



XIV JORNADA DE DIFUSIÓN DE LA MEJORA DE LA CALIDAD
DE LOS SERVICIOS QUE PRESTA EL PAS (GRA3622_1)

Ciberconsejos, y nuevas herramientas tecnológicas

gerardo.aburruzaga@uca.es

1 de 256

25-nov-2022



Universidad
de **Cádiz**

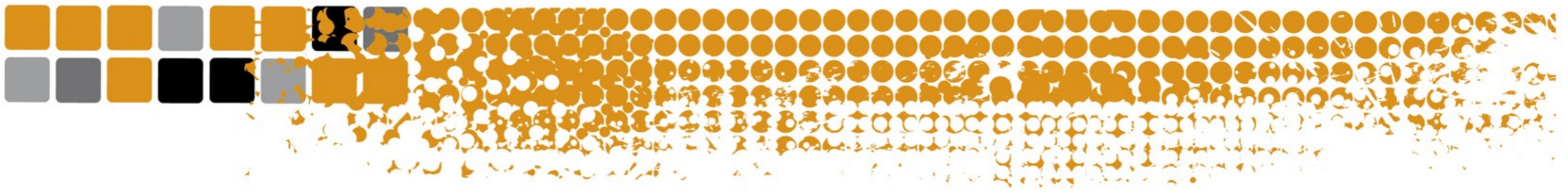
Parte 1: Ciberconsejos





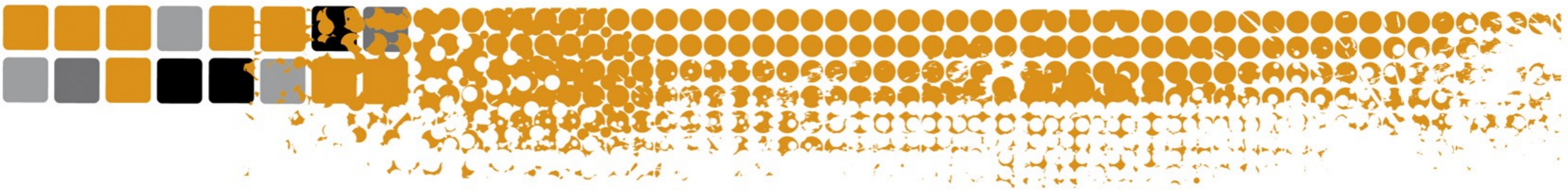
Contraseñas





¡Muchas gracias por
su atención!

gerardo.aburruzaga@uca.es
seguridad.informacion@uca.es
Área de Sistemas de Información
Edificio CITI



Admin

Utiliza siempre **contraseñas robustas**, difíciles de adivinar por otras personas y **nunca las compartas** o las pongas a la vista.

Consejo de Seguridad

crue
Universidades Españolas
TIC

Con el apoyo institucional de **incibe**
INSTITUTO NACIONAL DE CIBERSEGURIDAD

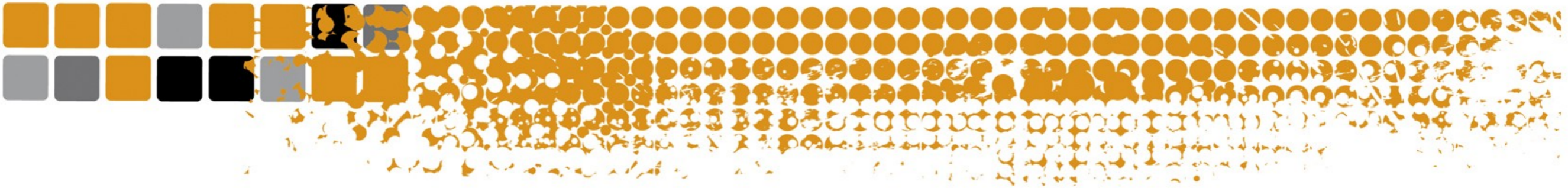


<https://nordpass.com/es/most-common-passwords-list/>

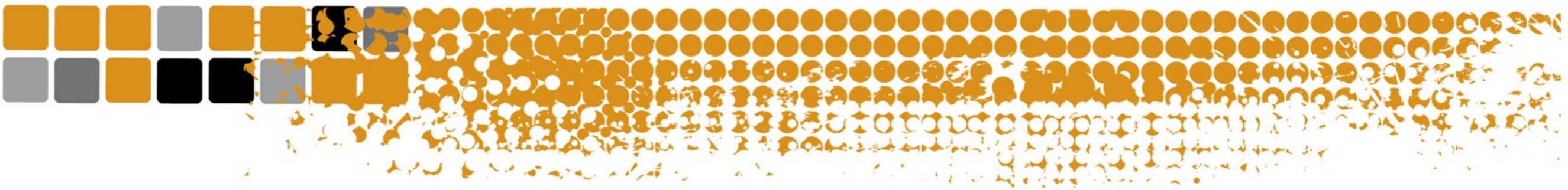
Resultados

España Consigue la lista de contraseñas de 2019-2021

RANGO	CONTRASEÑA	TIEMPO PARA DESCIFRARLA	RECUENTO
18	666666	< 1 Segundo	508
19	12345678910	< 1 Segundo	508
20	alejandro	3 Segundos	484
21	crisrina	3 Horas	475
22	realmadrid	< 1 Segundo	470
23	holahola	2 Segundos	457
24	tuputamadre	4 Meses	455
25	patata	2 Minutos	446
26	estrella	3 Horas	444
27	thiscrush	16 Horas	441
28	carmen	2 Minutos	437
29	Allom!	2 Minutos	422



Sanani123



Sanani123



\$5\$QXwTw4F0\$3UIAQuj.BpKI/c0e1tfAqT8yNMPP/HUPQaOAVOemDd5

hash



Propiedades del *hash*

1. Función de un solo sentido. Imposible obtener la contraseña a partir del *hash*.



Propiedades del *hash*

1. Función de un solo sentido. Imposible obtener la contraseña a partir del *hash*.
2. Misma longitud: depende del algoritmo, no de la contraseña.



Propiedades del *hash*

1. Función de un solo sentido. Imposible obtener la contraseña a partir del *hash*.
2. Misma longitud: depende del algoritmo, no de la contraseña.
3. Un pequeño cambio en la contraseña produce un *hash* totalmente distinto.

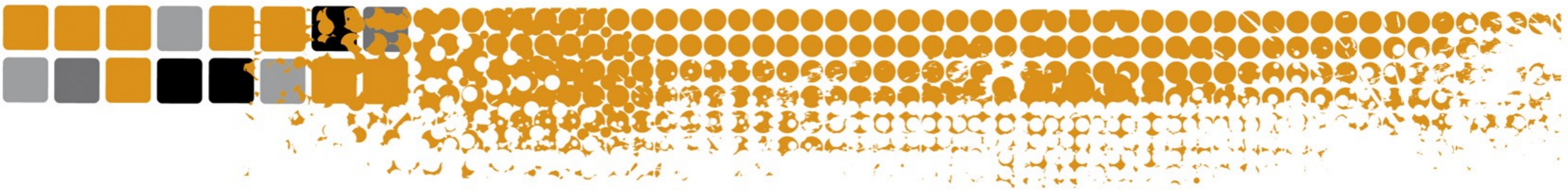


sanani123



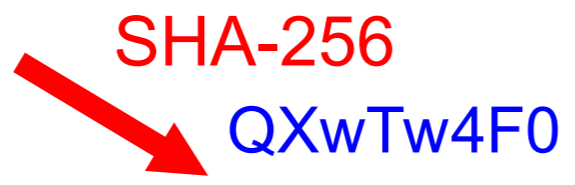
\$5\$QXwTw4F0\$p6rjYBNe15my.h54rt.Rt8Txmt1fp1MVBITmOHCIsQ.
\$5\$QXwTw4F0\$3UIAQuj.BpKI/c0e1tfAqT8yNMPP/HUPQaOAVOemDd5

hash



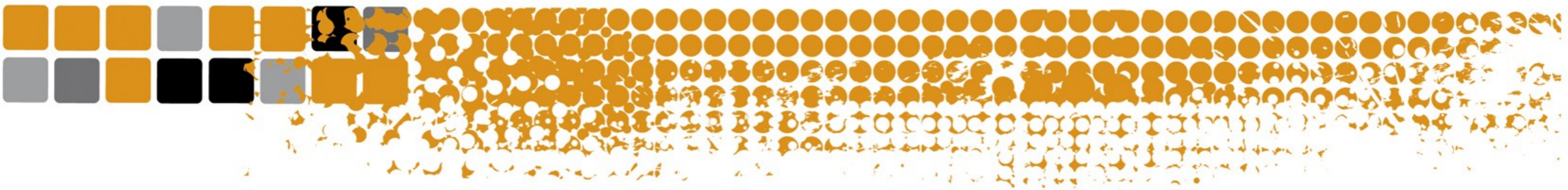
Ataque de diccionario

- 123456
- 12345
- password
- password1
- 123456789
- 12345678
- 1234567890
- abc123
- computer
- tigger
- 1234
- qwerty
- money
- carmen
- mickey
- secret
- summer
- ...



\$5\$QXwTw4F0\$3UIAQuj.BpKI/c0e1tfAqT8yNMPP/HUPQaOAVOemDd5

hash



Ataque de diccionario



```
john --format=sha512crypt \  
--wordlist=/var/lib/john/wordlists/all password.txt
```

~ 5 millones de palabras

Loaded 1 password hash (sha512crypt, crypt(3) \$6\$ [SHA512 128/128 AVX 2x])

Cost 1 (iteration count) is 5000 for all loaded hashes

Press 'q' or Ctrl-C to abort, almost any other key for status

zuiverheidsonderzoek (*pruebas de pureza*)

0:01:16:30 DONE



Ataque de fuerza bruta

Todas las combinaciones posibles.

Caracteres: 27 letras minúsculas + 27 mayúsculas
+ 10 dígitos + 11 signos = 75 caracteres

Longitud contraseña: de 4 a 8 caracteres

$$75^4 + 75^5 + 75^6 + 75^7 + 75^8 = 1,01 \cdot 10^{15}$$

Promedio: $\sim 5 \cdot 10^{14}$ (500 billones)



Contraseñas fuertes

5 recomendaciones

1. Larga

- a) Mínimo 10 caracteres (~ 4 meses fuerza bruta)
- b) Mejor 12 o más
- c) Con cada carácter de más el tiempo aumenta exponencialmente
- d) **8 O MENOS: SE ADIVINA CON UN PC EN UN TIEMPO RAZONABLE**



Contraseñas fuertes

<https://password.kaspersky.com/es>

Bdx&9[k/

⊗ ¡Hace tiempo que deberías haber cambiado la contraseña!

- Malas noticias
 - ⚠ Palabras de uso frecuente
- Tu contraseña no aparece en ninguna base de datos de contraseñas filtradas.



¡Ups! Pueden crackear tu contraseña antes, incluso, de que digas ¡Ups!



Contraseñas fuertes

<https://password.kaspersky.com/es>

<{(LjG)Tipfq)7

<{(LjG)Tipfq)7

14 caracteres

✓ ¡Buena contraseña!

- Tu contraseña es resistente al pirateo.
- Tu contraseña no aparece en ninguna base de datos de contraseñas filtradas.

Tu contraseña puede ser descifrada con un ordenador común en...

327 siglos



En ese tiempo puedes ir y volver a la Luna 1333 veces.





Contraseñas fuertes

5 recomendaciones

2. Mezcla

- a) Letras MAYÚSCULAS
- b) Letras minúsculas
- c) Dígitos 0123456789
- d) Símbolos </?&\$%;-_>.

Contraseñas fuertes

5 recomendaciones

faikahseiqueac

14 letras minúsculas

 ¡Es hora de cambiar la contraseña!

- Tu contraseña se puede crackear fácilmente.
 - ⚠ Palabras de uso frecuente
- Tu contraseña no aparece en ninguna base de datos de contraseñas filtradas.



Esta contraseña puede ser descifrada más rápidamente que el tiempo que se tarda en volver de un breve paseo



Contraseñas fuertes

5 recomendaciones

3. No información personal

- a) Nombres personales o de usuario
- b) Fechas señaladas
- c) Direcciones de correo
- d) Direcciones postales...



Contraseñas fuertes

5 recomendaciones

4. No solo mayúscula inicial

a) Mayúsculas aleatorias

b) No sustituciones típicas de dígitos

ill \rightarrow 1

aA \rightarrow 4

oO \rightarrow 0

B \rightarrow 8 ...



Contraseñas fuertes

Mi recomendación

1. Caracteres aleatorios
mezclados de longitud 14 o más

iV-UpEE, ?Y=, =1
:G9L, /g\$o8J0Ux
A\|jzuXa`=1#3=



Contraseñas fuertes

Mi recomendación

**2. 4 o más palabras de diccionario
separadas por algún símbolo,
longitud > 25**

**filete-absoluto-asohora-
camarroya-rebozo-apicultor**

Tengo_1_amatoma_muy_grande

Contraseñas fuertes

Mi recomendación

Tengo_1_amatoma_muy_grande

✓ ¡Buena contraseña!

- Tu contraseña es resistente al pirateo.
- Tu contraseña no aparece en ninguna base de datos de contraseñas filtradas.

Tu contraseña puede ser descifrada con un ordenador común en...

10000+ siglos



Puedes encontrar la respuesta al sentido de la vida, al universo y a todo lo demás sin tener que preocuparte de que alguien crackee tu contraseña



Contraseñas fuertes

5 recomendaciones

5. Gestor de contraseñas





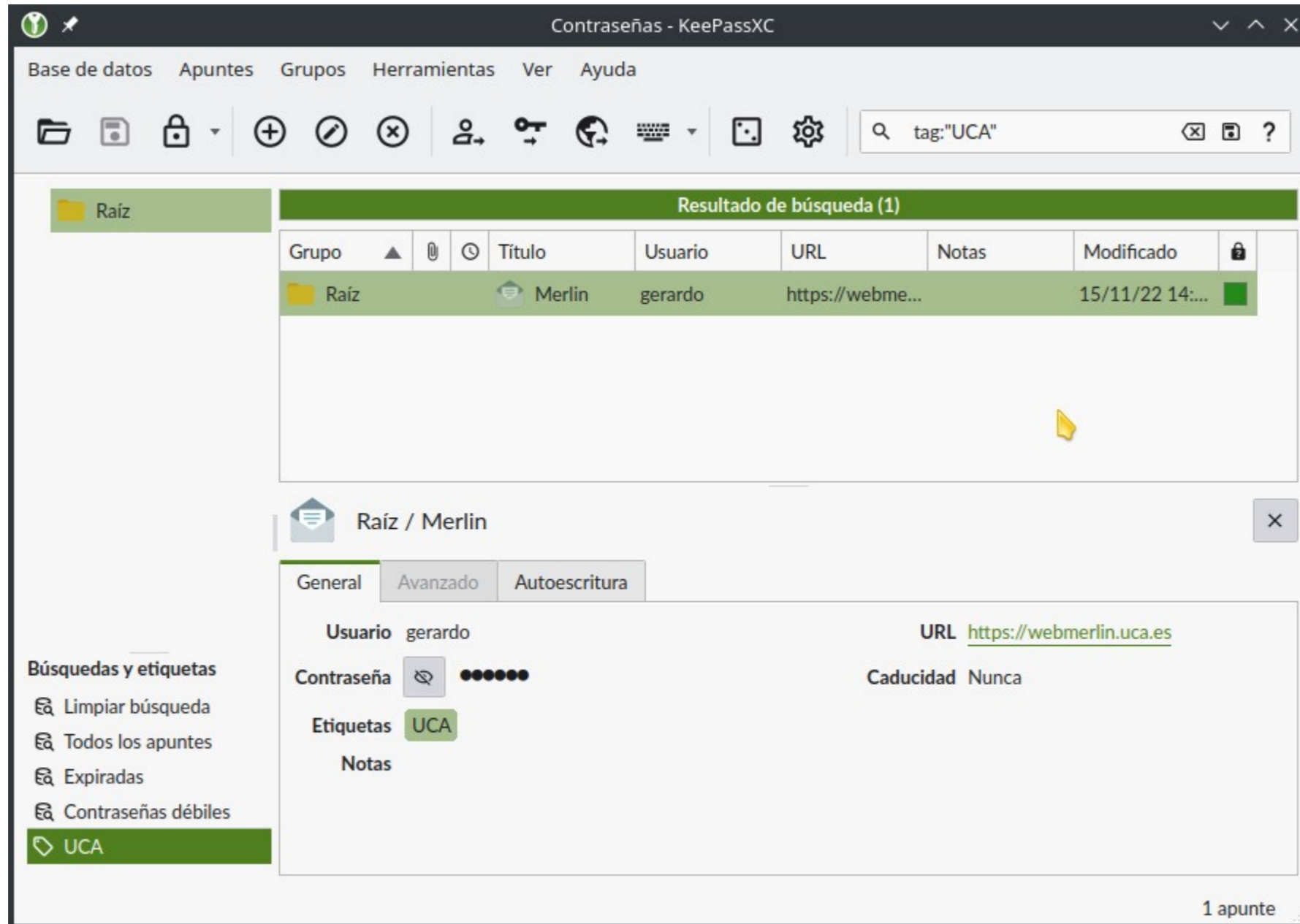
Gestores de contraseñas

Password managers

- Enpass
- Bitwarden
- LastPass
- 1Password
- Kaspersky Password Manager
- KeepassXC (DX)
- Nordpass

Gestores de contraseñas

Password managers



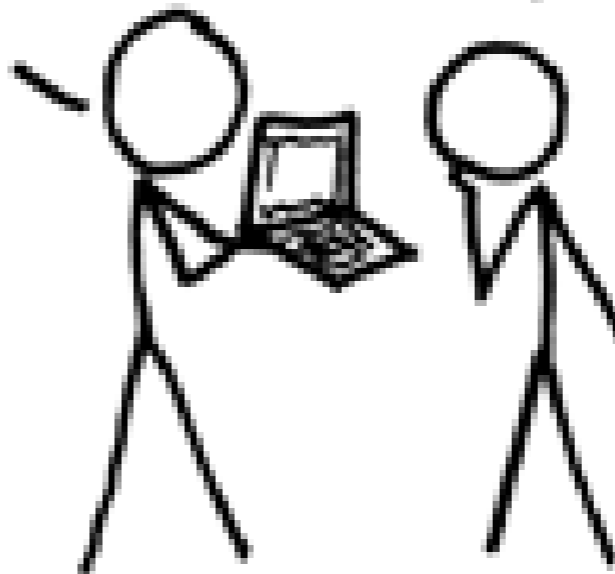


A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

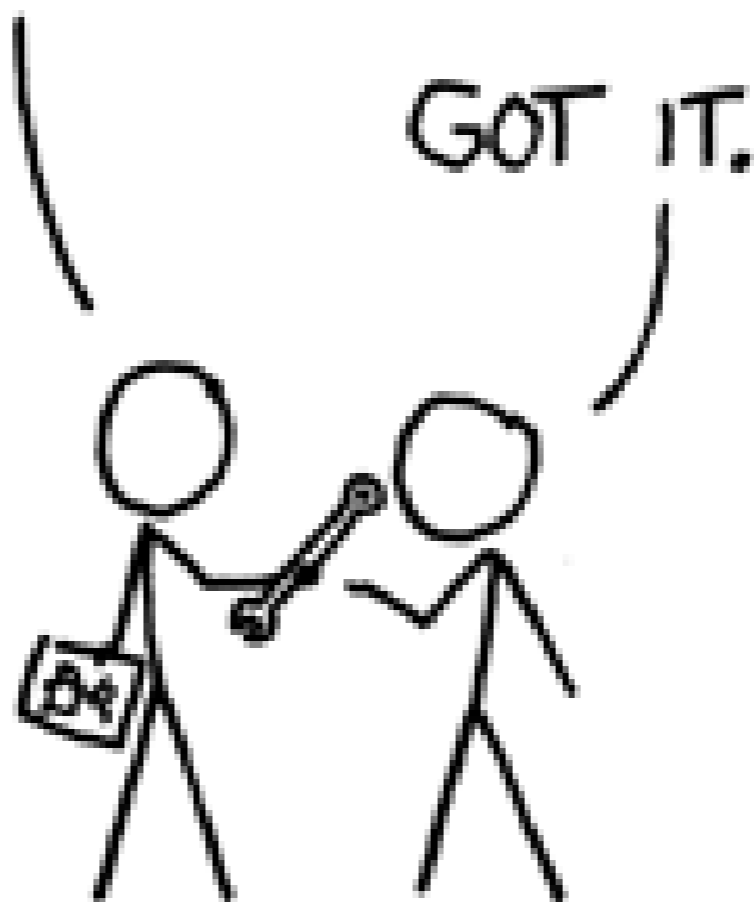
BLAST! OUR
EVIL PLAN
IS FOILED!

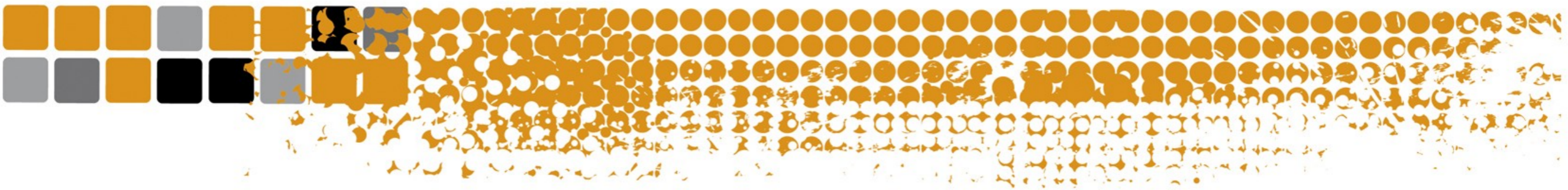
NO GOOD! IT'S
4096-BIT RSA!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.








PHISING



PHISHING: tipos

- *Spray and pray* (tradicional, gral.) 
- *Vishing* 
- *Qrishing* 
- *Smishing* 
- *URL phishing* <https://www.google.com>
- *Evil twin*  WIFI SSID: *cafeteriaECI*
- Etcétera



PHISHING



Seguridad / PDCON (1)

Carpetas:

- Entrada
- Salida
- AdmonElectronica
- Aplicaciones
- Actas
- AlojamientoAlgeciras
- AppCRUE
- Area_de_Personal
- Automatricula
- Becas_propias
- CAU
- CELAMA
- CeslonEspacios
- ColaboracionDocentePIF
- ColegioMayor
- Comision
- ConcursoMeritosPAS
- ContratacionPDI
- CRUE-HERCULES
- DG3E
- Discoverer-OBI
- Docentia_Calidad
- ECAIRO-LimOn
- Elecciones
- EncuestaEgresados
- eVotino

Cuota de disco:

(41,11 de 2250 MB 1 %).

Informe completo curso "Docker DCK-101"

Emisor: Lorena Valderrábano Blanco <lorena.valderrabano@cleformacion.com>

Destinatario: "Gerardo Aburruzaga Garcia" <gerardo.aburruzaga@uca.es>

CC: "Unidad de Formación" <formacion.personal@uca.es>

Fecha: 16 de noviembre de 2022 10:13:06

Fichero Ligado:

- INFORME_347-JESÚS SALINAS-UNI. CÁDIZ-09-NOV-2022.pdf
- DIPLOMAS_347-JESÚS SALINAS-UNI. CÁDIZ-09-NOV-2022.rar

Información Seguridad

Información Seguridad:

Emisor real: lorena.valderrabano@cleformacion.com

Camino del mensaje:

Host:	AM6PR04MB6197.eurprd04.prod.outlook.com	AM6PR04MB6197.eurprd04.prod.outlook.com	eur01-db5-obe.outbound.protection.outlook.com (40.107.15.81)	m0316693.pops.net	mx08-006a4e02.pphosted.com (143.55.148.243)	smtp22.uca.es (10.84.3.16)	buzon8.uca.es
Fecha:	16/11/2022 10:13:06	16/11/2022 10:13:06	16/11/2022 10:13:13	16/11/2022 10:13:16	16/11/2022 10:13:16	16/11/2022 10:13:17	16/11/2022 10:13:17

DomainKeys Identified Mail (DKIM): OK

Las cabeceras del email no han sido manipuladas y ha sido enviado correctamente desde el dominio: cleform.onmicrosoft.com

Sender Policy Framework (SPF): OK

El emisor está autorizado a enviar mensajes del dominio

Buenos días Gerardo,

Adjunto envío el informe completo del formador y los certificados de asistencia correspondiente al curso "Docker DCK-101" impartido los días 3.4.8.9 de noviembre.

Además, envío el link con el resultado de las valoraciones de los alumnos al curso: https://forms.office.com/Pages/AnalysisPage.aspx?AnalyzerToken=8yy0ZcVjix5mbGfZFBqEZ2LrCdkXVXO&id=5qiWSofdekqMkaEm2h1qfz0rT8n3TPdHviaVHBY6fVRUREpGSDRCM0laSkllNEpETUIUNUkTThFVlQIQCNjPTEu...!D9dNQwwGXtAIXSWyb32IDLt42B7MtULsd_cjF3-wxjT1Cwi_oDVerNleaCgF_KdQFZZ-q-iFz24HZrY2u59WOFkrqf3OPH_I9i5AcGs-B3nSpmGEs&sid=5qiWSofdekqMkaEm2h1qfz0rT8n3TPdHviaVHBY6fVRUREpGSDRCM0laSkllNEpETUIUNUkTThFVlQIQCNjPTEu

Un saludo,

Lorena Valderrábano Blanco
Directora Desarrollo de Negocio

https://urldefense.com/v3/__https://forms.office.com/Pages/...



PHISHING



De Recibos.Pro
gfi@hacienda.com.mx

A area.sistinfo@uca.es

Responder

Responder a todos

Reenviar

Archivar

No deseado

Eliminar

DKIM

Beauharnois, QC

Más

19/10/22, 21:10

Asunto Enc: Se adjunta la factura con folio FAE MDFATC1724I15256 en formato XML y PDF. (649468)

Thunderbird piensa que este mensaje es correo basura.

Saber más

No es basura



Factura emitida

Tu factura ya está disponible en formato PDF y XML, la hemos anexado al cuerpo de este correo. También puedes descargarla, dando clic en el siguiente botón.

Tienes hasta el **19 de Octubre de 2022 hasta las 10:25 p.m.** para modificar tus datos de facturación. Después de esta fecha, no podrás hacer ningún cambio.

Gracias por su atención

1 adjunto: MDFATC1724I15256.html 146 bytes

Guardar

MDFATC1724I15256.html

213 de 256

PHISHING



<https://virustotal.com/es>

The screenshot shows the VirusTotal analysis interface. At the top left, a circular badge displays a score of 2/90. A red warning icon and text state: "2 security vendors flagged this URL as malicious". The URL being analyzed is https://Lead.me/bdQXFE?45020155A787F5A-5290-4B6E-8F5E-803E1D0DD985_Serie_IWAVZ_y_Folio_158502022.html. The status is 200, and it was analyzed on 2022-10-20 07:29:34 UTC, 27 days ago. A "multiple-redirects" tag is visible. Below the URL, there are tabs for "DETECTION", "DETAILS", "LINKS", and "COMMUNITY". The "DETECTION" tab is active, showing a "Security Vendors' Analysis" table.

Vendor	Verdict	Vendor	Verdict
Comodo Valkyrie Verdict	Phishing	CRDF	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean

[MDFATC1724I15256.html](#)

Más **inciber**consejos

Tu **CONTRASEÑA** es
la puerta de entrada
a tu información

* * * * *



#ProtegeTuUniversidad

 **incibe_**

INSTITUTO NACIONAL DE CIBERSEGURIDAD

 **crue**
Universidades
Españolas

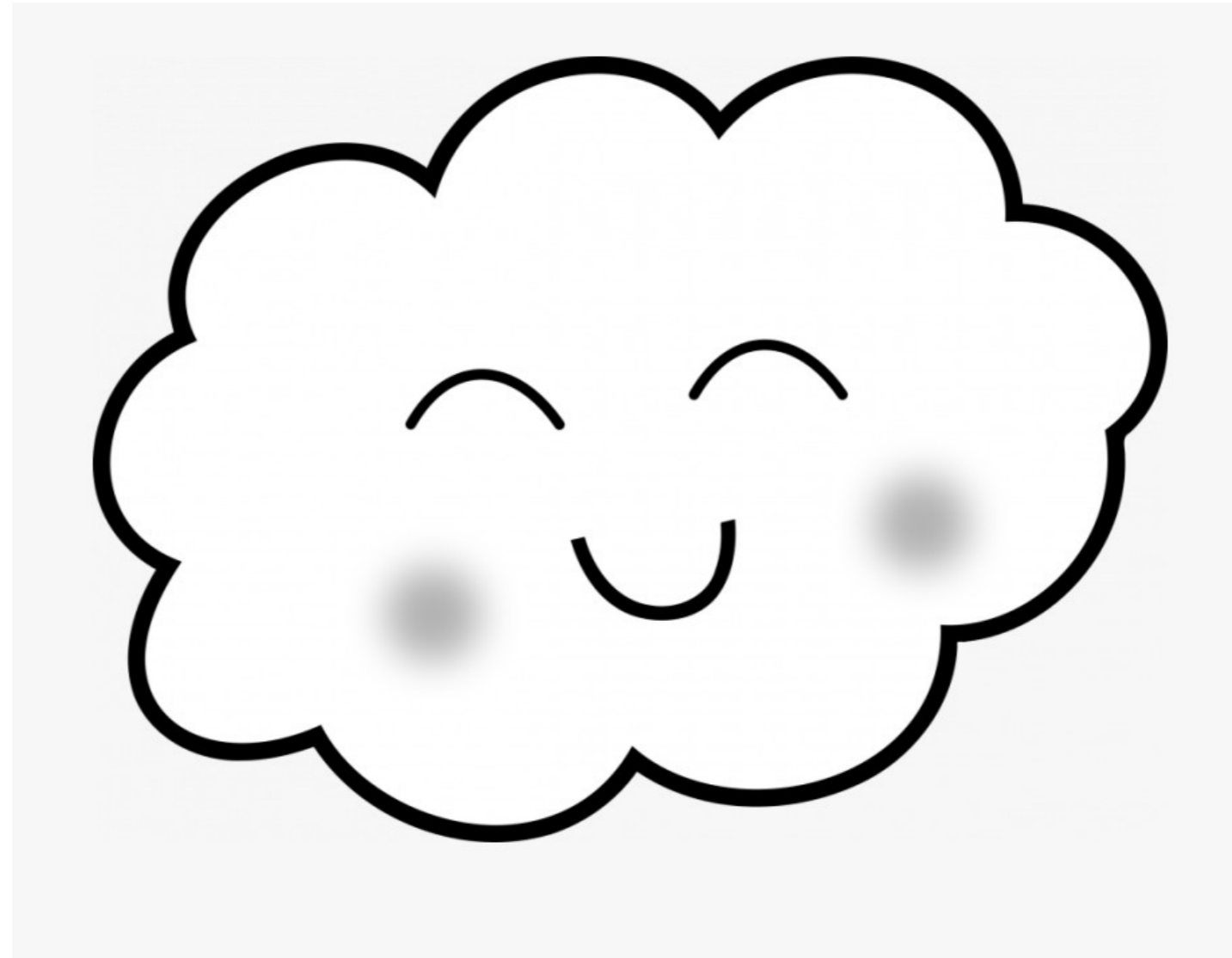

UCA
Universidad
de Cádiz

Más inciberconsejos

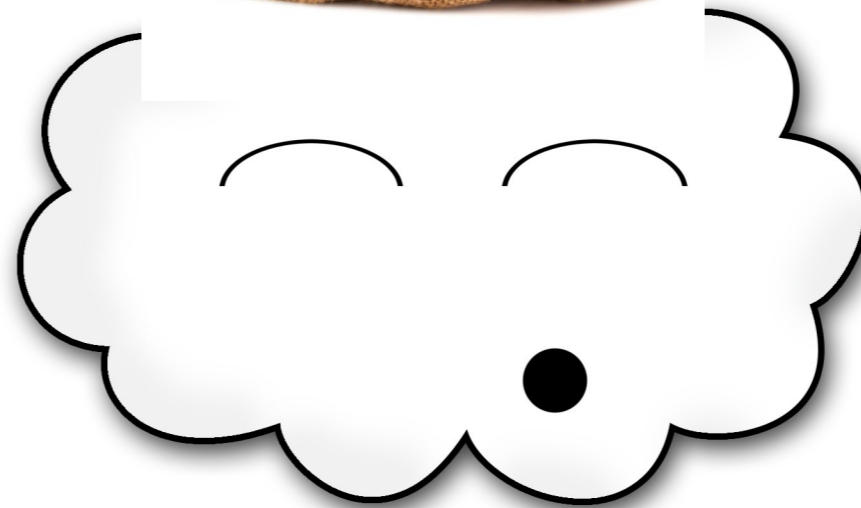
Las **contraseñas**,
como el cepillo de dientes,
son sólo para **TU USO**



Parte 2: Nubedades tecnológicas



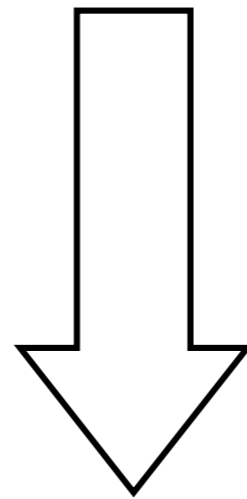
Nube de almacenamiento





Nube de almacenamiento

Owncloud <https://nube.uca.es> 5 GB



Nextcloud <https://ucadrive.uca.es>
500 GB

UCAdrive (*Nextcloud*)

Escalable

Más posibilidades (apps)

Software libre (*open source*)

Multiplataforma



Sincronización

Versiones y recuperación de eliminados

Compartición

UCAdrive (*Nextcloud*)

<https://ucadrive.uca.es/ayuda>





(Ahora sí...)

¡Muchas gracias por
su atención!

gerardo.aburruzaga@uca.es

seguridad.informacion@uca.es

Área de Sistemas de Información

Edificio CITI

314 de solamente 43