

GESTIÓN ELECTRÓNICA DE DOCUMENTOS CURSO 2006-2007



T. 4. Los documentos electrónicos y su gestión

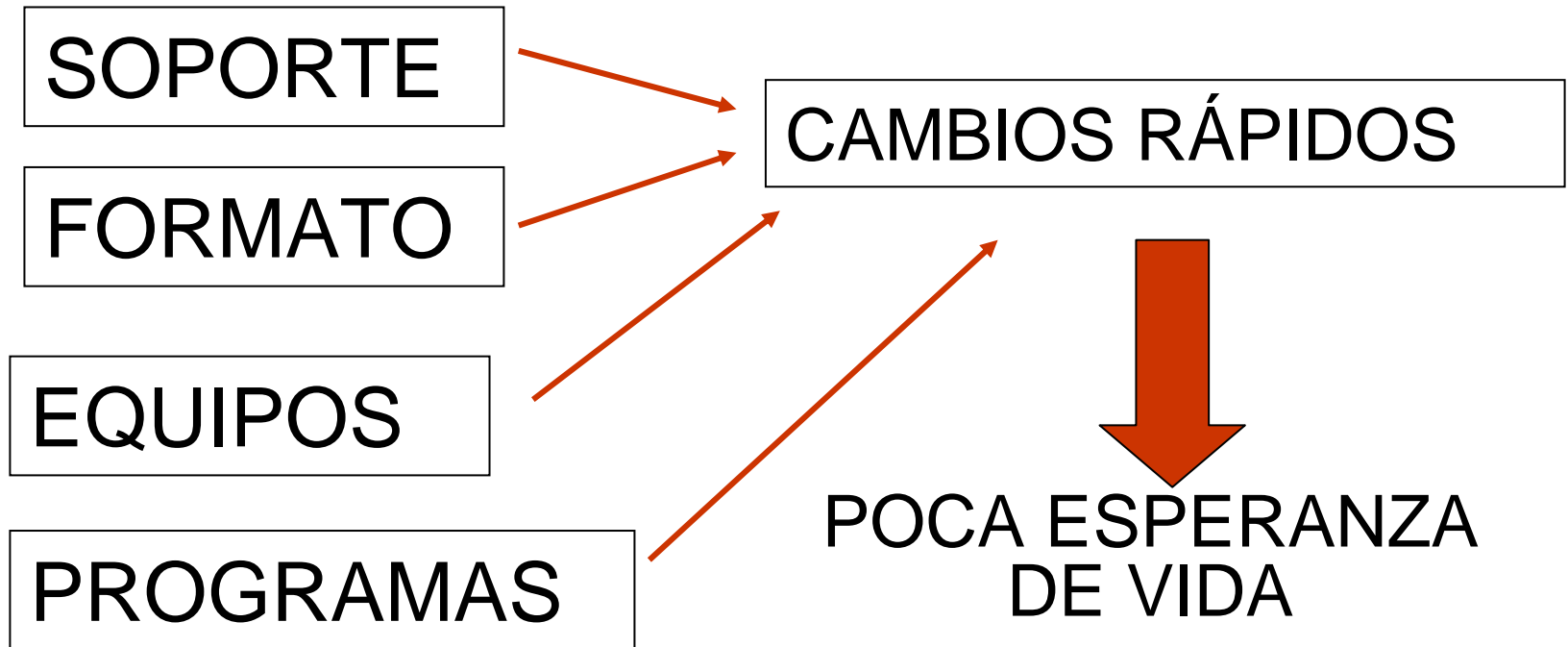
T.4 LOS DOCUMENTOS ELECTRÓNICOS Y SU GESTIÓN

Bibliografía

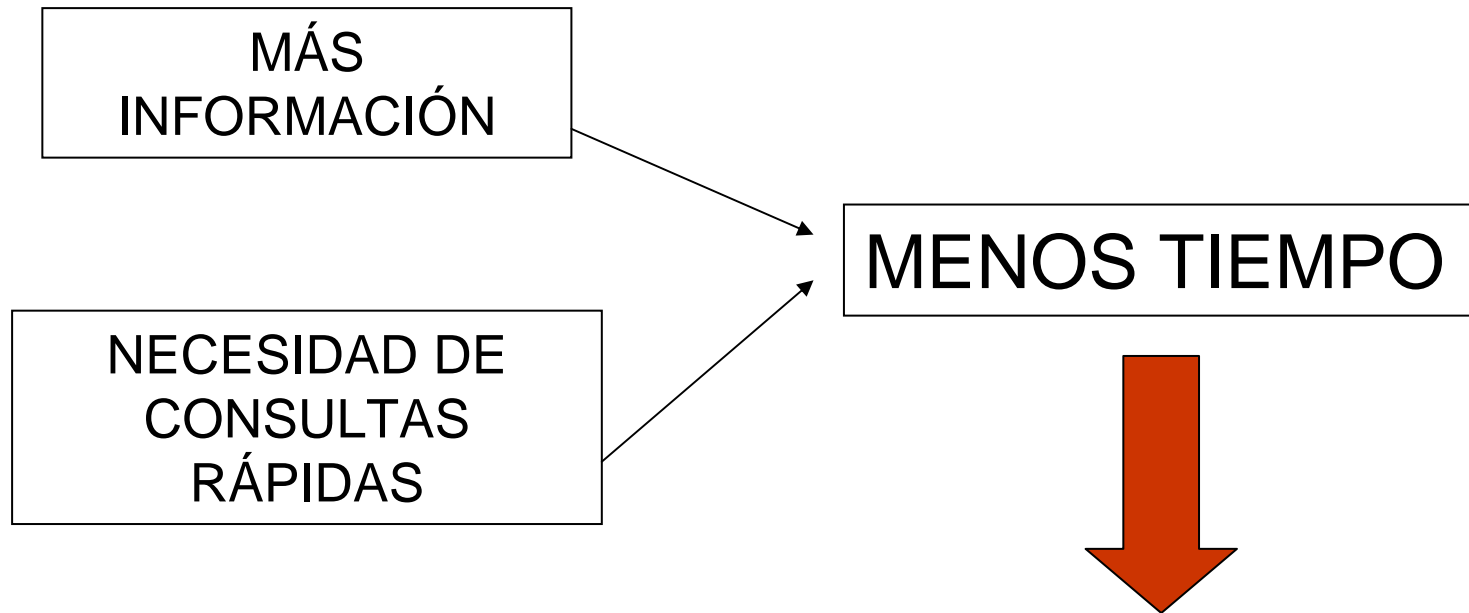
1. Introducción
2. El documento electrónico de archivo
3. Los metadatos
4. La gestión de los documentos electrónicos



1. Introducción



1. Introducción



¿CÓMO HACEMOS ESTO?



2. El documento electrónico de archivo

▣ RD 263/1996

- Medios electrónicos → fax
- Medios telemáticos → correo electrónico
- Medios informáticos → factura electrónica

▣ Ley 59/2003

- Los redactados en soporte electrónico y que contengan firma electrónica



2. El documento electrónico de archivo

▣ Ley 11/2007

- *Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico, según un formato determinado y susceptible de identificación y tratamiento diferenciado.*



2. El documento electrónico de archivo

Documento electrónico archivístico

Documento generado o producido por cualquier persona o entidad en el desarrollo de la gestión de sus intereses o como prueba de sus actividades

“ha sido creado, o puede ser manipulado, transmitido o tratado por un **ordenador**”

Grupo Foris en su artículo “Los documentos electrónicos y los archivos”. Boletín ACAL . n. 35 (2000) p.5-8.



2. El documento electrónico de archivo

Propio de los
doc de archivo

Documento electrónico

Específico de
los
doc.
electrónicos

Aquel documento que es producido, recibido o reunido por una persona física o jurídica de modo **involuntario, natural y espontáneo** en el transcurso y como apoyo de sus actividades, de la que es testimonio, haciendo **uso de la electrónica**, que se **conserva y transmite** también mediante los medios electrónicos, en depósitos de conservación permanente, tras efectuar una **selección** a partir de la identificación y valoración de las series, con medidas de **autenticación** y **preservación** adecuadas y con una **organización** respetuosa con su modo de producción, con el fin de **garantizar su valor** informativo, legal y cultural, así como de permitir su **acceso** y uso también mediante las tecnologías de la información.



2. El documento electrónico de archivo

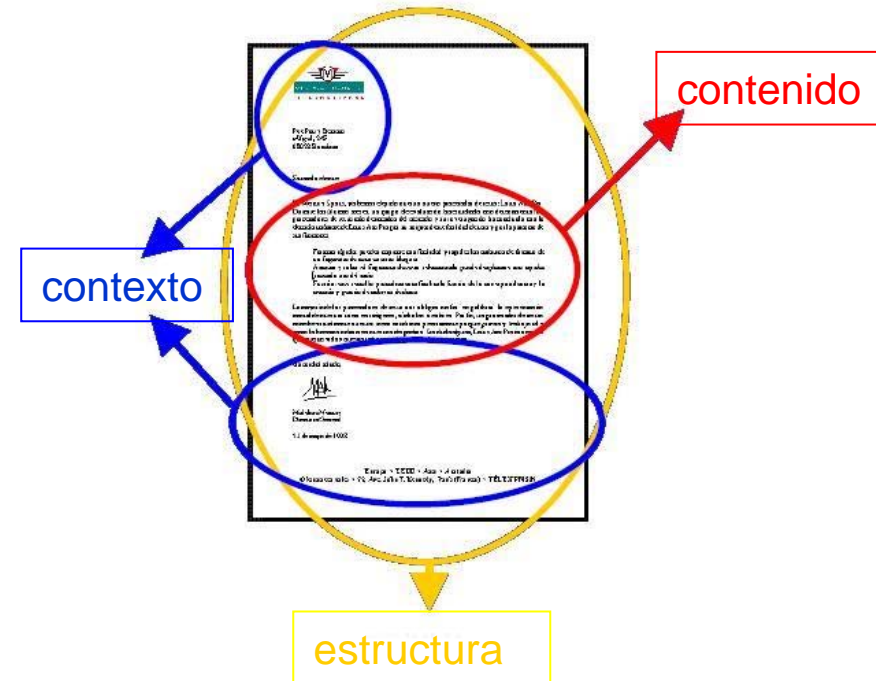
- ▣ Creado, transmitido y mantenido por medios magnéticos
- ▣ Grabado en código binario



2. El documento electrónico de archivo

Documento electrónico

“información registrada, producida, recibida en torno a la implantación, realización y ámbito de una actividad institucional o personal que engloba el **contenido**, **contexto** y **estructura** y permite probar la existencia de la actividad que lo generó”.



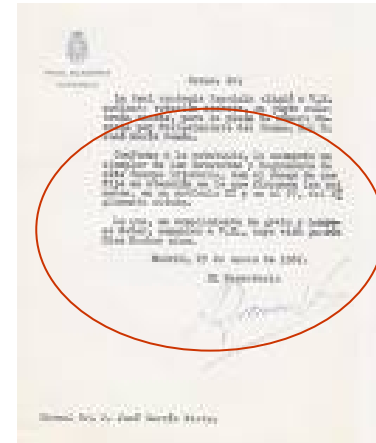
[Definición del CIA]



2.1. El documento electrónico y sus partes

CONTENIDO = DATOS

- Textuales (páginas, párrafos, palabras)
- Numéricos
- Gráficos
- Sonoros
- Enlaces hipertexto



A screenshot of a web form titled 'JUNTA DE AVALUACIÓN'. The form contains various fields for data entry, including checkboxes, text boxes, and tables. A red circle highlights a specific section of the form, which appears to be a table or a list of items. The form is in Spanish and is likely used for administrative or evaluation purposes.



2.1. El documento electrónico y sus partes

Estructura

“forma en la está registrado el documento, lo que incluye la utilización de signos, diseño, formato, soporte”

Guide for Managing Electronic Record from an Archival perspective



2.1. El documento electrónico y sus partes

- Estructura física
- Estructura lógica

Imprimir Rectabolear Salir

JUNTA DE ANDALUCÍA CONSEJERÍA DE EMPLEO

CONSEJO REGULADOR DE LA TEMPORALIDAD

ANEXO 1

SOLICITUD DE RESERVA

☐ TEMPORALIDAD RESERVA ☐ RESERVA DE TEMPORALIDAD

1. DATOS DE LA SOLICITANTE

Nombre: _____ Apellido: _____

DNI: _____

Dirección: _____

2. ACOMPAÑANTES

Nº	Nombre	Apellido	DNI	Relación
1				
2				
3				
4				

3. TIPO DE TEMPORALIDAD

☐ TEMPORALIDAD RESERVA ☐ RESERVA DE TEMPORALIDAD

4. RESERVA

Reserva de: ☐ RESERVA DE TEMPORALIDAD ☐ RESERVA DE RESERVA

5. RESERVA

Reserva de: ☐ RESERVA DE TEMPORALIDAD ☐ RESERVA DE RESERVA

6. DECLARACIÓN, AUTENTICACIÓN, FIRMA Y SELLO

DECLARACIÓN

Yo, _____, declaro que soy titular de la reserva de temporalidad de la Junta de Andalucía.

AUTENTICACIÓN

Yo, _____, declaro que soy titular de la reserva de temporalidad de la Junta de Andalucía.

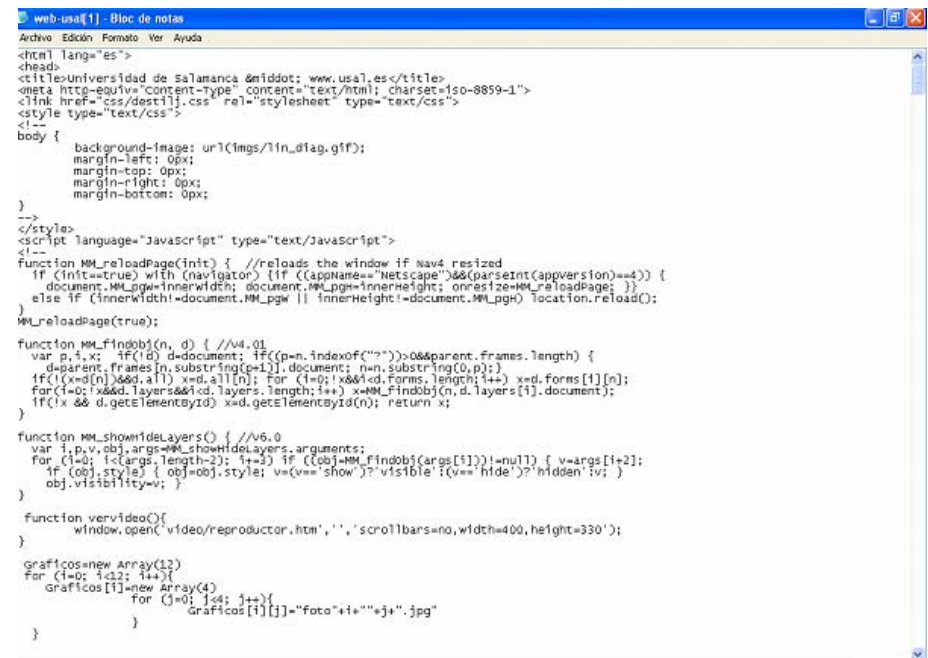
FIRMA Y SELLO

Firma: _____

Sello: _____



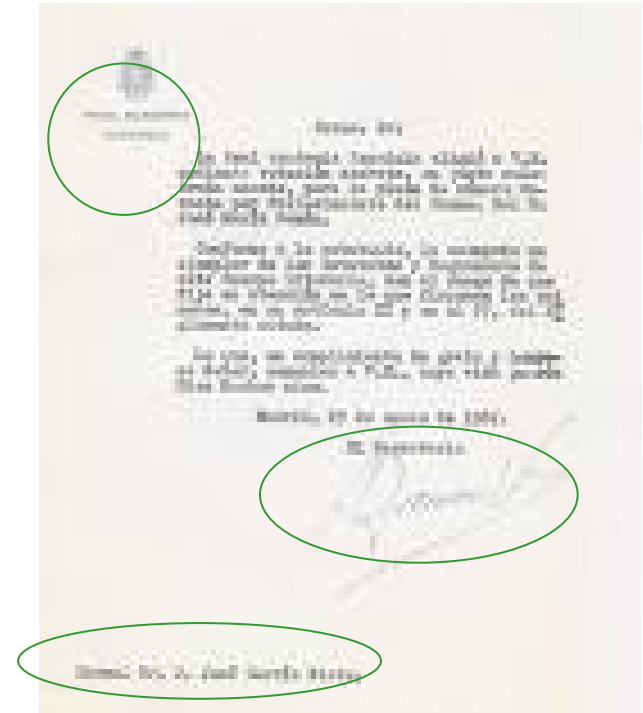
2.1. El documento electrónico y sus partes



2.1. El documento electrónico y sus partes

Contexto

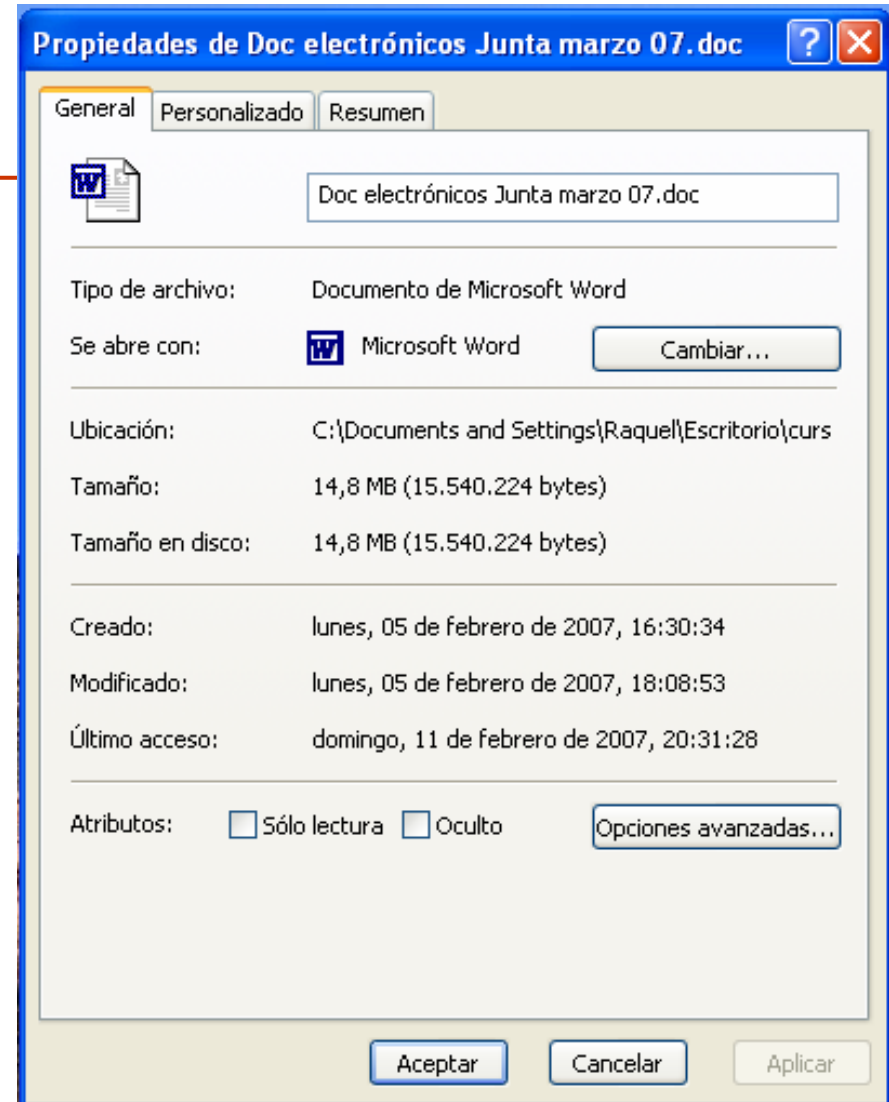
- Información necesaria para una comprensión completa y adecuada de:
 - Los documentos
 - Las actividades y operaciones
 - Procesos asociados a los documentos



2.1. El documento electrónico y sus partes

Contexto

- Información necesaria para una comprensión completa y adecuada de:
 - Información para la gestión y conservación
 - Información la recuperación y el acceso a esos documentos



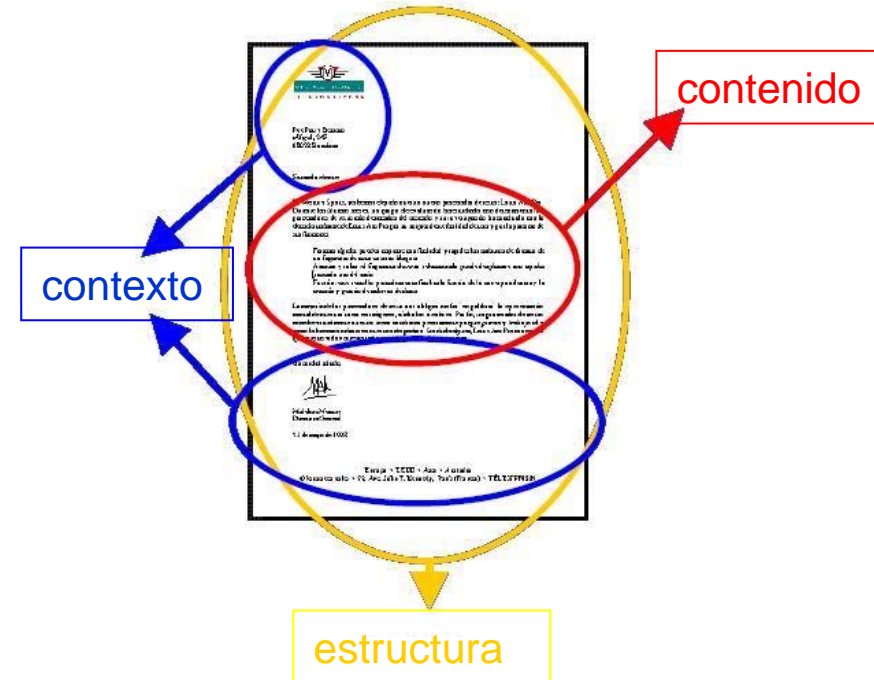
2.1. El documento electrónico y sus partes

Documento electrónico

“información registrada, producida, recibida en torno a la implantación, realización y ámbito de una actividad institucional o personal que engloba el **contenido**, **contexto** y **estructura** y permite

→ **probar** la existencia de la actividad que lo generó”.

[Definición del CIA]



2.2. Características de los documentos de archivo

Comunes al resto de los documentos de archivo

- ❑ La involuntariedad en la producción
- ❑ Unicidad e irrepetibilidad
- ❑ Organicidad
- ❑ Valor probatorio

Propias de los documentos electrónicos

- ❑ Necesitamos de la tecnología
 - crearlos
 - mantenerlos
 - transmitirlos
- ❑ El soporte es magnético u óptico



2.3. Los soportes

Soporte: objeto físico susceptible sobre el cual se pueden grabar y recuperar los datos.

- Magnéticos
- Ópticos



2.3.1. Soportes magnéticos



disquete



Disco duro



Memoria flash



2.3.1. Soportes magnéticos

- Varía su capacidad de almacenamiento
- Bajo coste
- Cuidado con los campos magnéticos
- Fácilmente modificable su contenido



2.3.2. Soportes ópticos



cd



cd-r (regrabable)



DVD



2.3.2. Soportes ópticos

- ❑ Son más estables que los ópticos
- ❑ Gran capacidad de almacenamiento
- ❑ No hay experiencia de duración



2.3.3. Comparación de los soportes

Soporte	Disco magnético	Disco óptico
Acceso a los datos	Acceso aleatorio rápido	Acceso aleatorio rápido, pero más lento que el disco magnético
¿Permite modificar los datos?	Sí	Sí, en algunos productos
Capacidad de almacenamiento actual por unidad	Hasta 200 gigabytes	hasta 4 gigabytes
Vida útil prevista de una unidad	Aprox. 5 años	Muy variable, según la calidad (de 5 años a varias décadas)



2.4. Los formatos

Formato: conjunto de reglas o especificaciones mediante las cuales se pueden organizar datos de diversa naturaleza, para poder acceder posteriormente a estos a través de los intérpretes (programas) adecuados.

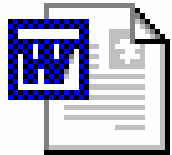


2.4. Los formatos

Texto



.txt

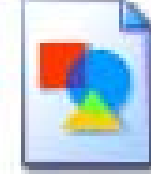


.doc

Imagen fija



jpg



gif



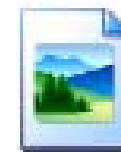
pdf



bmp



psd



tiff



2.4. Los formatos

Sonido

RealAudio

MP3

WMA

WAV

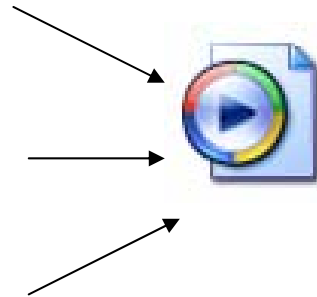


Imagen en movimiento

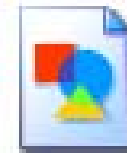
Avi

Mpg

divx



gif



2.5. Tipos de documentos electrónicos

Según la conexión

- Documentos en línea
- Documentos fuera de línea



2.5. Tipos de documentos electrónicos

Según la estructuración de la información

- ▣ Textuales
- ▣ Multidimensionales
- ▣ Documentos multimedia



2.5. Tipos de documentos electrónicos

Contenedores de datos

- Hojas de cálculo
- Bases de datos
- Formularios



2.6. Atributos

- Auténtico
 - Fiable
 - Íntegro, preciso y completo
 - Accesible o disponible
- Mecanismos que lo garantizan
- Distintas estrategias



2.6.1. Autenticidad

Aquél que puede probar:

- que es lo que afirma ser
- que ha sido creado o enviado por la persona de la cual se afirma que lo ha creado o enviado
- que ha sido creado o enviado en el momento en que se indica



2.6.2. Fiabilidad

Cuando el contenido del documento puede ser considerado una representación completa y precisa de las actuaciones, actividades o hechos de los que da testimonio



2.6.3. Integridad

Cuando podemos asegurar que está completo e inalterado.

Los documentos deben estar protegidos frente a modificaciones no autorizadas. Las anotaciones, adiciones o supresiones autorizadas deben indicarse de forma explícita y dejar rastro (traza)



2.6.4. Disponibilidad

Cuando puede ser localizado, recuperado, presentado o interpretado.

El documento debería:

- Mostrar la actividad o actuación que lo produjo.
- Proporcionar la información necesaria para la comprensión de las actuaciones que lo crearon y usaron.
- Señalar el contexto amplio de las actividades y las funciones de la organización.
- Mantener los vínculos existentes con otros documentos como reflejo de una secuencia de actividades.



2.6. Atributos

Autenticidad
Fiabilidad
Integridad

La encriptación → códigos hash
- la firma electrónica
- los certificados digitales

La filigrana electrónica

Disponibilidad

→ **Estrategias de conservación**



2.7. Etapas en la evolución de los documentos electrónico de archivo

- A finales de los años 40.
- A principios de los 80
- Desde mediados de los 90.
- A partir de finales de los 90



2.8. El ciclo de vida de DEA

Planificación del ciclo de vida de DEA

- ❑ Determinar qué actividades generan documentos.
- ❑ Definir la estructura y el contexto atribuidos al documento que debe ser capturado cuando desarrollamos una actividad.
- ❑ Identificar leyes, políticas y normas relevantes e incorporar las características que se especifican en ellos.
- ❑ Identificar los niveles de seguridad y las necesidades, tales como la capacidad de restringir el acceso a las funciones del sistema y a los documentos.



2.8. El ciclo de vida de DEA

Planificación del ciclo de vida de DEA

- ❑ Controlar las copias en el sistema de salida y entrada, la actualización y la producción de informes.
- ❑ Determinar cuándo algunos de los documentos puede tener valor para los objetivos no relacionados directamente con las funciones de gestión.
- ❑ Asignar responsabilidades para asegura que los documentos son generados y capturados



2.9. Comparación del documento electrónico de archivo con los documentos en otros soportes

ELECTRÓNICO	PAPEL	MICROFORMA
Soporte muy frágil y poco estable. No hay experiencia de cuanto duran estos soportes.	El soporte es estable y hay experiencia de que se conserva bien a lo largo del tiempo	El soporte es estable y hay experiencia de que se conserva bien a lo largo del tiempo (más de 100 años)
El ciclo de vida incluye la fase de diseño del documento	El ciclo de vida comienza en la etapa de creación del documento	El ciclo de vida comienza en la etapa de creación del documento
Se pueden tratar prácticamente de manera automática	Imposibilidad de tratar y recuperar de manera rápida	Es necesario invertir tiempo en el tratamiento.



2.9. Comparación del documento electrónico de archivo con los documentos en otros soportes

ELECTRÓNICO	PAPEL	MICROFORMA
Necesita inversión en recursos tecnológicos que es necesario ir actualizando	No necesita inversión en recursos.	Necesita inversión en recursos tecnológicos pero no es necesario seguir invirtiendo en la actualización
Para ser consultados necesita un decodificador de la información	No necesita decodificador de la información	Necesita de un aparato que aumente la imagen pero no de un decodificador de la información.
Fácil de recuperar	Fácil de consultar	Fácil de consultar gracias al sistema de recuperación óptica



2.9. Comparación del documento electrónico de archivo con los documentos en otros soportes

ELECTRÓNICO	PAPEL	MICROFORMA
Fácil de modificar	Dificultad para modificar su contenido lo que le confiere un alto valor jurídico y legal	Perdura el valor intrínseco del documento. No se puede modificar
Gran capacidad de almacenamiento y a bajo coste	Ocupa mucho espacio de almacenamiento	Ocupa poco espacio de almacenamiento
Fácil de reproducir	Fácil de reproducir	La reproducción algo compleja.
Contenido, contexto y estructura, separados	Contenido, contexto y estructura, unido	Contenido, contexto y estructura, unido



3.1. Los metadatos: concepto

- ▣ Datos que describen el contexto, contenido y estructura de los documentos, así como su gestión a lo largo del tiempo

ISO 15489-1:2001



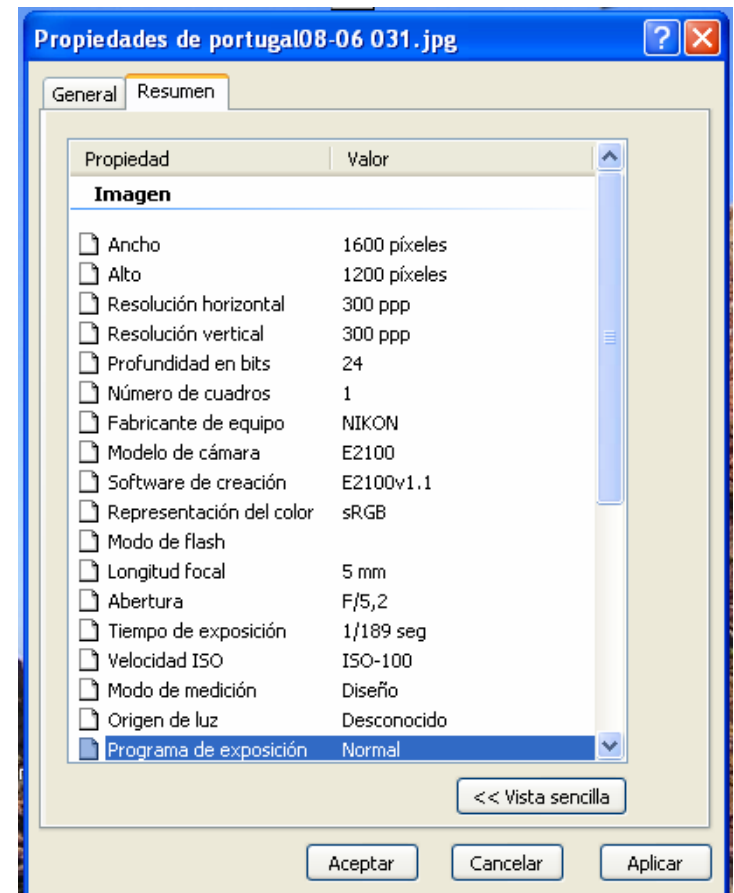
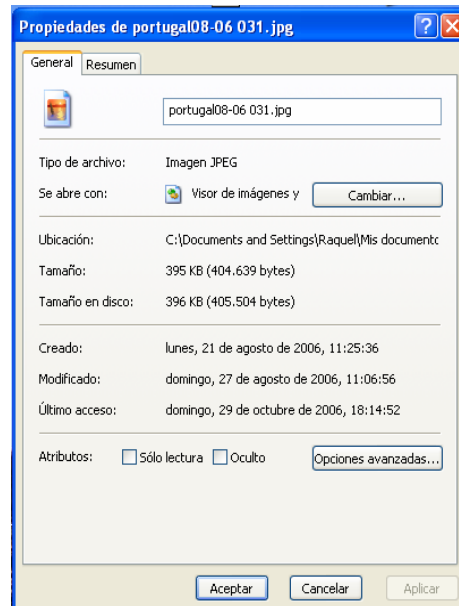
3.1. Los metadatos: concepto

"información estructurada o semiestructurada que permite la creación, gestión y la utilización de los documentos de archivo a lo largo del tiempo, tanto dentro de los ámbitos que se crearon como entre ellos".

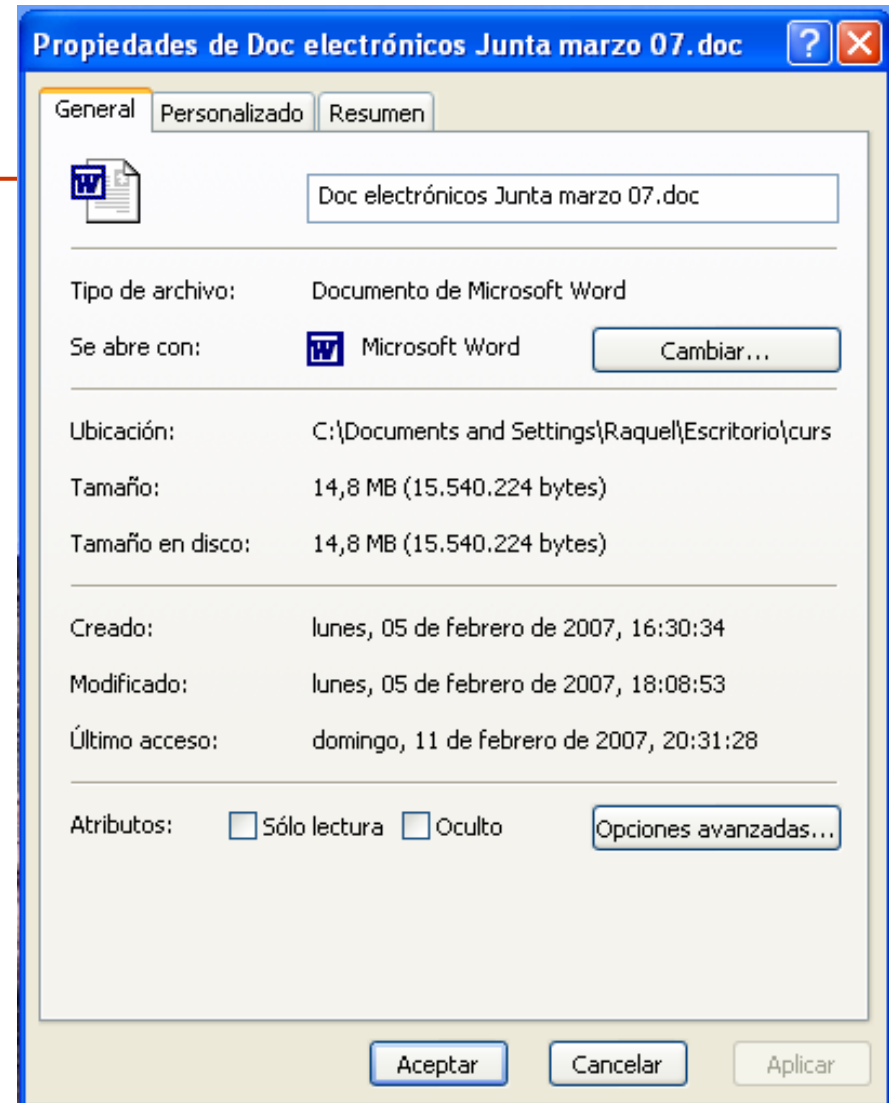
[Especificación MoReq]



3.1. Los metadatos: concepto



3.1. Los metadatos: concepto



3.2. Utilidad de los metadatos

METADATOS

- IDENTIFICAR
- AUTENTIFICAR
- CONTEXTUALIZAR

DOCUMENTOS

INDIVIDUOS

PROCESOS

SISTEMAS

NORMAS



3.2. Utilidad de los metadatos

- ▣ Facilitan la capacidad de entender los documentos
- ▣ Soportan y aseguran el valor probatorio de los documentos.
- ▣ Ayudan a asegurar la autenticidad, fiabilidad e integridad de los documentos
- ▣ Sirven de base para una recuperación eficiente



3.2. Utilidad de los metadatos

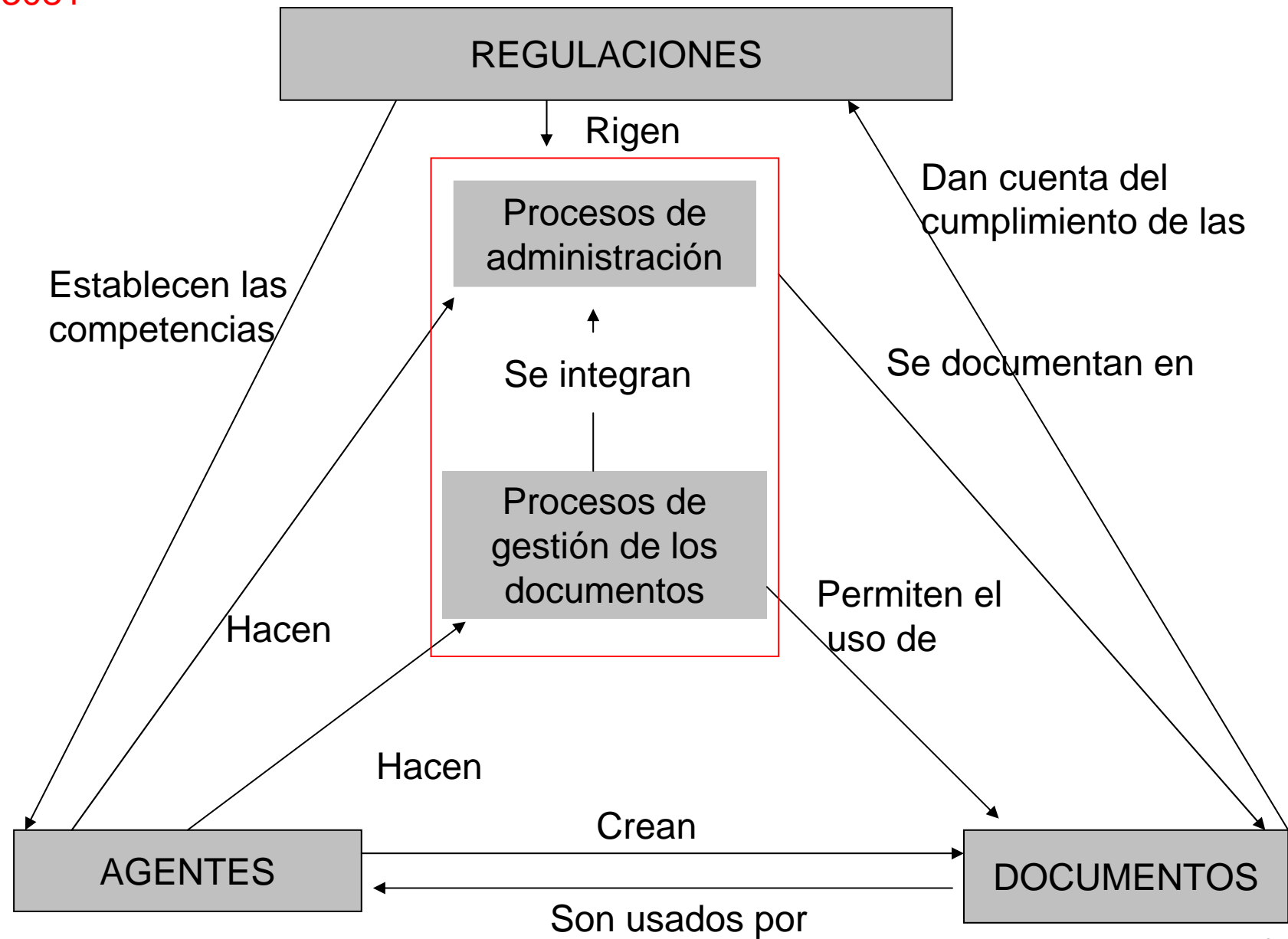
- ▣ Sirven de respaldo las estrategias de interoperabilidad, permitiendo que se incorporen oficialmente al sistema documentos creados en diversos entornos administrativos y técnicos y que se mantengan durante tanto tiempo como sea necesario.
- ▣ Proporcionan enlaces lógicos entre los documentos y el contexto de su creación, manteniéndolos de forma estructurada, fiable e inteligente.
- ▣ Aportan la historia del documento



3.3. Metadatos para la gestión de los documentos

- ❑ El documento mismo
- ❑ Las políticas y normas
- ❑ Los agentes
- ❑ Las actividades o procesos que generan los documentos
- ❑ Los procesos de gestión





3.4. Pautas para la gestión

- ISO 23081-1:2005
- Conjuntos de metadatos desarrollados a nivel nacional o local: Australia, Canadá, Reino Unido, Minnesota (EEUU)
- Dublin Core
<http://es.dublincore.org/documents/>



3.4. Pautas para la gestión

- ❑ Especificación MoReq

<http://www.mcu.es/archivos/docs/moreq.pdf>

- ❑ Manual para archiveros. Versión española del manual editado por el Consejo Internacional de Archivos.

<http://www.mcu.es/archivos/docs/documentosElctronicos.pdf>



3.4. Pautas para la gestión

□ Sobre conservación

■ Proyecto INTERPARES

<http://www.interpares.org/>

■ ISO 14721:2003 (Open Archival Information System: OAIS)

■ ISO 19005-1. Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF (PDF/A)



3.4. Pautas para la gestión

- ▣ Sobre seguridad de la información
 - ISO 17799:2005, code of practice for information security management



3.5. Metadatos necesarios para la gestión

- ❑ Registro
- ❑ Términos y condiciones
- ❑ Estructura
- ❑ Contexto
- ❑ Contenido
- ❑ Historia del uso



3.6. Tipos de metadatos

- 3.6.1. Por el momento en el que se crean
- 3.6.2. En función de cómo han sido creados
- 3.6.3. En función de la utilidad
- 3.6.4. En función de su permanencia en el sistema
- 3.6.5. En función de su estructura
- 3.6.6. En función de la semántica
- 3.6.7. Por las formas de uso



3.6.1. Por el momento en el que se crean

■ En el momento de la incorporación

- Contexto de creación
- Contexto de la organización
- Contenido
- Individuos implicados (quien lo crea o captura)
- Apariencia
- Estructura
- Atributos técnicos

ISO 23081

■ Posteriores a la incorporación

- Elementos que garantizan la autenticidad, fiabilidad, disponibilidad, integridad



3.6.2 En función de cómo han sido creados

- Automáticos
- Manuales



3.6.3. En función de la utilidad

Para definir el contenido

- ▣ Fecha y hora de creación del documento
- ▣ Identificar y describir la persona involucrada en la creación del mismo
- ▣ Documentar
 - la estructura
 - la forma
 - las propiedades físicas y químicas
 - las características técnicas del documento
 - las relaciones entre los datos y elementos de formato del documento
 - los requisitos para que el documento pueda estar disponible o ser reproducible y representable



3.6.3. En función de la utilidad

Para definir el contenido

- ❑ Facilitar
 - la migración a un software diferente
 - la representación mediante emulación

- ❑ Iniciar actividades de gestión de datos y formato para proteger el deterioro del soporte

- ❑ Documentar
 - las relaciones entre el documento y las actividades que lo han generado
 - los vínculos entre documentos o entre un documento individual y la unidad documental de la que forma parte.



3.6.3. En función de la utilidad

Para definir el contexto

- ❑ Cambios que deben sufrir
- ❑ Contexto jurídico-diplomático.
- ❑ Definición del soporte
- ❑ Elementos de validación
- ❑ Controles de seguridad
- ❑ Utilización del recurso.
- ❑ Información acerca de quien ha utilizado el recurso



3.6.3. En función de la utilidad

Para documentar el contexto sirve

- ❑ Código del cuadro de clasificación
- ❑ Plazos de validez administrativa
- ❑ Plazos de conservación/eliminación y acceso
- ❑ Quien puede utilizarlos dentro y fuera del sistema
- ❑ Dónde se van a conservar y en qué formato.
- ❑ Contexto tecnológico.
- ❑ Entorno, soporte y formato en que deben conservarse



3.6.3 En función de la utilidad

- ❑ Accesibilidad
- ❑ Conservación
- ❑ Descripción



3.6.3 En función de la utilidad

- ▣ Búsqueda y recursos de información
- ▣ Seguridad



3.6.4. En función su permanencia dentro del sistema

- ❑ Metadatos estáticos
- ❑ Metadatos dinámicos
- ❑ Metadatos de larga duración
- ❑ Metadatos de corta duración



3.6.5. En función su estructura

- ▣ De estructura **estandarizada**.
- ▣ **Desestructurados** (campos de notas).



3.6.6. En función de la semántica

- ▣ Realizados mediante vocabularios controlados.
- ▣ Realizados mediante lenguaje natural



3.6.7. Por la forma de uso

- ❑ Los metadatos acompañan al propio documento
- ❑ Los metadatos forman ficheros separados de meta-información
- ❑ Base de datos creada con los metadatos (con punteros a los recursos que describen)



3.7. Formatos de los metadatos

- ▣ Alfabéticos
- ▣ Alfanuméricos
- ▣ Numéricos
- ▣ De fecha
- ▣ Lógicos



3.8. Características del estándar ideal de metadatos

- ❑ Que sean fácil de crear y mantener
- ❑ Que utilicen una semántica que pueda entenderse de forma común
- ❑ Que puedan crearse de forma automática (si no todos, sí algunos)
- ❑ Que pueda describir la forma, el contenido y la localización de la información
- ❑ Que su escritura permita contenerlos en otros objetos
- ❑ Que se puedan usar para construir múltiples índices
- ❑ Que pueda interoperar en los sistema de indización que existan
- ❑ Que pueda ampliarse según las necesidades



3.9 Beneficios de los esquemas de metadatos

- 1) Permiten una gestión de metadatos consistente e integrada
- 2) Permiten la interoperabilidad mediante la comparación o mapeo de diferentes conjuntos de metadatos
- 3) Permiten expresar las interrelaciones de elementos y su semántica
- 4) Permiten controlar las relaciones entre elementos y su semántica inherente



3.9 Beneficios de los esquemas de metadatos

- 5) Permiten asegurar y mantener la consistencia en sistemas de información (por ejemplo sistemas de gestión de documentos)
- 6) Favorecen el desarrollo modular, la ruptura o vinculación de sistemas de información
- 7) Proporcionan una base para el desarrollo de sistemas de información o bases de datos



4. La gestión de los documentos electrónicos

El diseño

- Identificar las acciones que darán lugar a los documentos
- Establecer las normas de diseño de un sistema de clasificación eficaz
- Definición de normas y especificaciones que garantizarán los valores y perdurabilidad de la conservación
- Establecer el sistema de valoración de la documentación electrónica
- Identificación de los responsables de cada tarea a lo largo del ciclo de vida



4.2. La autenticación

La autenticación

- Proyecto CERES

<http://www.cert.fnmt.es/>

- Proyecto EROS

<http://www.nationalarchives.gov.uk/recordsmanagement/>

- Proyecto INTERPARES

<http://www.interpares.org/>



4.2. La autenticación

Métodos de autenticación

- la firma digital o electrónica
- La encriptación
- La filigrana electrónica
- Los certificados digitales



4.1.2. la firma electrónica

- ▣ Ministerio de Hacienda HAC/118/2003 de 12 de mayo por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria (BOE 116, 15 de mayo de 2003)



4.1.2. La firma electrónica

¿Cómo se genera una firma electrónica?

- ❑ Se obtiene una huella digital del documento digital que se quiere firmar. Esta huella digital garantiza que dos documentos diferentes generan diferentes huellas digitales y dos documentos iguales siempre generan la misma huella digital.
- ❑ Se realiza el cifrado (mediante algoritmos matemáticos) de la huella digital con la clave privada del certificado. De esta forma se garantiza la autenticidad ya que es el propietario del certificado el único que ha podido realizar este cifrado.
- ❑ Se encapsula toda la documentación en un documento firmado que incluye:
 - Documento original (opcional)
 - Huella digital cifrada con la clave privada.
 - Parte pública del certificado.



2.1.2. La firma electrónica

Verificación de una firma electrónica

- ❑ 1. Se descifra la huella digital cifrada con la clave privada mediante la clave pública del certificado.
 - ❑ 2. Se obtiene la huella digital del documento original.
 - ❑ 3. Se comparan las huellas digitales. Si coinciden, la firma es correcta (hay integridad, el documento no ha sido modificado).
 - ❑ 4. Se consulta a la autoridad de certificación emisora por la validez del certificado y si es válida, la firma además de correcta es válida (garantizada la autenticidad del origen de la firma).
-
- ❑ <http://www.fomento.es/oficinavirtual/firma.html>



4.2.2. La encriptación

Encriptar consiste en sustituir los elementos (letras o palabras) de un texto legible por un conjunto de caracteres (letras, números o símbolos) que resultarán incomprensibles para cualquier persona que no sepa (no tenga la clave necesaria) reconvertirlos en el texto original.



4.2.2. La encriptación

- ▣ Algoritmos de encriptación
 - Clave simple → simétricos
 - Doble clave → asimétricos



4.2.2. La encriptación

El hash

resumen criptográfico que consiste en aplicar una determinada transformación a una información almacenada

- que sea de una sola vía
- Resistente a colisiones
- Que el tamaño del hash sea menor que el documento de partida



Claves simétricas

En el dorso de mi tarjeta VISA dice: **ncea**



En el de la Master Card tengo escrito: **iiñc**

MasterCard
International



En el teléfono móvil aparece escrito: **qsuo**



Y junto al cierre de la caja fuerte: **inocua**



Claves simétricas

Es una costumbre que tengo desde hace mucho tiempo, más de **quince** años, y siempre me ha sido muy útil.

/// Nunca olvido un número de identificación personal

/// Siempre lo tengo a mano cuando lo necesito.

/// Y nadie puede descubrir mis números.

ncea



i iñc

MasterCard
International



qsuo



inocua



¿...o sí?



Claves simétricas

El NIP de la VISA es

4567

ncea



El de la Master Card es

3385

iiñc

MasterCard
International



El del móvil es

1029

qsuo



Y el de la caja fuerte es

349527

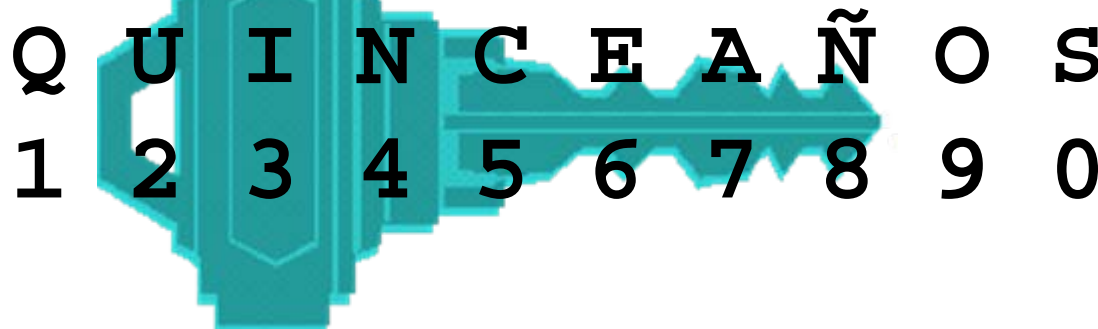
inocua



Claves simétricas

Hay una clave sencilla, simétrica y pnemotécnica que convierte los números en letras y viceversa:

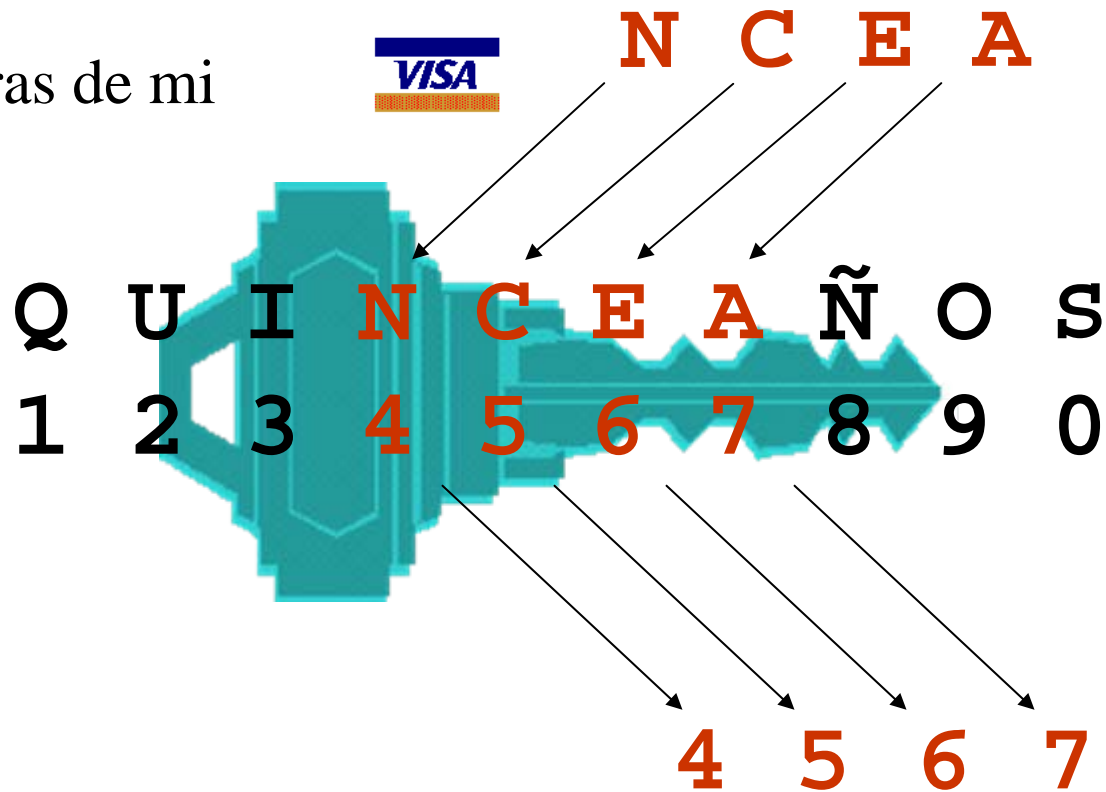
Y la clave es ...



Claves simétricas

Es muy sencillo convertir

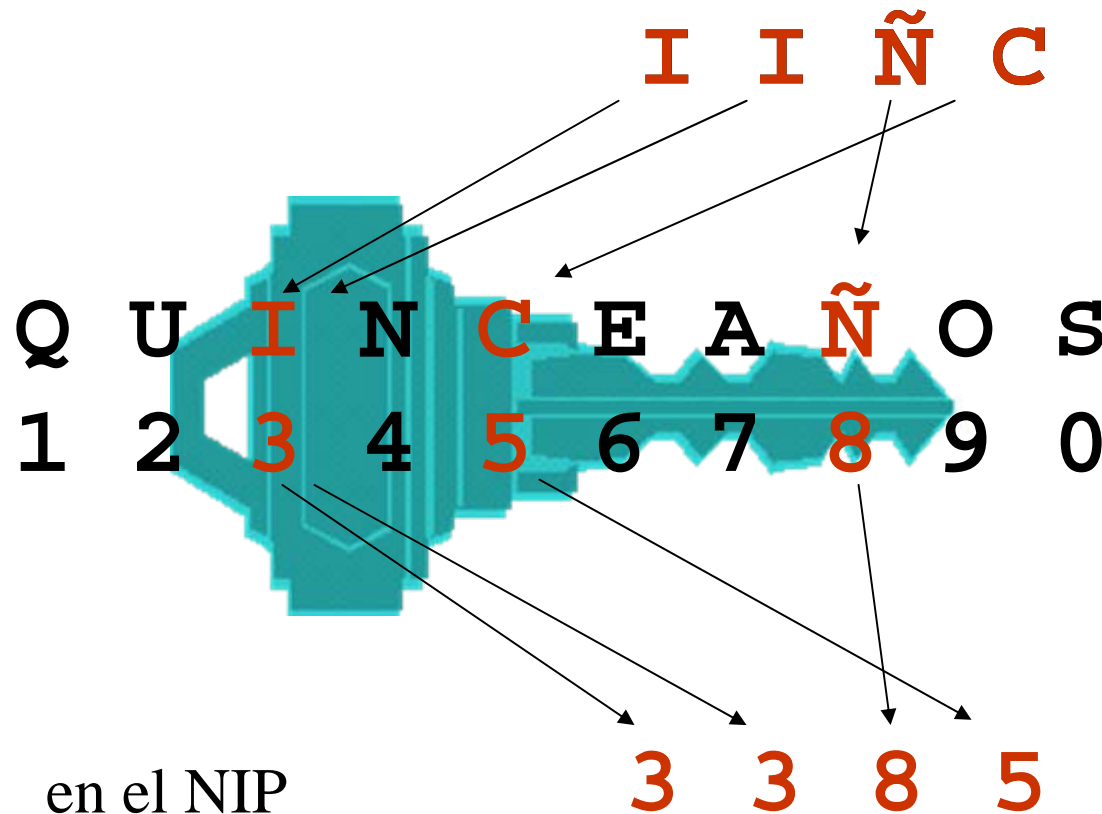
las letras de mi
VISA



en el NIP



Claves simétricas



MasterCard
International



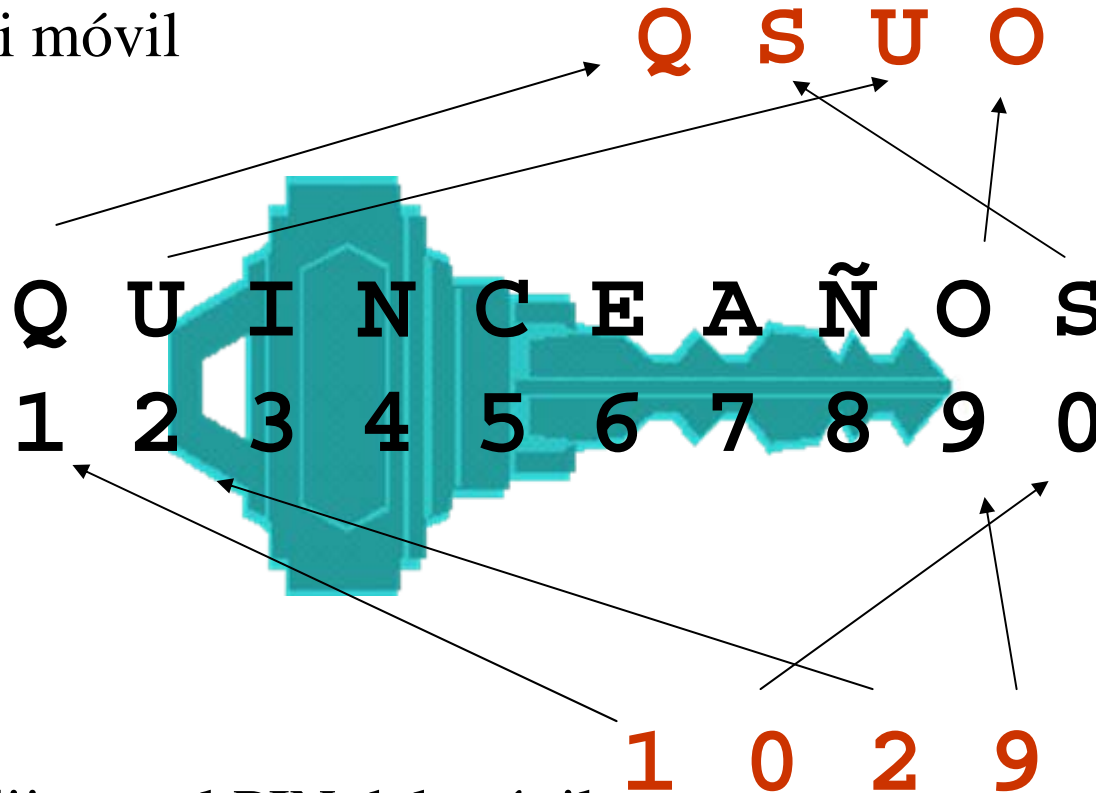
las letras de mi MASTER-CARD



Claves simétricas



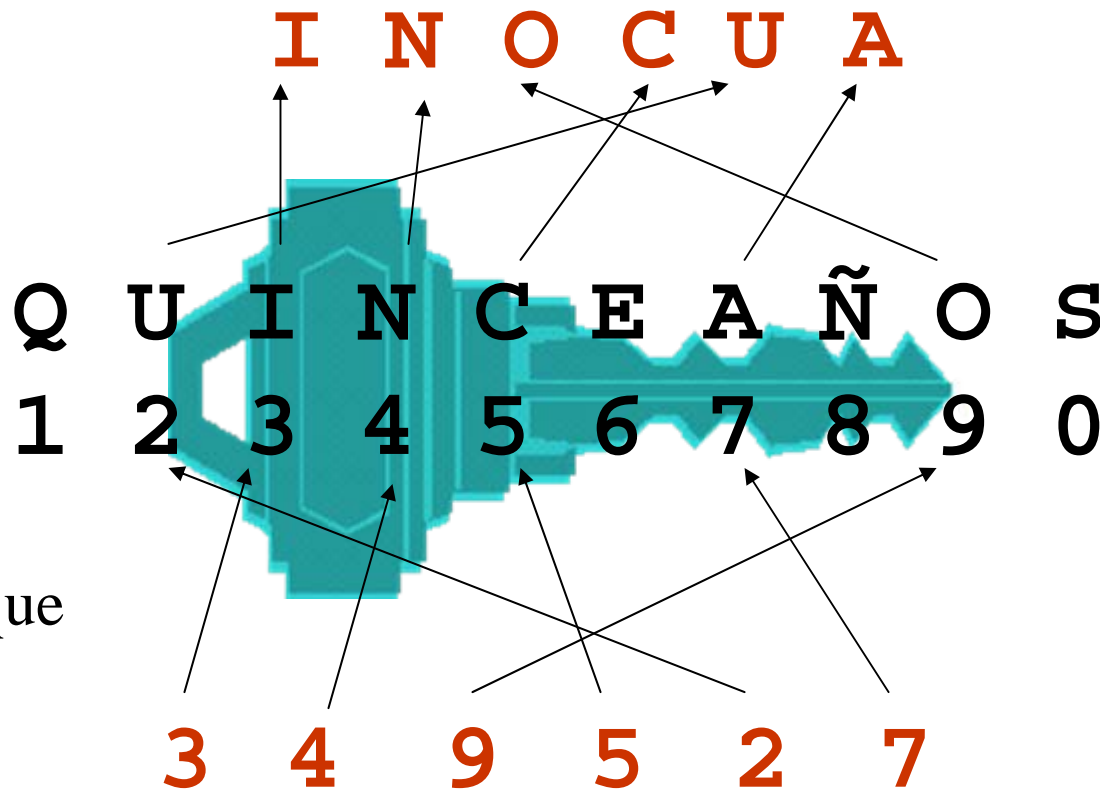
El pin de mi móvil



Cuando me dijeron el PIN del móvil:

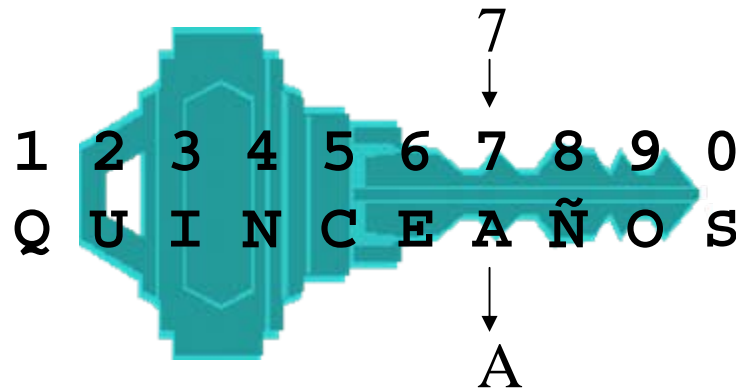


Claves simétricas

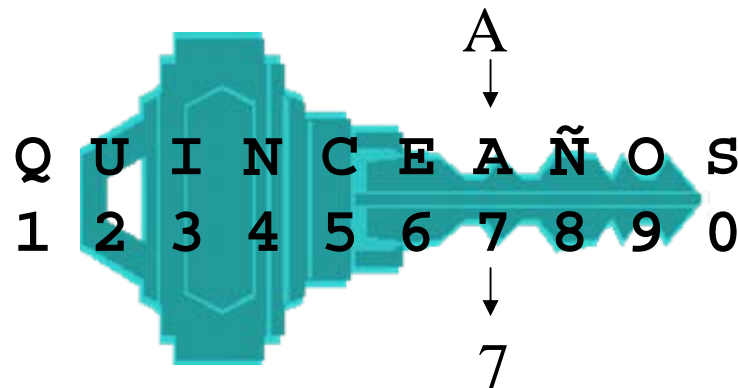


Lo mismo que
el de la caja
fuerte





Y también para pasar del texto encriptado al texto original.



Claves simétricas

Ventajas de las claves simétricas

- ▣ Son sencillas. Los ordenadores las manejan fácil y rápidamente
- ▣ Hay claves simétricas muy sofisticadas y seguras. Las más conocidas son **DES**, RC2, RC4, IDEA, SkipJack etc...



Claves simétricas

Inconvenientes de las claves simétricas

- ❑ Si quiero que otra(s) persona(s), pero sólo ellas, entiendan lo que he encriptado ¿Cómo les envío la clave?
- ❑ Los ordenadores actuales desenscriptan muy fácilmente las claves simétricas.



Claves asimétricas

Claves asimétricas

- En 1976 los matemáticos Whit Diffie y Martin Hellman crearon los sistemas criptográficos de clave asimétrica o pública.



Claves asimétricas

La criptografía
asimétrica

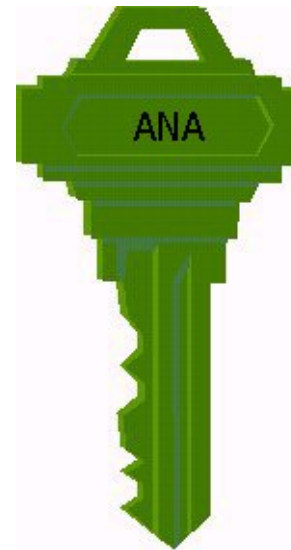
utiliza dos claves:

la clave privada

y la clave pública.



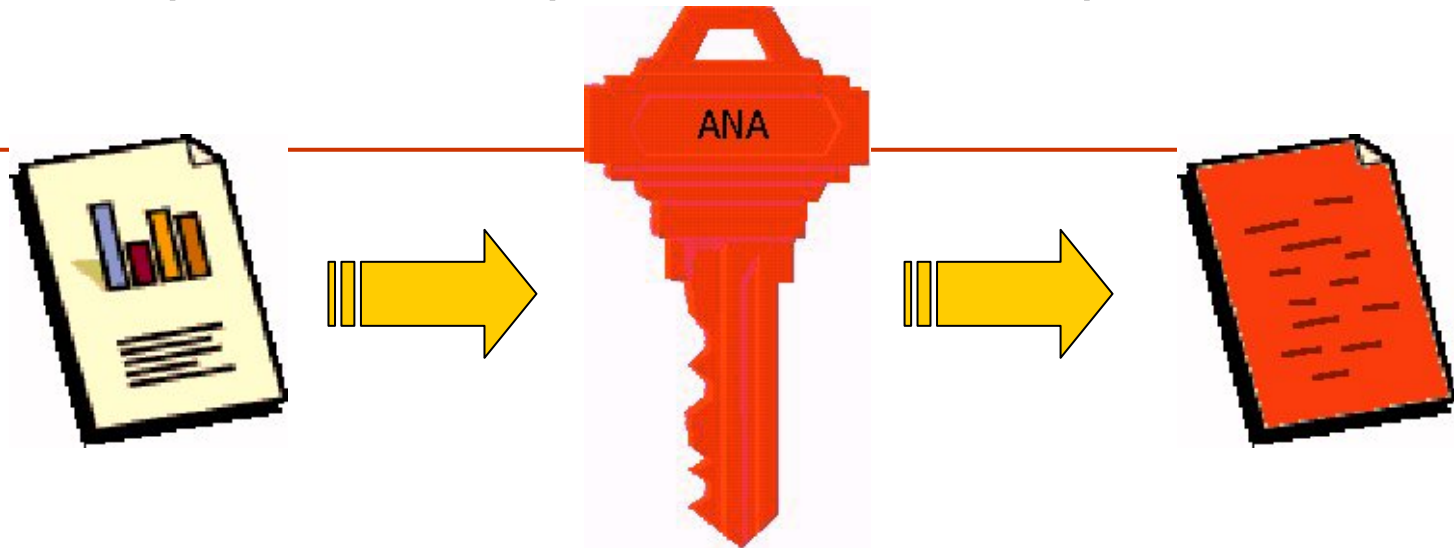
La clave privada
de Ana sólo
la debe conocer
Ana



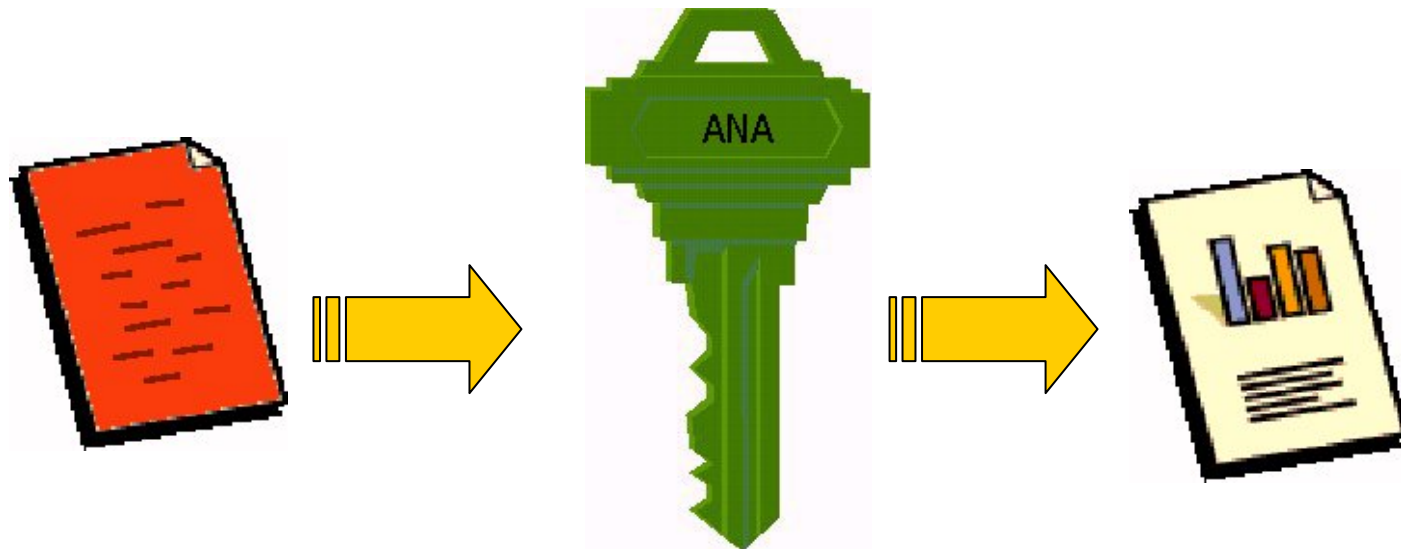
La clave pública
de Ana la puede
conocer cualquiera
ya que está en bases
de datos públicas



Lo que esté encriptado con la clave privada de ANA



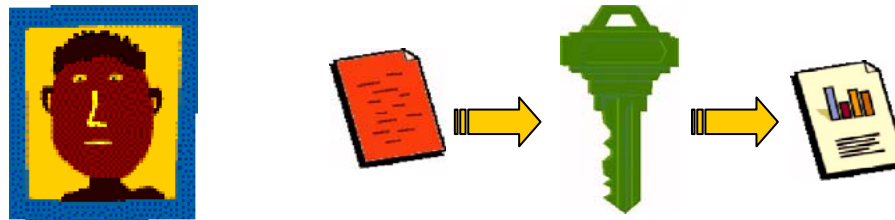
necesita la clave pública de ANA para desenscriptarse



Si Ana envía a Benito un mensaje
encriptado con su clave privada



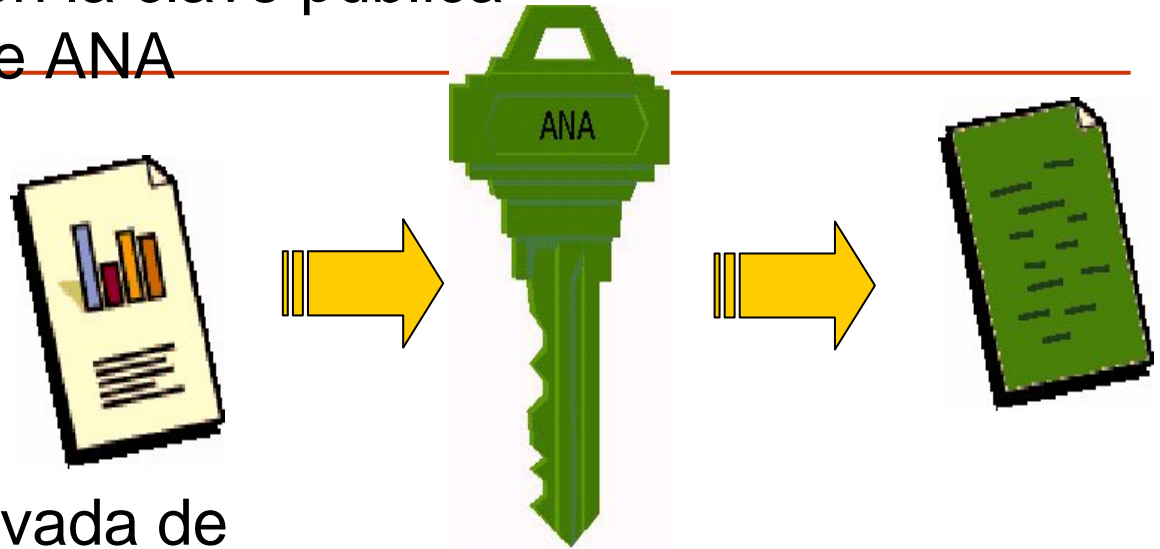
Benito necesitará la clave pública
de Ana para desenscriptarlo



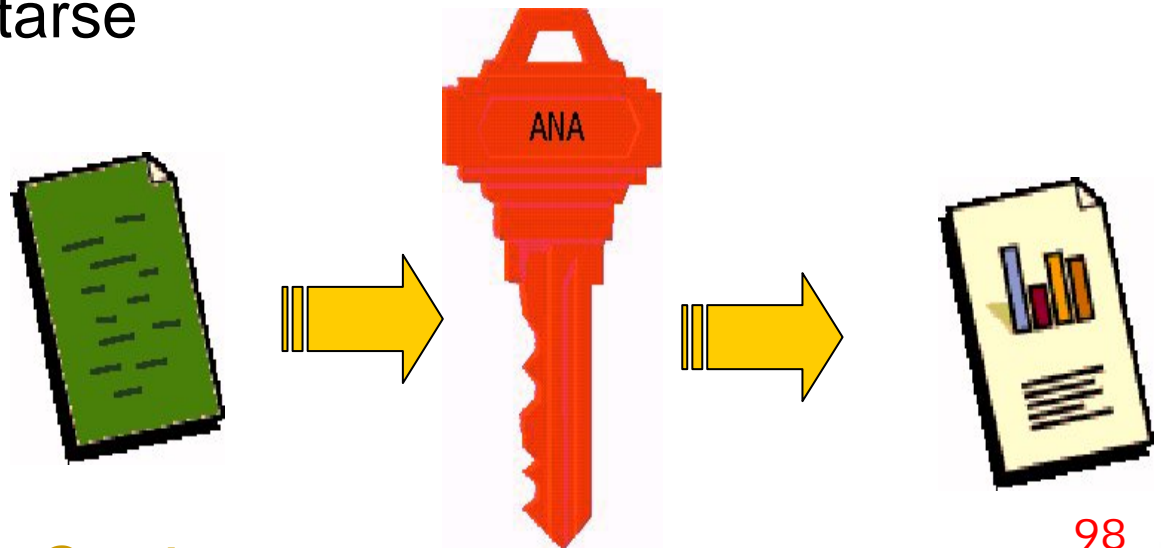
**Y así Benito estará seguro de que ha sido Ana
y no otra persona la que envió el mensaje**



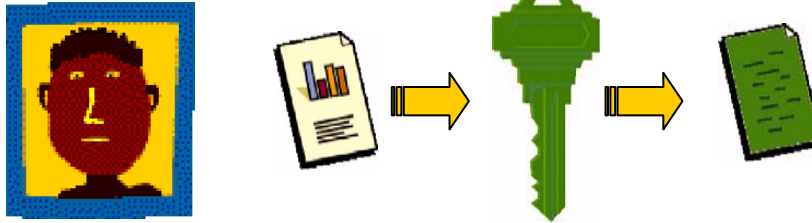
Y, al revés, lo que esté
encriptado con la clave pública
de ANA



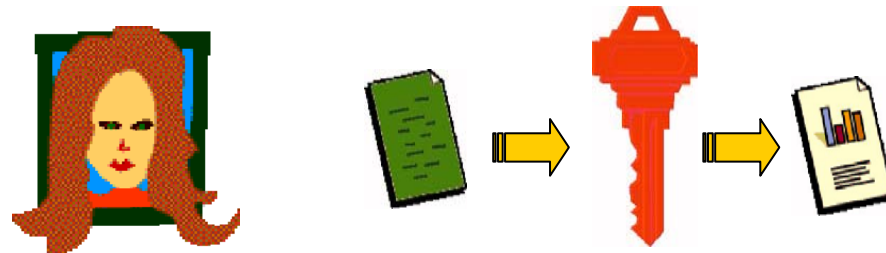
necesita la clave privada de
ANA para desenscriptarse



Si Benito quiere enviar un mensaje a Ana lo encriptará con la clave pública de Ana



Ana necesitará usar su clave privada para descryptar el mensaje de Benito



Sólo Ana puede entender los mensajes encriptados con su clave pública



Claves asimétricas

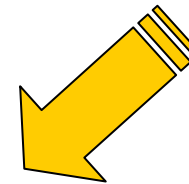
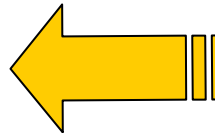
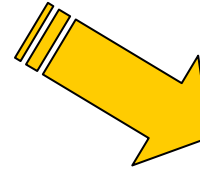
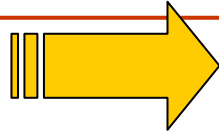
Las ventajas de las claves asimétricas se perciben plenamente cuando se combinan las claves de dos personas.

Supongamos que ANA quiere enviar un mensaje a BENITO



T. 4. Los documentos electrónicos y su gestión

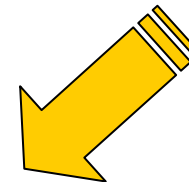
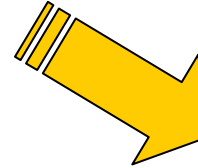
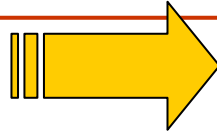
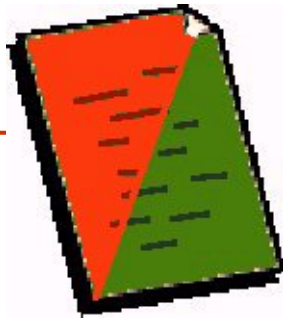
Ana encripta el mensaje
con su clave privada



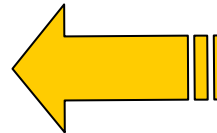
y con la clave
pública de Benito

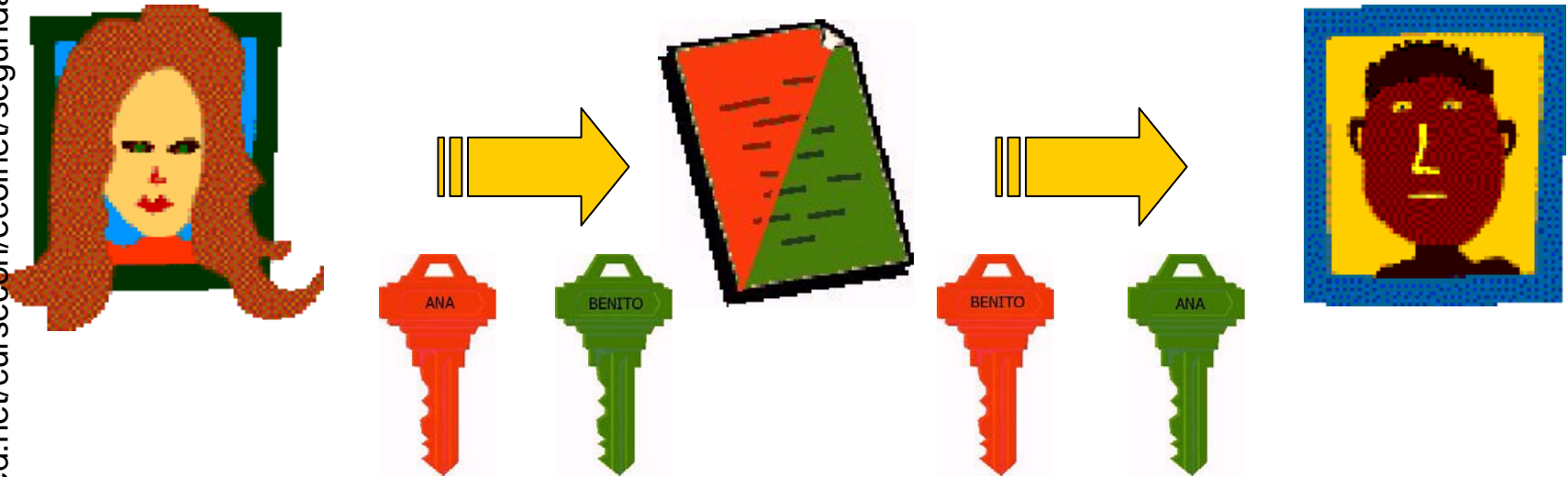


Benito descripta el
mensaje con su clave
privada



y con la clave
pública de Ana





Ana está segura de que
sólo Benito ha podido leer
el mensaje

Benito está seguro de que
ha sido Ana la que lo ha
enviado



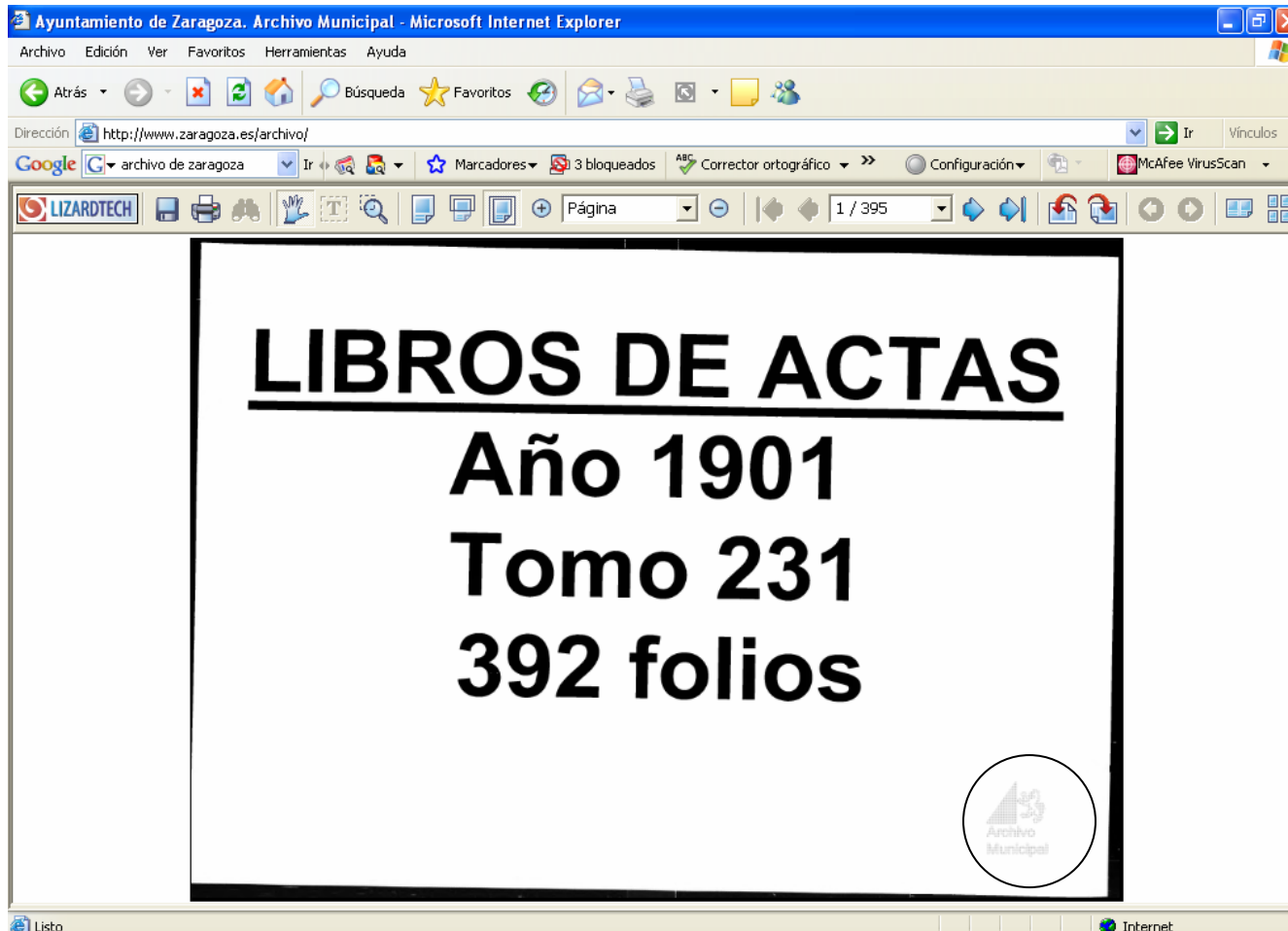
4.2.3. Los certificados electrónicos

Certificados electrónicos (estándar X.509) campos.

- Versión.
- Número de serie.
- Identificador del algoritmo empleado para la firma digital.
- Nombre del certificador.
- Periodo de validez.
- Nombre del sujeto.
- Clave pública del sujeto.
- Identificador único de certificador.
- Identificador único de sujeto.
- Extensiones
- Firma digital de todo lo anterior generada por el certificador.



4.2.4 Las marcas de agua



4.2.4. Las marcas de aguas



4.2.4. Las marcas de agua

Características

- Robustez
- Ambigüedad
- imperceptibilidad



4.2.5. Tareas a realizar en la fase de autenticación

- Análisis del estado del soporte
- Identificación de los datos necesarios para su lectura
- Eliminación de virus informáticos
- Reproducción digital (si es necesario)
- Instalación y testeo del funcionamiento
- Comprobar la integridad del documento
- Identificación de los límites y componentes del documento



4.2.6. La integridad documental

Los documentos han de ser:

- Completos
- Fijos
- Referenciados
- Fiables
- Auténticos



4.3. El registro

Datos mínimos según la ISO 15489

- Un identificador único atribuido por el sistema
- La fecha del registro
- El título del documento y una breve descripción
- El productor.



4.9. La conservación

▣ Problemas

- Obsolescencia de hardware/software
- Degradación de los soportes



4.9. La conservación

Precauciones con respecto a los soportes

- ❑ Comprobar que los soportes están en condiciones idóneas.
- ❑ Sustituir rutinariamente los soportes antes del final de su ciclo de vida
- ❑ Mantener varias copias de cada documento y la información asociada a él y compararlas regularmente



4.9. La conservación

Algunas reglas

- ▣ Temperatura de conservación $18^{\circ} \pm C$
- ▣ Humedad relativa de conservación: $40\% \pm 5\%$
- ▣ Frecuencia de grabación 10 años



5.9. La conservación

Soportes

- ❑ Soportes magnéticos: algunos son
 - Disquete
 - Cartucho magnético

- ❑ Soportes ópticos
 - CD-Rom
 - DVD
 - Disco WORM
 - Disco óptico regrabable



4.9. La conservación

□ Esperanza de los soportes

Ejemplos de la expectativa de vida de los soportes (Jones/Beagrie):

Soporte	25 HR 10°	30 HR 15°	40 HR 20°	50 HR 25°	50 HR 28°
D3 cinta mag.	50 años	25 años	15 años	3 años	1 año
DLT cinta mag. estuche	75 años	40 años	15 años	3 años	1 año
CD/DVD	75 años	40 años	20 años	10 años	2 años
CD-ROM	30 años	15 años	3 años	9 m.	3 m.



4.9. La conservación

Nome da Mídia	Temp. °C	Umidade Relativa %	Durabilidade - Anos
CD-ROM	40	80	2
	30	60	10
	20	40	50
	10	25	200
WORM	40	80	5
	30	60	20
	20	40	100
	10	25	200
CD-R	40	80	2
	30	60	5
	20	40	30
	10	25	100
MAGNETO-ÓPTICO	40	80	2
	30	60	5
	20	40	30
	10	25	100
Microfilme com Qualidade Arquivística (Prata)	40	80	20
	30	60	50
	20	40	200
	10	25	500

Esperanza de los soportes

Fuente :

<http://www.cenadem.com.br/ged10.php>



4.9.5. Estrategias de conservación

Objetivos globales de la conservación digital:

Asegurar la legibilidad e inteligibilidad de los objetos digitales conservados.

Conservar la autenticidad e integridad de los mismos.

Problemas a los que se enfrenta la conservación digital:

Las normas de codificación y los formatos de los ficheros

La obsolescencia del hardware.

La dependencia del software.

El deterioro del soporte de almacenamiento.



4.9.5. Estrategias de conservación

Reto principal de la conservación digital:

La dependencia del software.

o lo que es lo mismo

El hecho de que los objetos digitales dependan de una aplicación software para hacerlos accesibles y con sentido.

- Durante las últimas dos décadas, se han propuesto un gran número de estrategias, para la conservación de objetos digitales a largo plazo.
- El plazo de legibilidad de un objeto digital puede oscilar entre:

5 - 20 años en el caso de *hardware*

5 - 10 años en el de *software*



4.9.5. Estrategias de conservación

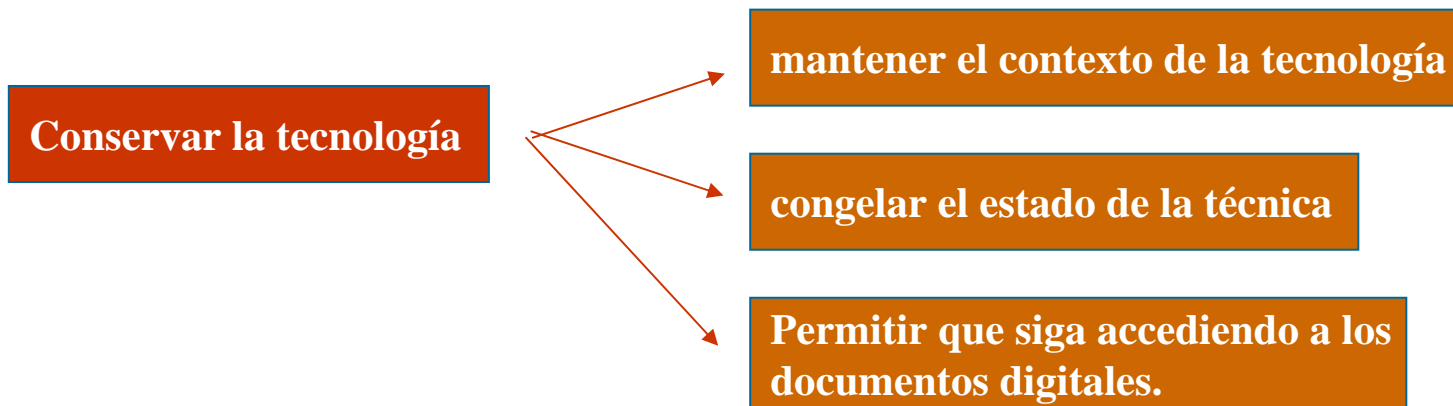
- ▣ La preservación de la tecnología
- ▣ La emulación
- ▣ La conversión
- ▣ La migración



Preservación de la tecnología

Creación de museos cibernéticos o tecnológicos donde podemos encontrar *hardware* y *software* obsoletos.

Propuesta por *David Bearman*.



Preservación de la tecnología

Inconvenientes:

- ❑ Además de conservar el *hardware* y *software* originales, hay que ocuparse de mantenerlos en funcionamiento cuando su obsolescencia sea ya completa.
- ❑ Opción económicamente inviable e irreal.
- ❑ Posible aplicación a corto y medio plazo o medida extrema en el caso de información de gran importancia e imposibilidad de migrarla a un nuevo entorno tecnológico actualizado.



Preservación de la tecnología

Principales críticos de esta estrategia:

Jeff Rothenberg y Terry Cook.

"La probabilidad de conseguir que una pieza de la maquinaria continúe funcionando durante décadas no es muy elevada; ya que los recambios, chips y software serían difíciles de reproducir. Un sistema informático es mucho más complejo que una máquina de vapor" (Terry Cook).



La emulación

Parte la posibilidad de poder recrear la apariencia y la funcionalidad originales de un objeto digital mediante la utilización de aplicaciones que imiten (emuladores) el funcionamiento de los programas (*software*) originales con los que fueron creados cuando éstos están ya obsoletos.

Principal defensor *Jeff Rothenberg*.



La Emulación

Crítica

- ❑ Conservar emuladores de cada software no tiene sentido, pues también se quedarían obsoletos.
- ❑ Debemos conservar asociado al objeto la información necesaria para saber como desarrollar un emulador que permita leerlo.



La emulación

- El objeto y su entorno *software*, consiste en la suma de:
 - *el objeto digital.*
 - *los ficheros que representan la cadena de bits ejecutable original que permitía reproducir el objeto.*
 - *los ficheros que representan la cadena de bits del sistema operativo que permitía que se ejecutase el software.*



La emulación

- ▣ La explicación en un formato comprensible permanentemente del *software* y *hardware* emulado, el ciclo de vida del objeto, su contexto de creación, etc. (*Fichero leame con las instrucciones para el proceso de abrir y poner en marcha el objeto encapsulado*).
- ▣ El emulador de la plataforma informática original. (*No se trata de un programa ejecutable, sino de la especificación de los atributos tecnológicos considerados relevantes para la recrear el comportamiento del objeto original*).



La emulación

- Proceso:

Anotación



Encapsulación



Transliteración



Emulación

Crear las explicaciones sobre el contexto del documento y sobre cómo abrir y usar la encapsulación.

Construir una estructura lógica que contenga todos los elementos citados.

Actualizar periódicamente las anotaciones textuales para mantenerlas inteligibles.

Abrir la encapsulación, crear el emulador específico y hacerlo funcionar en el ordenador futuro.

Se creará un emulador para cada formato de objeto, no para cada objeto.



La migración

Transferencia periódica de materiales digitales de una configuración de *hardware* / *software* a otra o de una generación de tecnología a la siguiente.

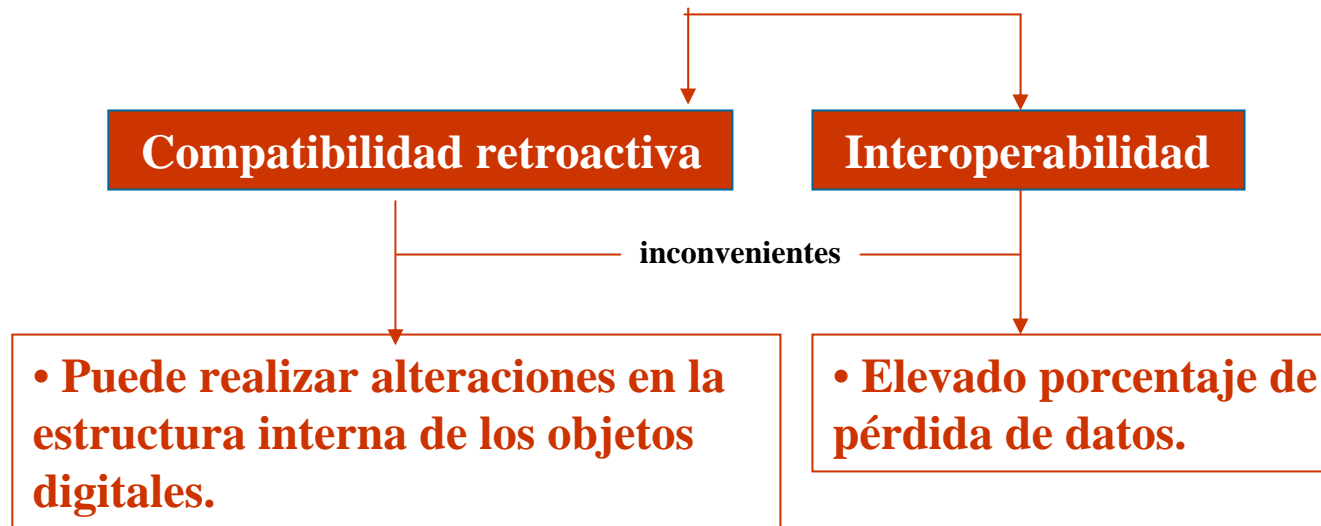
Se trata de la solución más aceptada.

- ▣ Objetivo: que los objetos digitales sean accesibles por los sistemas informáticos existentes en cada momento, es decir, que los usuarios puedan recuperar, presentar y usar estos objetos independientemente del constante cambio de la tecnología.
- ▣ Solución: migración periódica de éstos a formatos inteligibles por los sistemas actuales.



La migración

Estrategias de migración



La migración

Problemas:

- ❑ Resulta caro (en recursos materiales y humanos), laborioso y lento.
- ❑ Conlleva riesgos de pérdida de datos:
 - Bien por errores de grabación.
 - Bien por incompatibilidades entre formatos.
- ❑ Cada migración presenta una problemática distinta, pues el curso de la tecnología y su ritmo de obsolescencia son imprevisibles.



La migración

Jeff Rothenberg, hace falta alguna investigación que “prediga acertadamente cuando será necesaria hacer una migración, cuánta reforma será necesaria y cuanto costará realizarla”.



La migración

Recomendaciones generales ante la migración

- ❑ Identificar en cada tipo de documento electrónico los componentes que garanticen la autenticidad a largo plazo.
- ❑ Evaluar si los elementos invisibles pueden hacerse visibles y estabilizarse
- ❑ En los casos de no poder migrar en condiciones seguras, evaluar el pasar a otro soporte, ej, microfilm.
- ❑ Adoptar los procedimientos de autenticación automatizados y bien documentados.



La conversión

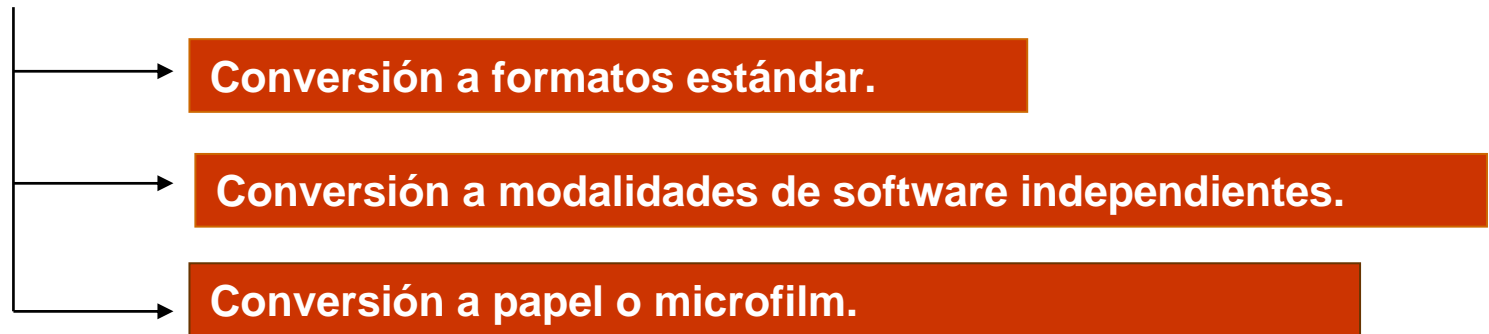
Diseñada para resolver tres retos:

- La gran variedad de paquetes *software* y formatos de almacenamiento en uso.
- La rápida sustitución del software por nuevas aplicaciones.
- La dependencia del software de muchos objetos digitales.



La conversión

Tres tipos de estrategias de conversión



La conversión

A formatos estándar.

- Utilización de formatos no propietarios que pueden exportar, y por tanto garantizar la conservación, de los objetos digitales sin una pérdida sustantiva de la funcionalidad del software. (*Margaret Hedstrom*)
- En la actualidad los formatos preferidos se construyen sobre la base de metalenguajes como SGML o XML.



La conservación: conversión

A formatos estándar.

Críticos:

- ▣ *Jeff Rothenberg* se trata de un “método útil intermedio, mientras se está desarrollando una solución a largo plazo”.
- ▣ *David Bearman*, “aún no existen métodos informáticos estándar que demuestren ninguna probabilidad de ser válidos siempre; en realidad, muchos de ellos han quedado completamente obsoletos en el transcurso de un par de generaciones de software”.



La conversión

A modalidades de *software* independientes.

- ▣ Consiste en convertir los objetos digitales a formatos “planos” independientes del *software* (texto simple ASCII).

Ventaja: se transfieren los objetos digitales fuera de una modalidad de software dependiente. Asegurando su accesibilidad por largos períodos de tiempo.

Inconveniente: la pérdida de códigos usados para la representación o formato del documento.



La conversión

A papel o microfilm

Consiste en crear copias de los objetos digitales en papel o en microfilm ya que estos soportes son más estables químicamente que los soportes digitales.

Ventaja: conserva la accesibilidad al contenido.

Inconveniente: pierde las funcionalidades del objeto digital original.



La conversión

A papel o microfilm

Críticos:

“tratar de imprimir cualquier documento que no sea sencillo o tradicional produce la pérdida de su única funcionalidad y además, imprimir estos documentos hace que dejen de ser susceptibles de lectura por ordenador, lo que a su vez hace desaparecer los atributos digitales (copia perfecta, acceso, distribución,...). Por encima de esta pérdida de funcionalidad, los documentos digitales impresos sacrifican su forma original, que puede ser de interés histórico, contextual y evidencial” (*Jeff Rothenberg*)



4.9.6. Organismos que trabajan en el ámbito de la preservación de los documentos electrónicos.

- ❑ DLM-FORUM <http://europa.eu.int/ISPO/dlm/>
- ❑ Proyecto INTERPARES <http://www.interpares.org/>
- ❑ European Commission on Preservation and Access
<http://www.knaw.nl/ecpa>
- ❑ The EROS project (Public Record **Office**).
<http://www.nationalarchives.gov.uk/recordsmanagement/>
- ❑ Council on Library and Information Resources:
<http://www.clir.org>



4.9.6. Organismos que trabajan en el ámbito de la preservación de los documentos electrónicos.

- ❑ Research Library Group: The Commision on Preservation access: <http://www.rlg.org>
- ❑ The preservation of the integrity of electronic records (UCB)
<http://ucblibraries.colorado.edu/dean/strategicplan.htm>
- ❑ Victoriam electronicis records strategy (VERS)
<http://vers.imagineering.com.au/>
- ❑ El Archivo Nacional de Australia <http://www.naa.gov.au/>

