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

25-nov-2022

Parte 1: Ciberconsejos

Contraseñas

¡Muchas gracias por su atención!

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

257 de 256

UCA
Universidad de Cádiz

UCA
Universidad
de Cádiz

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	cristina	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

SHA-256

QXwTw4F0

5QXwTw4F0$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

SHA-256

QXwTw4F0

5QXwTw4F0$p6rjYBNe15my.h54rt.Rt8Txmt1fp1MVBlTmOHClsQ.

5QXwTw4F0$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 de 256

SHA-256

QXwTw4F0

5QXwTw4F0$3UIAQuj.BpKI/c0e1tfAqT8yNMPP/HUPQaOAVOemDd5

hash

UCA
Universidad de Cádiz

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: ~ $5 \cdot 10^{14}$ (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

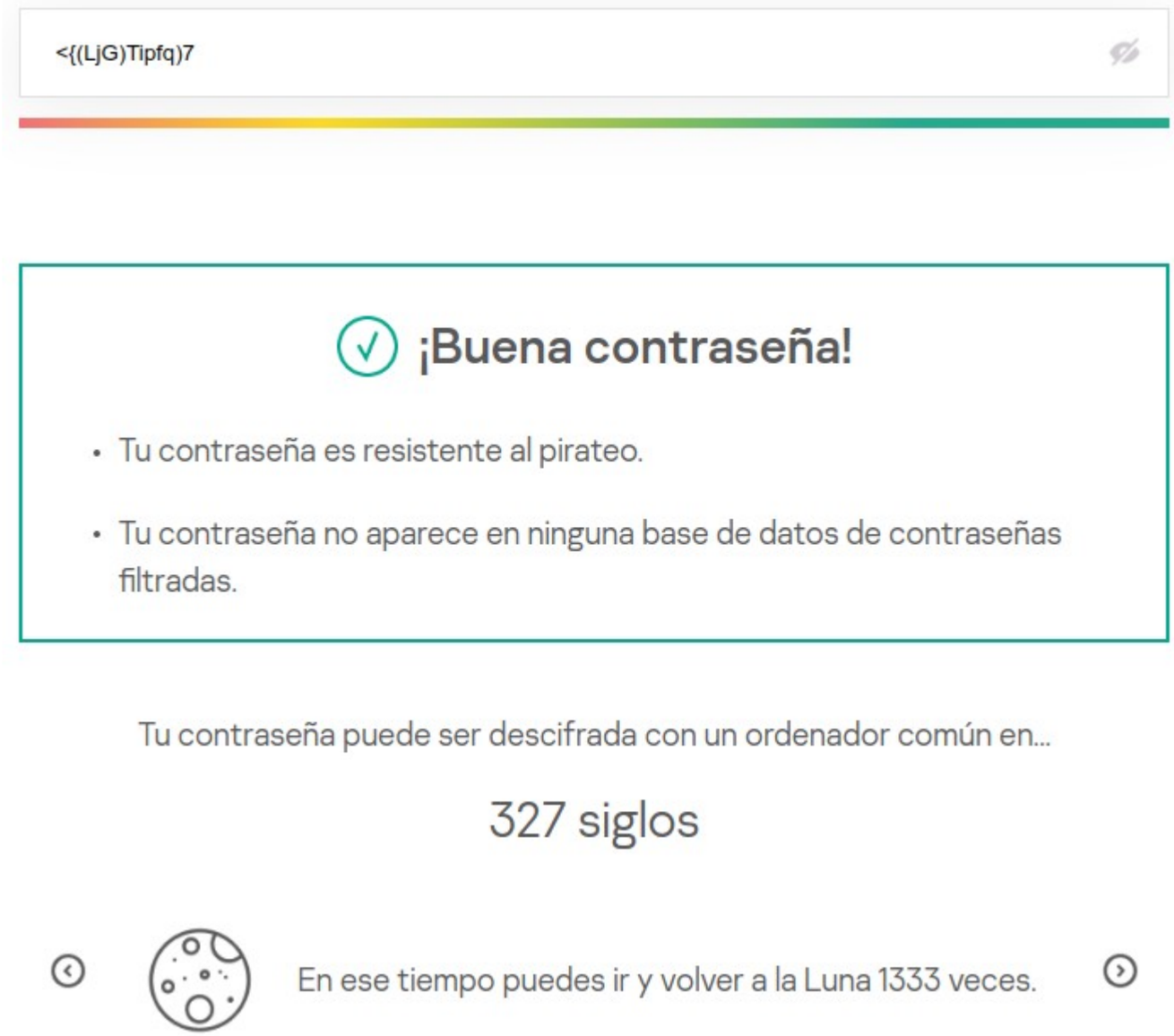
https://password.kaspersky.com/es

Bdx&9[k/

Contraseñas fuertes

https://password.kaspersky.com/es

<{(LjG)Tipfq)7



14 caracteres

Contraseñas fuertes

5 recomendaciones

2. Mezcla

a) Letras MAYÚSCULAS

b) Letras minúsculas

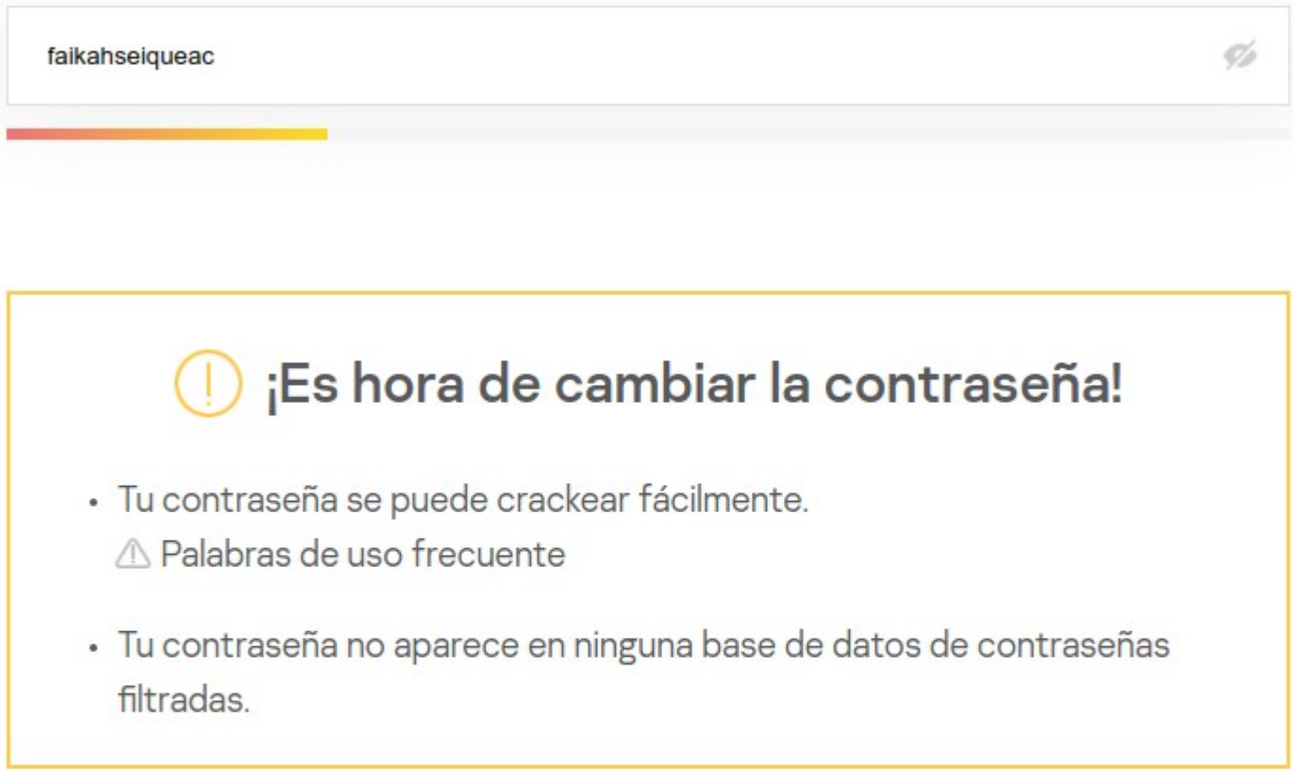
c) Dígitos 0123456789

d) Símbolos </?&$%;-_>.

Contraseñas fuertes

5 recomendaciones

faikahseiqueac



14 letras minúsculas

5 recomendaciones

3. No información personal

a) Nombres personales o de usuario

b) Fechas señaladas

c) Direcciones de correo

d) Direcciones postales…

5 recomendaciones

4. No solo mayúscula inicial

a) Mayúsculas aleatorias

b) No sustituciones típicas de dígitos

ill → 1

aA → 4

oO → 0

B → 8 ...

Contraseñas fuertes

Mi recomendación

1. Caracteres aleatorios mezclados de longitud 14 o más

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

5 recomendaciones

5. Gestor de contraseñas

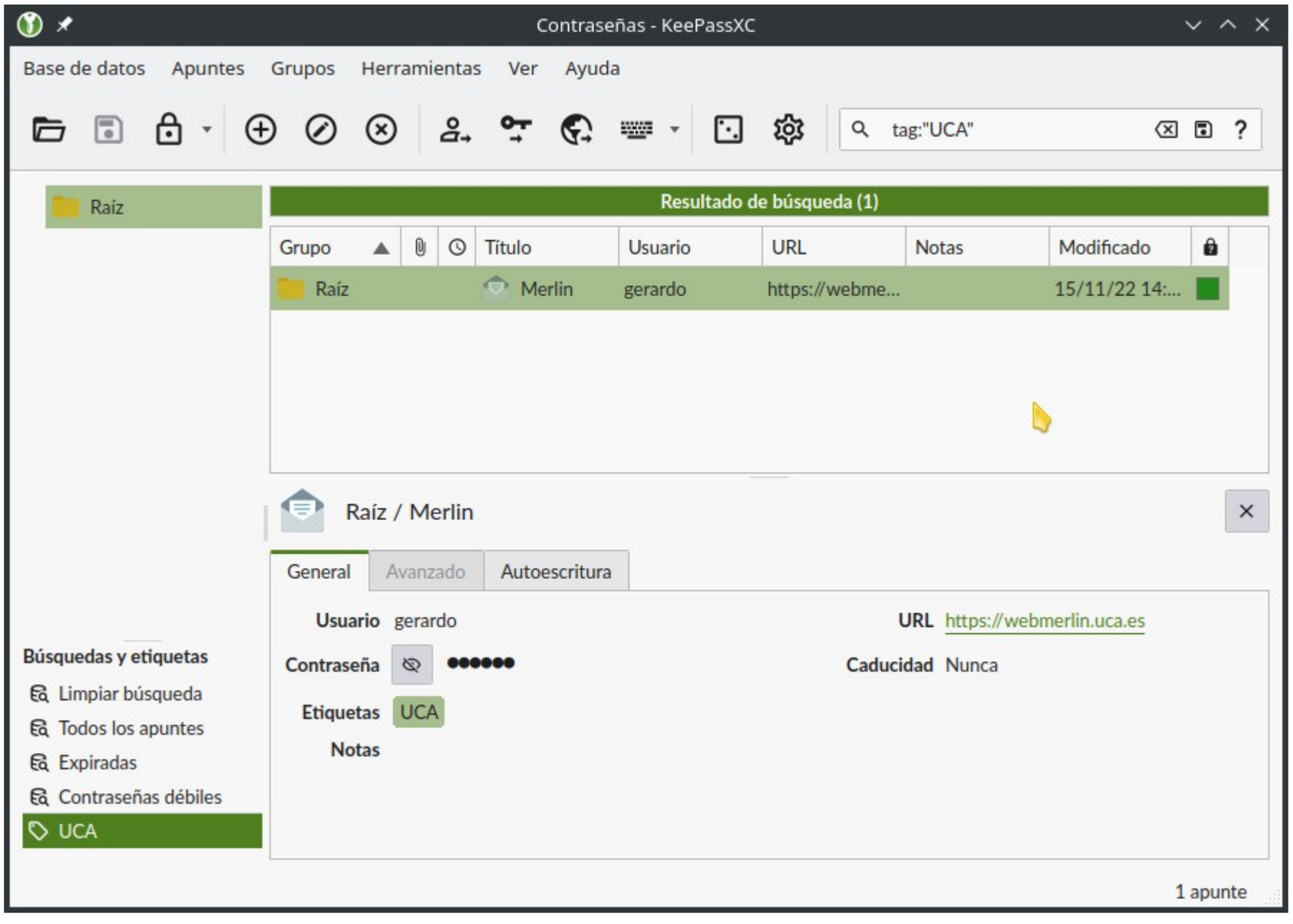
Gestores de contraseñas

Password managers

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

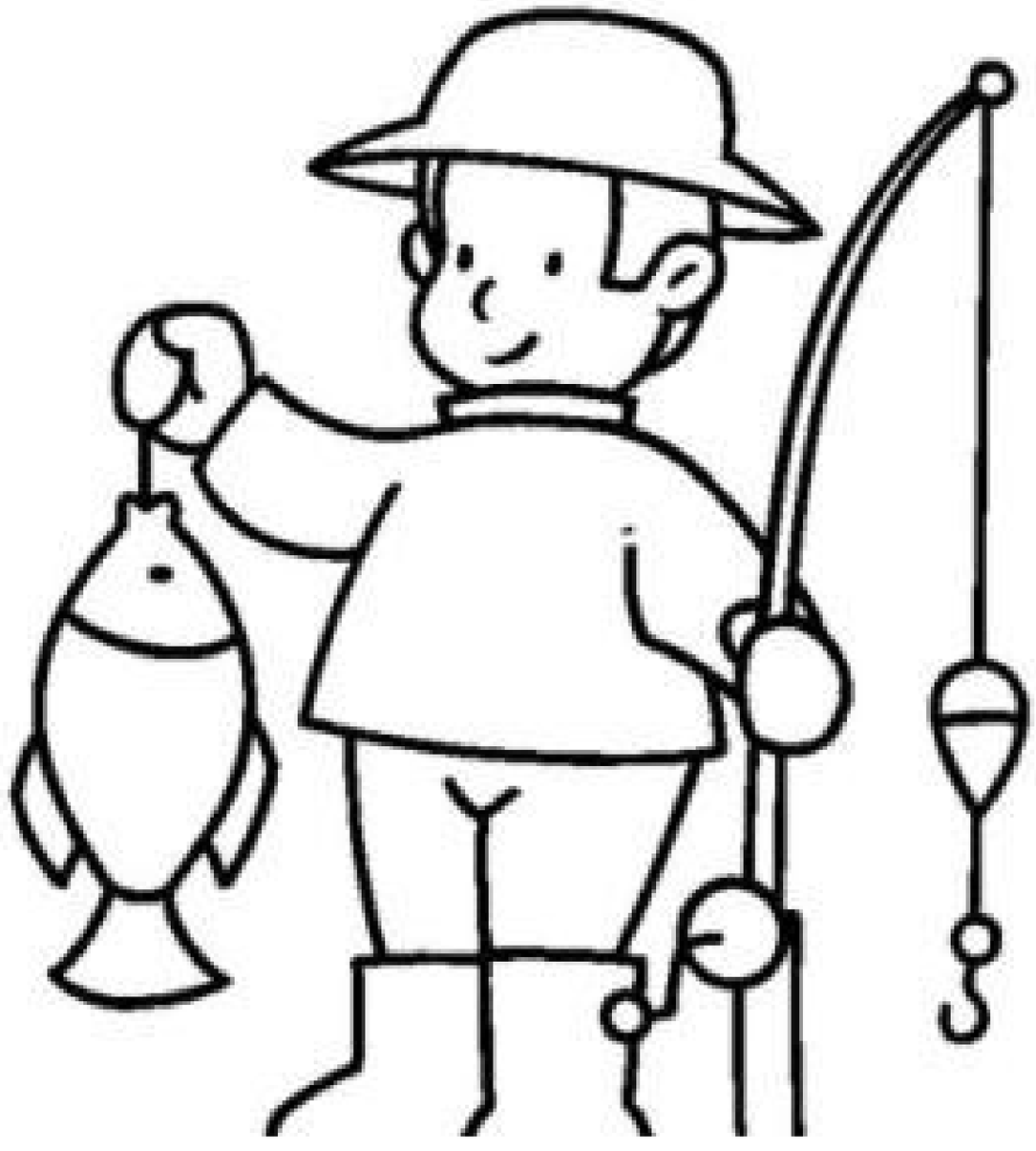
Gestores de contraseñas

Password managers



UCA Universidad de Cádiz

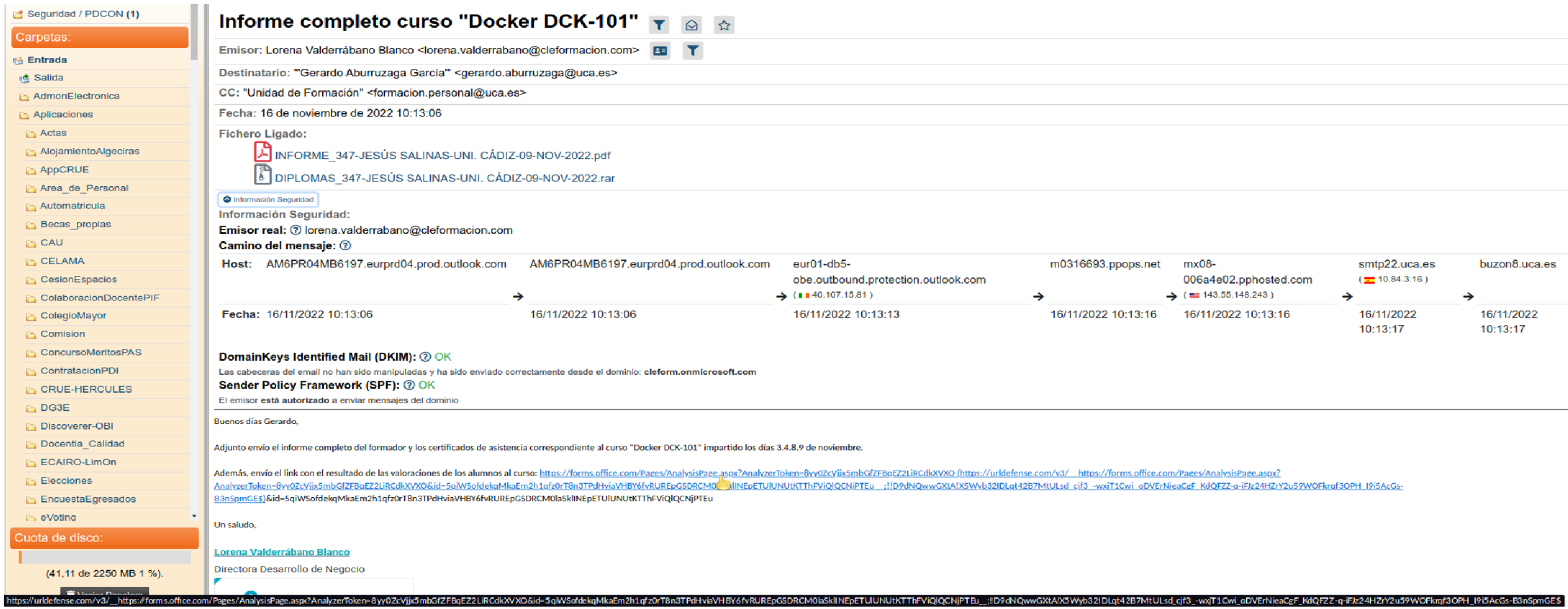
PHISING



PHISHING: tipos

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

PHISHING



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

UCA Universidad de Cádiz

PHISHING

De R Recibos.Pros gfi@hacienda.com.mx

Responder | Responder a todos | Reenviar | Archivar | No deseado | Eliminar | DKIM | Beauharnois, QC | Más

A area.sistinfo@uca.es

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

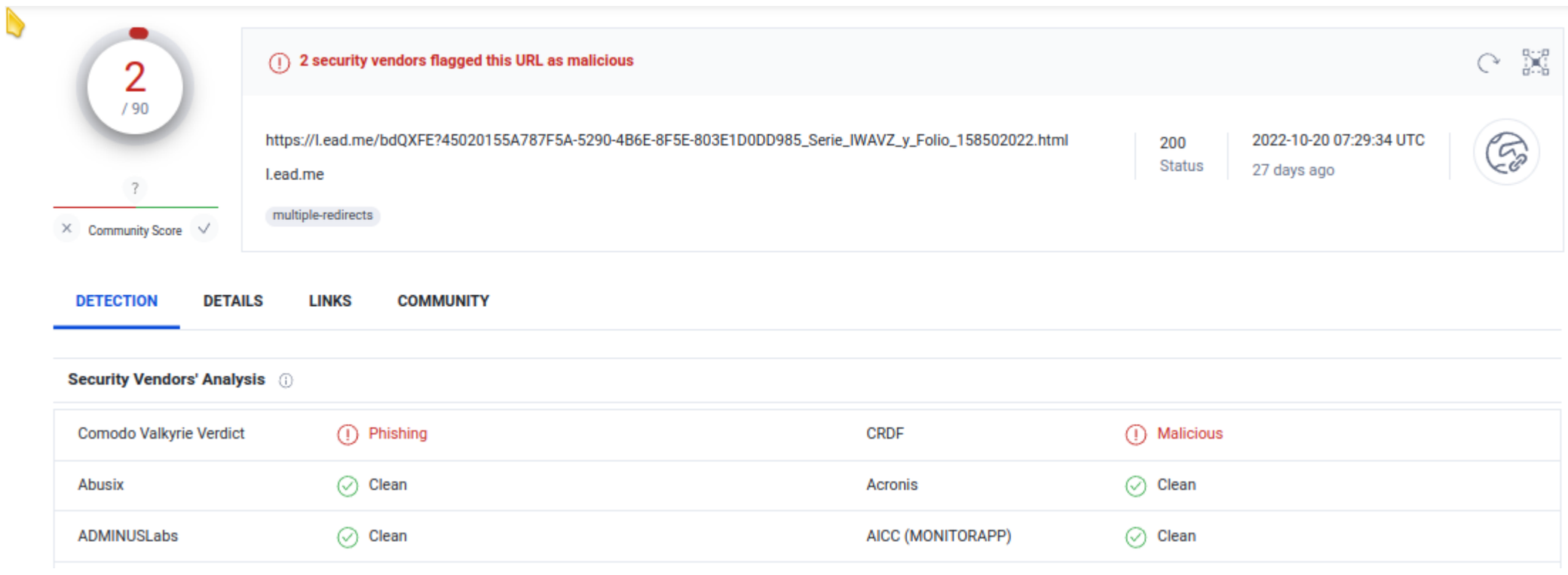
Guardar

MDFATC1724I15256.html

UCA Universidad de Cádiz

PHISHING

https://virustotal.com/es



MDFATC1724I15256.html

UCA
Universidad de Cádiz

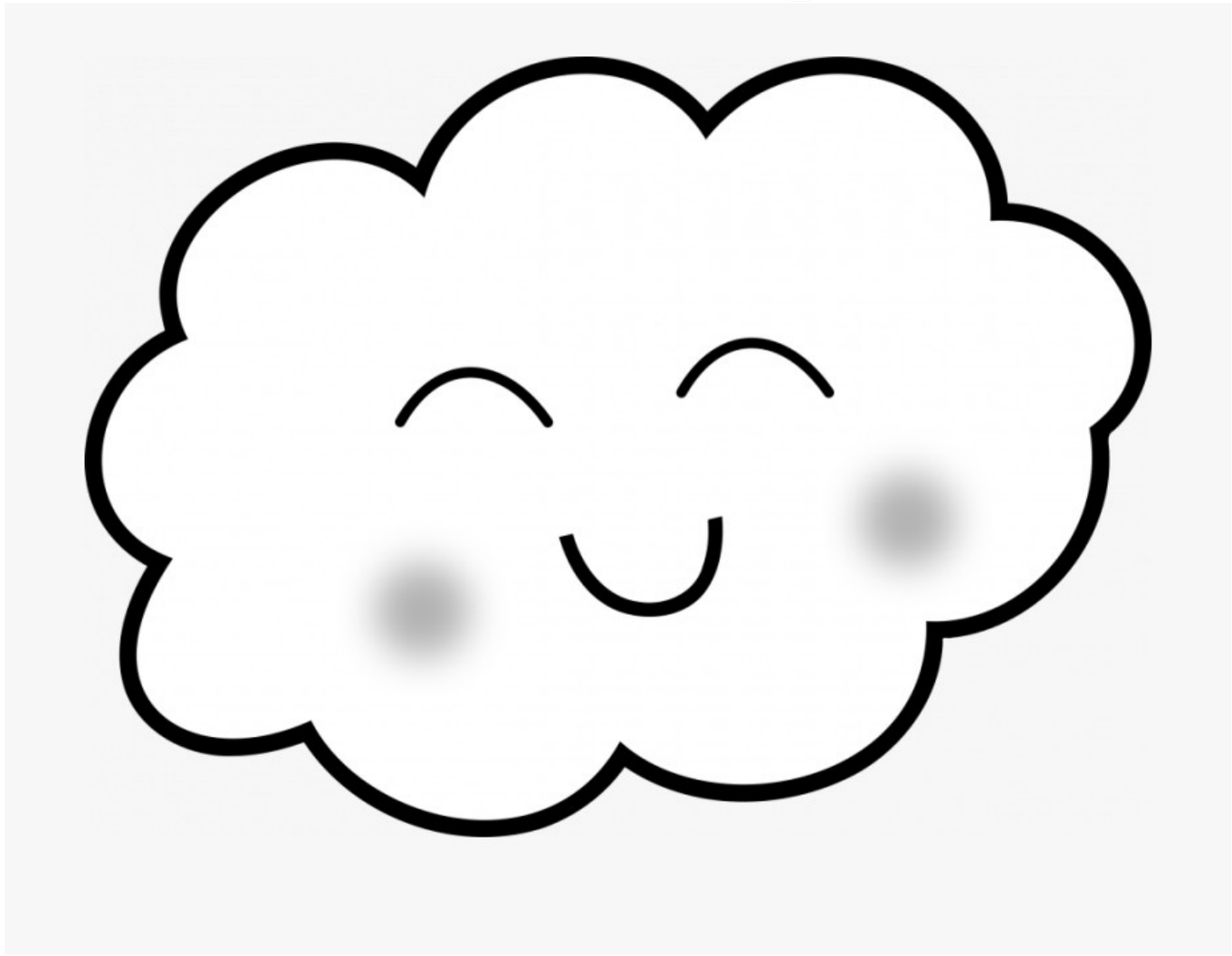
Más inciberconsejos

UCA
Universidad
de Cádiz

Más inciberconsejos

UCA
Universidad
de Cádiz

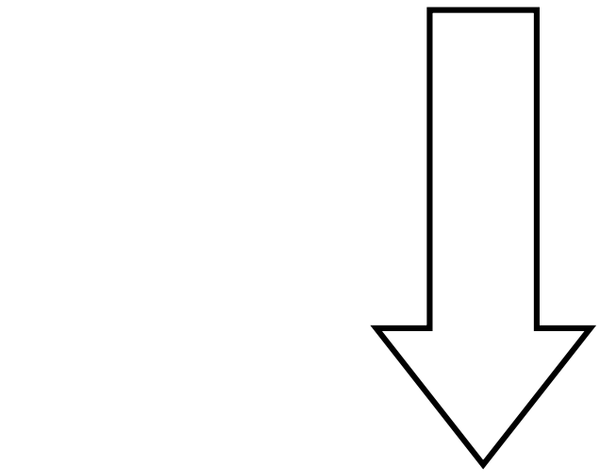
Parte 2: Nubedades tecnológicas



Nube de almacenamiento

Nube de almacenamiento

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



Nextcloud https://ucadrive.uca.es

500 GB

UCA
Universidad de Cádiz

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

UCA
Universidad de Cádiz

(Ahora sí...)

¡Muchas gracias por su atención!

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

UCA
Universidad de Cádiz