

# CIBERSEGURIDADE

Medidas de prevención e boas prácticas en Ciberseguridade

Belén Pérez Rodríguez



**Belén Pérez Rodríguez**



**Twitter:** @BPR\_Vigo



**LinkedIn:** <https://www.linkedin.com/in/belenpr/>



Colegio Oficial  
de Ingenieros Técnicos  
Industriales de Vigo



### Certifications:

CCNA, CCNP-R&S, CCNA-Security (Cisco)

CEH, CHFI (E-Council)

CA Administrator QRadar (IBM)

CPN-23 (CCI)

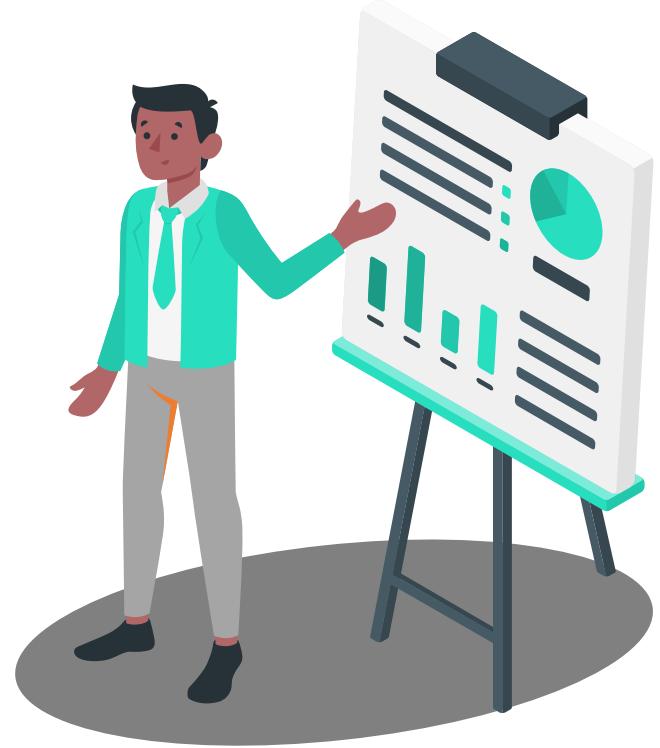
# Curso superior en Ciberseguridade - 2022

## Medidas de prevención e boas prácticas en Ciberseguridade



## POSTO DE TRABALLO:

- A - TECNOLOGÍAS DA INFORMACIÓN ( IT )
- B - CIBERSEGURIDADE
- C - USUARIO IT
- D - OTRO



## Coñecementos de CIBERSEGURIDADE:

- A - NADA
- B - ALGO
- C - BASTANTE
- D - EXPERTO



# Contido

1. Nocións básicas de Ciberseguridade
2. Enxeñería social
3. Phishing e ataques dende correos electrónicos  
PAUSA
4. Contrasinais
5. Conexións por USB
6. Consellos

1. Nocións básicas de Ciberseguridade

## CIBERSEGURIDADE

Conxunto de servizos, mecanismos, ferramentas, protocolos ou políticas que **garanten** os nosos datos (información), servizos, procesos e, polo tanto, a continuidade da actividade normal da **Organización**.

(NEGOCIO)

Prevención - Protección - Resposta

1. Nocións básicas de Ciberseguridade

# CIBERSEGURIDADE

Garantir o acceso só aos autorizados:

- Garantir a privacidade
- Evitar as filtracións de información

Garantir que os usuarios poidan acceder cando o precisen



Garantir a exactitude e integridade da información e os métodos do seu proceso

## Non REPUDIO

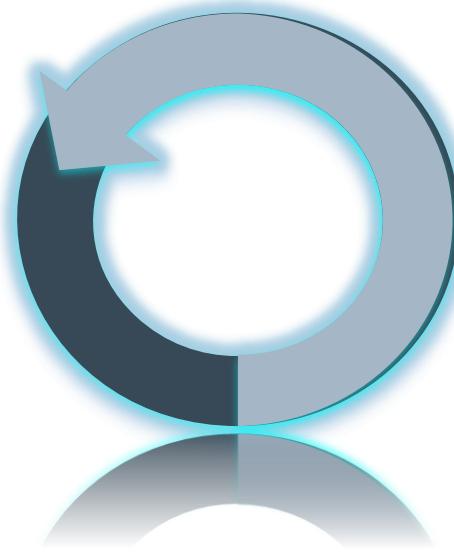
Garantía da autoría

## Resiliencia

Recuperación fronte a desastres

1. Nocións básicas de Ciberseguridade

## CIBERSEGURIDADE

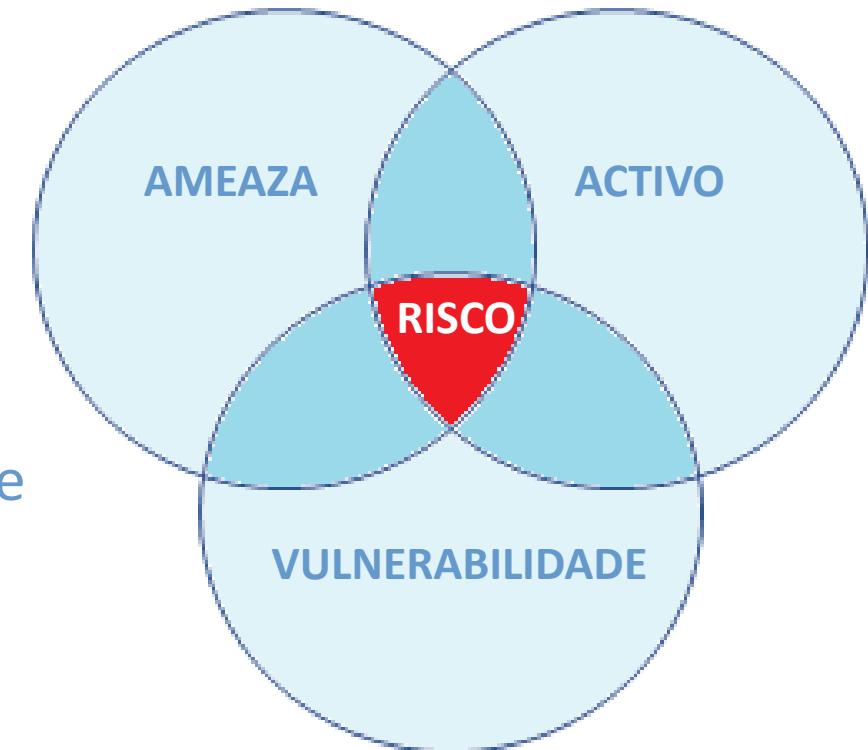


- O 100% DE SEGURIDADE NON EXISTE:  
**SEMPRE HAI RISCOS**
- O LIGO DÉBIL NA CADEA:  
**SER HUMANO**
- NON HAI SOLUCIÓNNS MÁXICAS OU ESTÁNDARES
- A CIBERSEGURIDAD NON É ALGO TEMPORAL

1. Nocións básicas de Ciberseguridade

## CIBERSEGURIDADE

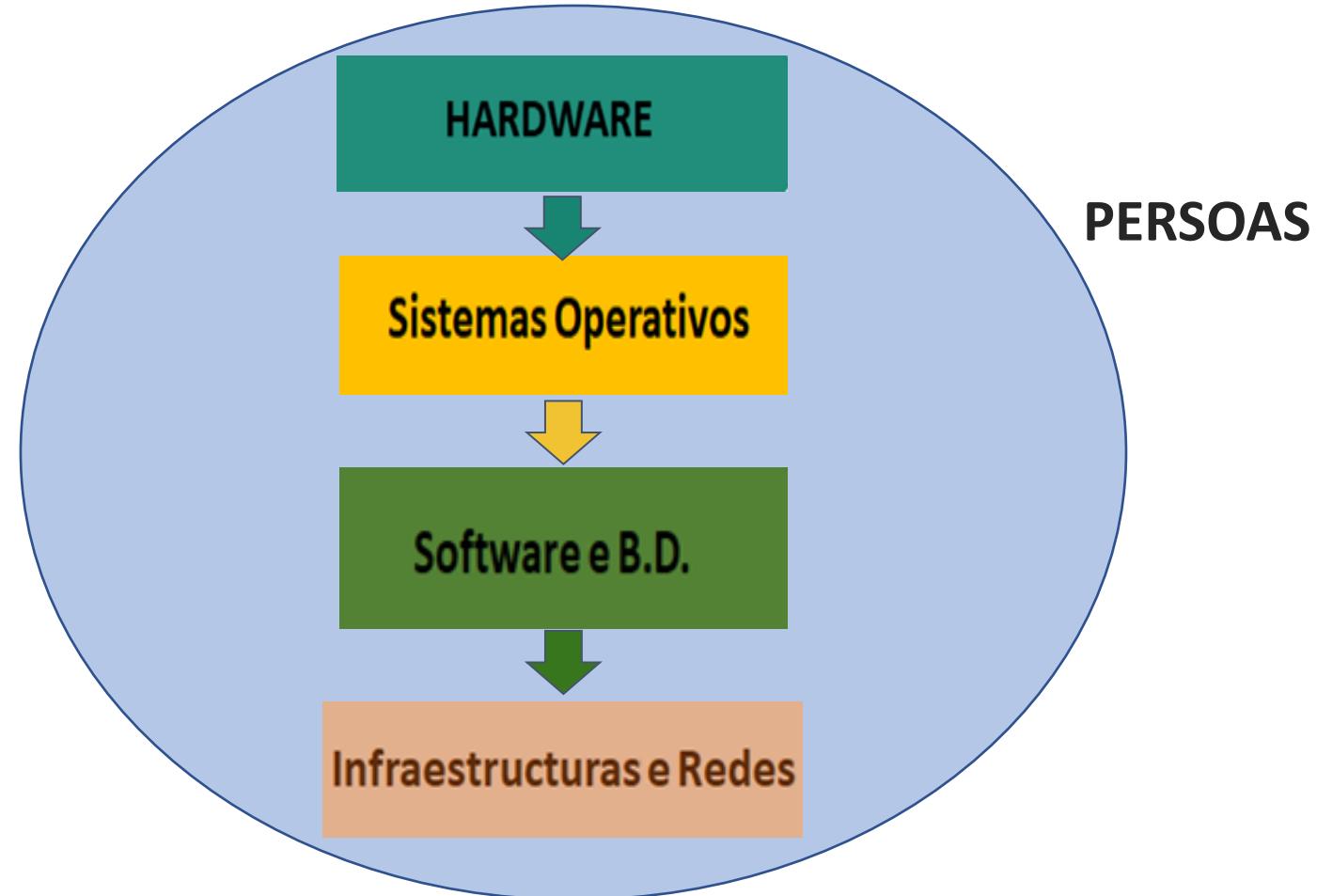
- ACTIVO:** Todo o que xera valor
- VULNERABILIDAD:** Debilidade ou fallo
- AMEAZA:** Acción que se aproveita dunha vulnerabilidade para atentar contra un sistema de información, proceso, servicio...
- RISCO:** probabilidade de que unha ameaza se convirta nun evento real e xere perdas (**IMPACTO**)



1. Nocións básicas de Ciberseguridade

# CIBERSEGURIDADE

## ACTIVOS



PERSOAS

1. Nocións básicas de Ciberseguridade

# CIBERSEGURIDADE

## VULNERABILIDADES

### HARDWARE:

Portos Accesibles  
Alimentación  
Ambiente...



### SISTEMAS:

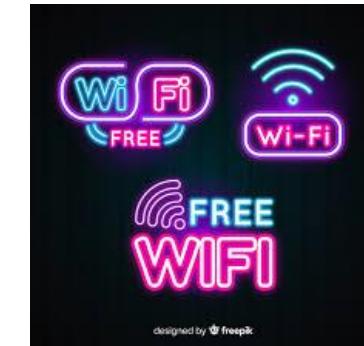
WINDOWS  
LINUX  
IOS ...

### APLICACIÓNNS:

Qué é o que mais usamos  
Para qué o usamos

### REDES:

Todos conectados  
Portos abertos



	1999-2019	2019
Debian Linux	3,067	414
Android	2,563	360
Linux kernel	2,357	357
Mac OS X	2,212	357
Ubuntu	2,007	351
Mozilla Firefox	1,873	342
Google Chrome	1,858	342
iPhone iOS	1,655	250
Windows Server 2008	1,421	248
Windows 7	1,283	246
Adobe Acrobat Reader DC	1,182	242
Adobe Acrobat DC	1,182	235
Windows 10	1,111	190
Adobe Flash Player	1,078	184
Windows Server 2012	1,050	

1. Nocións básicas de Ciberseguridade

## CIBERSEGURIDADE

### □ AMEAZAS

### HACKTIVISMO



### CIBERESPIONAJE



### CIBERTERRORISMO



### CIBERGUERRA



### CIBERCRIMEN



1. Nocións básicas de Ciberseguridade

## CIBERSEGURIDADE

### RISCO (PROBABILIDADE)

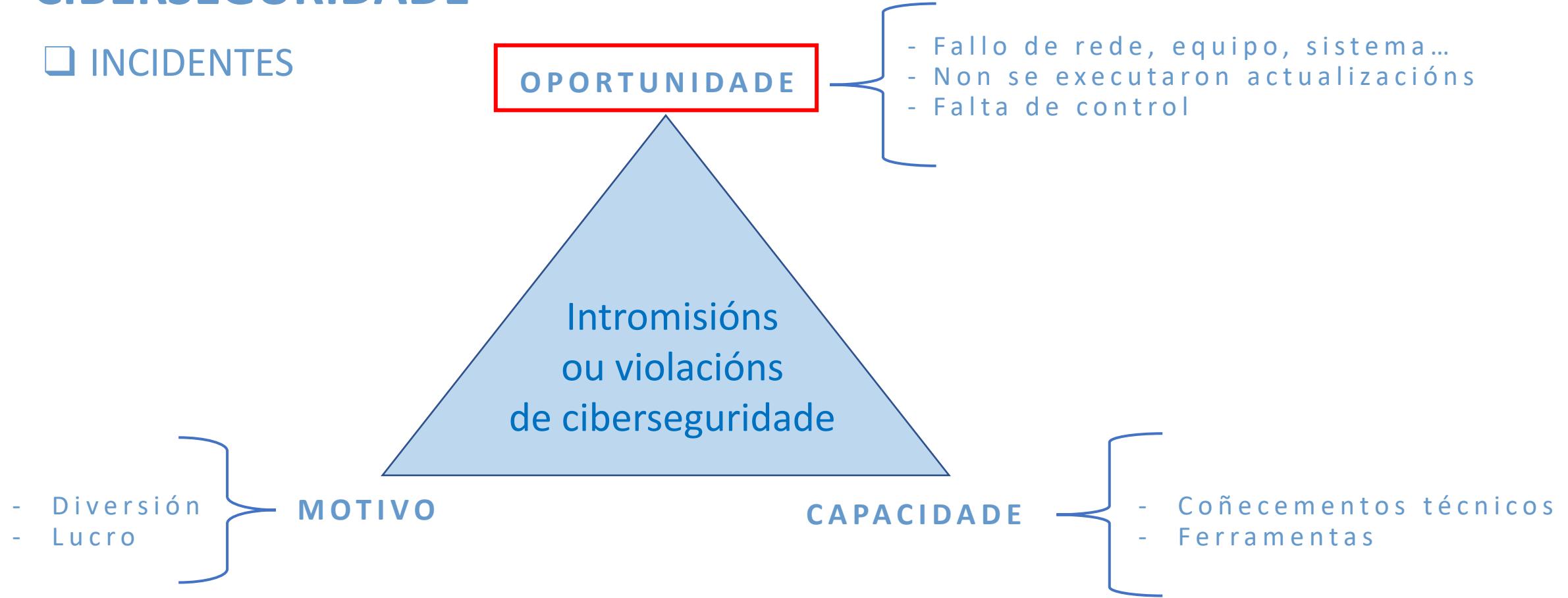


**UAB**  
Universitat Autònoma  
de Barcelona

1. Nocións básicas de Ciberseguridade

## CIBERSEGURIDADE

### □ INCIDENTES



1. Nocións básicas de Ciberseguridade

## CIBERSEGURIDADE

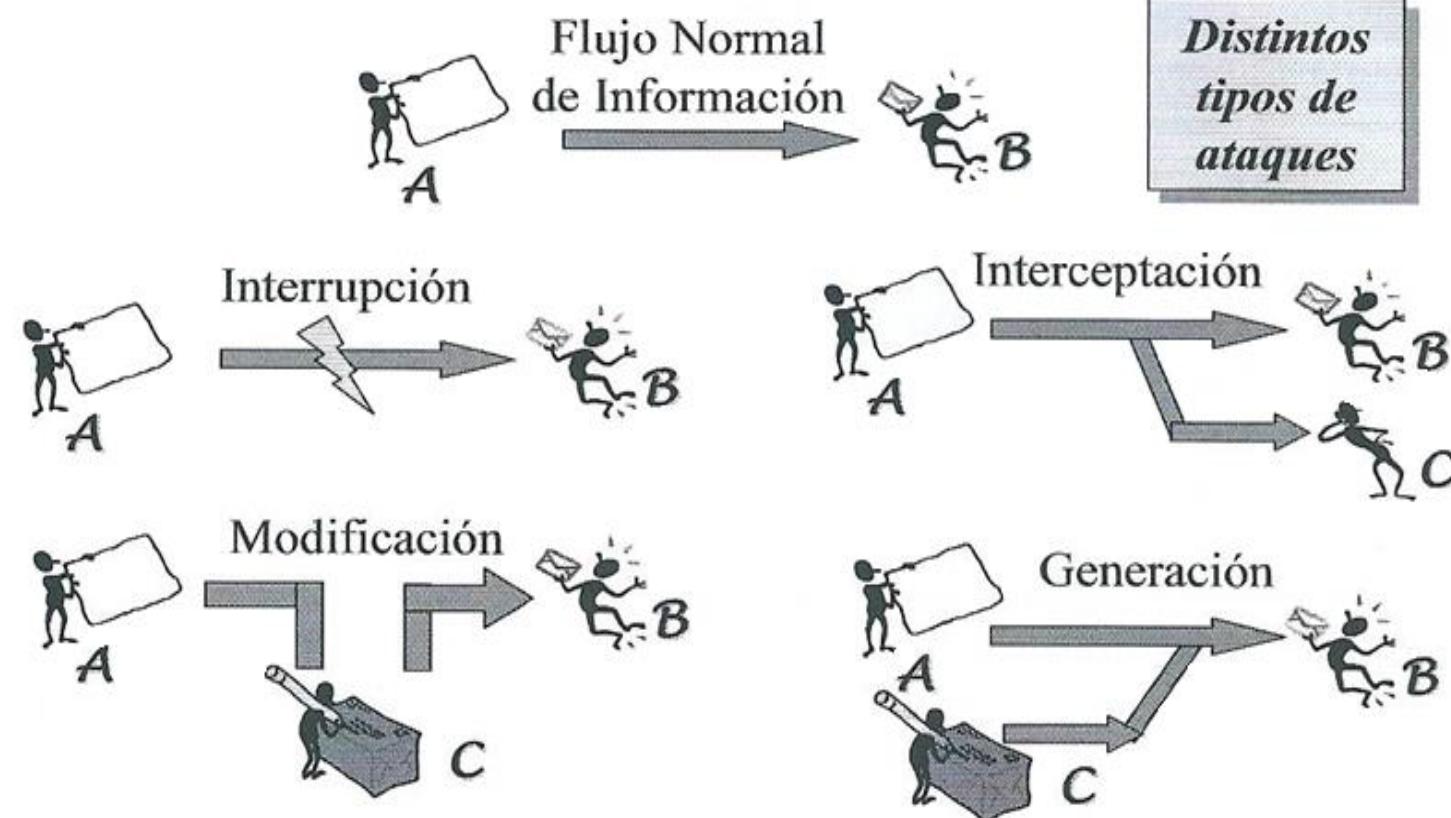
### INCIDENTES - CATEGORIAS

- Interrupción do servicio (DoS-DDoS)
- Acceso á información (Fuga ou robo de datos)
- Modificación da información
- Xeración de información falsa

1. Nocións básicas de Ciberseguridad

# CIBERSEGURIDADE

## INCIDENTES - CATEGORIAS



## 1. Nocións básicas de Ciberseguridade

# CIBERSEGURIDADE

## DoS

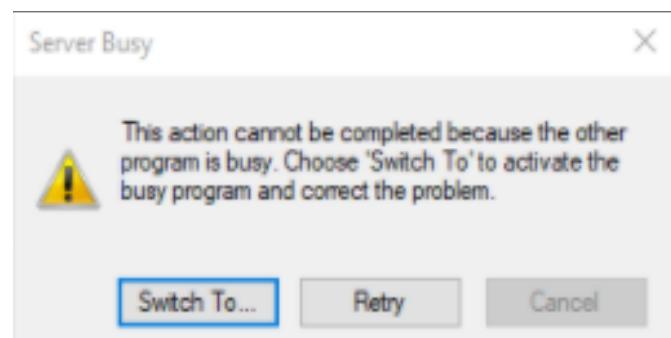


### Sin conexión a Internet

Prueba a:

- Comprobar los cables de red, el módem y el router
- Volver a conectarte a una red Wi-Fi
- Ejecutar Diagnósticos de red de Windows

DNS\_PROBE\_FINISHED\_NO\_INTERNET



404, That's an error.

The requested URL /cosas\_impressionantes was not found on this server. That's all we know.



No se puede acceder a este sitio web

La página [nnnz2 mega.nz](http://nnnz2 mega.nz) ha rechazado la conexión.

Prueba a:

- Comprobar la conexión
- Comprobar el proxy y el cortafuegos

ERR\_CONNECTION\_REFUSED

Volver a cargar

DETALLES



## ORIXE DOS CIBER-INCIDENTES



**85% - Accións de persoas**



**15% - Fallos de seguridade ou Inaccións**

# PREGUNTA

## ENXEÑERÍA SOCIAL:

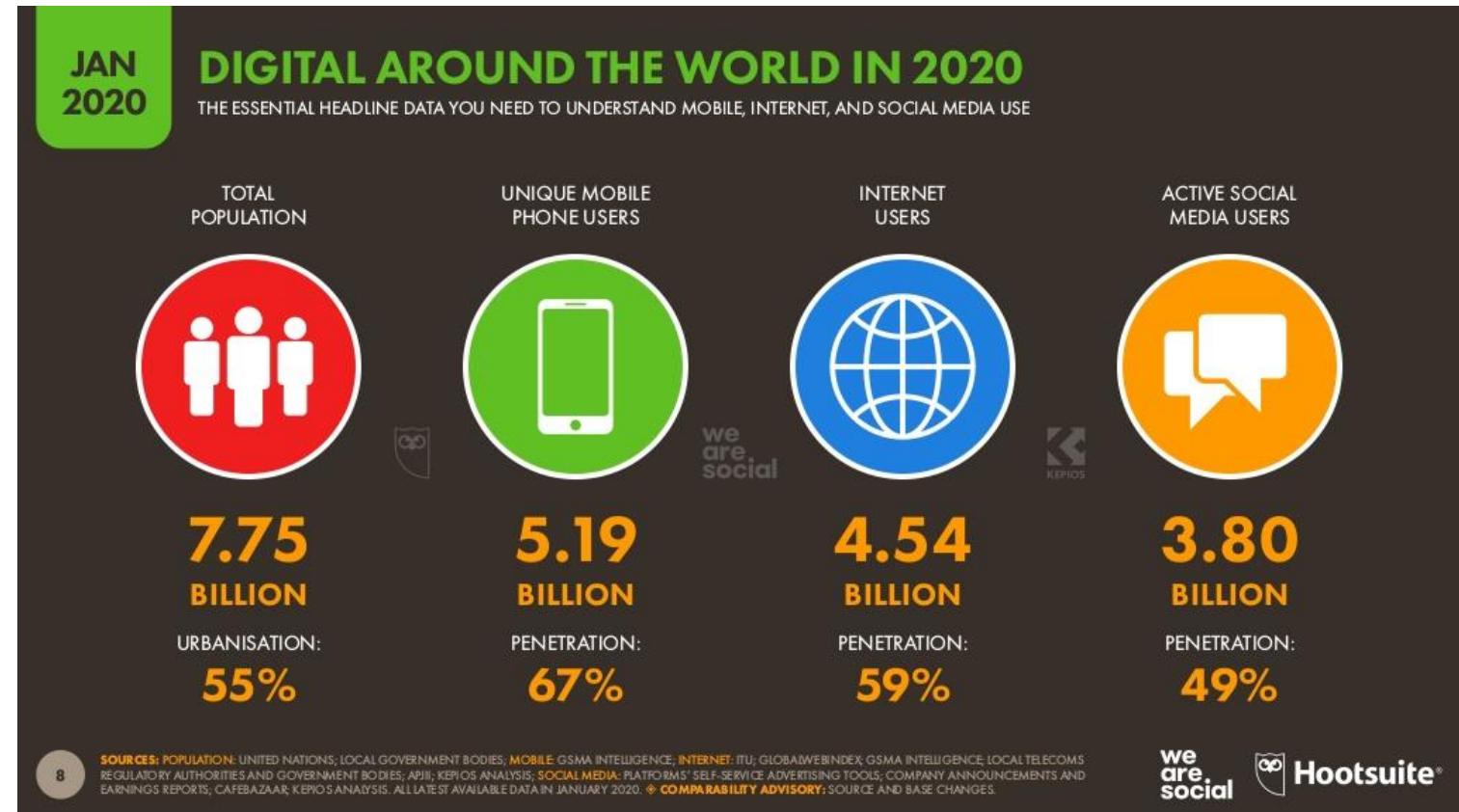
- A – SEI O QUE É E NUNCA PICARÍA
- B – SERÍA O PRIMEIRO EN PICAR
- C – DEPENDE



Ciberseguridade

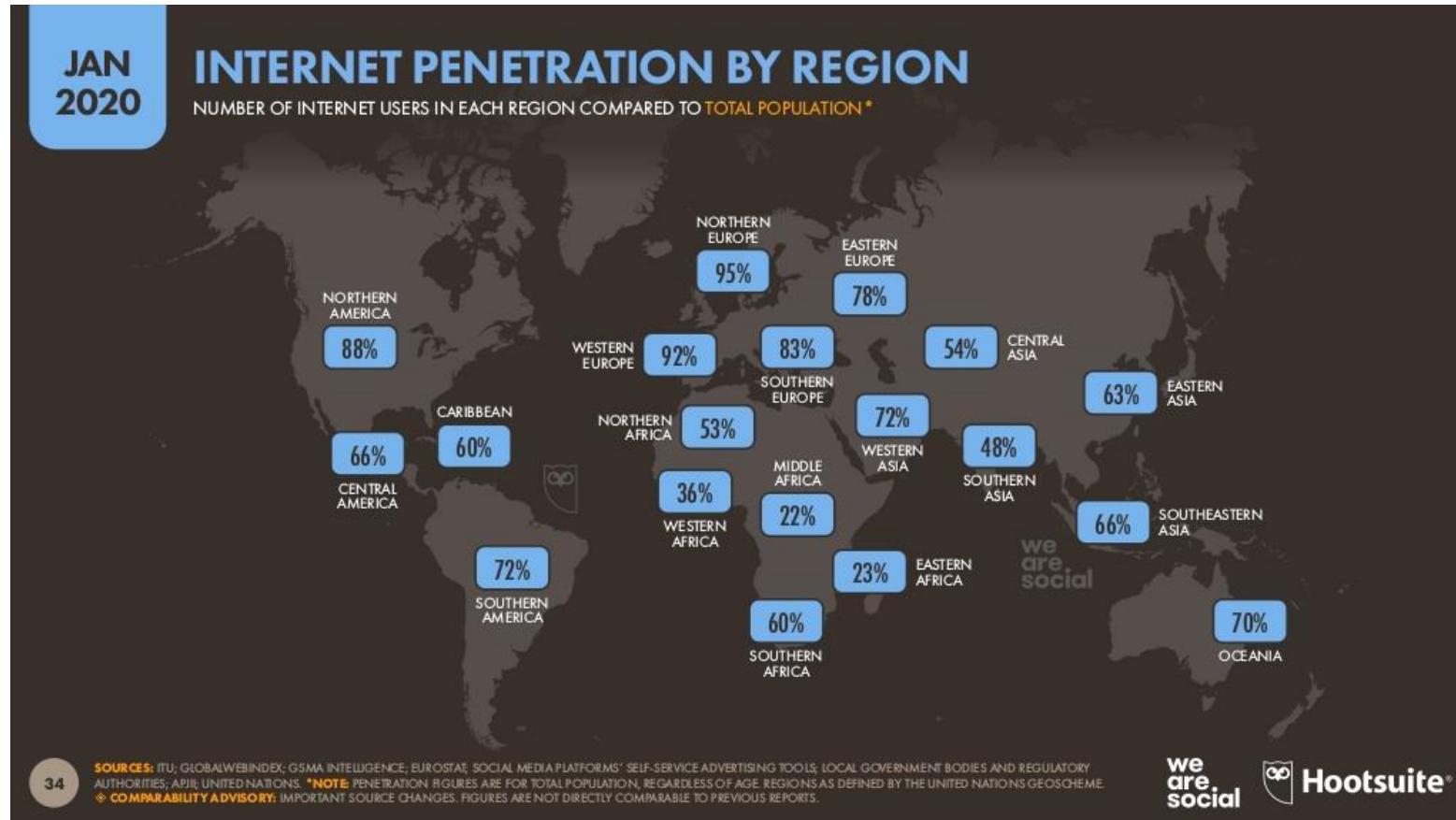
## 2. ENXEÑERÍA SOCIAL

Feito de manipular ás persoas para revelar información confidencial ou realizar certas accións sen o seu coñecemento real ou das implicacións.



Ciberseguridade

## 2. ENXEÑERÍA SOCIAL



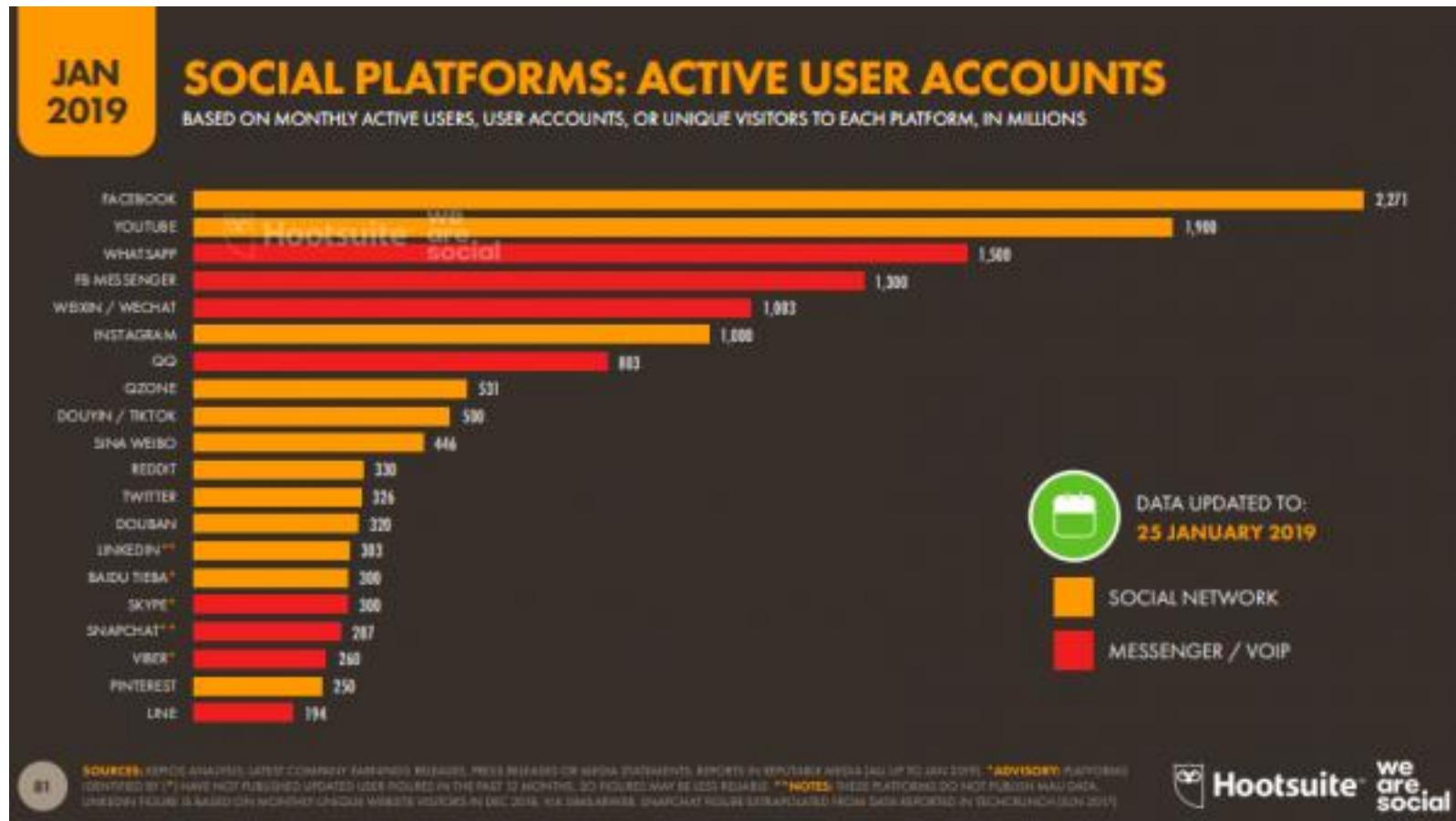
## Ciberseguridade

## 2. ENXEÑERÍA SOCIAL



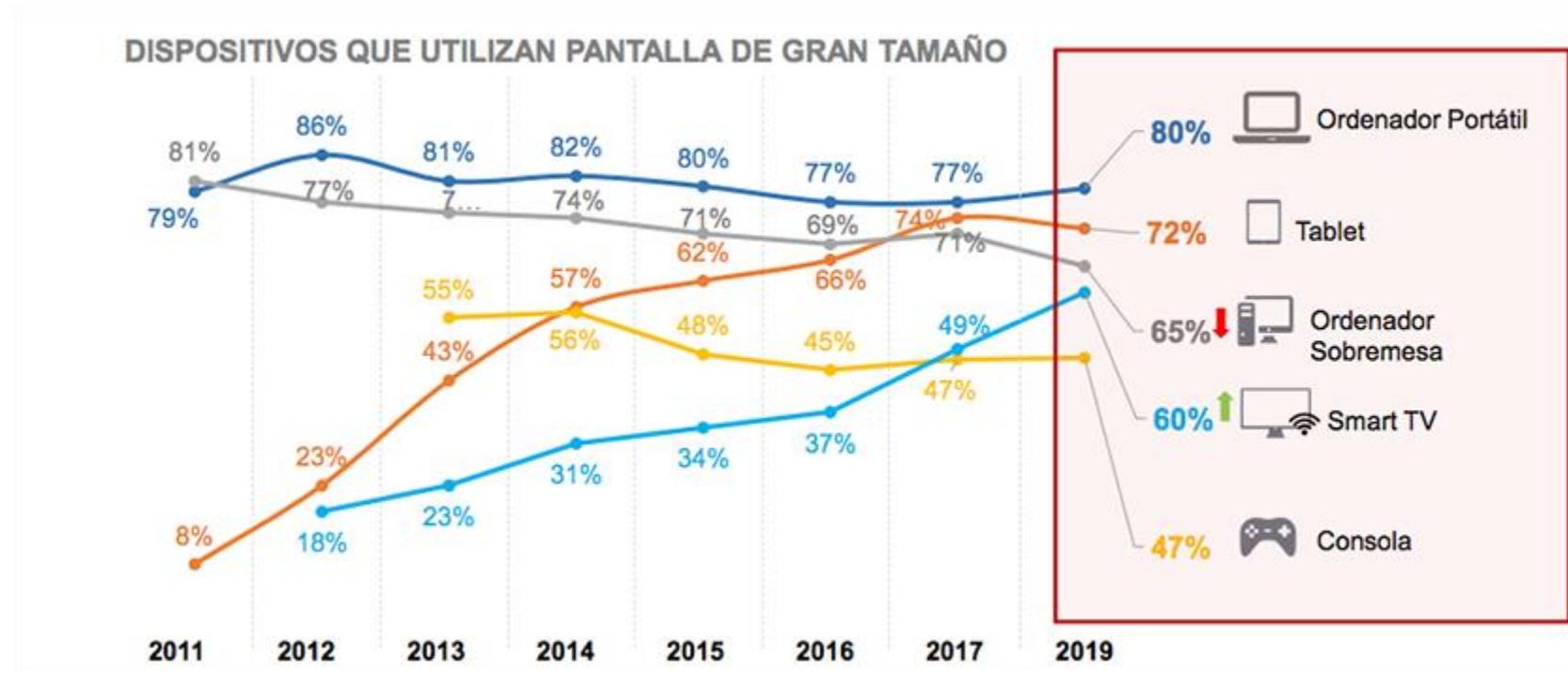
## Ciberseguridade

## 2. ENXEÑERÍA SOCIAL



Ciberseguridade

## 2. ENXEÑERÍA SOCIAL



Ciberseguridade

## 2. ENXEÑERÍA SOCIAL

### Obxectivos:

- Obtención de datos confidenciais para un posterior uso indebido  
(datos = diñeiro)
- Roubo de cartos (credenciais bancarias)
- Acceso a dispositivos ou sistemas para acceso a información, uso ilegítimo dos mesmos ou extorsión
- Roubo de identidades
- Ciberbullying (ciberacoso) ou extorsión

## Ciberseguridade

# 2. ENXEÑERÍA SOCIAL



Ciberseguridade

## 2. ENXEÑERÍA SOCIAL

### Vulnerabilidades humanas

- Sexo
- Avaricia
- Vaidade
- Confianza
- Preguiza
- Compaixón
- Urxencia
- Gula
- Envexa
- Ira



Ciberseguridade

## 2. ENXEÑERÍA SOCIAL

### Medio de ataque

- Correo electrónico
- Teléfono: chamadas ou SMS
- Dispositivos USB
- Códigos QR
- Códigos de barras
- Redes sociais...

## Ciberseguridade

## 2. ENXEÑERÍA SOCIAL

### Casos habituais

Publicado el  
28/09/2020  
Importancia : Media

#### Correos electrónicos suplantan a Bankia, Banco Santander y otras entidades bancarias

DEPORTES

#### A Víctor Sánchez del Amo le exigían 20.000 euros a cambio de no difundir su vídeo sexual

Según el «Diario Sur», el vídeo habría sido grabado sin consentimiento del entrenador y posteriormente chantajeado

imagináte la escena: estás conectado y una atractiva jovencita de un país exótico entra en contacto contigo. ¡Y en poco tiempo se ha enamorado de ti locamente! Esta podría ser la trama de un cuento de princesas...

... Si no fuese porque, muy probablemente, se trate de un engaño.

Nos has oido decir muchas veces que, en internet, muchas veces las cosas no son como parecen. Y también que los cibercriminales utilizan anzuelos atractivos para que el usuario pique. ¿Hay algo más atractivo que una chica guapa, joven y soltera que te quiere conocer? El [amor en la red](#) a veces tiene sus riesgos...

Echa un vistazo a las capturas de e-mail siguientes. ¿Te resultan familiares? Recibes un correo electrónico donde una chica se muestra interesada en chatear contigo, o te presentan una página de contactos gratuita donde cientos de jovencitas están esperando conocerte.

De: Lina <[kikrikat@betsysblooms.net](mailto:kikrikat@betsysblooms.net)>  
Asunto: [Find a Russian wife here](#)  
Para: mi <[\[REDACTED\]](#)>

Hello!  
Spring has finally come! Romance is in the air!

Beautiful and still single (!!!) Russian and Ukrainian women are eager to meet you!  
They have placed their profiles at SingleRussianGirls dating site and waiting for your emails.

Don't loose time and come get registered [FREE](#)

De: Dianne <[DianneMondz@megared.net.mw](mailto:DianneMondz@megared.net.mw)>  
Asunto: [I want to chat with you](#)  
Para: mi <[\[REDACTED\]](#)>

[Russian women waiting to meet YOU! Click here](#)



Dianne  
Sent with Airmail

Embargado por la emoción, se te ocurre pinchar en el enlace para ver qué pasa y, joh, sorpresa!, te encuentras un sitio de contactos con perfiles de chicas guapísimas, normalmente de países del este, a los que puedes acceder simplemente proporcionando tus datos.

¿Y qué puede ocurrir si continúo el contacto con alguien?

Lo más probable es que empiezarás a recibir largas y bonitas cartas de amor (te recomendamos que eches un vistazo a este [blog](#) donde un usuario compartió el intercambio de correspondencia con "Olga" para prevenir a posibles despiadados contra el engaño), hasta que llega el momento de conocerlos en persona.... Ella te pedirá que le envíes dinero para el viaje y, una vez lo haya recibido, no volverás a saber nada de ella.

En realidad, Olga no existe. No es más que un avatar creado por una mafia que lo que busca es, a toda costa, tu dinero. A pesar de que el engaño es muy antiguo, sorprendentemente hay usuarios que siguen cayendo en la trampa.

¿Cómo reaccionar en estos casos?

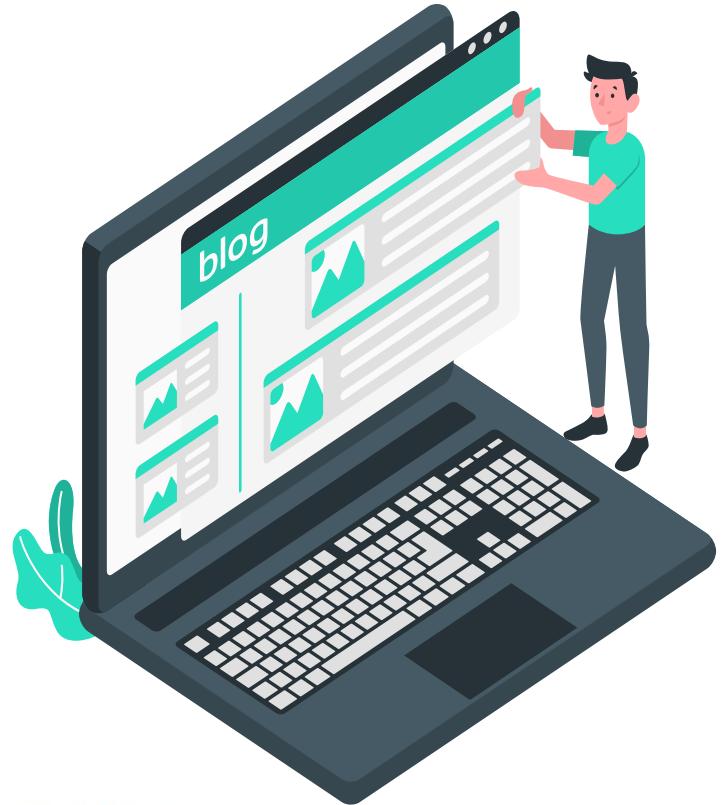
- Lo más prudente en estos casos es cortar toda comunicación de raíz. Piénsalo.... ¿es realista pensar que alguien que ni siquiera te conoce, que además es joven, guapa e inteligente, se ha enamorado locamente de tí?

- En muchos casos, tras hacer una pequeña investigación, puedes darte cuenta del engaño. Basta con hacer una búsqueda de la fotografía en internet o del alias que utiliza y podrás sorprenderle.

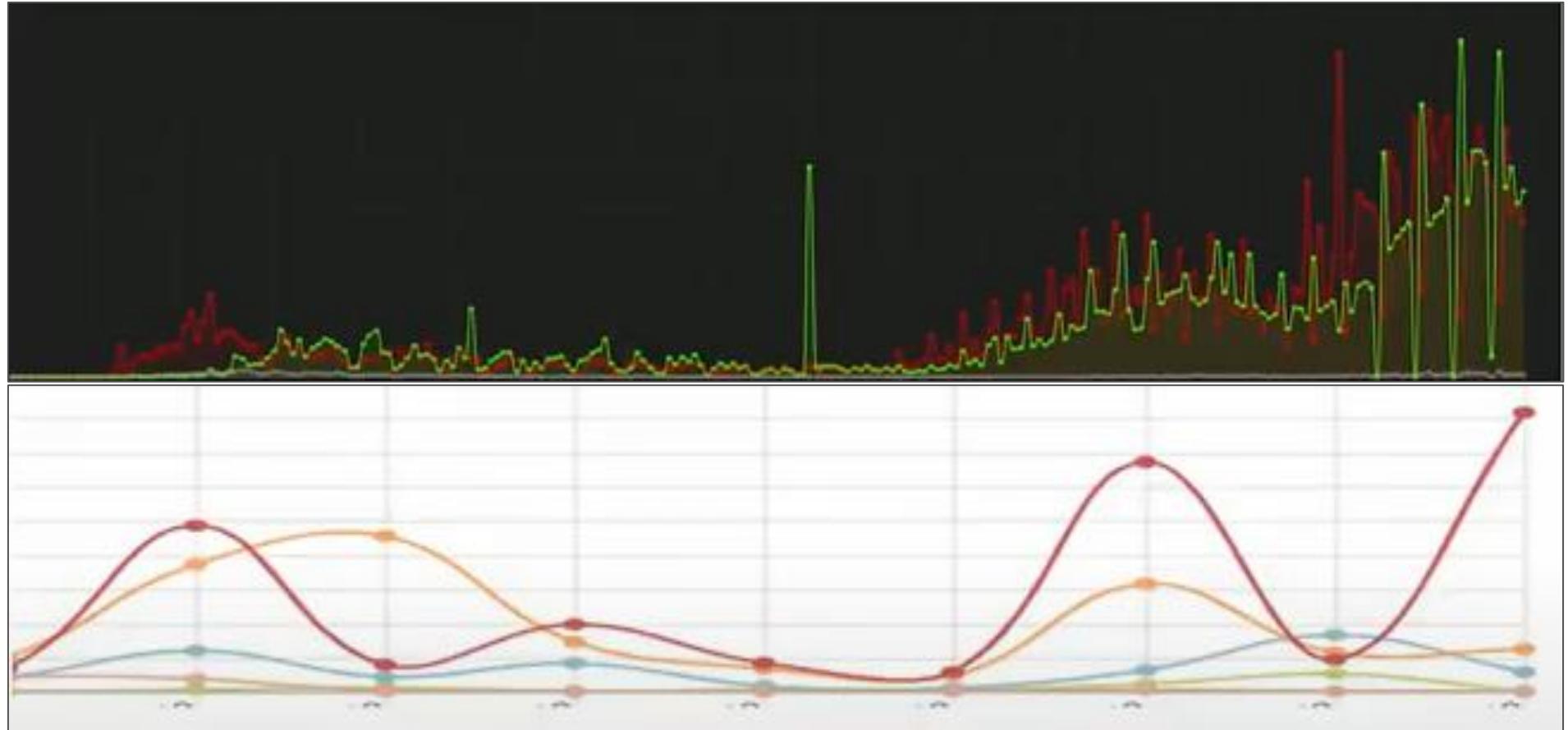
- Nunca, en ningún caso, accedas a enviarle dinero por internet. Se trata de un fraude, y nunca más verás el dinero... ni a la chica.

## VERACIDADE DOS EMAILS:

- A – SEI COMO IDENTIFICAR A VERACIDADE
- B – DEPENDE DA ORIXE
- C – DEPENDE DO CONTIDO
- D – NINGUNHA DAS ANTERIORES



Ciberseguridade



## Ciberseguridade

# 3. Phishing e ataques dende correos electrónicos

## Formatos:

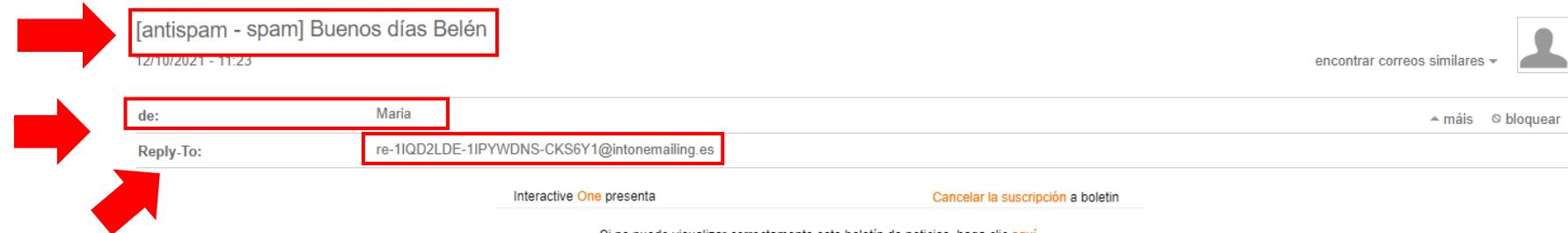
- Spamming (versión moderna dos timos)
- Phishing:
  - Tradicional (correos xenéricos)
  - Spear Phishing (correos personalizados)
- Smishing: phishing por SMS
- Vishing: por chamada telefónica
- Redes sociais
- QRishing: a través dos códigos QR
- Códigos de barras...

## Ciberseguridade

## 3. Phishing e ataques dende correos electrónicos

### Modelo de SPAM

- **Spamming** (versión moderna dos timos): gaña cartos, gangas, herdanças...



Interactive One presenta [Cancelar la suscripción a boletín](#)

Si no puede visualizar correctamente este boletín de noticias, haga clic [aqui](#).

Buenos días Belén,

TIENES que [VER ESTO...](#)

Sí estás buscando una manera real de conseguir ingresos reales (y estoy hablando de alrededor de 1000 \$ al día), esto te interesa.

Esto video te interesa.

Sí es así, mira este breve video: Ve aquí: [Video](#)

Te puedes registrar JUSTO AHORA!

Que tengas un gran día

Generador de ingresos [1365 \\$ dia!!](#)

Esta oferta es un anuncio comercial del cliente publicitario. Si tiene alguna pregunta sobre los productos o servicios anunciados, diríjase directamente al vendedor. Si desea borrarse con [belenpr@mundo-r.com](#) de la lista de distribución por correo electrónico, pulse en: [cancelar la suscripción](#) | [Aclaración al cliente](#) | [Aviso legal](#)

Este boletín es un servicio gratuito de Interactive One GmbH • Sieglitzhofer Str. 9 • D-91054 Erlangen • Alemania

## Ciberseguridade

### 3. Phishing e ataques dende correos electrónicos

#### Modelo de Phishing tradicional

- Correos xenéricos suplantando identidades

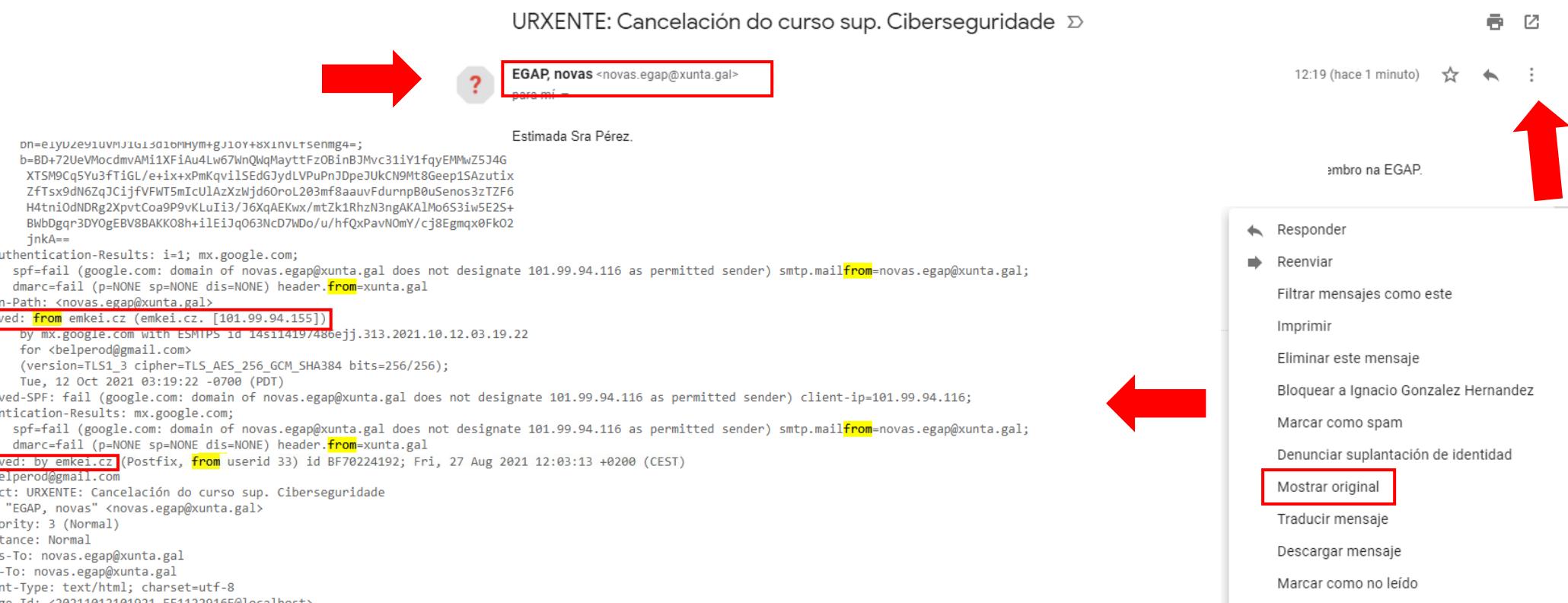


## Ciberseguridade

## 3. Phishing e ataques dende correos electrónicos

### Modelo de Spear Phishing

#### □ Correos con suplantación completa de identidades



URXENTE: Cancelación do curso sup. Ciberseguridade

Estimada Sra Pérez.

ARC-Authentication-Results: i=1; mx.google.com;  
spf=fail (google.com: domain of novas.egap@xunta.gal does not designate 101.99.94.116 as permitted sender) smtp.mail[from=novas.egap@xunta.gal];  
dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=xunta.gal  
Return-Path: <novas.egap@xunta.gal>  
Received: from emkei.cz (emkei.cz. [101.99.94.155])  
by mx.google.com with ESMTPS id 145114197486ejj.313.2021.10.12.03.19.22  
for <belperod@gmail.com>  
(version=TLS1\_3 cipher=TLS\_AES\_256\_GCM\_SHA384 bits=256/256);  
Tue, 12 Oct 2021 03:19:22 -0700 (PDT)  
Received-SPF: fail (google.com: domain of novas.egap@xunta.gal does not designate 101.99.94.116 as permitted sender) client-ip=101.99.94.116;  
Authentication-Results: mx.google.com;  
spf=fail (google.com: domain of novas.egap@xunta.gal does not designate 101.99.94.116 as permitted sender) smtp.mail[from=novas.egap@xunta.gal];  
dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=xunta.gal  
Received: by emkei.cz (Postfix, from userid 33) id BF70224192; Fri, 27 Aug 2021 12:03:13 +0200 (CEST)  
To: belperod@gmail.com  
Subject: URXENTE: Cancelación do curso sup. Ciberseguridade  
From: "EGAP, novas" <novas.egap@xunta.gal>  
X-Priority: 3 (Normal)  
Importance: Normal  
Errors-To: novas.egap@xunta.gal  
Reply-To: novas.egap@xunta.gal  
Content-Type: text/html; charset=utf-8  
Message-ID: <20210827120313.F511232016@localhost>

12:19 (hace 1 minuto) ⚡ ↗ ⌂ ⋮

✉ ambro na EGAP.

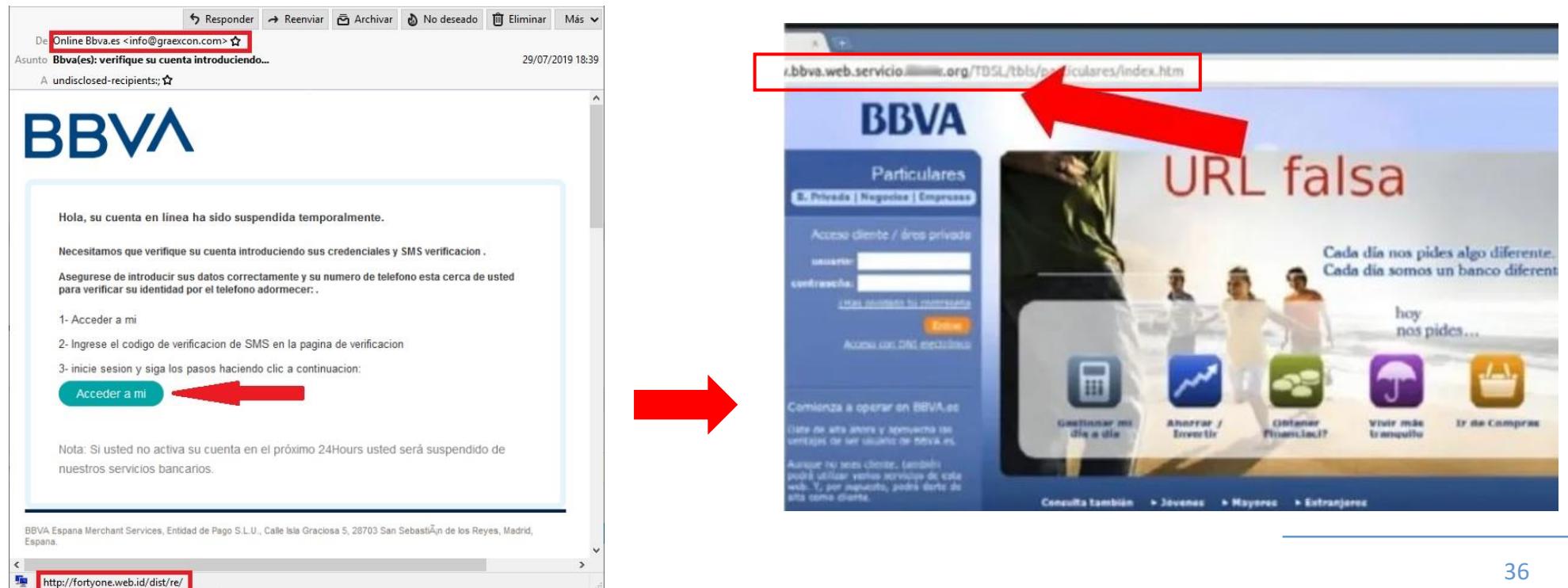
Responder Reenviar  
Filtrar mensajes como este  
Imprimir Eliminar este mensaje  
Bloquear a Ignacio Gonzalez Hernandez  
Marcar como spam  
Denunciar suplantación de identidad  
**Mostrar original** Traducir mensaje  
Descargar mensaje Marcar como no leído

## Ciberseguridade

## 3. Phishing e ataques dende correos electrónicos

### Modelo de Pharming

#### □ Correos con enlaces maliciosos a sitios falsos

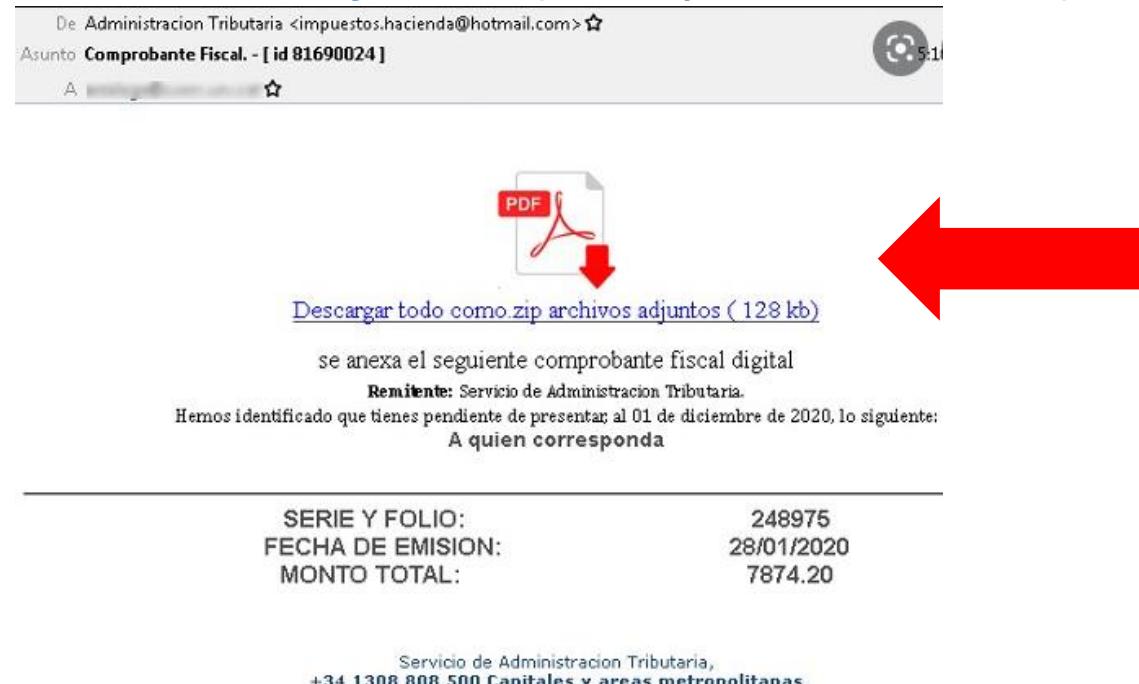


## Ciberseguridade

### 3. Phishing e ataques dende correos electrónicos

#### Modelo de Malware Phishing

##### Correos con ficheiros adjuntos (.txt, .pdf, .csv, .xls,...)



Ciberseguridade

### 3. Phishing e ataques dende correos electrónicos

#### Medio de ataque

- ❑ Malware Phishing: correos con adjuntos

Virus muy sencillo (DoS - start)



Antivirus.bat

Virus agresivo de Eliminación de información (erase)



antivirus.cmd

## Ciberseguridade

### 3. Phishing e ataques dende correos electrónicos

#### ❑ Malware profesionalizado



# SABEMOS QUÉ É ISTO:



A - SI

B - NON

## Ciberseguridade

# 3. Phishing e ataques dende correos electrónicos

## Exemplos actuais

**Secuestro de WhatsApp: cómo pueden robarle la cuenta con este ataque**



30/12/2020 | Redacción

LinkedIn WhatsApp anunció a comienzos de este año que ha superado la cifra de 200 millones de usuarios. Esto la convierte en la aplicación de mensajería más popular del planeta y, a su vez, en objeto codicido por los ciberdelincuentes. En ese sentido, a lo largo de 2020 hemos conocido una nueva modalidad de ataque a esta red llamada «secuestro de WhatsApp», que a día de hoy sigue utilizándose.

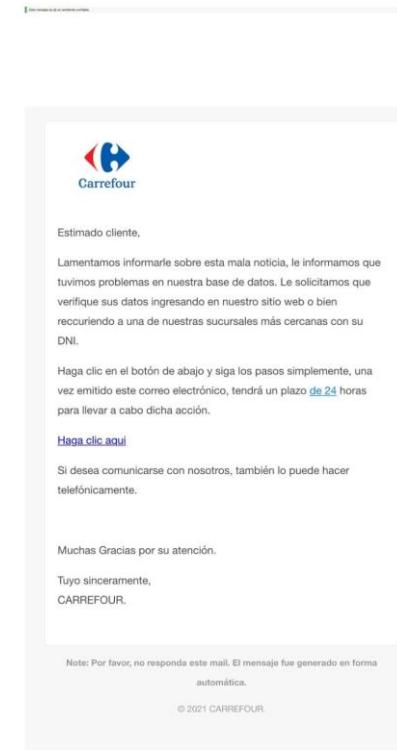
Ola de estafados en Galicia por transferencias fraudulentas: “Me quedé con 10 céntimos en la cuenta”



Laura Gómez • A Coruña  
19/09/2021 • 17:49h. Actualizado: 20/09/2021 • 12:31h.



Andrea Rabondo lee la denuncia que ha puesto en la Guardia Civil tras ser estafada. CEDIDA



**Phishing a través de tu QR o Qrishing: así funciona esta estafa de la que alerta la Policía en España**

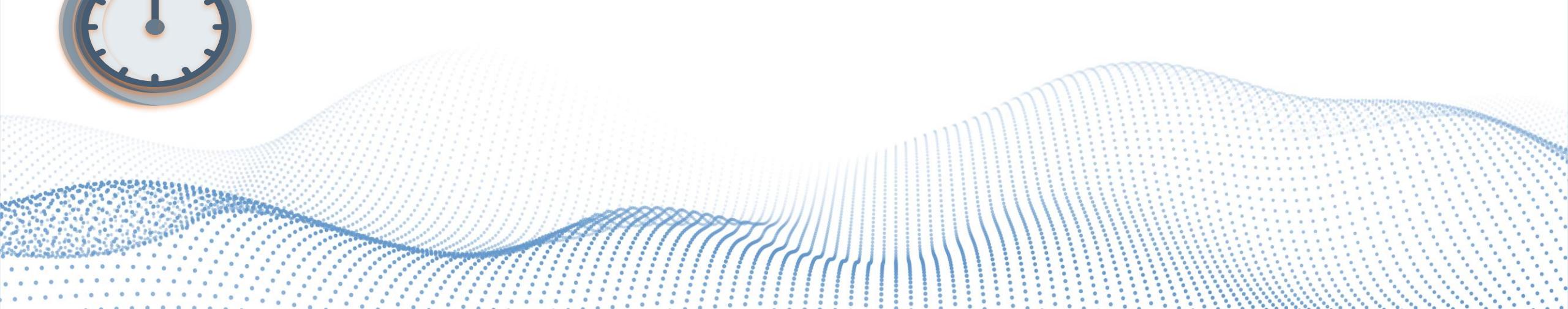
[Facebook](#) [Twitter](#) [Pinteres](#) [Google+](#)



<https://www.incibe.es/protege-tu-empresa/avisos-seguridad>

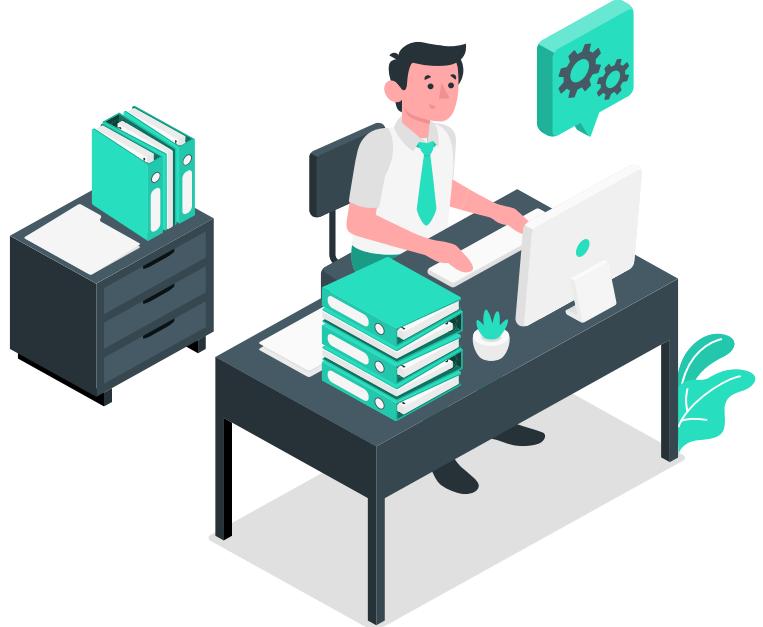
<https://www.incibe.es/suscripciones>

# PARADA 10 -15'



# CONTRASINAIS:

- A – SEMPRE USO A MESMA
- B - USO DIFERENTES PERO NON AS CAMBIO
- C - USO DIFERENTES E CAMBIOAS A MIÚDO



Ciberseguridade

## 4. Contrasinais

### AAA: Autenticación, autorización e auditoría

- AUTENTICACION:** Sei (contrasinal ou código), Son (dato biométrico) ou Teño (token, 2FA)
- AUTORIZACIÓN:** tes as credenciais de acceso e damos permiso para o que o teu perfil está autorizado.
- AUDITORÍA:** rexistro de todas las transacciones.

Ciberseguridade

## 4. Contrasinais

### TIPOS DE ATAQUES

- FORZA BRUTA:** intentar todas las combinaciones
- DICIONARIO:** verificación de listado limitado de combinación (filtraciones ou específicas).
- RAINBOW TABLES:** combinaciones de hashes (identificadores de contrasinais)

Ciberseguridade

## 4. Contrasinais

### TIPOS DE ATAQUES

#### FORZA BRUTA

**Time it takes a Hacker to Brute Force your password**

@coders.bro

Numbers of Character	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 Secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Are you in green zone?

## Ciberseguridad

## 4. Contrasinais

## TIPOS DE ATAQUES

 DICCIONARIO

muyseguridad.net/2011/02/28/diccionarios-de-contrasenas-para-ataques-de-fuerza-bruta

1º [www.skullsecurity.org](http://www.skullsecurity.org)

En la web se pueden encontrar las 500 pass más usadas, amplia variedad de diccionarios (por idiomas, actores, porno, etc...), nombres sacados de facebook, también tiene una lista con la localización de archivos (linux, windows), extensiones de aplicaciones web (phpmyadmin, apache, phpbb etc...), sin duda es la web más completa que he visto para encontrar el diccionario específico que buscamos para fuerza bruta.

\*.txt.bz2  
\*.txt

2º [www.insidepro.com](http://www.insidepro.com)

Trae consigo diccionarios por idiomas y algunos hecho por la misma web (InsidePro), también trae el mítico diccionario de milw0rm.com y uno de hashkiller.com, además también trae un compacto con los nombres de Facebook. A mi personalmente me gusta mucho por que es muy ordenada y clara la web.

\*.rar ->  
\*.dic

3º [packetstormsecurity.org](http://packetstormsecurity.org)

Aquí se puede encontrar diccionarios de los que se les ocurra (asteroides, rock, mitos y leyendas, cine, jazz, nombres, etc...). El único problema es que tienes que buscarlos en una larga lista sin orden lógico.

\*.txt  
\*.txt.gz

4º [www.cotse.com \(1\)](http://www.cotse.com (1))  
[www.cotse.com \(2\)](http://www.cotse.com (2))

Una web que ofrece muchos tópicos: Contraseñas comunes, los términos de Drogas de la calle, nombres de host, las palabras de la Biblia King James, palabras en latín, Minix / usr / dict, nombres de películas, música clásica, música country, jazz, música de otros, la música rock, espectáculos musicales, mitos y leyendas, apellidos de actores, nombres de actor, apellidos anglosajones, entre muchos otros.

\*

Ciberseguridade

## 4. Contrasinais

### TIPOS DE ATAQUES

 DICIONARIO

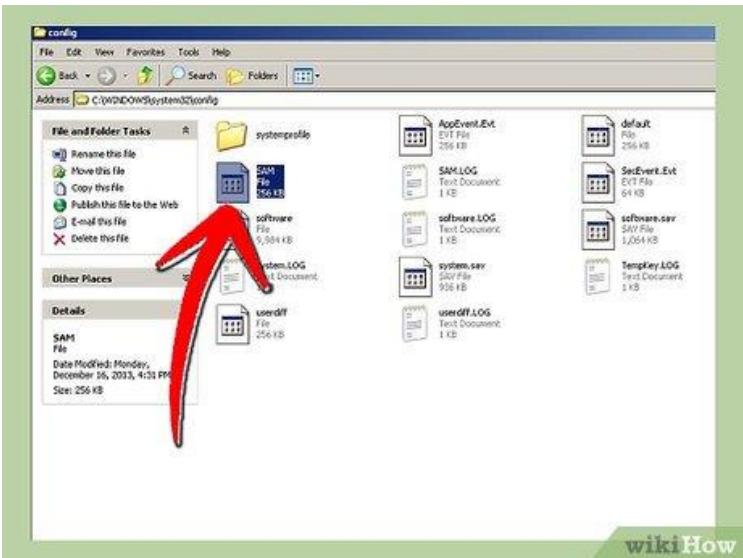
Ranking	Contraseña	Número de usuarios expuestos	Tiempo para romper la contraseña por fuerza bruta
1 ↑ (2)	123456	2543285	Menos de un segundo
2 ↑ (3)	123456789	961435	Menos de un segundo
3 (nueva)	picture1	371612	3 horas
4 ↑ (5)	password	360467	Menos de un segundo
5 ↑ (6)	12345678	322187	Menos de un segundo
6 ↑ (17)	111111	230507	Menos de un segundo
7 ↑ (18)	123123	189327	Menos de un segundo
8 ↓ (1)	12345	188268	Menos de un segundo
9 ↑ (11)	1234567890	171724	Menos de un segundo
10 (nueva)	senha	167728	10 segundos
11 ↑ (12)	1234567	165909	Menos de un segundo
12 ↓ (10)	qwerty	156765	Menos de un segundo
13 ↑ (16)	abc123	151804	Menos de un segundo
14 (nueva)	Million2	143664	3 horas
15 ↑ (28)	000000	122982	Menos de un segundo
16 ↓ (15)	1234	112297	Menos de un segundo
17 ↓ (14)	iloveyou	106327	Menos de un segundo
18 (nueva)	aaron431	90256	3 horas
19 ↑ (29)	password1	87556	Menos de un segundo
20 (nueva)	qqwww122	85476	52 minutos
21 ↑ (199)	123	84438	Menos de un segundo
22 (nueva)	omgpop	77492	2 minutos
23 ↑ (39)	123321	73506	Menos de un segundo
24 ↑ (36)	654321	69148	Menos de un segundo
25 ↓ (22)	qwertyuiop	64632	Menos de un segundo

## Ciberseguridade

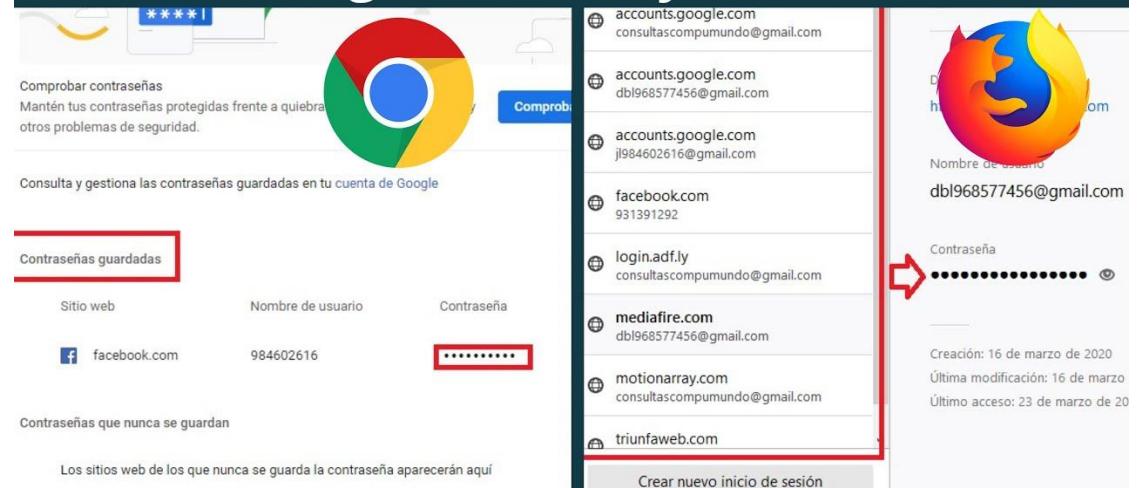
## 4. Contrasinais

### TIPOS DE ATAQUES

#### ☐ RAINBOW TABLES



### Mira Todas las Contraseñas Guardadas en Google Chrome y Firefox



The image compares the password management interfaces of Google Chrome and Mozilla Firefox. Both browsers show a list of saved logins on the right side of the screen.

**Google Chrome:**

- Header: 'Mira Todas las Contraseñas Guardadas en Google Chrome y Firefox'
- Left sidebar: 'Comprobar contraseñas' (Check passwords) with a note about protecting accounts from password cracking.
- Central area: 'Contraseñas guardadas' (Saved passwords) table with columns: Sitio web (Site), Nombre de usuario (Username), and Contraseña (Password).
- Table data:
  - facebook.com, Nombre de usuario: 984602616, Contraseña: [REDACTED]
  - mediafire.com, Nombre de usuario: dbl968577456@gmail.com, Contraseña: [REDACTED]
  - motionarray.com, Nombre de usuario: consultascompumundo@gmail.com, Contraseña: [REDACTED]
  - triunfaweb.com, Nombre de usuario: [REDACTED], Contraseña: [REDACTED]
- Bottom right: 'Crear nuevo inicio de sesión' (Create new session).

**Mozilla Firefox:**

- Header: 'Contraseña' (Password) with a red arrow pointing to it.
- Table data:
  - accounts.google.com, Nombre de usuario: consultascompumundo@gmail.com, Contraseña: [REDACTED]
  - accounts.google.com, Nombre de usuario: dbl968577456@gmail.com, Contraseña: [REDACTED]
  - accounts.google.com, Nombre de usuario: jib984602616@gmail.com, Contraseña: [REDACTED]
  - facebook.com, Nombre de usuario: 931391292, Contraseña: [REDACTED]
  - login.adf.ly, Nombre de usuario: consultascompumundo@gmail.com, Contraseña: [REDACTED]
  - mediafire.com, Nombre de usuario: dbl968577456@gmail.com, Contraseña: [REDACTED]
  - motionarray.com, Nombre de usuario: consultascompumundo@gmail.com, Contraseña: [REDACTED]
  - triunfaweb.com, Nombre de usuario: [REDACTED], Contraseña: [REDACTED]
- Bottom right: 'Creación: 16 de marzo de 2020', 'Última modificación: 16 de marzo', and 'Último acceso: 23 de marzo de 2020'.

Ciberseguridade

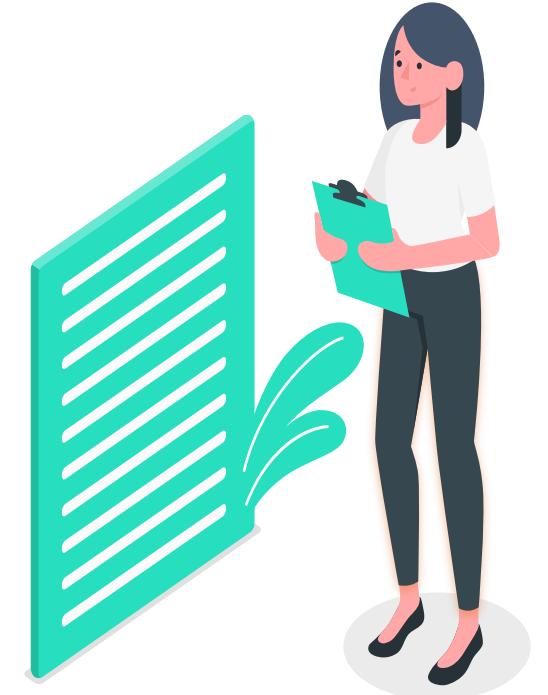
## 4. CONTRASINAIS + ENXEÑERÍA SOCIAL



<https://www.youtube.com/watch?v=RfAdux3XidM>

## ATAQUES USB:

- A - COÑEZO 1 TIPO
- B - COÑEZO 2 TIPOS
- C - COÑEZO 3 TIPOS
- D - ¿PÓDENME ATACAR POR UN USB?

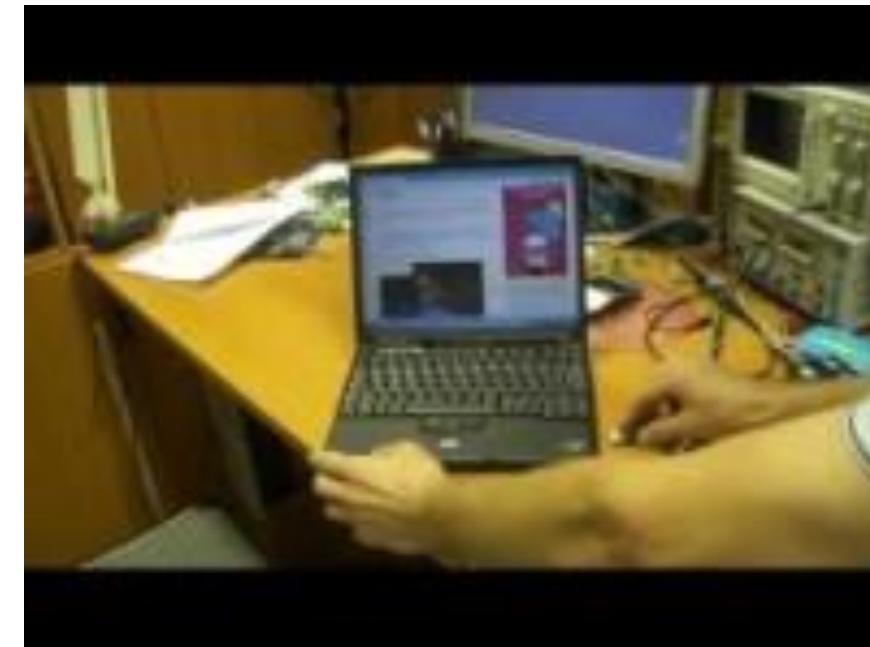


Ciberseguridade

## 5. Conexións por USB TIPOS DE ATAQUES



[http://www.youtube.com/watch?v=qDoCGt\\_7k6s](http://www.youtube.com/watch?v=qDoCGt_7k6s)



[http://www.youtube.com/watch?v=\\_TidRpVWXBE](http://www.youtube.com/watch?v=_TidRpVWXBE)

# CONSELLOS



## 6. CONSELLOS

¿Qué é o mais importante?

### **COPIAS DE SEGURIDADE - REGRA 3-2-1**

<https://www.osi.es/es/copias-de-seguridad-cifrado>

Cuidado ca información sensible

<https://www.aepd.es/es/guias-y-herramientas/herramientas>

Aplicar parches e actualizacíons de forma inmediata.

<https://www.osi.es/es/herramientas>

## 6. CONSELLOS

### Enxeñería social



- CUIDADO ca información que publicamos en redes sociais (internet): persoal ou da organización
- NUNCA dar información por mail, teléfono, redes sociais (especialmente credenciais)

## 6. CONSELLOS

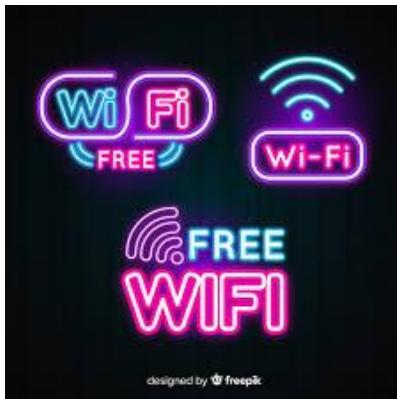
### Enxeñería social



- CUIDADO cas redes ou dispositivos compartidos



## 6. CONSELLOS EXEMPLO WIFI PÚBLICA



\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

pop

No.	Time	Source	SPort	Destination	DPort	Info
11941	48.316964	212.51.32.236		110	192.168.0.14	58828 S: +OK POP3 PROXY server ready <19A823867CA7C727D3260DAF25650390ADCF28E4@quevedo03-1
11944	48.335552	192.168.0.14	58828	212.51.32.236		110 C: CAPA
11948	48.349207	212.51.32.236		110	192.168.0.14	58828 S: +OK Capability list follows
11959	48.367903	192.168.0.14	58828	212.51.32.236		110 C: AUTH DIGEST-MD5
11965	48.378595	212.51.32.236		110	192.168.0.14	58828 + cmVhbG09ImxvZ2luLm11bmRvLXJuY29tTixub25jZT81RUZCfDMSNEVBQUI0NDQ4NzU3NzUyMThCN081Nk
12082	48.682001	192.168.0.14	58828	212.51.32.236		110 C: dxNlcm5hbm91imJwcI9mncnV1Ymp2l1xyZkRsb1012fsad8pY55jb201L05vbmlP5)FRkIwVtzwRUFBQ
13149	53.9088626	212.51.32.236		110	192.168.0.14	58828 S: -ERR ERROR 119 invalid user or password rr 30
13150	53.911179	192.168.0.14	58828	212.51.32.236		110 C: USER prueba@galicia.com
13152	53.921097	212.51.32.236		110	192.168.0.14	58828 S: +OK Password required
13153	53.922095	192.168.0.14	58828	212.51.32.236		110 C: PASS 12345608K_
15927	63.946628	212.51.32.236		110	192.168.0.14	

Post Office Protocol: Protocol

Packets: 17879 - Displayed: 11 (0.1%) - Dropped: 0 (0.0%) | Profile: Default

## 6. CONSELLOS

### Enxeñería social

- CONFIGURAR a seguridad das



#### Configuración de la seguridad

Navegación segura	La navegación segura esti
Notificaciones de inicio de sesión	Las notificaciones de inicio
Aprobaciones de inicio de sesión	No se requiere un códig
Generador de códigos	El generador de códigos ei
Contraseñas de aplicación	No has creado contraseñas de aplicación.
Contactos de confianza	No tienes configurado ningún contacto de confianza.
Dispositivos reconocidos	No hay dispositivos conocidos.
Sesiones activas	Estás conectada desde Vigo, PO, ES y 2 sitios más.
Desactiva tu cuenta.	

Google Cuenta

Buscar en la cuenta de Google

Inicio

Información personal

Datos y personalización

Seguridad

Contactos e información compartida

Pagos y suscripciones

Gestiona tu información, privacidad y seguridad para mejorar tu experiencia en Google

Privacidad y personalización

Consulta los datos almacenados en tu cuenta de Google y elige qué actividad se debe guardar para personalizar tu experiencia en Google

Gestionar tus datos y opciones

Almacenamiento de cuenta

El espacio de almacenamiento que comparte entre los servicios de Google, como Gmail y Fot

6 % utilizado: 1,03 GB

Gestionar almacenamiento

Ver perfil

Belén Pérez Rodríguez  
CISO en Grupo Nueva Pescanova (CEH, CHFI, CPN)

Cuenta

Configuración y privacidad

Ayuda

Idioma

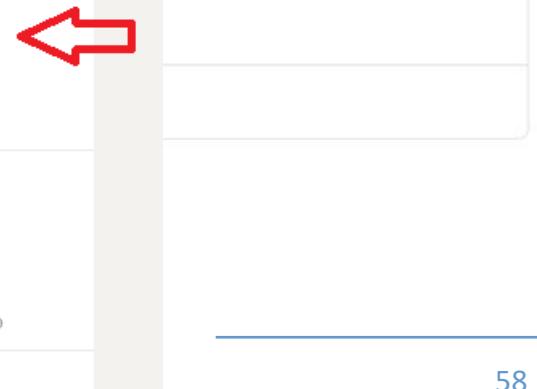
Gestionar

Publicaciones y actividad

Empresa: ViCONgal

Cuenta de anuncios de empleo

Cerrar sesión



## 6. CONSELLOS

### Phishing



- ATENCIÓN os correos que chegan dende contas fora da organización (**DICLAIMER**)
- ATENCIÓN os correos que piden credenciais, datos de terceiros ou traen adxuntos.
- NUNCA abrir ficheiros que cheguen por correo de fontes non confiables.
- NUNCA PINCHAR en enlaces que cheguen por correo.
- DESCONFIADE das gangas, premios, herdanzas o regalos inesperados
- CUIDADO ca información que publicamos en redes sociais (internet): persoal ou da organización
- Cos mails que vemos dende o móvil

# 6. CONSELLOS

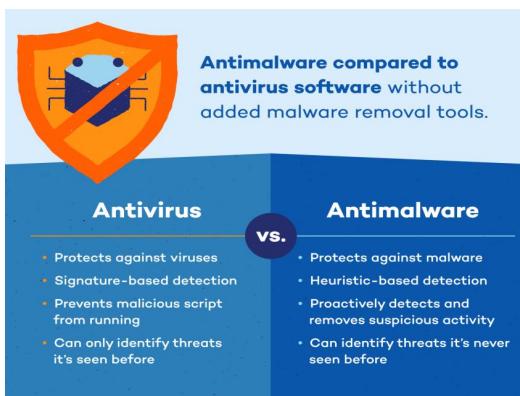
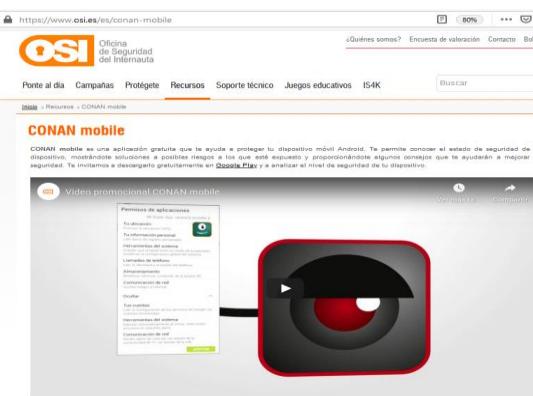
## Phishing

<https://urlscan.io/>

<https://www.expandurl.net/>

<https://getlinkinfo.com/?>

<https://www.virustotal.com/>

<https://www.osi.es/conan-mobile>

**CONAN mobile**

CONAN mobile es una aplicación gratuita que te ayuda a proteger tu dispositivo móvil Android. Te permite conocer el estado de seguridad de tu dispositivo, mostrándote soluciones a posibles riesgos a los que está expuesto y proporcionándote algunos consejos que te ayudarán a mejorar tu seguridad. Te invitamos a descargarlo gratuitamente en [Google Play](#) y a analizar el nivel de seguridad de tu dispositivo.



<https://www.osi.es/servicio-antibotnet>

**Servicio AntiBotnet**

Nuestro servicio AntiBotnet pone a tu disposición mecanismos para poder identificar si desde tu conexión a Internet (siempre que lo utilices dentro de España) se ha detectado algún incidente de seguridad relacionado con botnets u otras amenazas, ofreciéndote información y enlaces a herramientas que te pueden ayudar en la desinfección de tus dispositivos.

Este servicio se ofrece de dos formas:

- La primera se lleva a cabo mediante los operadores de servicios de Internet que colaboran con nosotros notificándote de los incidentes de seguridad que afectan a tu conexión. Si has recibido un mensaje de tu operador, consulta el código que te ha proporcionado y obtén la información directamente.
- La segunda es mediante el uso de nuestras herramientas online.

**Si tu operador de servicios de Internet te ha enviado un código de Incidente**

**Usa el servicio online y obtén respuesta al instante**

**Consulta tu código**

**Cómo funciona el servicio de notificación de códigos?**

**Chequea tu conexión**

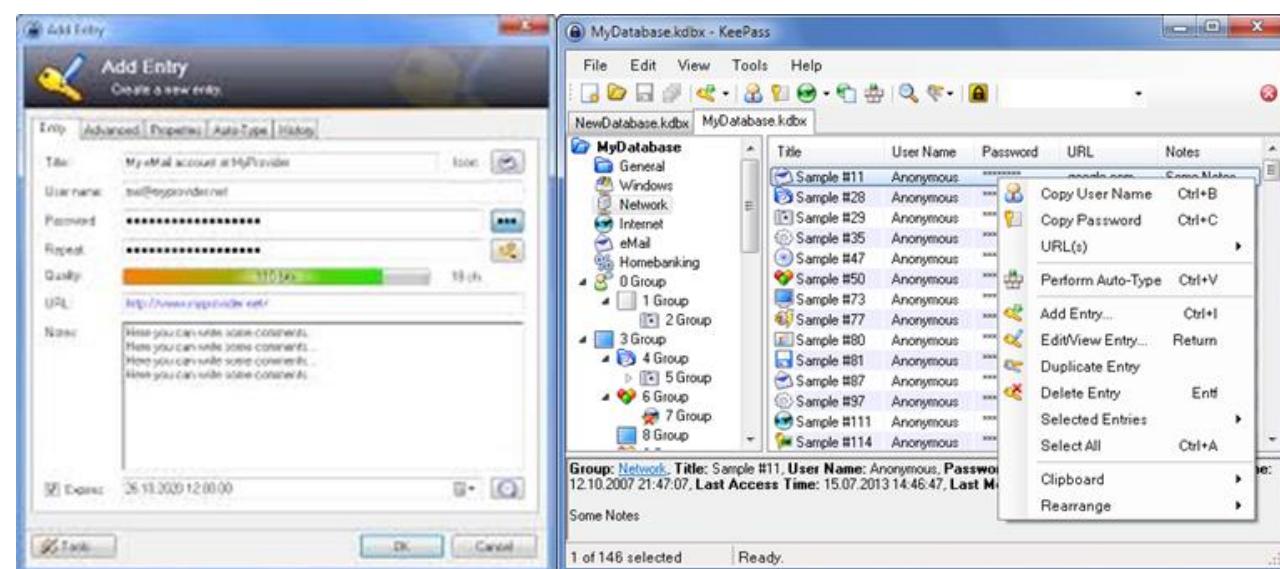
**Cómo funciona el servicio de chequeo?**

## 6. CONSELLOS Contrasinais

<https://haveibeenpwned.com/>



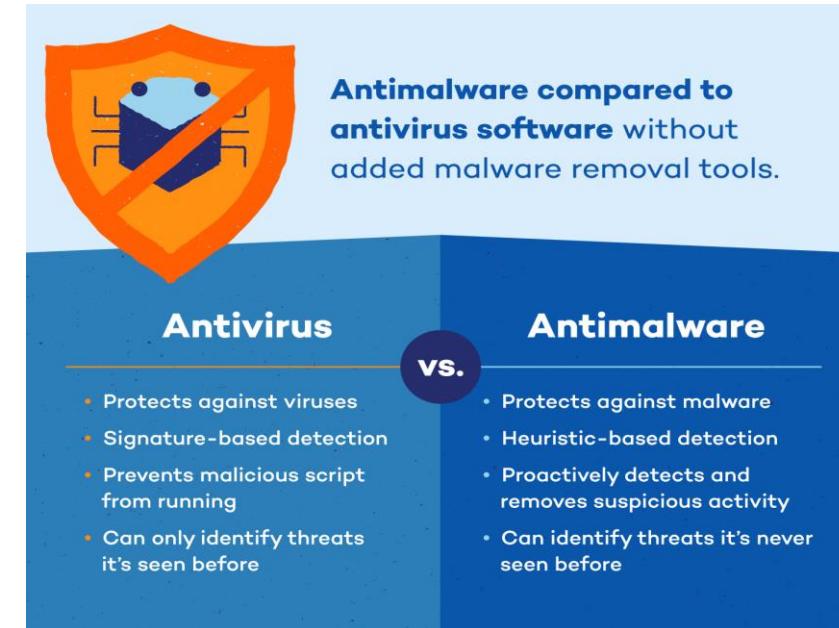
2FA



Xestores de contrasinais

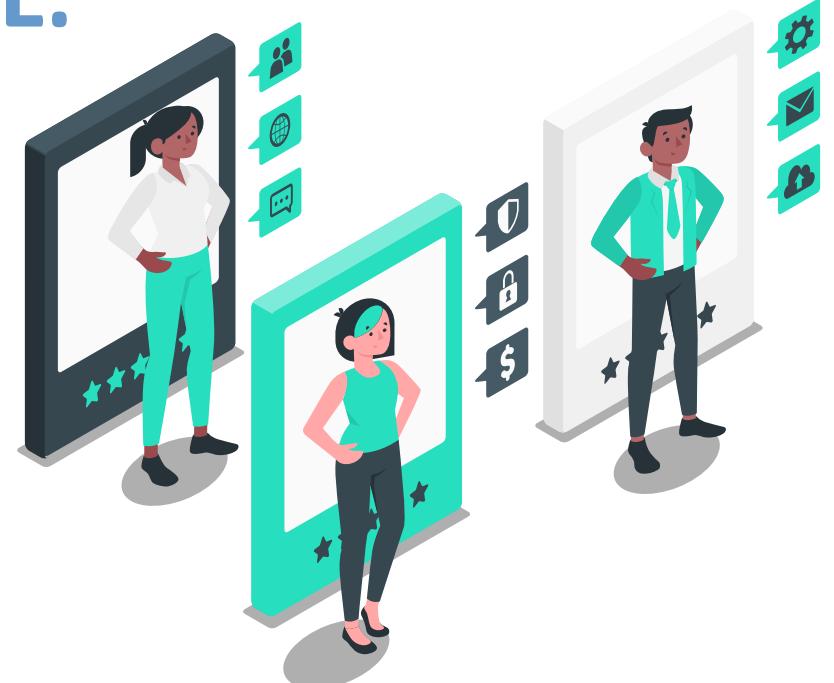
## 6. CONSELLOS

### Conexións USB



# TEÑO ANTIMALWARE NO MÓVIL:

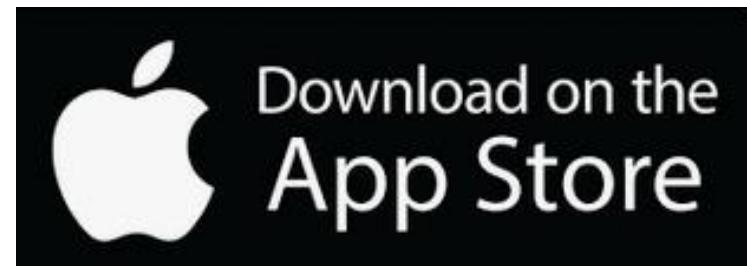
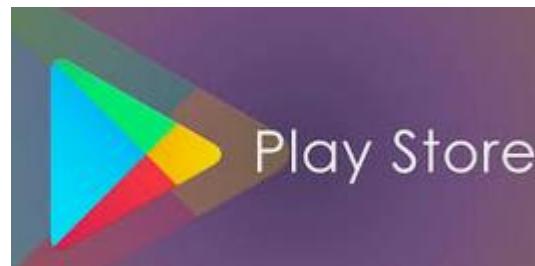
- A - SI
- B - NON
- C – NON HAI PARA MÓVIL
- D – SO SE NON USO IPHONE



## 6. CONSELLOS

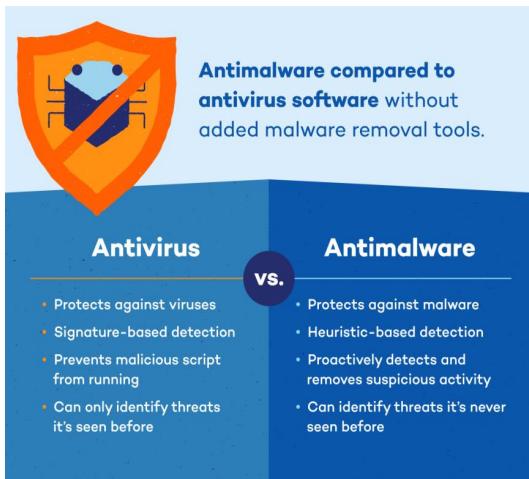
### Smartphones

- MANTER AS APLICACIÓNS ACTUALIZADAS
- RESTRINXIR ACCESOS
- DESCARGAR APPS DE SITIOS **CONFIABLES**
- USAR MFA SEMPRE QUE SEXA POSIBLE
- DESINSTALAR APPS NON USADAS E/OU PREINSTALADAS



# 6. CONSELLOS

## Smartphones




CONAN mobile

¿Qué es CONAN mobile?

Una aplicación GRATUITA que realiza la comprobación integral de SEGURIDAD de tu smartphone y tablet.

¿Qué necesito para utilizarlo?

Un dispositivo Android con versión 2.2 o superior y acceso a Internet.

¿Cómo puedo instalarlo?

La aplicación está disponible en Google Play.

¿Qué tipo de información me proporciona?

Estado global de seguridad de tu dispositivo.

Riesgo Requiere atención Correcto Pendiente

Análisis de seguridad detallado:

Configuración

Analisis de la configuración del sistema operativo Android que pueden suponer un riesgo de seguridad, clasificados de acuerdo a su nivel de riesgo.

Problemas Requiere atención

Aplicaciones

Analisis de peligrosidad de las aplicaciones instaladas en el dispositivo. Los resultados del análisis pueden ser:

Malicosa: Basada de aplicaciones que han sido fabricadas o que tienen un comportamiento peligroso según varios antivirus.

Sospechosa: es detectada como peligrosa por varios antivirus.

Permisos

Clasificación de los permisos que declaran las aplicaciones tanto por permisos más relevantes (Básico) como por categoría de riesgo (Completo).

Alto Media Bajo Otros

Servicio proactivo

Alerta a los usuarios de comportamientos anómalos y potencialmente maliciosos.

Eventos

- Cambios en el fichero /etc/host
- Detección de conexiones a redes WiFi inseguras
- Comprobación de nuevas aplicaciones
- Llamadas y envío de mensajes a números de tarificación especial (servicios Premium)
- Detección de conexiones potencialmente maliciosas
- Detección de amenazas de seguridad relacionadas con Botnets

Conexiones

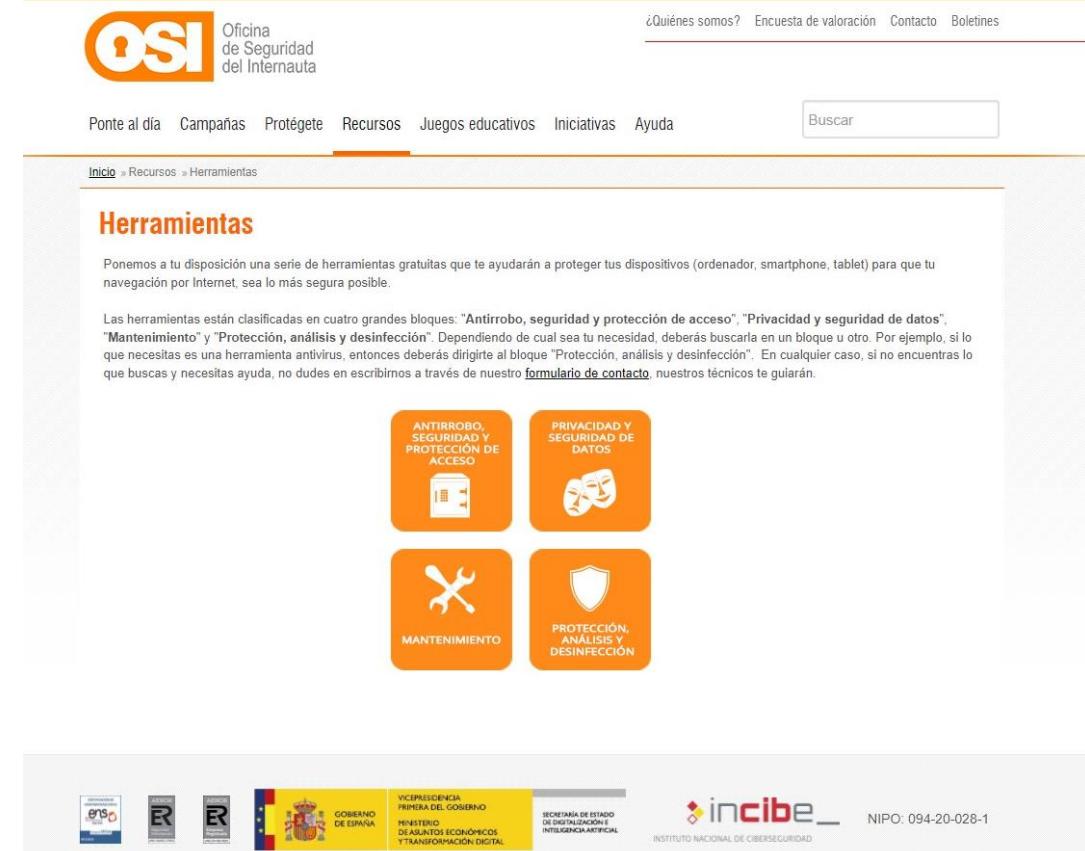
Muestra las conexiones de red realizadas por las aplicaciones instaladas advirtiendo al usuario de aquellas que son potencialmente maliciosas. Además se podrá obtener información extendida de cada una de las conexiones, como por ejemplo, la geolocalización de la dirección IP.

Consejos OSI

Recomendaciones de la Oficina de Seguridad del Internauta.

incibe\_ osi

<https://www.osi.es/es/herramientas>



osi Oficina de Seguridad del Internauta

¿Quiénes somos? Encuesta de valoración Contacto Boletines

Ponte al día Campañas Protégete Recursos Juegos educativos Iniciativas Ayuda Buscar

Inicio » Recursos » Herramientas

## Herramientas

Ponemos a tu disposición una serie de herramientas gratuitas que te ayudarán a proteger tus dispositivos (ordenador, smartphone, tablet) para que tu navegación por Internet, sea lo más segura posible.

Las herramientas están clasificadas en cuatro grandes bloques: "Antirrobo, seguridad y protección de acceso", "Privacidad y seguridad de datos", "Mantenimiento" y "Protección, análisis y desinfección". Dependiendo de cual sea tu necesidad, deberás buscarla en un bloque u otro. Por ejemplo, si lo que necesitas es una herramienta antivirus, entonces deberás dirigirte al bloque "Protección, análisis y desinfección". En cualquier caso, si no encuentras lo que buscas y necesitas ayuda, no dudes en escribirnos a través de nuestro [formulario de contacto](#), nuestros técnicos te guiarán.

<b>ANTIRROBO, SEGURIDAD Y PROTECCIÓN DE ACCESO</b>	<b>PRIVACIDAD Y SEGURIDAD DE DATOS</b>
<b>MANTENIMIENTO</b>	<b>PROTECCIÓN, ANÁLISIS Y DESINFECCIÓN</b>

incibe\_ INSTITUTO NACIONAL DE CIBERSEGURIDAD NIPO: 094-20-028-1

Ciberseguridad

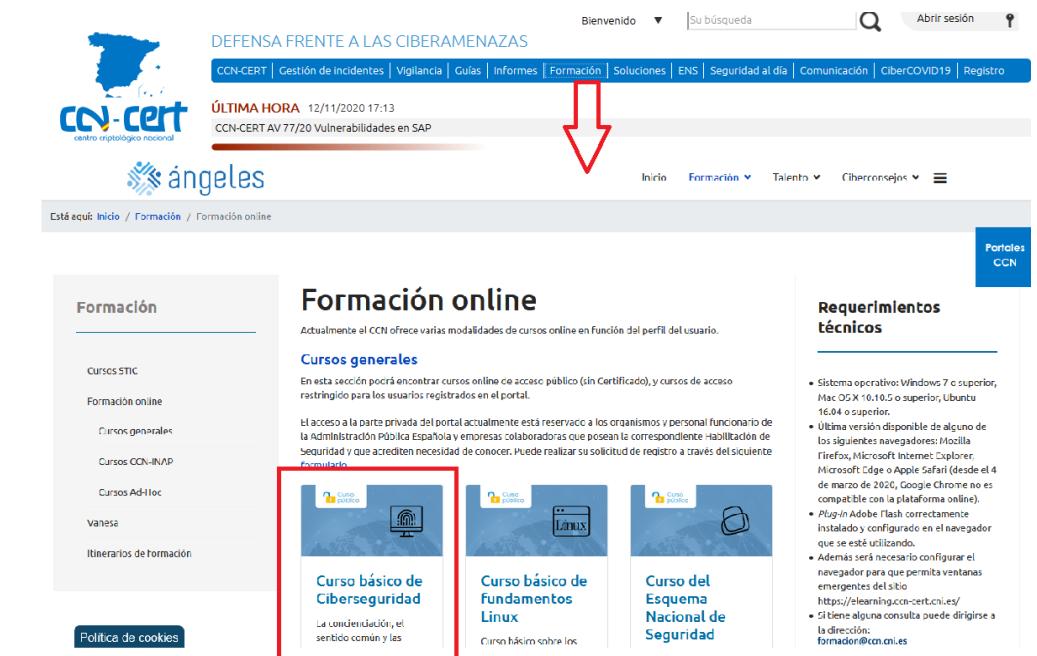
# 6. CONSELLOS

## Formación



<https://www.incibe.es/protege-tu-empresa/formacion>

<https://www.incibe.es/formacion>



<https://angeles.ccn-cert.cni.es/index.php/es/menu-formacion-es>



# DUDAS PREGUNTAS ACLARACIONES



## Contacto

**Belén Pérez Rodríguez**

@BPR\_Vigo

<https://www.linkedin.com/in/belenpr/>

[belperod@gmail.com](mailto:belperod@gmail.com)