CERTIFICADOS ELECTRÓNICOS

los cimientos de la seguridad

SAPaC

Miguel Macías Enguídanos

SUETONIO
s. II d. C.

Los Doce Césares

… si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.

Para los negocios secretos utilizaba una manera de cifra que hacía el sentido ininteligible, estando ordenadas las letras de manera que no podía formarse ninguna palabra; para descifrarlas tiene que cambiarse el orden de las letras, tomando la cuarta por la primera, esto es D por A, y así las demás

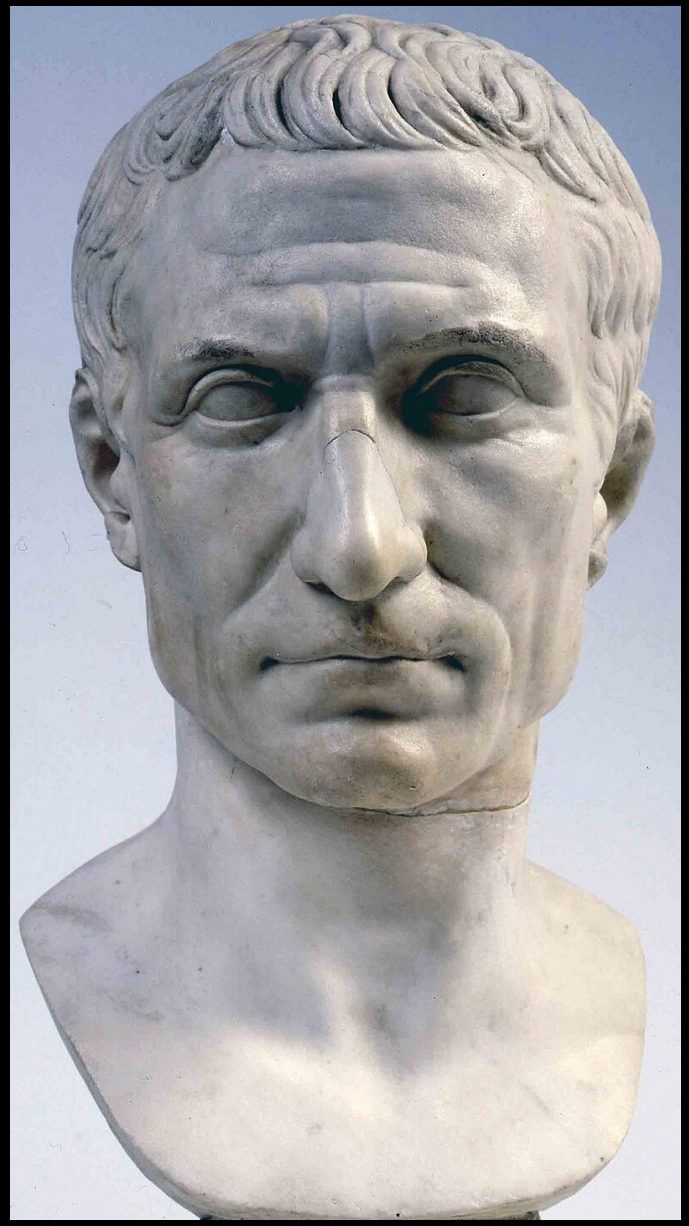
Z A B C D E F

Z A B C D E F

Cayo Julio César
s. I a. C.

CIFRADO

FLIUDGR



Autor desconocido
Musei Vaticani

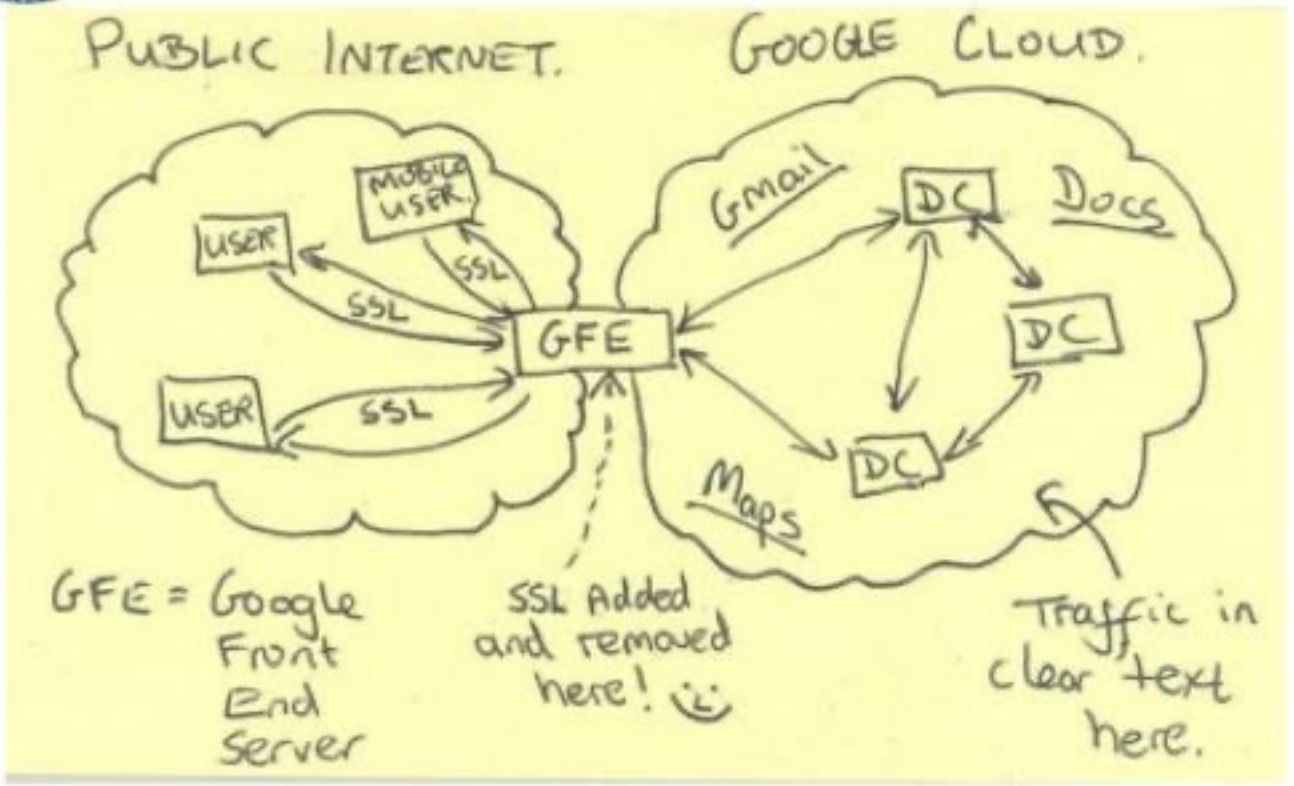
Huawei: por qué algunos países prohíben la tecnología 5G del gigante chino y cuáles son los temores de espionaje

Tim Bowler
Periodista de Negocios de la BBC

15 julio 2020

https://www.bbc.com/mundo/noticias-53413017

Current Efforts - Google



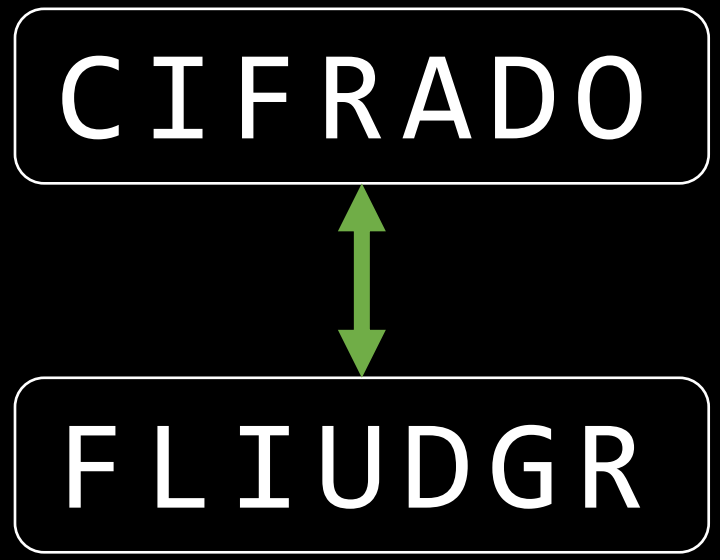

1
Los mensajes y las llamad
cifrados de extremo a extremo. Nadie fuera de este chat, ni siquiera WhatsApp, puede leerlos ni escucharlos. Pulsa para obtener más información.
Hola 6:28

ANDY GREENBERG SECURITY FEB 7, 2024 9:00 AM

Ransomware Payments Hit a Record $1.1 Billion in 2023

After a slowdown in payments to ransomware gangs in 2022, last year saw total ransom payouts jump to their highest level yet, according to a new report from crypto-tracing firm Chainalysis.

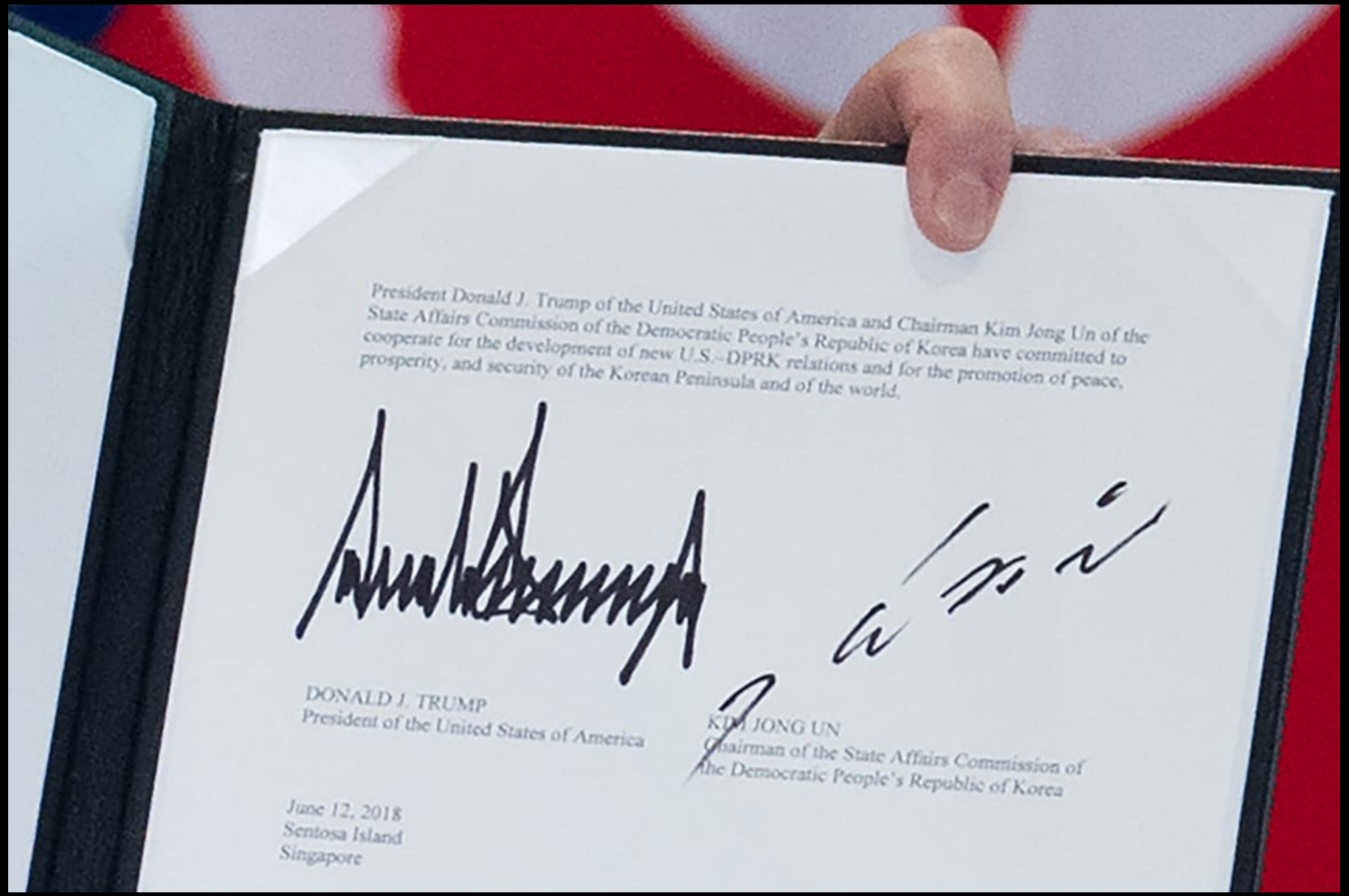
https://www.wired.com/story/ransomware-payments-2023-breaks-record/


CIFRADO
FLIUDGR

Copilot
Microsoft

Alejandro IV
s. XIII d. C.

Bula Papal



https://www.politico.eu/article/kim-trump-statement-full-text-signed/

DNI ELECTRÓNICO 4.0

NATIONAL eID 4.0

ANVERSO / FRONT

Parche Holográfico
DOVID

Tinta Ópticamente Variable
Optically Variable Ink

Ventana Transparente con Grabado Láser
Laser Engraved Clear Window

Embosados en Alto Relieve
Raised embossing

Fondos Offset de Seguridad
Offset Security Background

CLI en bajo relieve
Inlaying CLI

Foto más grande
Extra Large Photo

CAN
CAN

Tintas UV
UV Inks

REVERSO / REVERSE

Tinta Ópticamente Variable
Optically Variable Ink

Microtextos
Microlettering

Chip de Interfaz Dual
Dual Interface Chip

Tintas UV
UV Inks

divisiondedocumentacion@policia.es

soy A

certificado electrónico

https://forococoches.com/foro//showthread.php?p=472784138

… tengo certificado digital y puedo acceder perfectamente a las áreas personales de la Aeat, seguridad social, Dtg, pero no soy capaz de que reconozca dicho certificado, en ningún trámite del registro online de Registradores.org, (registradores de España).
Me sale una pantalla que indica " certificado electrónico no válido "

Desconecto el antivirus, limpio cookies, desactivo VPN...nada vale para solventar el problema.

Desinstala, y vuelve a instalarlo con el nivel máximo de seguridad. Te lo preguntará durante la instalación.

soy A

D

Período de validez

Propósito

Período de validez

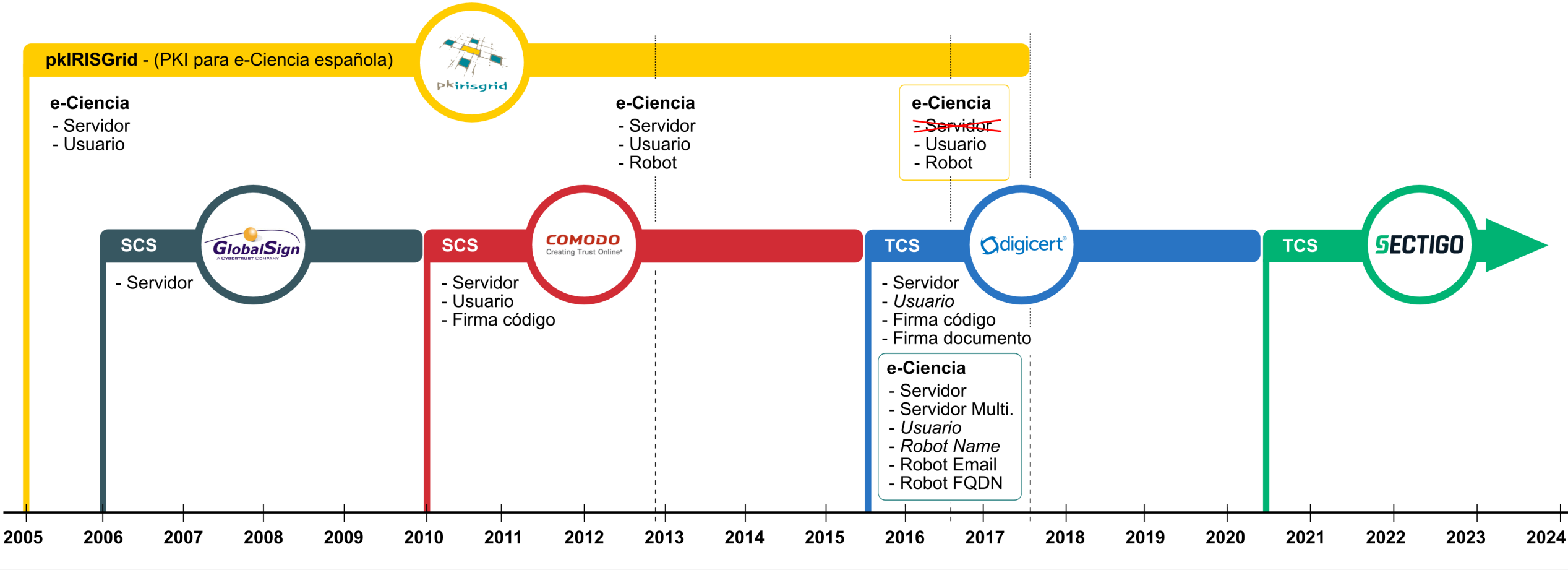
¿Es válido ahora?

Certificados

Propósito

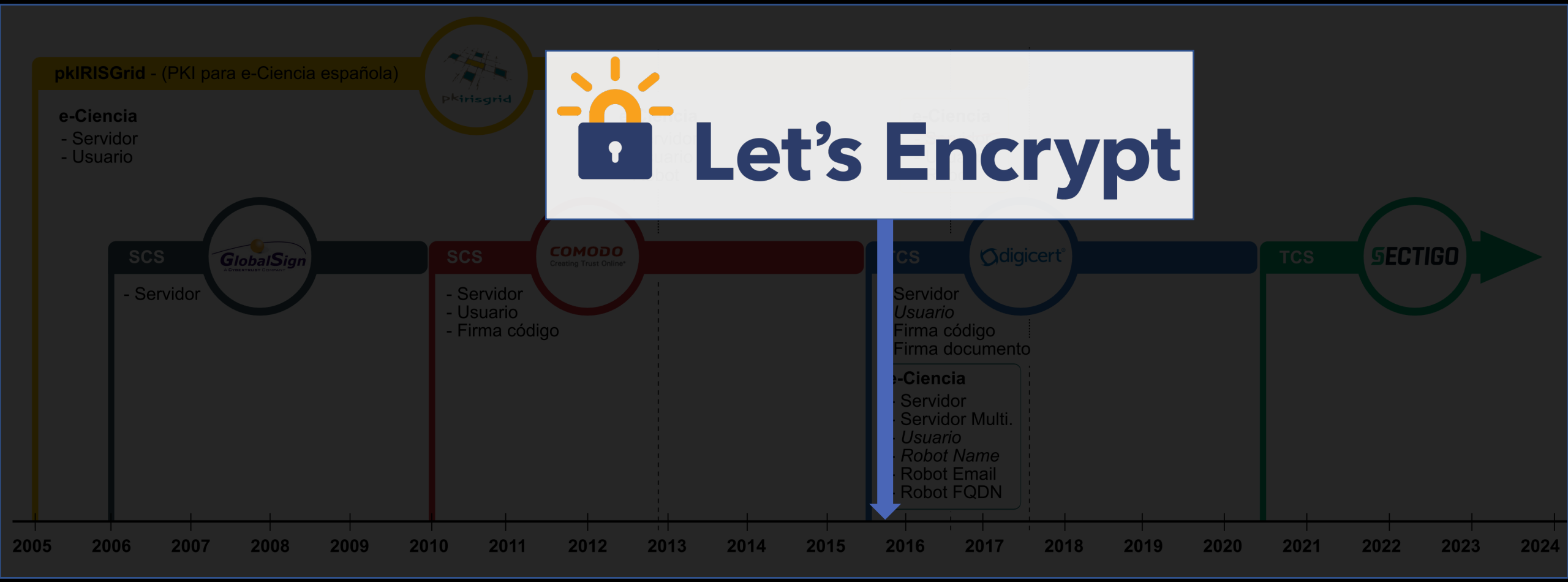
- de servidor
  - autenticidad de un servicio
- personales
  - administración electrónica
  - seguridad en el correo
- ...

TCS



https://www.rediris.es/tcs/caracteristicas/evolucion/

de servidor


pkIRISGrid - (PKI para e-Ciencia española)
pkirisgrid
e-Ciencia
- Servidor
- Usuario
Let's Encrypt
SCS
GlobalSign
- Servidor
SCS
COMODO
Creating Trust Online
- Servidor
- Usuario
- Firma código
CS
digicert
Servidor
Usuario
Firma código
Firma documento
e-Ciencia
Servidor
Servidor Multi.
Usuario
Robot Name
Robot Email
Robot FQDN
TCS
SECTIGO
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024

09/05/2024

8 208 708

certificados
de servidor

censys

09/05/2024

5 939 013

certificados de confianza

censys

09/05/2024

5 939 013

certificados de confianza

```
  4 M  Let's Encrypt

650 K  Google Trust Services LLC
434 K  Amazon
211 K  GoDaddy.com, Inc.
145 K  DigiCert Inc
135 K  Microsoft Corporation
109 K  ZeroSSL
 95 K  Sectigo Limited
 73 K  cPanel, Inc.
 17 K  IdenTrust
…
```

censys

731 143 637

certificados de servidor

```
375 M  Let's Encrypt

 82 M  GoDaddy.com, Inc.
 57 M  Amazon
 55 M  Google Trust Services LLC
 34 M  DigiCert Inc
 32 M  Sectigo Limited
 28 M  Cloudflare, Inc.
 27 M  Microsoft Corporation
 13 M  ZeroSSL
  7 M  cPanel, Inc.
…
```

censys

soy A

D

certificado
electrónico


TCS


SECTIGO®

TCS

SECTIGO®

certificados
corporativos

SECTIGO®

~~certificados corporativos~~

… Sectigo no está funcionando y es urgente que renovemos los certificados…

… bueno, los obtendremos de otra CA…

de servidor

OV

EV

95 %

personales

de firma de código

servicios expuestos

RDP

AS: RedIRIS

82 %

autofirmados

13 %

TCS

censys

SECTIGO®

digicert®

~~certificados corporativos~~

SECTIGO®

digicert®

~~certificados corporativos~~

Let's Encrypt

NOTA DE SEGURIDAD : La Sede Electrónica del Ayuntamiento de ... utiliza un certificado de servidor seguro que garantiza la confidencialidad y autenticidad de los datos y contenidos que se proporcionan. Es posible que al acceder a la misma aparezca alguna de las siguientes alertas de seguridad:

Internet Explorer

Firefox

Google Chrome

Si recibe alguna de estas alertas de seguridad, acceda a las siguientes Instrucciones de configuración

NOTA DE SEGURIDAD : La Sede Electrónica del Ayuntamiento de ... utiliza un certificado de servidor seguro que garantiza la confidencialidad y autenticidad de los datos y contenidos que se proporcionan. Es posible que al acceder a la misma aparezca alguna de las siguientes alertas de seguridad:

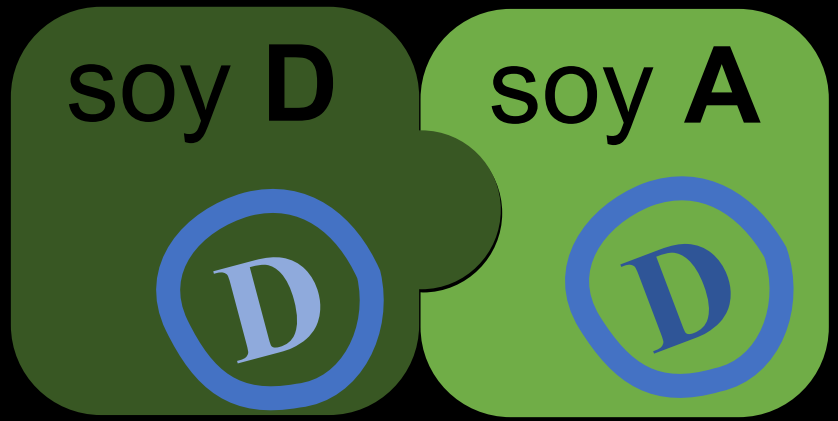
Internet Explorer

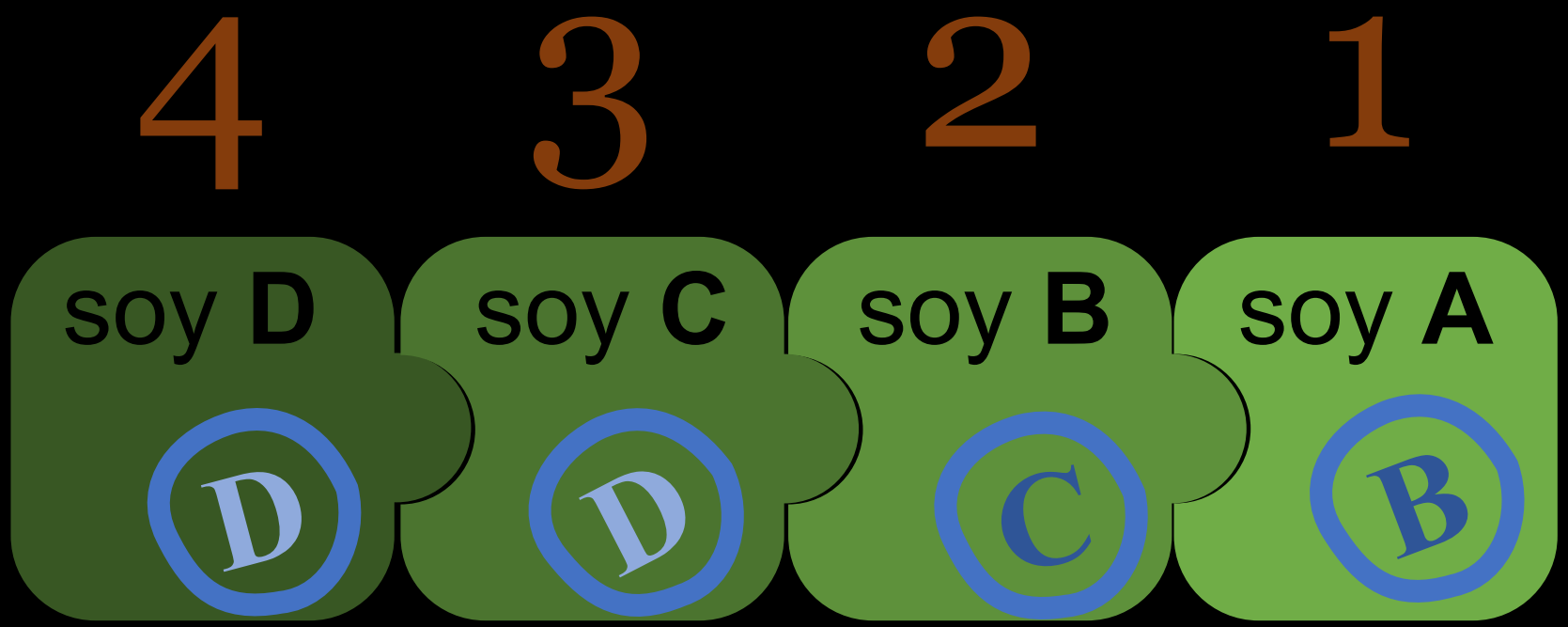
Firefox

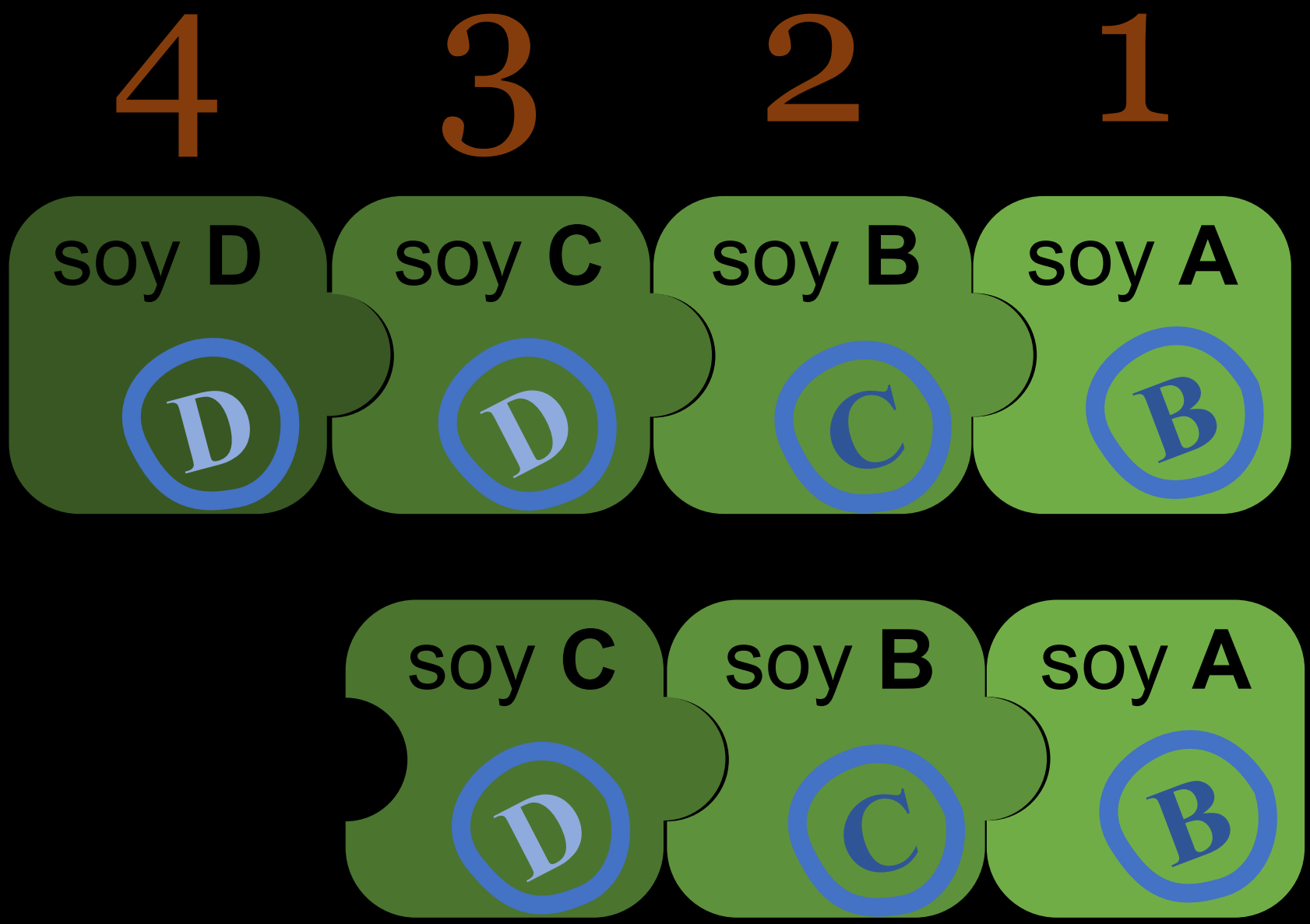
Google Chrome

Si recibe alguna de estas alertas de seguridad, acceda a las siguientes Instrucciones de configuración

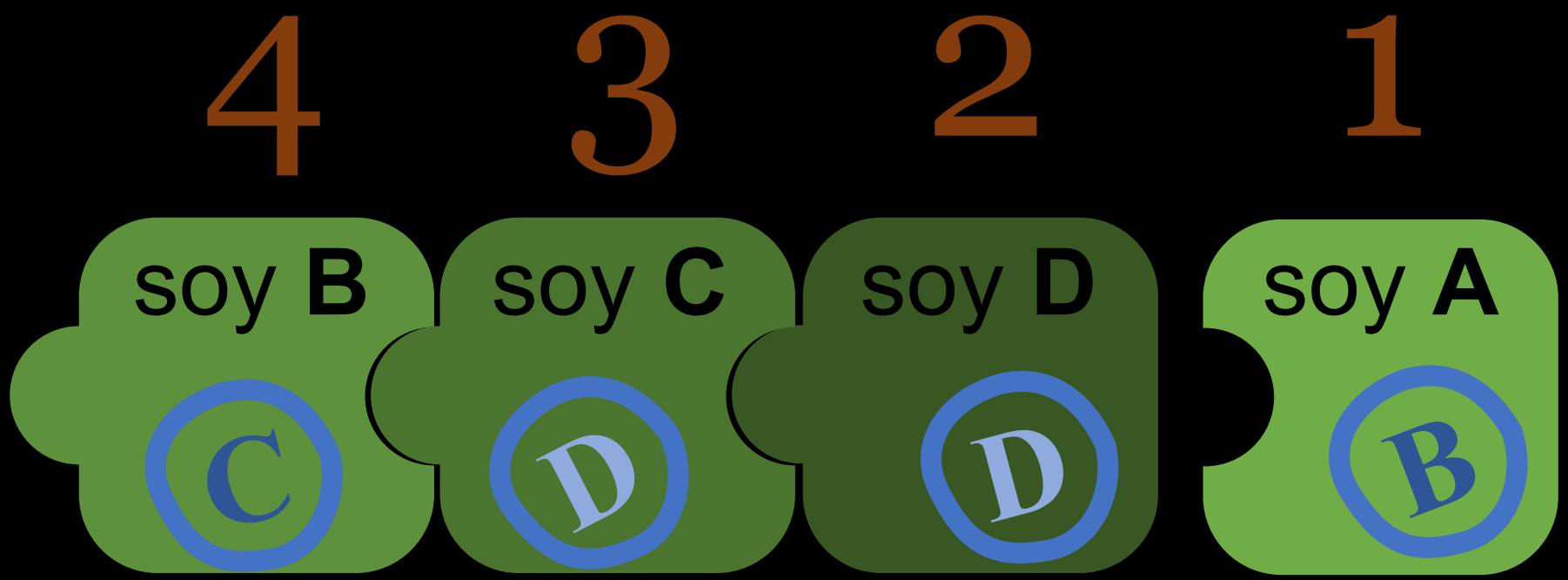
2 1



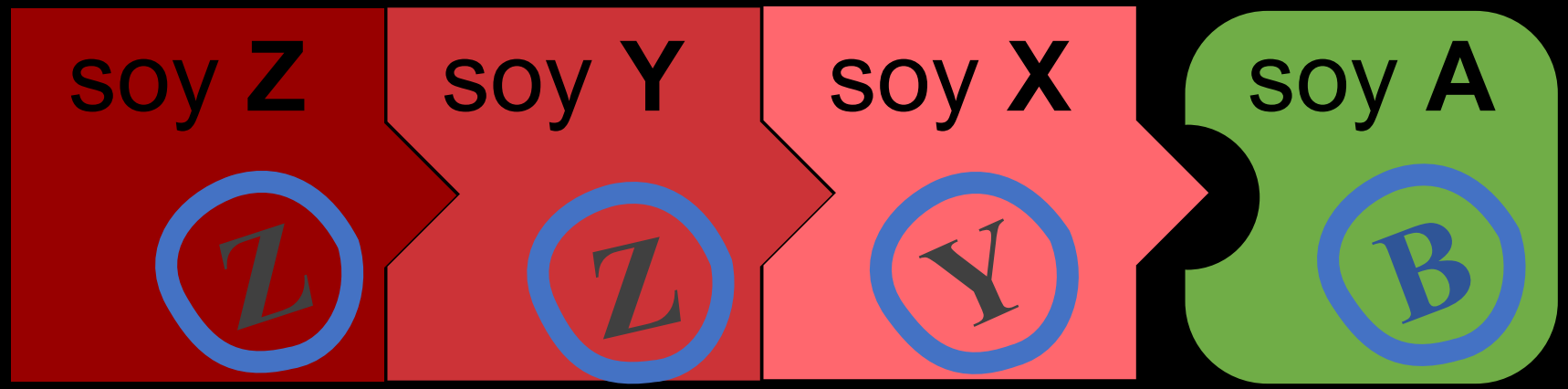

4
3
2
1
soy D
soy C
soy B
soy A
D
D
C
B


4
3
2
1
soy D
soy C
soy B
soy A
D
D
C
B
soy C
soy B
soy A
D
C
B

~~4~~ ~~3~~ ~~2~~ 1


4
3
2
1
soy B
C
soy C
D
soy D
D
soy A
B

4 3 2 1



emisor: GÉANT

468 307

servicios analizados

22 %

cadena errónea

censys

Descargar los certificados raíz de la Sede Electrónica

Para acceder a la Sede Electrónica sólo se requiere tener instalados en el navegador los siguientes certificados de seguridad de la AC Raíz de la FNMT Servidores Seguros:

- Certificado Raíz de la FNMT Servidores Seguros
- Certificado intermedio FNMT Servidores Seguros Tipo 1

4 690
certificados intermedios

```
594  The USERTRUST Network
513  DigiCert Inc
258  GlobalSign
178  GlobalSign nv-sa
142  QuoVadis Limited
123  SSL Corporation
117  Hellenic Academic and
     Research Institutions Cert.
     Authority
...
 20  Internet Security Research
     Group
...
```

censys

Nos ponemos en contacto para informarles de que a partir del próximo viernes 26 se actualizará el certificado utilizado en la Plataforma @firma para establecer la confianza HTTPs (dominio *redsara.es).

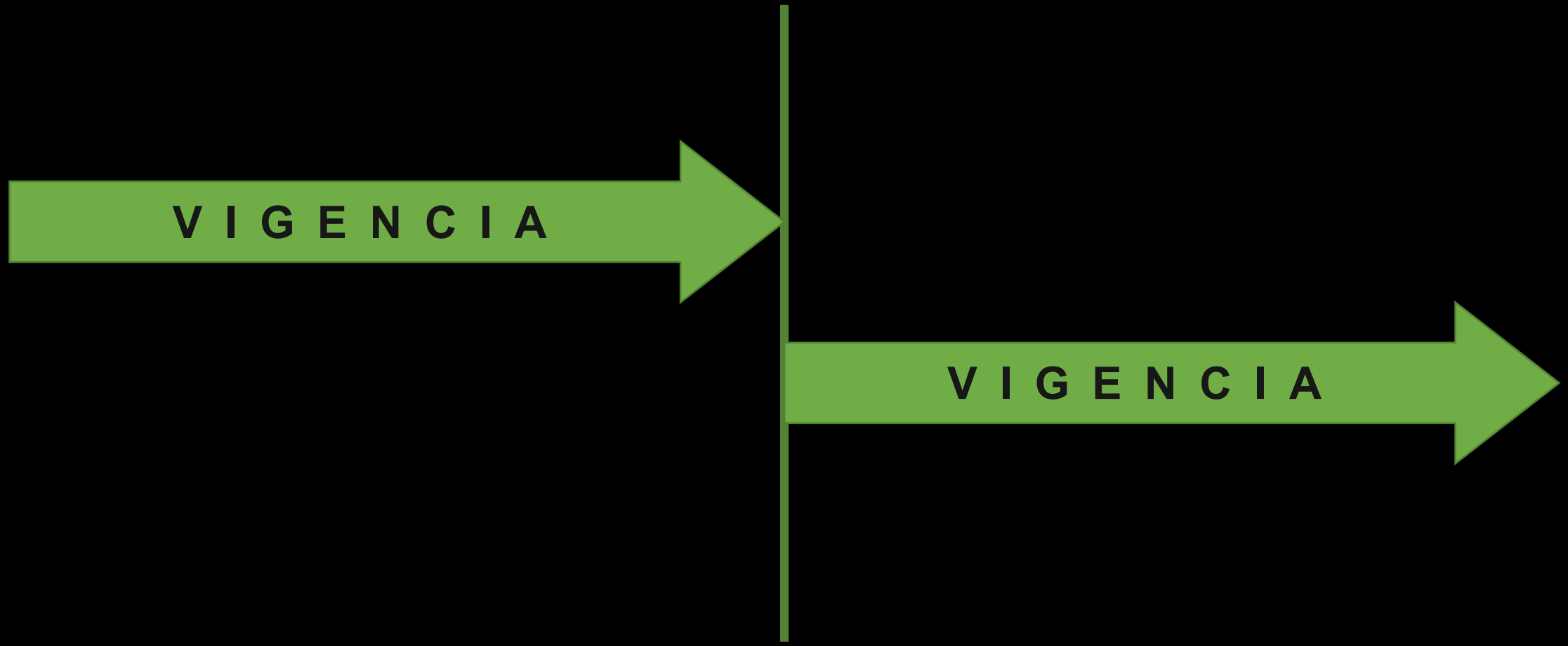
Este es un aviso para los responsables de las aplicaciones integradas con los servicios web de GEISER. Les informamos que el certificado de sitio web (.seap.minhap.es) caduca el próximo día 8 de marzo. *El nuevo certificado entrará en vigor el próximo lunes 7 de marzo a las 8:30 hora peninsular.

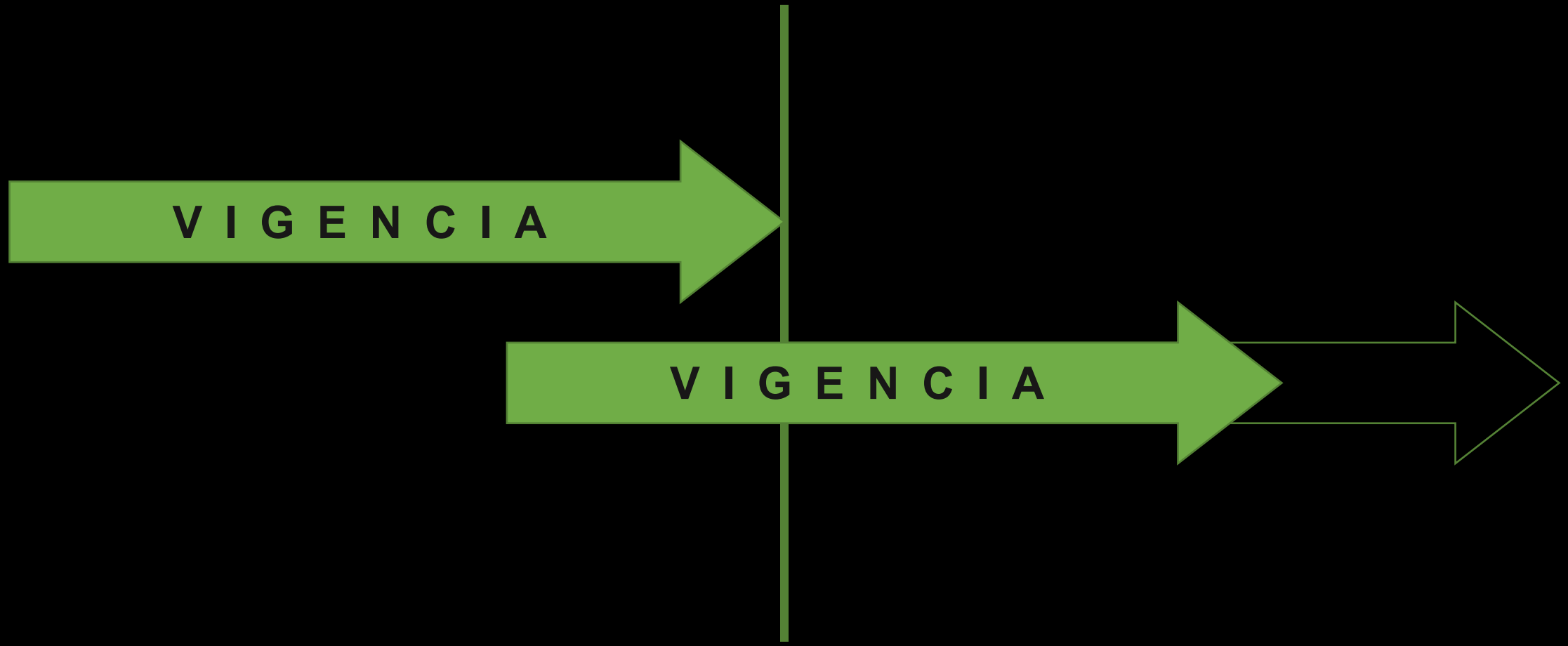
The **top 1000** most visited websites in the World

https://ahrefs.com/top

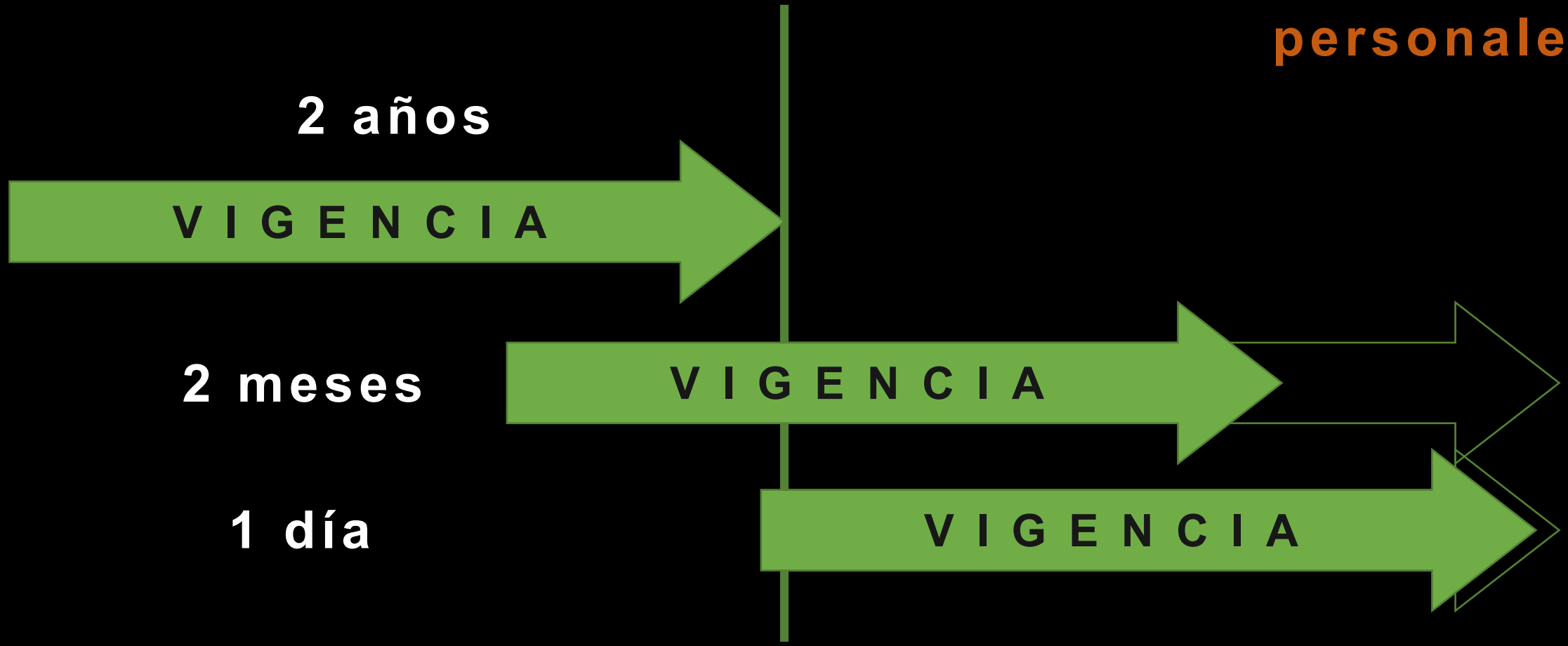
~ 30

cambios de certificados diarios

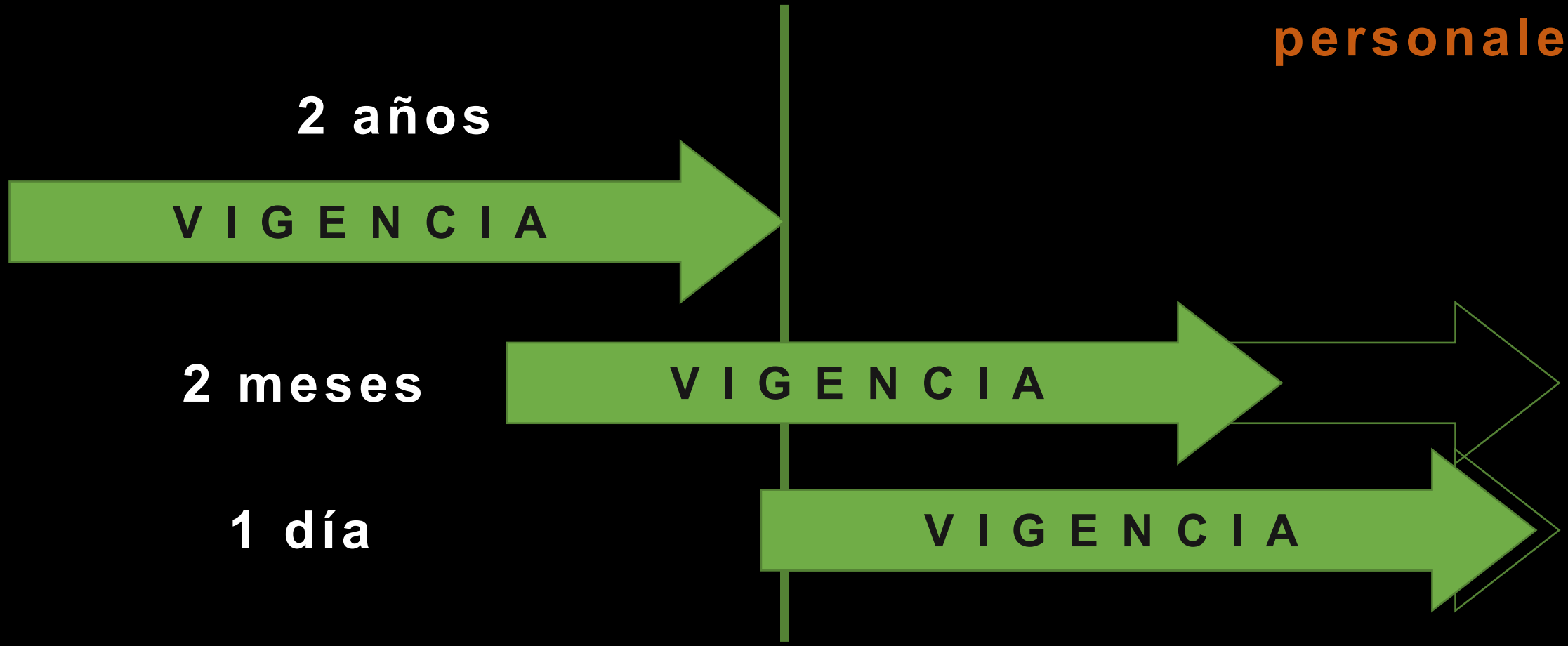

V I G E N C I A
V I G E N C I A


V I G E N C I A
V I G E N C I A

Certificados personales



Certificados personales



12 años

ahorro una renovación

servidor

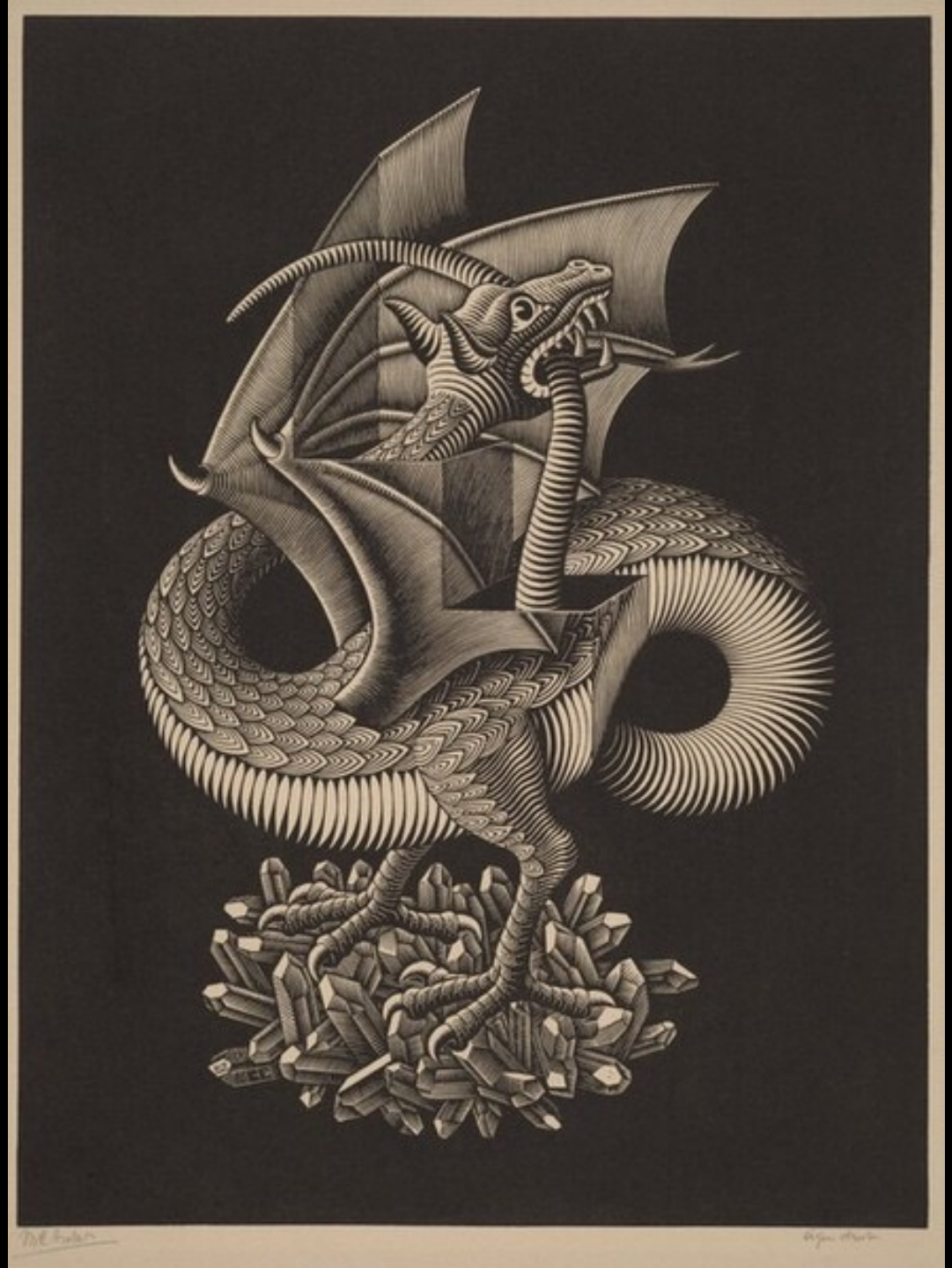
cliente

autor

lector

La firma de Schrödinger

1929 René Magritte



1952

M.C. Escher

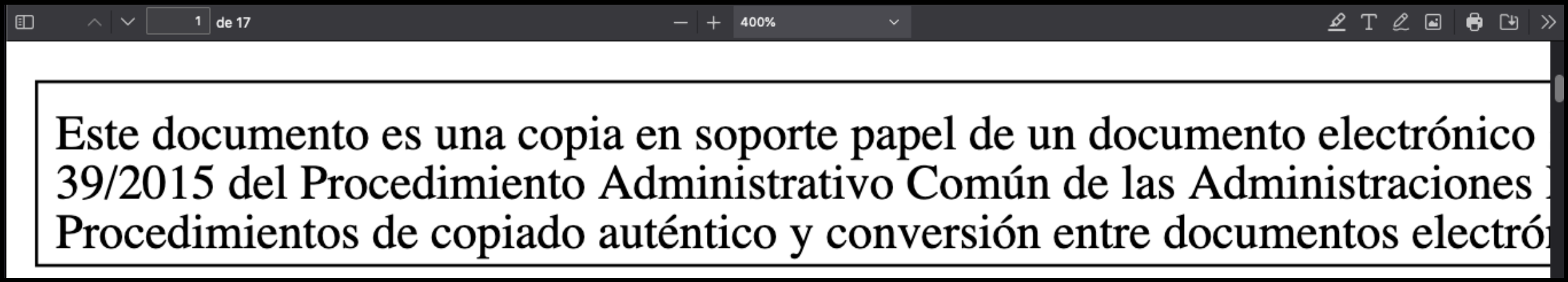
Aproximadamente ..... resultados (0,34 segundos)

Plataforma de Contratación del Estado
https://contrataciondelestado.es › wcm › connect

PDF

Documento firmado electrónicamente

20 feb 2024 — **Este documento** es una **copia** en soporte papel ...



2024 Administración electrónica

Documento firmado electrónicamente

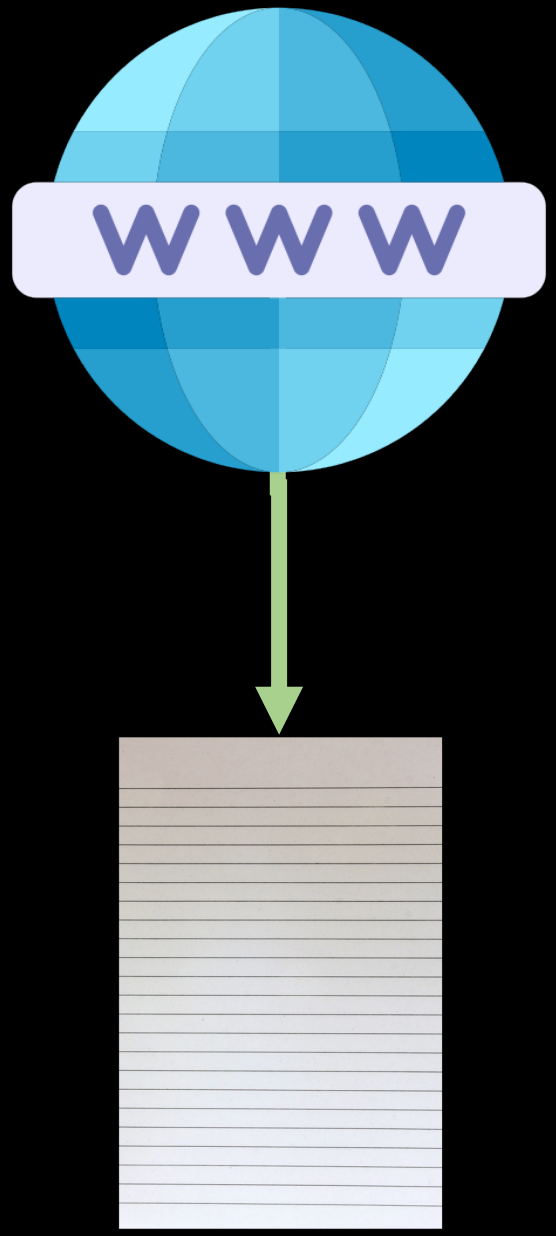
Firmado por	Fecha de firma	Sello de tiempo
MIG[redacted]MAS	18[redacted]38	18[redacted]41

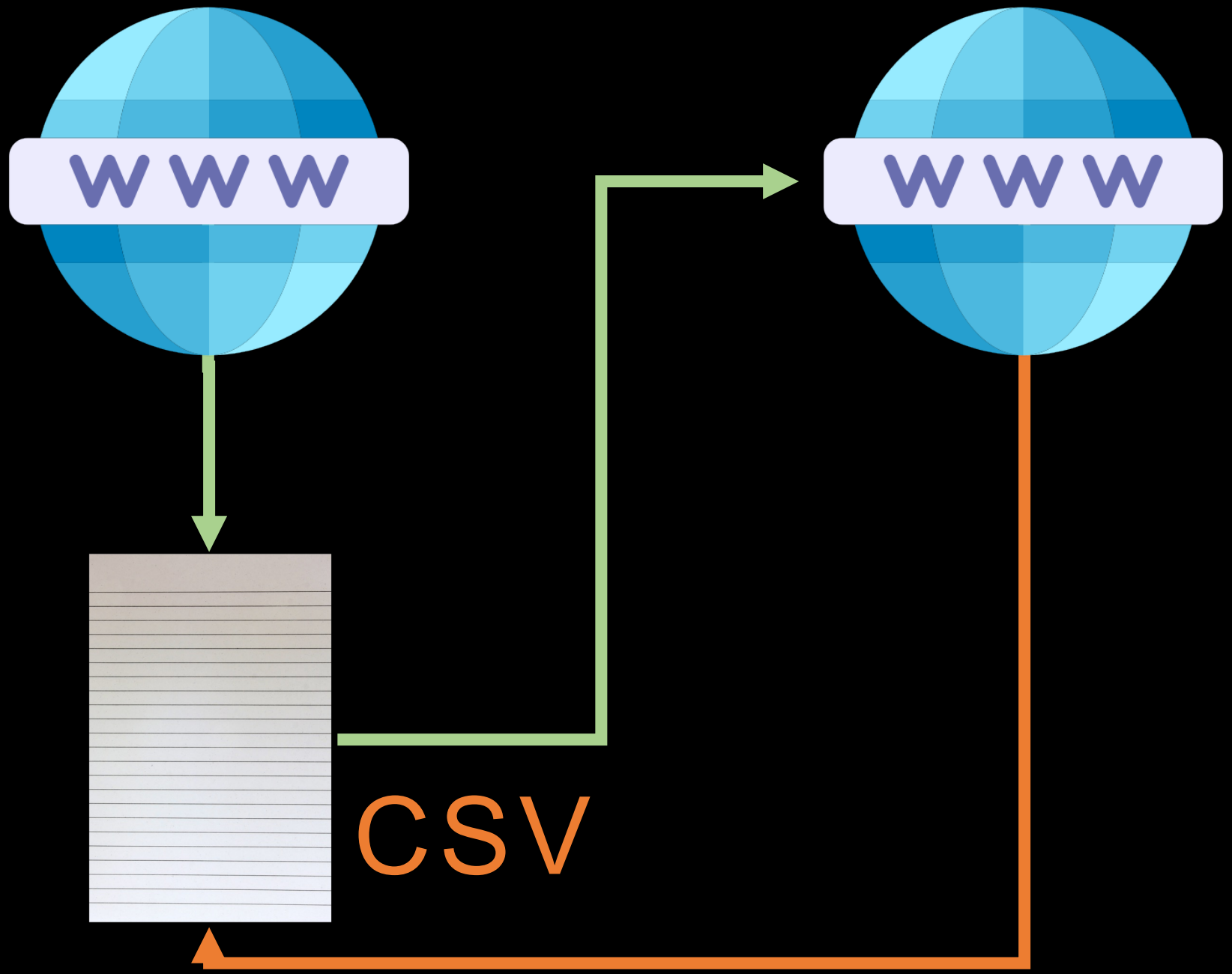
URL de validación	https://s[redacted]es https://p[redacted]sv

Código CSV

MA[redacted]3H

Este documento es una copia en soporte papel de un documento electrónico según lo dispuesto en el artículo 27 de la Ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas y la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos.


WWW


WWW
WWW
CSV

.gob.es VALIDe

Resultado de Validar Firma

Firma inválida

El formato de la firma no es válido

Descargar Justificante

Documento firmado electrónicamente

Firmado por	Fecha de firma	Sello de tiempo
MIG[redacted]MAS	18[redacted]38	18[redacted]41

URL de validación	https://s[redacted]es https://p[redacted]sv

Código CSV

MA[redacted]Q3H

Este documento es una copia en soporte papel de un documento electrónico según lo dispuesto en el artículo 27 de la Ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas y la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos.

FIRMADO

FIRMADO

Documento firmado electrónicamente

Firmado por	Fecha de firma	Sello de tiempo
MIG[redacted]MAS	18[redacted]38	18[redacted]41

URL de validación	https://s[redacted]es https://p[redacted]sv

Código CSV

MA[redacted]Q3H

Este documento es una copia en soporte papel de un documento electrónico según lo dispuesto en el artículo 27 de la Ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas y la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos.

La petición no es correcta. El formato de la firma no es válido

Recibí un golpe en el tobillo izquierdo,
pero algo me decía que era el derecho

Lee Hendrie
futbolista

Sociedad de Arqueometría Aplicada al Patrimonio Cultural

Miguel Macías Enguídanos
miguel.macias@sapac.es