPOSITO|CACE830914602|Camilo Cruz Estrada|

Sello Digital

F5FH7G2gd35Y8H29gD3Jhd07h5h3SHH2Dw5WUJ5hñ25f5F21hWñkARdEw

Este documento es una impresión de un comprobante fiscal digital

Folio
Art. 29 fracción III, Regla 2.22.8.

Regla 2.22.8.

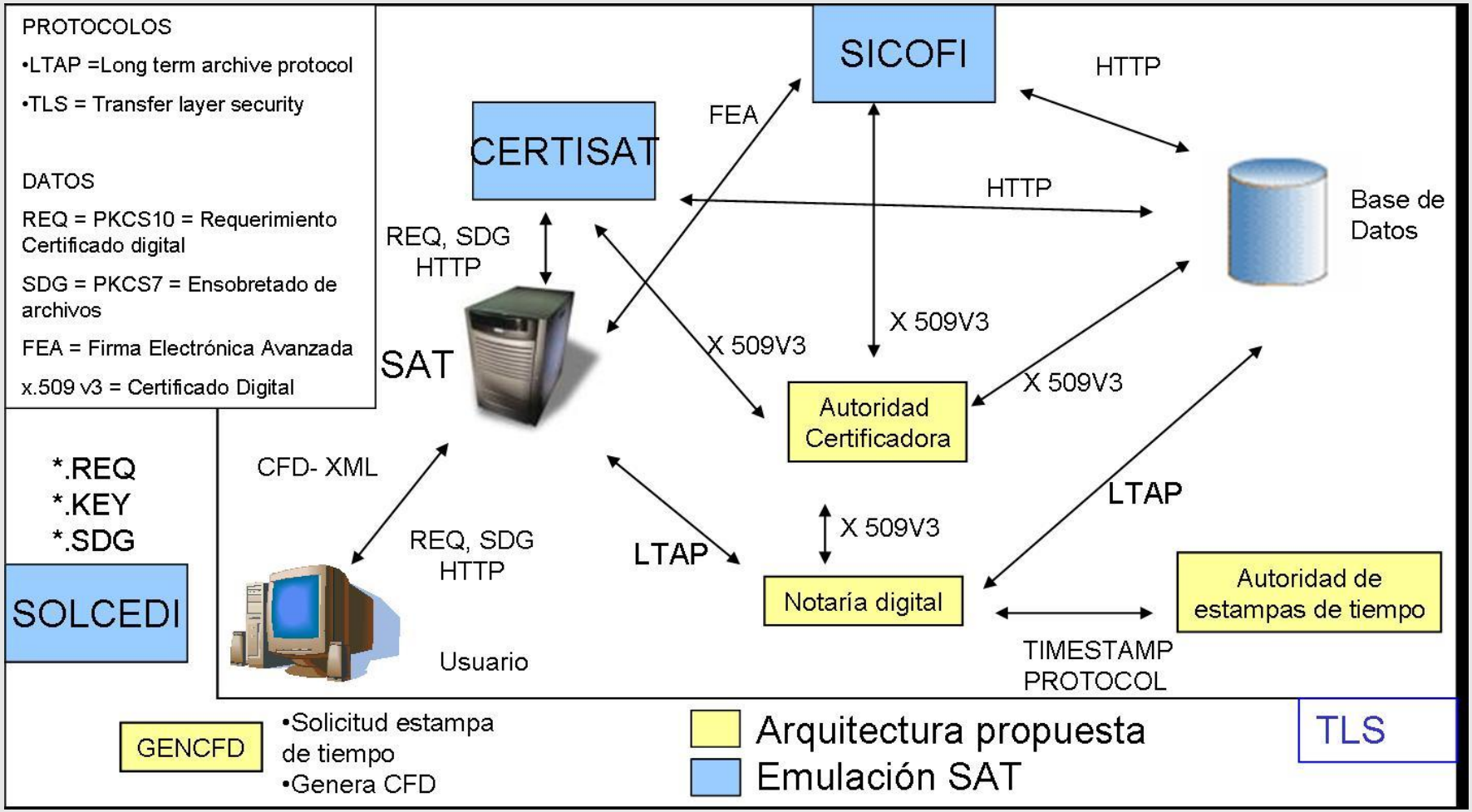
Regla 2.22.8.

ello digital
t. 29 fracción I, 22.8.

Regla

Leyenda

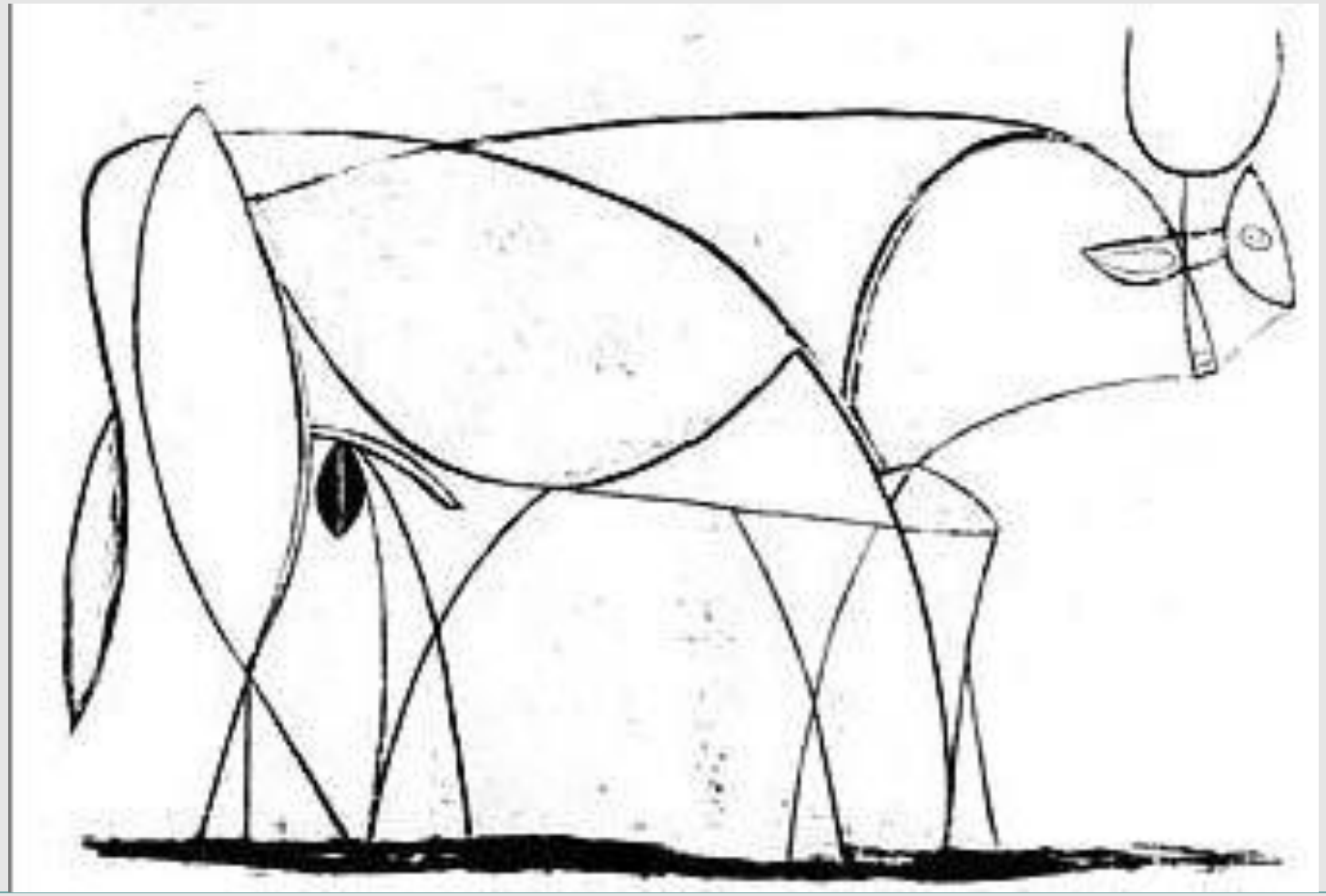
Notaría digital integrada con el Sistema del SAT [González-García'07]



Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México

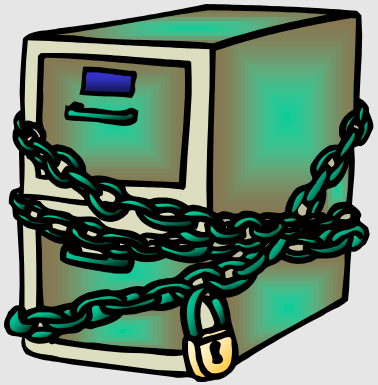
Notaría digital integrada con el Sistema del SAT [González-García'07]

elecciones electrónicas seguras



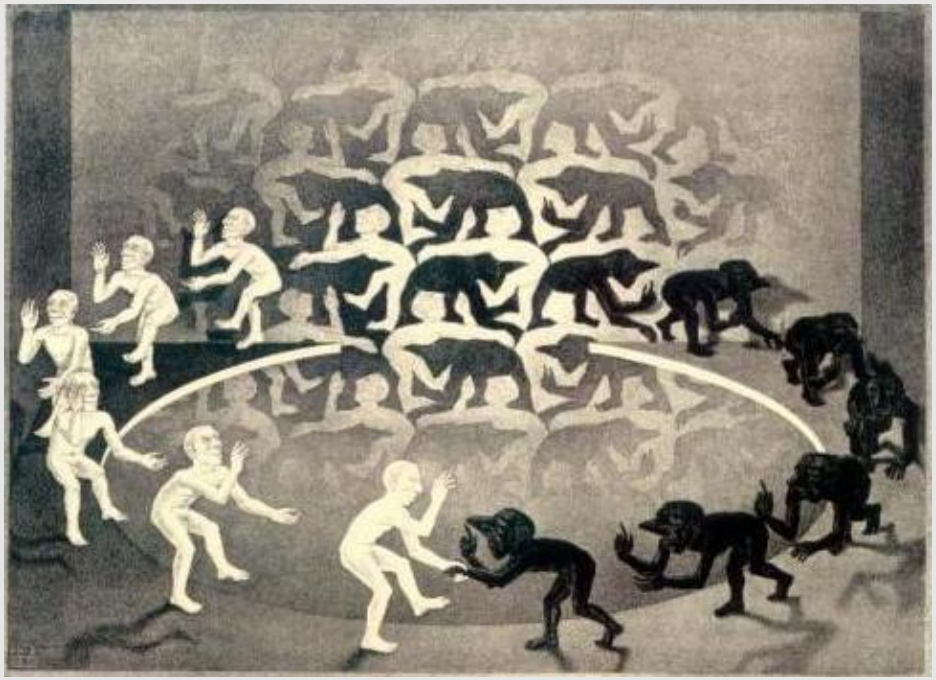
Elecciones Electrónicas

- Escenarios
  - Elecciones generales
  - Reuniones de accionistas
  - Computación distribuida segura
- Objetivos
  - anonimato
  - Sistema justo
  - Sistema auditable
- Herramientas
  - Algoritmo RSA
  - Firmas a ciegas
  - Protocolos seguros no rastreables



Elecciones y Urnas Electrónicas

- El Instituto Electoral del Distrito Federal (IEDF) aprobó el uso de urnas electrónicas para la recepción y cómputo de votos en el proceso electoral local ordinario 2008-2009.



Antecedentes y motivación

Mediante el uso de elecciones electrónicas en medios inalámbricos, se puede obtener:

- Mayor comodidad Se podrá votar desde cualquier lugar que cuente con acceso a la red correspondiente (Intranet ó Internet).
- Privacidad física Las personas podrán emitir su voto sin necesidad de ser vistas por los demás votantes o personal administrativo.
- Mayor participación Debido a los puntos anteriores y a que el uso de dispositivos inalámbricos aumenta cada día.

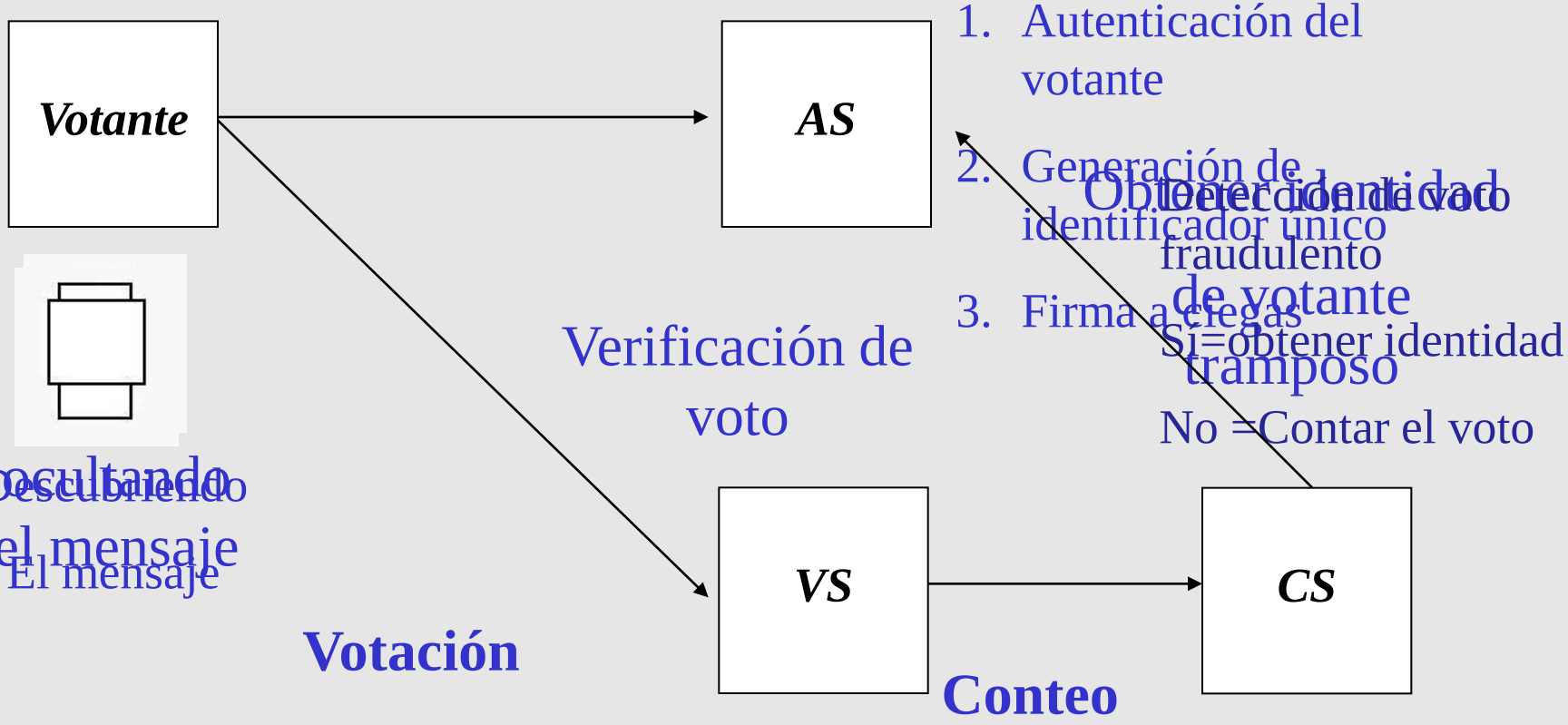
Antecedentes y motivación

- ***Firma digital*** Es un conjunto o bloque de caracteres que viaja junto a un documento, fichero o mensaje, y que garantiza autenticidad, integridad y no-repudio. Esquemas principales: DSA, ECDSA, ElGamal, RSA.

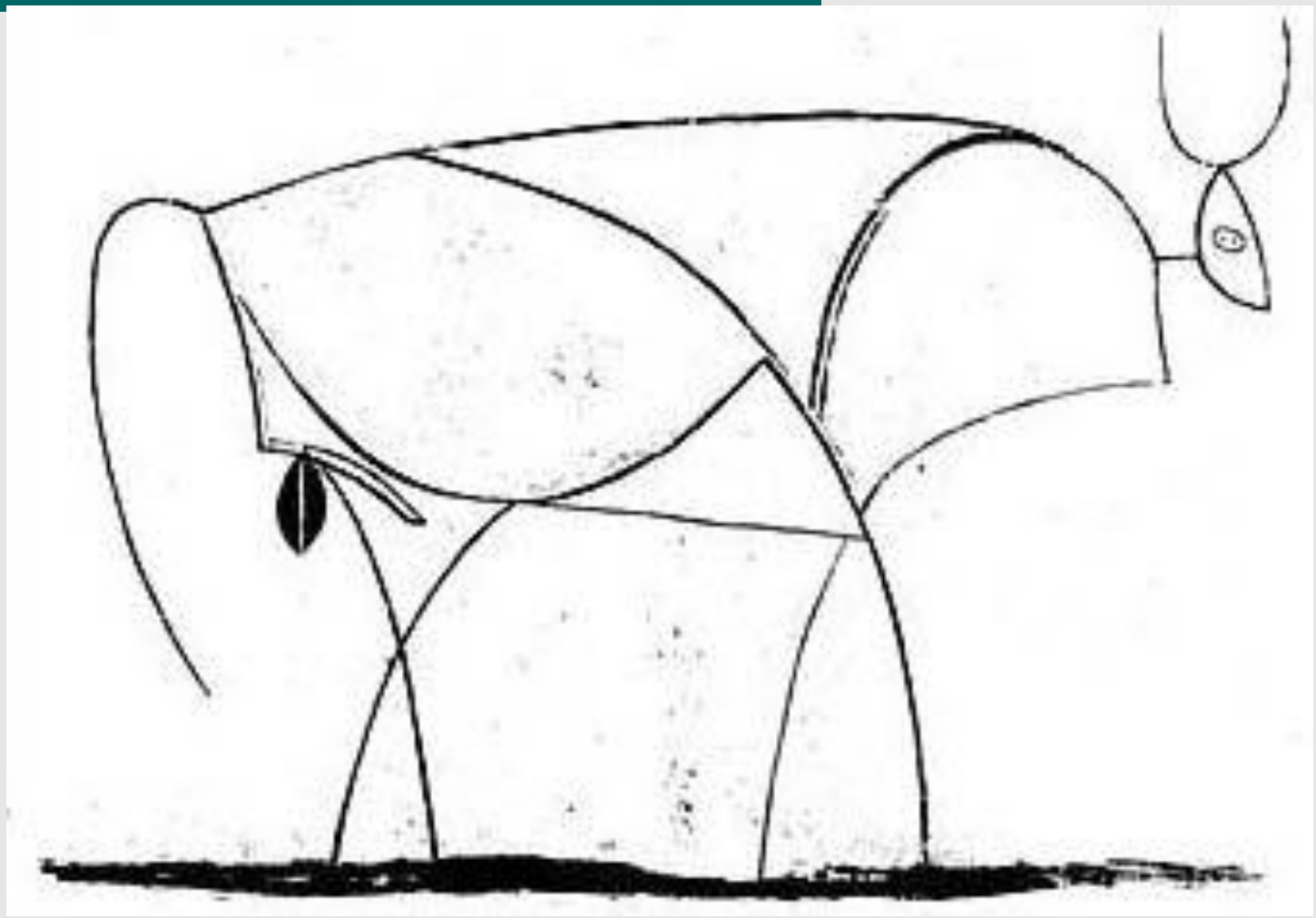
- ***Firma a ciegas*** Un tipo especial de firmas digitales, en las que se firma algo que no se conoce. Las firmas a ciegas son indispensables para implementar un sistema de elecciones electrónicas.

Ejemplo de esquema de elecciones electrónicas [López-García et al. '08]

Esquema de votación



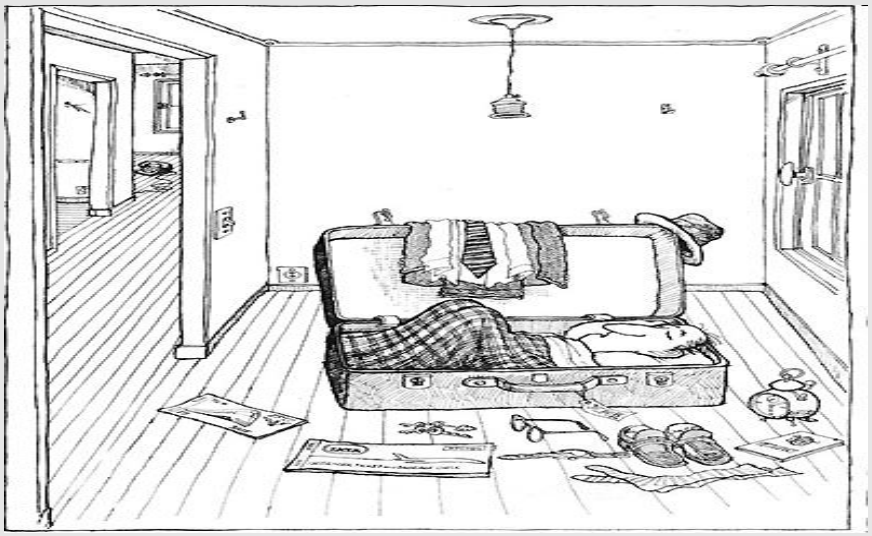
Otras Aplicaciones



Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México

Registro Nacional de Usuarios de Telefonía Móvil en México

- Creación del Registro Nacional de Usuarios de Telefonía Móvil (RNUTM)
- Se estima que hay más de ochenta millones de usuarios de teléfonos celulares en México y se especula que en tres años más, esa cifra podría alcanzar los cien millones de usuarios



Primera Escuela
Información y los

28 de octubre de

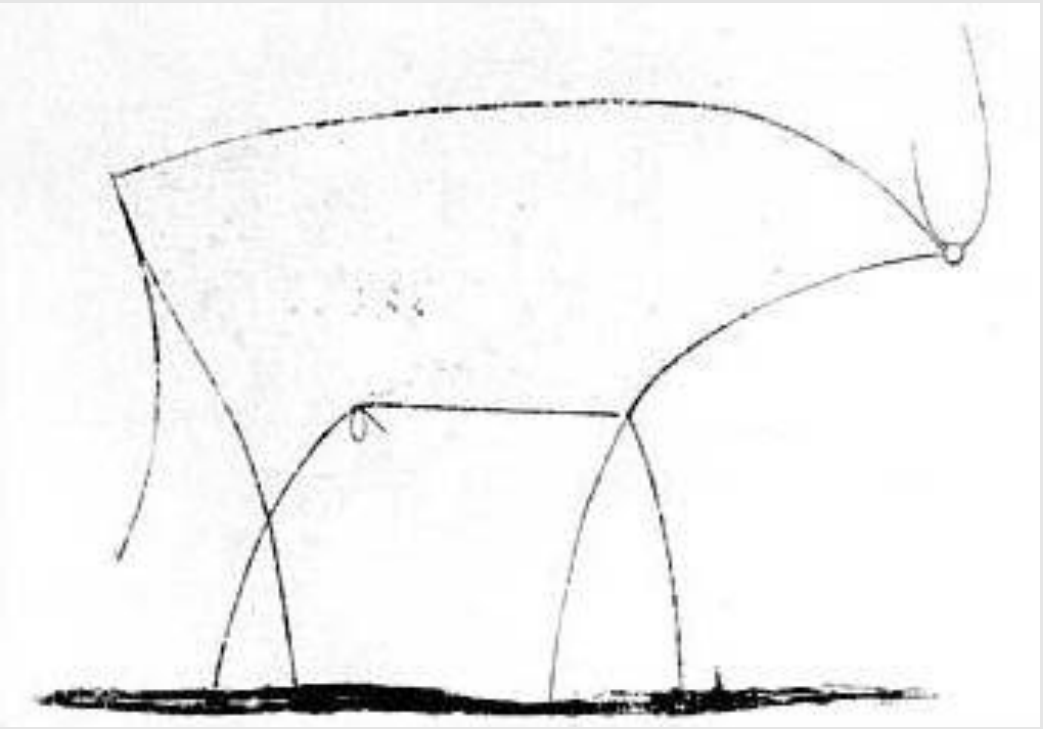
y alto
México

Jurisdicción y legislación

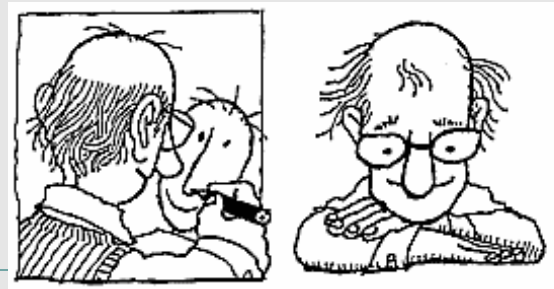
- La jurisdicción y legislación en México con respecto a delitos cibernéticos tiene todavía un largo camino por andar
- Existen lagunas jurídicas en la gran mayoría de las aplicaciones descritas en esta presentación

Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México

La última lámina es para decir…



¡Gracias!



Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México