



Sesión para iniciarse en la administración electrónica

Juan Arana Pérez

Coordinador Administración
Electrónica Universidad de Zaragoza

juan.arana@unizar.es
@tramita_unizar



Objetivos

- **Pedir el certificado electrónico de administración pública.**
- **Autofirma. Descargar e instalar una aplicación de firma en PC-MAC**
- **Firmar con Autofirma**
- **Firmar con circuitofirmas.unizar.es**
- **Trasladar certificado entre ordenadores. Copia de seguridad de un certificado**
- **Punto General de Acceso. administracion.gob.es**
- **Dónde está la documentación de la universidad**

AYUDAR A DIFUNDIR la administración electrónica para usos personales y profesionales

Documentación

www.unizar.es

> Sede electrónica 

www.unizar.es > Sede Electrónica (I sombreada) > Formación

Presentación:

http://sededocumentacion.unizar.es/curso/eadmin_sesion_1_hora.pdf



academico.unizar.es/cds/cds

>

Firma electrónica de actas



Almacenes de Certificados - Windows

- Internet Explorer
- Chrome

- Mozilla

- Formato .pfx
.p12 (disco,
pendrive)
- Depósito
Servidor-UNIZAR



Certificado electrónico

04. Técnicas

Resumen (hash)

Cifrado

Certificado electrónico

05. Criptografía. Resumen (hash) / 1

Ejemplo 1:

mas consiguen quintaesencias que farragos (*Baltasar Gracian*)

Resumen: Frecuencia de letras

abcdefghijklmnopqrstu
vwxyz_
502041203000142022513000004

Ejemplo 2 (DNI)

17123654 Q

Ejemplo 4 (código IBAN bancario)

ES65 2085 0176 9900 0012 3456



Certificado electrónico

06. Criptografía. Resumen (hash) / 2

Algoritmos de Resumen más frecuente utilizados

MD5
SHA1
SHA256

Probarlo en:

<http://onlinemd5.com/>

Certificado electrónico

07. Criptografía. Cifrado / 1

Algoritmos de Resumen más frecuente utilizados

ABCDEFGHIJKLMNÑOPQRSTUVWXYZ_
1234567890123456789012345678

Mensaje: HOLA MUNDO

Clave: 439871

Transformación:

HOLA MUNDO [+] 4398714398 -> LRTIGNYPMW

Desencriptar (su mando la clave complementaria o restando la clave inicial):

24 25 19 20 21 27



Certificado electrónico

08. Cómo funciona



Resumen SHA 256

F37D6C1D1B76797C69FC274BD3491
166368DEEA341FE8786F9F23D1F6C8
7D386

Encriptación RSA
(clave privada del
certificado)

C0A1FDE13BF933146367D45135B524
18B3C2F8AA891EED13D87E564AF1C
A1D64



Fin