



Financiado por  
la Unión Europea  
NextGenerationEU



Gobierno  
de España

MINISTERIO  
PARA LA TRANSFORMACIÓN DIGITAL  
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE  
ESTADO  
DE DIGITALIZACIÓN  
E INTELIGENCIA ARTIFICIAL



Plan de  
Recuperación,  
Transformación  
y Resiliencia

incibe\_  
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# SOBREVIVIENDO EN LAS REDES SOCIALES



Campus Tecnológico-Deportivo para  
Jóvenes

Universidad de Oviedo



JOSÉ MANUEL REDONDO LÓPEZ PROYECTO "F-31 'DESCUBIERTA'" v1.4





# ACERCA DEL USO DE CONTENIDO GENERADO POR IA



José Manuel  
Redondo López

- En esta presentación se usan algunas imágenes generadas por IA
  - Salvo error, cualquier imagen a la que no se le atribuya una fuente u origen expreso
- La IA generativa usada para ello es Microsoft Copilot
  - <https://copilot.microsoft.com/>
- Se ha restringido el uso de estas imágenes a la ilustración de los conceptos explicados en algunas de las páginas
  - Es decir, **como refuerzo visual** a lo explicado en algunas transparencias
  - El procedimiento ha sido describirle a la IA con toda la precisión posible los elementos que quería que apareciesen en la imagen (**prompt**)
    - Y la selección del mejor resultado obtenido, a juicio del autor de esta presentación
    - **No se ha mencionado ni indicado que se copie el estilo a ningún autor, ni que se plagien obras concretas**
- El autor declara expresamente su apoyo al trabajo de los artistas, ilustradores y creadores, de extrema importancia en la actualidad
  - El uso de estas técnicas se ha hecho solo con fines de mejora de las explicaciones, y cuando la alternativa era **no contar con refuerzos visuales** por restricciones de tiempo y presupuesto



José Manuel  
Redondo López

# ¡BIENVENIDO!

## • ¿Hace poco que te has metido en RRSS y no sabes exactamente qué hacer para protegerte?

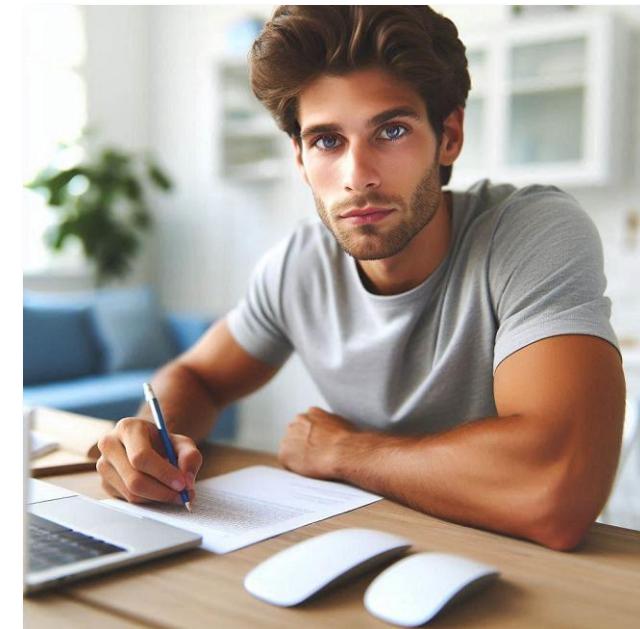
- Te voy a contar los **peligros** principales a los que te puedes enfrentar 🎯
- Y también formas de **defenderte** contra ellos ⚡
- Así podrás **investigar contenidos y personas** y ¡protegerte! 🛡️
- A ti y a los demás ¡se el/la “campeón/a de seguridad” de tus panas!

## • Las RRSS pueden ser un sitio donde aprendas y compartas mucho, hagas amigos, te rías y lo pases bien 😊

- No me verás decirte que no las uses, todo lo contrario ⚡
- ¡Pero no dejes que ningún/a loser te arruine la experiencia! 😢

## • Recuerda que es tu “ventana al mundo”

- Y que en el mundo hay muchos tipos de personas
- A unos querrás tenerlos cerca...y **otros querrás bloquearlos para siempre**
- Debes aprender a distinguirlos...¡y a expulsarlos de tu ciber-vida!



¿Estás listo/a para tomar nota y aprender? ☺



José Manuel  
Redondo López

# ¿Y TODO EL RESTO DE MATERIAL?

- **¿Sabías que en Asturias hay un programa de formación integrado por niveles en ciberseguridad? Ahora ya sí**

- Yo soy la persona que está detrás de esta idea
- Toco muchos “palos” y cada uno tiene un nombre de barco

- **¿Cómo “enrolarte” en la armada asturiana?**

- Ofrezco **muchos contenidos gratuitos**
  - Durante este curso se hará referencia a otros complementarios que te regalo y que forman parte de la misma iniciativa
  - Puedes encontrarlos en: [https://github.com/jose-r-lopez/Formacion\\_-Seguridad\\_Joven/wiki](https://github.com/jose-r-lopez/Formacion_-Seguridad_Joven/wiki)
  - En el futuro quiero subir videos explicando cada curso en mi canal: <https://www.youtube.com/@JoseRedondo-dj7xk>
- También **imparto clases en la Universidad de Oviedo**
  - Grado en Ingeniería Informática del Software (GIISOF)
  - Máster Universitario en Ingeniería Web (MIUNGEWEB)
  - Micro credenciales (MU), Diplomas y Máster de Formación Permanente (MFP) en temas de Ciberseguridad (Títulos Propios)



**TODOS (gratuitos y no gratuitos) están conectados entre ellos y regidos por los mismos estándares de creación y criterios de calidad**

**Gratis no implica peor, sino pensado para servicio público**



**La "Armada Asturiana" por José Manuel Redondo López**



**Respuesta a indecentes**  
S-64 "Narval"



**No apto para menores**  
*Peligros para los menores en Internet*  
"A-71 Juan Sebastián Elcano"



**La Mente del Crimen**  
*Mentes criminales y engaño*  
M-31 "Segura"



**Ataques contra Personas**  
Ciberacoso  
P-74 "Atalaya"



**Investigación de Webs**  
*Detección de webs problemáticas*  
S-74 "Tramontana"



**Investigar Redes Sociales**  
*Técnicas de investigación para RRSS*  
F-31 "Descubierta"



**Configuración Segura Básica**  
*Asegura tus PCs y dispositivos móviles*  
R-01 "Dédalo"

**Rango 1**  
(Marinero)



**Ciberseguridad General**  
*Ciberseguridad general para el día a día*  
F-74 "Asturias"



**Crime-spotting**  
*Ejemplos de fraudes reales para su estudio*  
"Nautilus"



**Para vosotr@s, Programador@s**  
*Técnicas básicas de codificación segura*  
C-23 "Ferrol"



**Vigilancia de Redes**  
*Ataque y defensa en redes modernas*  
F-83 "Numancia"

**Rango 2**  
(Marinero de Primera)



**Rango 3**  
(Cabo)





**La "Armada Asturiana" por José Manuel Redondo López**



### Introducción a la Ciberdefensa Personal

Técnicas generales contra ciberataques (Niveles A1, A2)  
Cursos G-9, PDI, Pr. DIGICOMPEDU. "BPM P-51 'Asturias'"



### Ciberdefensa Personal Avanzada

Técnicas avanzadas contra ciberataques (Niveles B1, B2)  
Cursos G-9, PDI, Pr. DIGICOMPEDU. "BPM P-51 'Asturias'"

### Investigación con Fuentes Abiertas (OSINT)

Técnicas de investigación con fuentes abiertas  
OCW (parcialmente). "A-21 Poseidón"



### Seguridad de Redes

Threat hunting  
TBA. L-52 "Castilla"

### Administración Segura de SO

Infrastructure as Code  
MUINGWEB, OCW. L-62 "Princesa de Asturias"

### Defensa contra el Cibercrimen

Identificación y lucha contra el cibercrimen  
Divulgación pública, cursos. P-45 Audaz"



**Rango 4 (Sargento)**



**Rango 5 (Suboficial Mayor)**



**Rango 6 (Capitán de Fragata)**



### Liderazgo en Ciberdefensa para Equipos

Herramientas y estrategias de protección (Nivel C1)  
Proyecto DIGICOMPEDU. "BPM P-51 'Asturias'"



### Identificación y Análisis de Vulnerabilidades en Web

Seguridad ofensiva:  
Reconocimiento y Explotación  
MUINGWEB, TK-210 "красный  
октябрь" (Octubre Rojo)



### Arquitecturas de Seguridad

Arquitectura de infraestructuras seguras  
Guías INCIBE, F-105 "Cristóbal Colón"



### Desarrollo Seguro de Software

Platform engineering seguro  
Guías INCIBE. F-113 "Menéndez de Avilés"



### El lado oscuro de la red

Desinformación y ciberguerra  
TBA. "Flying Dutchman"



### Post-Exploiting e Intrusión en Sistemas

Seguridad ofensiva:  
Post-Explotación  
TBA. K-329  
"Belgorod"



### Protección de Servidores y Aplicaciones Web

CISOs de perfil técnico  
MUINGWEB. D-73 "Blas de Lezo"

**Rango 7 (Vicealmirante)**





La "Armada Asturiana" por  
José Manuel Redondo López



## Introducción a la construcción de sistemas seguros y rol del CISO

CISOs de perfil técnico  
Microcredenciales. C-33  
"Blas de Lezo"

(D-73 + coordinación de 12 microcredenciales)



## Explotación y Post-Explotación de Sistemas

Seguridad ofensiva: Recorrido completo del MITRE ATT&CK  
TBA, RK-085 "Адмирал Нахимов"  
(Admiral Nakhimov)

(TK-210 + K-329)

Rango 8  
(Almirante)



## Defensa Integral de Sistemas

CISOs de perfil técnico + formación integral en ramas técnicas  
TBA. B-41 "Sigillum Regiae Universitatis Ovetensis" (SRUO)

(D-73 + F-113 + L-62)



## Técnicas, Tácticas y Procedimientos de Explotación y Post-Explotación a Máquinas y Usuarios

Seguridad ofensiva: Recorrido completo del MITRE ATT&CK + OSINT Framework  
TBA, B-51 "Rex Pelagius"

(RK-085 + A-21)

Rango 9  
(Almirante General)





# ÍNDICE

- 👻 [¿Para qué vale una red social?](#)
- 💰 [¿De dónde saca la pasta una red social?](#)
  - 🔥 [Las redes sociales son gratis ¿verdad? ¿VERDAD?](#)
  - 🤬 [No seas adicto a la bronca y al conflicto](#)
- 😱 [¿Cómo me “enfrento” a una red social?](#)
  - 📝 [Configurar una red social](#)
  - 😷 [Precauciones usando una red social](#)
- 🤔 [¿Qué pasa con la información que pongo en RRSS?](#)
  - 😢 [La persona detrás de una cuenta de una red social](#)
- 👤 [Precios en la dark web de los datos que nos roban](#)
- ➡️ [Más información...](#)



Accede a este  
Módulo en YouTube



# 👻 ¿PARA QUÉ VALE UNA RED SOCIAL?

Pensemos en los usos que le podemos dar...





José Manuel  
Redondo López

# ¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?



## ● En este bloque te voy a enseñar...

- A responderte a ti mismo/a estas preguntas
  - *¿Alguna vez te has parado a pensar en los pros y contras de una red social? ¿No? Pues yo te los voy a explicar aquí 😊*
  - *¿Te has parado a pensar que en las redes sociales hay tanto gente buena como mala?*
  - *¿O que, aparentemente, quiere ser amigo tuyo, pero su intención es otra MUY distinta? 😠*
- Además de advertirte de que, con esto de la **inteligencia artificial**, vas a tener que mirar todo varias veces
  - ¡Porque las formas de engañarnos están avanzando mucho! (los deepfakes y sus movidas)





José Manuel  
Redondo López

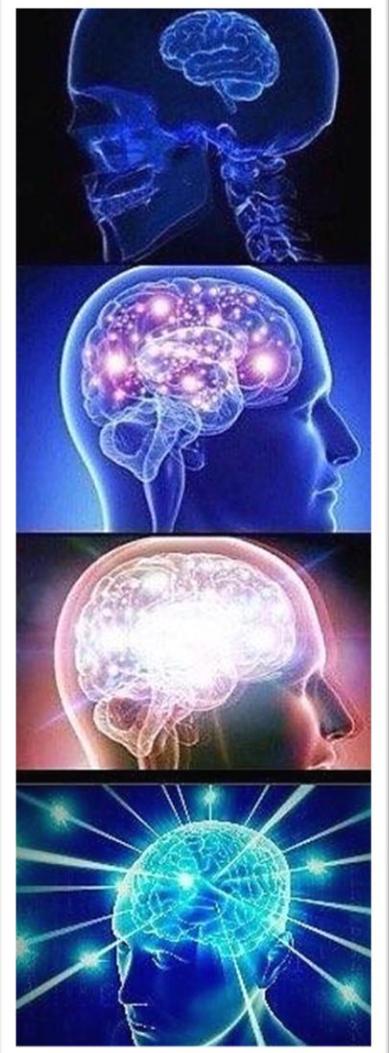
# ¿PARA QUÉ VALE UNA RED SOCIAL?

## ● *¿Alguna vez os habéis parado a pensar para todo lo qué vale una red social?*

- ¡Seguro que sí!
- Pero... ¿**todos** los "usos" que se le pueden dar? Eso es más complicado...

## ● Vamos a repasar los más típicos...

- ...y también vamos a ver cómo cada uso positivo tiene un..."lado oscuro"
- **¡Para saber cómo protegernos!**



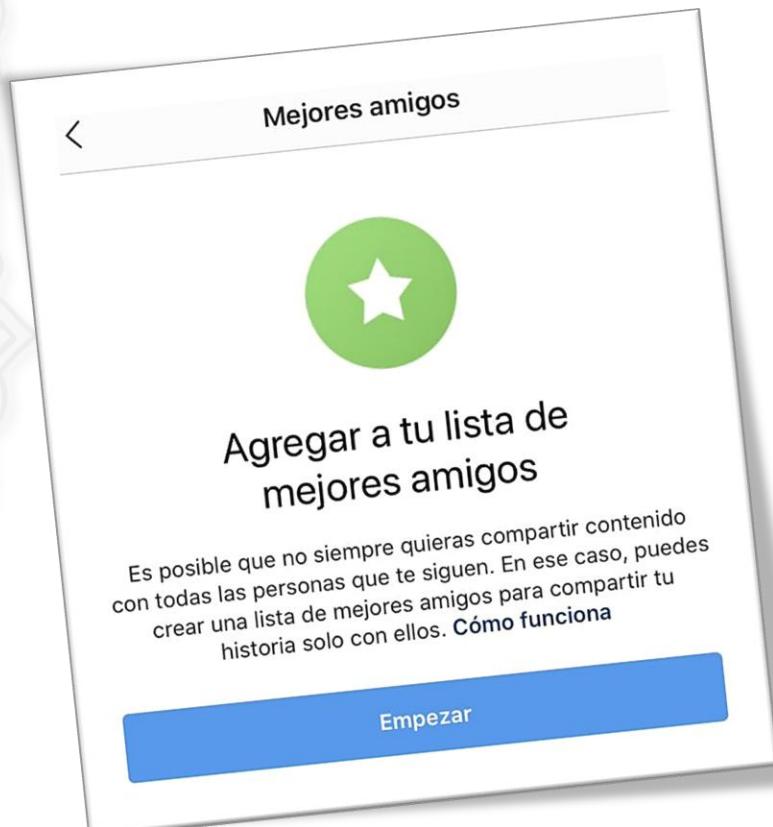
# ¡HACER AMIGOS!



José Manuel  
Redondo López

- ¡Darte a conocer a otras personas que merecen la pena es lo mejor de una red social!
- ¡Puedes tener amigos en todo el mundo!
  - En mi época (cuando los dinosaurios dominaban la tierra) eso se hacía en los bancos de un parque
- Conoces a otras personas con gustos, aficiones, hobbies...y muchas otras cosas en común contigo

¡Ganando!



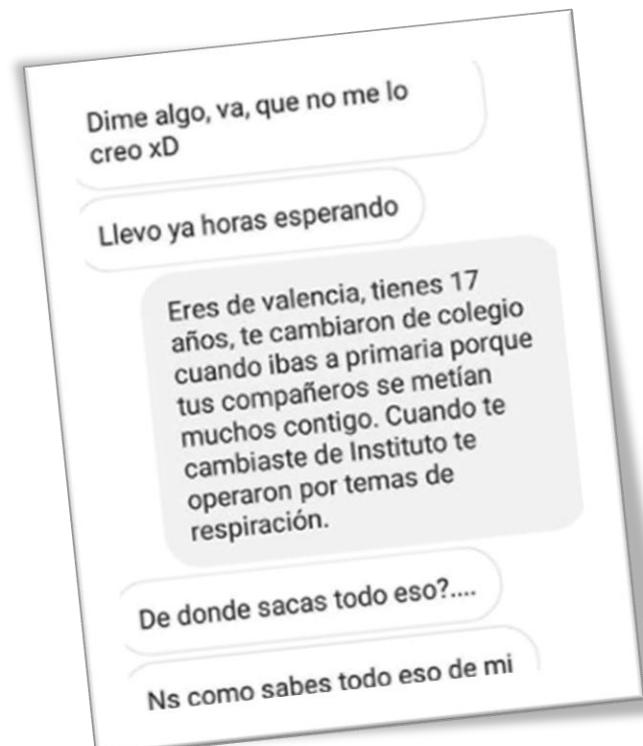
# ¿HACER “AMIGOS”?



José Manuel  
Redondo López

- Pero poder hacer amigos en todas partes tiene también su parte menos buena
- A veces hay cierto tipo de gente no recomendable...

- No son quienes dicen ser (**suplantan** a otras personas) 😎
- Bromistas / trolls / ...con **CERO gracia** 😢
- Ofrecen una imagen de sí mismos que **no es la real** 😏
  - No conoces a una persona, ¡conoces a un personaje!
- Gente que en realidad sólo quieren “**venderte**” algo 💰
  - No necesariamente que compres cosas (loot boxes, gachas,...)
  - También que pienses como él/ella...
- O personas directamente **malvadas** 😈



**¡Pero que no te “coman la cabeza”!**

# ¡COMPARTIR IDEAS, TRABAJOS...!

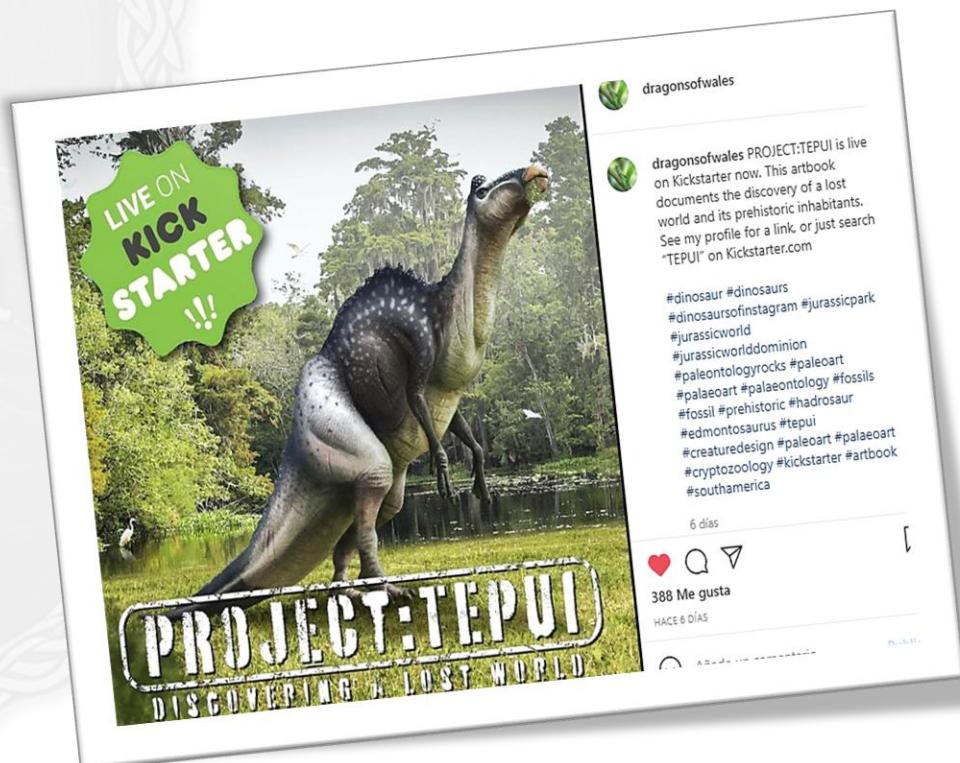


José Manuel  
Redondo López

- Seguro que eres alguien con cosas que decirle a los demás, expresarte, compartir...

- Ideas
- Trabajos artísticos o de cualquier tipo
- Tus hobbies (o lo que haces día a día)
- Tus deportes / aficiones y cómo las practicas (resultados, premios...)
- ...

¡Ganando!



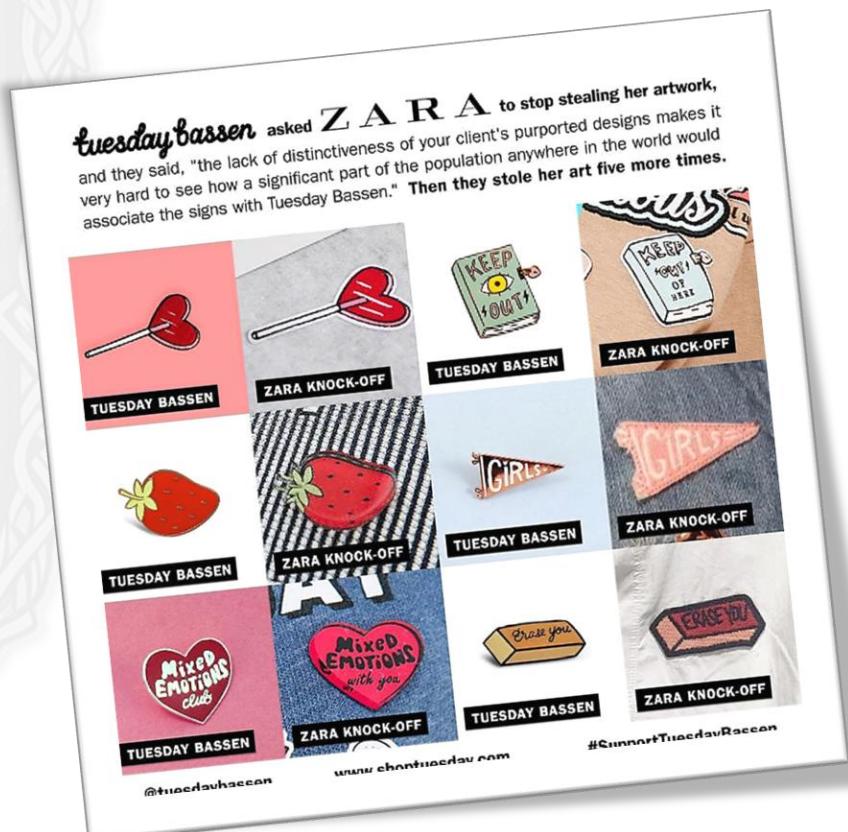
# ¿“COMPARTIR” IDEAS, TRABAJOS...?



José Manuel  
Redondo López

## ● Pero si compartes cosas de ti mismo, hay que tener en cuenta que...

- Si son obras artísticas/opiniones, alguien se las puede **apropiar, robar, decir que son tuyas...**  
  - Es importante firmar cada cosa que uno hace
  - ¿Subes imágenes? ¡Investiga sobre **marcas de agua!**
- Los **trolls y las críticas** pueden aparecer fácilmente, hagas lo que hagas 
  - Hay gente **MUY ABURRIDA** en la vida
  - Criticar por deporte, placer o porque necesita “casito”
  - **CUIDADO:** Esto puede hacerte daño 😞



**¡Pero hay que estar preparado para resistir a los envidiosos! (tu Nvidia hase fuersha ;))**



José Manuel  
Redondo López

# ¡INFORMARTE DE TODO!



- Las redes sociales tienen canales (o similares) temáticos de cosas que te interesan

- ¡Donde normalmente están todas las novedades de aquello que más te gusta! 😊

- Y posteado por gente que sabe de lo que habla

- Incluso lo prueban por ti

- Y, además, de tu rollo 🤦

- De **edad parecida** a la tuya (¡fuera carrozas!)
- O que **hablan para que se les entienda** (nadie quiere a un chulo bashilandote de sus movidas)

- A veces, incluso con sorteos o giveaways

- ¡A lo mejor te toca algo solo por seguir a alguien! 🍀



Fuente: <https://laboratoriodeperiodismo.org/los-usuarios-de-redes-sociales-buscan-cada-vez-mas-noticias/>

# QUE TE DESINFORMEN...



José Manuel  
Redondo López



## ¿CÓMO COMBATIR LA DESINFORMACIÓN?

### ● Pero también hay peña que está malita y te cuenta tremendos bulardos

- Para que **compres** lo que les interesa (les pagan)
- Para que **pienses** lo que les interesa (les pagan)
- Para que **odies** lo que les interesa (sorpresa, les pagan)
- Para que **les sigas** a ellos (y desprecies a otros)

  - A lo mejor no le pagan, pero gana dinero contigo

- Para que **creas** lo que les interesa (sí, les pagan)
  - Con los **deepfakes** y la IA es un **PROBLEMON**
  - No podemos creer lo que vemos en **fotos**
  - Tampoco lo que oímos en **audios**
  - Ni siquiera en **videos**
  - **Todo podría ser falso**
- Veremos más en el **M-31 "Segura"**



ORIGINAL

DEEPCODE



#### ¿QUÉ ES LA DESINFORMACIÓN?

Se trata de noticias falsas y engañosas que puedes encontrar en Internet o cualquier otro medio sobre un acontecimiento. Muchas veces son creadas de forma intencional, para manipular a los lectores y generar una reacción en ellos.

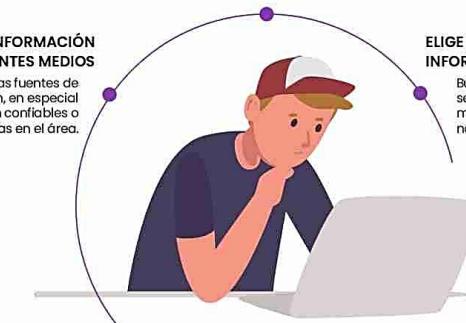
#### 5 CONSEJOS PARA COMBATIR LA DESINFORMACIÓN

##### NO CREAS EN TODO LO QUE TE DIGAN

Las personas a tu alrededor también pueden ser víctimas de la desinformación, y compartir noticias falsas sin saberlo.

##### REVISA LA INFORMACIÓN EN DIFERENTES MEDIOS

Utiliza distintas fuentes de información, en especial si son confiables o especialistas en el área.

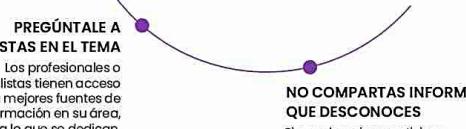


##### ELIGE UNA FUENTE DE INFORMACIÓN CONFIALBE

Busca si esta información se ha publicado en medios más confiables como noticieros o periódicos.

##### PREGÚNTALE A ESPECIALISTAS EN EL TEMA

Los profesionales o especialistas tienen acceso a mejores fuentes de información en su área, pues es a lo que se dedican.



##### NO COMPARTAS INFORMACIÓN QUE DESCONECES

Si no sabes si una noticia es verdadera, no la compartas con tus conocidos. Así también los ayudarás a combatir la desinformación.

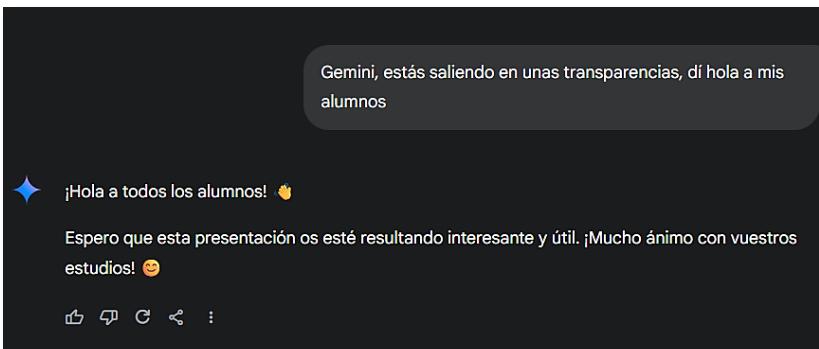
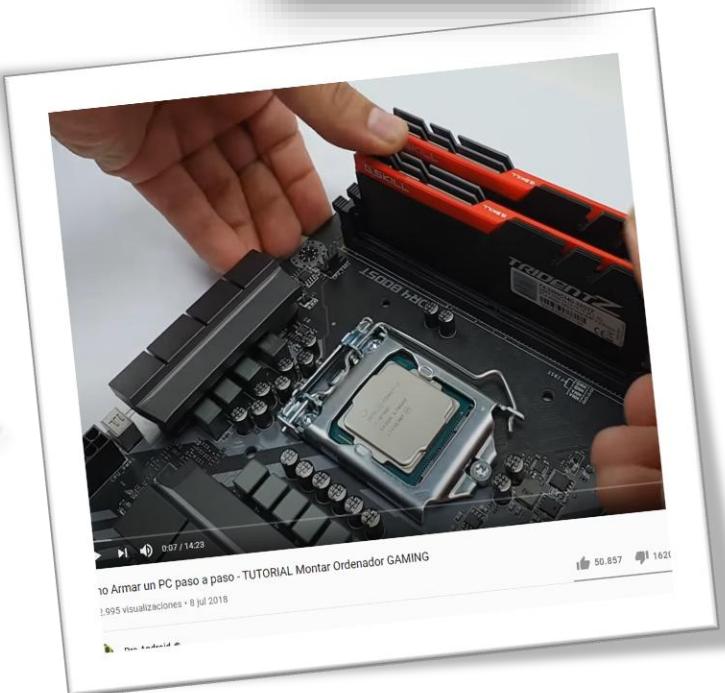
# ¡APRENDER COSAS NUEVAS!

- Internet es **EL SITIO** para aprender cosas nuevas 🤔
- Wikipedia 📖, YouTube 🎥, IAs generativas 🤖 ...
  - **TODA** la información de **TODAS** las cosas que puedas imaginar o querer aprender...
  - ¡Está ahí, a tu alcance!
- Hay información, cursos y tutoriales en video de lo que quieras, cuando quieras...
  - Normalmente, es mucho más fácil de aprender que leerlo en un libro 😊
  - Que no te digan lo contrario: **todo lo que puedas aprender te va a ser útil en algún momento**

## ¡Ganando!



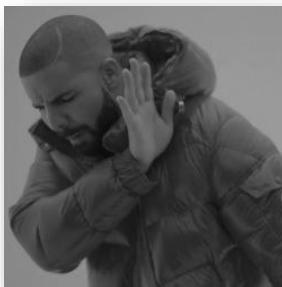
José Manuel  
Redondo López



# **“APRENDER” COSAS ¿NUEVAS?**



José Manuel  
Redondo López



- **El problema es que tienes que fiarte de tus “maestros”**
  - En Internet hay mucho “maestrillo” que te cuenta una historia
  - O se hace pasar por experto y en realidad...**a lo mejor no lo es**
- **No han pasado un proceso de selección...o te mienten sobre su preparación de lo que te cuentan**
- **También hay mucha “noticia falsa” (fake news) y desinformación para que te creas bulos**
  - ¡Y así conseguir manipularte! ¡NO LO PERMITAS!

**¡Pero no hay que creer todo lo que uno lee, hay que contrastar las cosas y, si dudas, pregunta a tu familia/profes siempre!**



# ¡SER POPULAR!



José Manuel  
Redondo López



- Si a la gente le mola lo que haces puedes ganar seguidores, popularidad y hacerte una “marca personal”
- Quizá con eso consigas ganar un buen dinero y tener un futuro profesional... ↗
  - Probando artículos de distinto tipo, haciendo críticas de temas que controles, opinando, entreteniendo...
- Lleva tiempo, es muy sacrificado y necesitas suerte 😊
  - Siempre ten un “plan B” por si acaso...
- Pero si te sale bien estás...

## ¡Ganando!

### 10 CONSEJOS PARA TENER ÉXITO EN LAS REDES SOCIALES



# ¿SER ¿POPULAR? ?



José Manuel  
Redondo López



MALAS PRÁCTICAS  
QUE NO DEBES HACER  
CON TU NEGOCIO EN  
SOCIAL MEDIA

- Hay peña a la que se le pira mucho y hace cualquier cosa para ganar seguidores
- Se engaña a si mismo y a los demás
  - Al final acaban siendo **víctimas de su propio ego** (el personaje “se come” a la persona) 😊
  - El contenido que genera **pierde calidad** muy fácilmente
    - Y lo que pudiese ganar “se quema” rápidamente 🔥
  - Al final, acaban promocionando juegos de **slots**, apuestas y **movidas turbias** similares por pasta y engagement 💰
  - Seguro que puedes poner nombres de gente que conoces...

**¡Vete con cuidado para que las redes sociales no te hagan daño!**



# ¡PAVO! ¡ME EXPLOTA LA CABEZA!



José Manuel  
Redondo López

- A ver, no quiero darte miedo, solo quiero que sepas lo que hay ahí fuera sin censuras

- **Repite:** **YO NO** te voy a decir que no uses redes sociales, **no soy nadie para prohibirte NADA**

- Pero es como aprender a conducir: si no sigues ciertas normas o tienes cuidado...te estrellas
- **Trust me**, ¡me he estrellado yo mismo unas cuantas (bastantes) veces!

  - Sí, soy un pureta , lo se, pero esto nació cuando yo era aún joven, y pagué la novatada
  - Ahora quiero intentar evitar que te "estrelles" como yo

- En la imagen ves consejos típicos que les dan a tus padres para ti en redes sociales

- Son buenos consejos, pero yo **quiero explicarte por qué se dan**: ¡no me gusta el "hazlo y punto"!

Plena inclusión  
Comunidad Valenciana

Entidad declarada de Utilidad Pública  
15.04.2019

10 consejos para educar en el buen uso de internet y las redes sociales

GENERALITAT VALENCIANA  
Vicepresidencia y Conselleria de Igualdad y Políticas Inclusivas  
POR SOLICITUD OTROS FINESES DE INTERÉS SOCIAL

- 1 Tener información sobre el buen uso de las redes sociales nos ayuda a conocer las ventajas y los riesgos de internet.
- 2 Habla con una persona de confianza sobre cómo usar las redes sociales. Te puede ayudar.
- 3 Controla el tiempo que usas internet. Usar mucho internet crea dependencia. Eso es malo. Haz un horario para usar internet.
- 4 Decide cuáles son los espacios donde puedes usar el móvil. Por ejemplo no uses el móvil cuando estas comiendo.
- 5 No compartas fotos, vídeos o mensajes de voz de contenido sexual, ni tuyas, ni de otras personas. Lo pueden ver muchas personas sin que tú lo sepas.



José Manuel  
Redondo López

# NUEVAS REDES SOCIALES

- Todo lo que vamos a ver se aplica a **cualquier red social**, clásica o nueva
  - Constantemente salen nuevas, muchas con una temática o tipos de contenido concretos
- Y en **TODAS ELLAS** hay “fauna peligrosa”
  - **Vendemotos/humos:** ¿Quieres saber más? Les dedico un curso complementario a este, el **“Juan Sebastián Elcano”**
  - **Acosadores** (bullies, narcisistas...): ¿Quieres saber más? Les dedico un curso complementario a este, el **P-74 “Atalaya”**
  - **Delincuentes:** ¿Quieres saber más? Les dedico dos cursos complementarios a este, el **M-31 “Segura”** y el **“Nautilus”**



## LAS NUEVAS REDES SOCIALES



**KICK**

Alternativa  
de Twitch



**LEMON**

Alternativa  
de TikTok



**THREADS**

Enlaza con  
Instagram y es  
competencia  
de Twitter



**BEREAL**

Promueve la  
auténticidad y  
la realidad



**KIWI**

Los usuarios  
formulan y  
responden  
preguntas



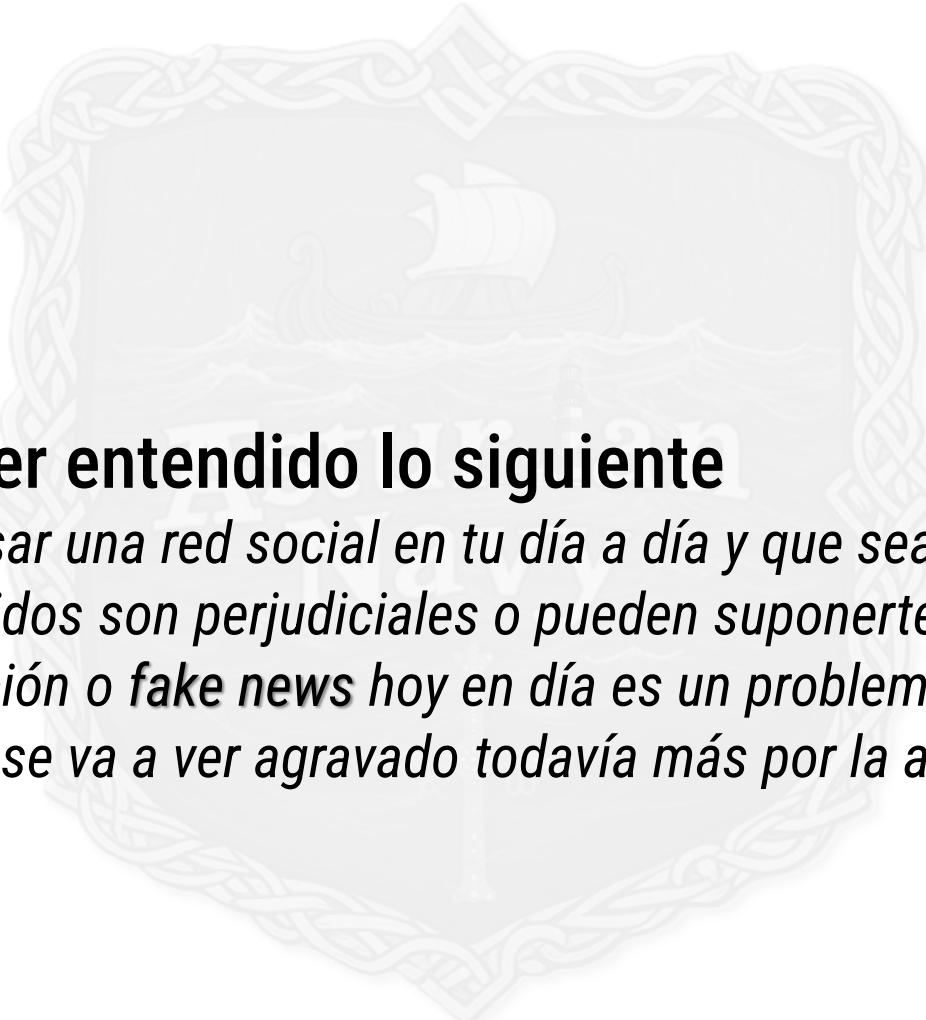
Cada año surgen nuevas plataformas  
en la era digital con el objetivo de  
conquistar y atraer nuevos usuarios.



José Manuel  
Redondo López

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?



## ● Asegúrate de haber entendido lo siguiente

- *Para qué puedes usar una red social en tu día a día y que sea algo útil y productivo*
- *Qué tipo de contenidos son perjudiciales o pueden suponerte un problema*
- *Que la desinformación o fake news hoy en día es un problema muy grave*
- *Que este problema se va a ver agravado todavía más por la aparición de los deepfakes*

< Ir al Índice

👉 ¿Son gratis?

东方财富  
Broncas y  
conflictos



# 💰 ¿DE DÓNDE SACA LA PASTA UNA RED SOCIAL?

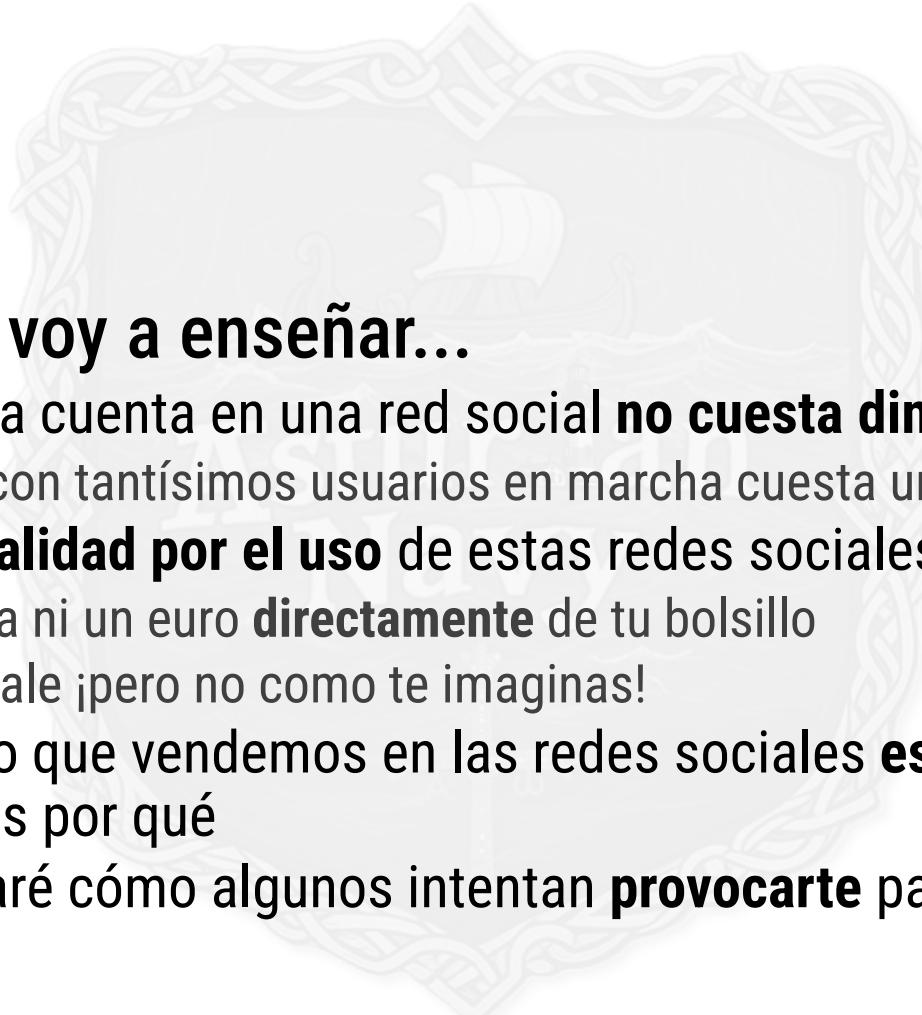
¿De verdad todo esto no cuesta dinero?





José Manuel  
Redondo López

# ¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?



## ● En este bloque te voy a enseñar...

- Por qué crearte una cuenta en una red social **no cuesta dinero**
  - Mantener algo con tantísimos usuarios en marcha cuesta un pastizal... 💰 💴 💳 💱 💲 💳
- **Cómo pagas en realidad por el uso** de estas redes sociales
  - Aunque no salga ni un euro **directamente** de tu bolsillo
  - En realidad, sí sale ¡pero no como te imaginas!
- Y es que, al final, lo que vendemos en las redes sociales **es a nosotros mismos** y nuestros gustos, y aquí verás por qué
- También te enseñaré cómo algunos intentan **provocarte** para generar visualizaciones y dinero





# Las redes sociales son gratis ¿verdad? ¿VERDAD?

El mercado donde tú eres un producto



# LAS REDES SOCIALES... ¿SON GRATIS?



José Manuel  
Redondo López



## • ¿En el sentido de no pagar por usarlas? La mayoría sí, son gratis

- Pero el motivo es que “**cobran**” de otro sitio...
- Aunque últimamente hay mucha **suscripción “premium”** con distintas excusas o ventajas (verificación, funciones extra...)

## • ¿Cómo dices? ¿**No cobran** y son rentables??



- Sí, en realidad ganan cantidades **ENORMES** de dinero

## • ¿Pero cómo? ¿De manera ilegal?

- ¡NOOO! Con **tus datos**, vendiéndolos a **empresas de anuncios**

## • ¡Eh! ¡Pero yo nunca les di permiso para eso!

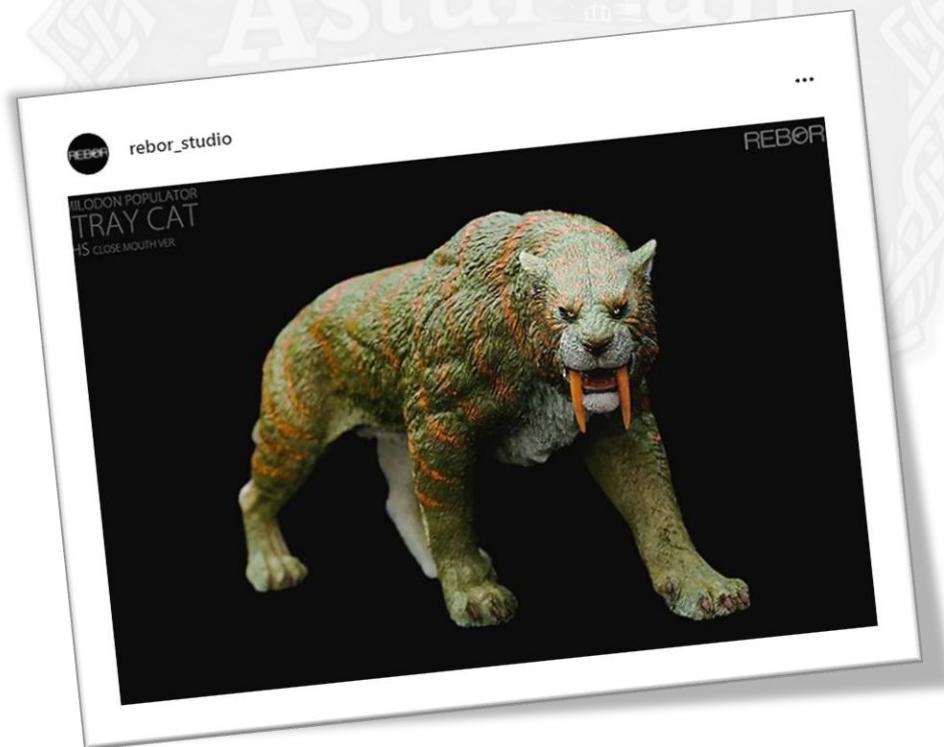


- En realidad, **sí lo hiciste**, al hacerte una cuenta...
- ¿Te leíste el “tocho” que te salió de “términos y condiciones”? (No, yo tampoco ☺)



# CÓMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

- Veamos ahora de donde viene la frase “**Si algo es gratis, tú eres el producto**” aplicada a las RRSS
  - Tranqui no te voy a soltar un rollo, aquí vamos a lo práctico, ¡con ejemplos!
- **Lo primero de todo, voy a enseñaros un anuncio de mi propio Instagram**
  - Se trata de una figura ultra-realista (bueno, vale, el color no...) de un Smilodon Populator, un tigre de dientes de sable



# CÓMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

## ● Espera ¿*Cómo sabe mi Instagram que me gusta la prehistoria?*

- Mucho, la verdad, ¡ha acertado de pleno! ☺

## ● Yo no le grito al móvil “¡me gustan los animales prehistóricos!” ni lo he declarado a Instagram

- ¡Pero es que no lo necesita! ¿cómo lo hacen?

## ● Bienvenido al apasionante (y bastante turbio) mundo del marketing dirigido



- Donde hay un perfil tuyo creado “en las sombras” para que, supuestamente, te salgan anuncios de cosas que te interesan solo a ti



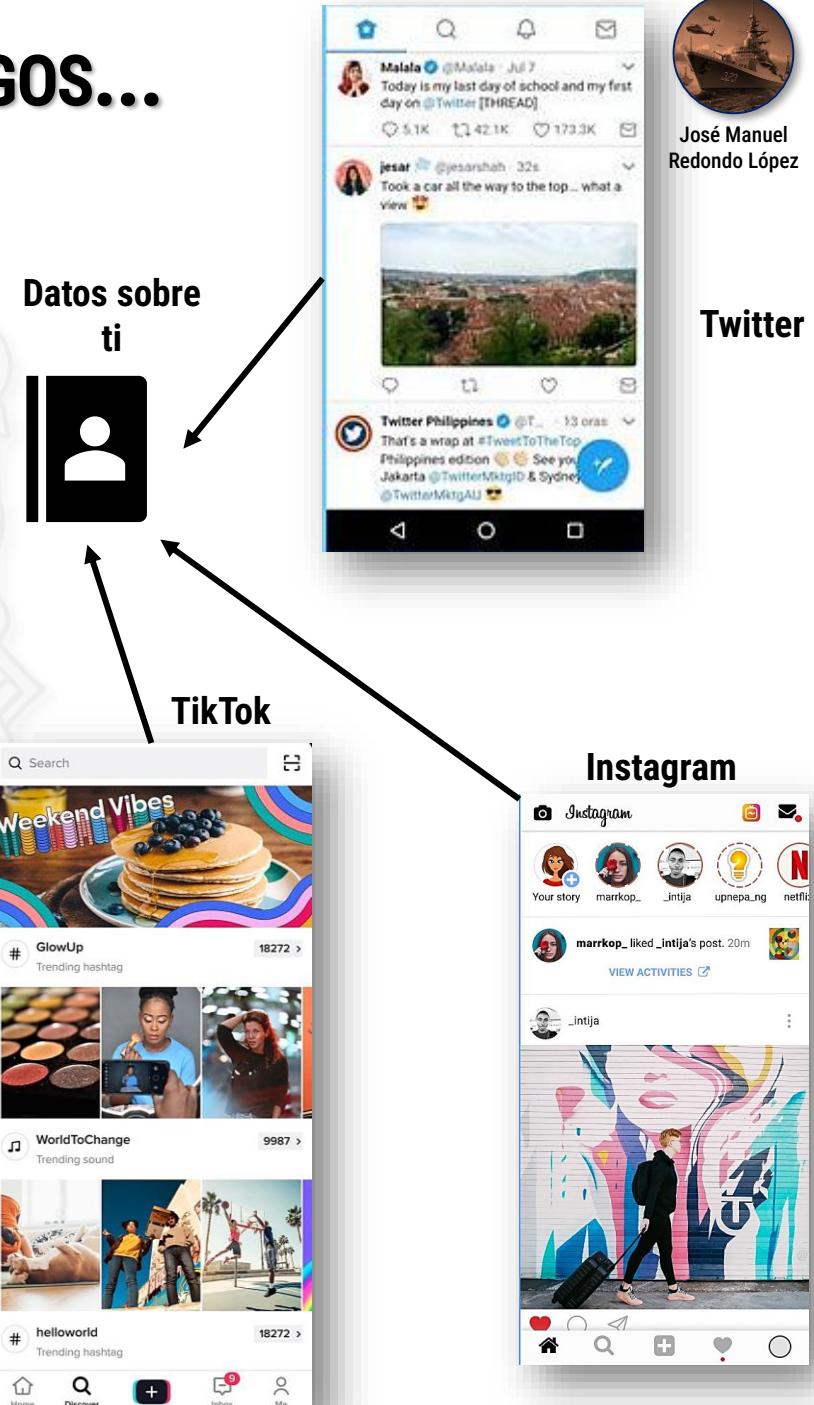
# CÓMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

- En el momento que cualquier está en la red, constantemente se recogen datos tuyos de **MUCHOS** sitios
- Y se asocian con identificadores vinculados a cada persona exclusivamente (¿“anónimo”? Not really...) 
  - Con asistentes  : Siri, el asistente de voz de Google, Cortana, Alexa... **SÍ TE ESCUCHAN** (en tu teléfono, PC, aparatos varios en casa...)
    - Pero es que **lo necesitan para funcionar** (se activan con “frases clave”)
    - ...y para **mostrarte anuncios**
      - <https://www.lavanguardia.com/tecnologia/20180504/443209404047/google-escuchas-telefono-espionaje-privacidad.html>
    - Puedes **desactivarlos, pero perderás opciones**
      - <https://www.xatakandroid.com/tutoriales/como-desactivar-asistente-google>
  - Con aplicaciones que tienen permisos para usar tú micrófono 
    - Normalmente, las aplicaciones del móvil **NO TE ESCUCHAN**
    - Pero si usan tu micrófono entonces...(llamadas, transcripciones...) ¿qué más hacen con la información que les cuentas?
    - Lo dicen sus términos y condiciones...que no se leen habitualmente



# COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

- **Mientras navegas por casi cualquier web** 🌎🌐🌐
  - La mayoría tiene “sondas” que recogen datos de tus gustos y acciones en ellas
- **Al usar las apps de distintas redes sociales** 😍
  - **TODAS** esas aplicaciones recogen datos de tu teléfono 📱
    - Tantos como permisos les des...
    - Pero, aunque les des los mínimos, lo hacen 😞
  - Tu **ID de teléfono** (todos los teléfonos tienen un ID distinto) 📊
    - Sí, no eres tú directamente, pero es TÚ teléfono ¿lo captas?
  - Tu **localización** (más o menos aproximada) 🌏
  - Predice tu **rango de edad**
    - Por lo que **haces / sigues / “faveas”...**
    - Hay **muchha investigación en esto**, lo creáis o no...
  - Por **palabras o frases clave** en lo que escribes ⌨
    - Gustos de todo tipo, etc.
    - ... (muchos más datos útiles para identificarte, imposibles de listar aquí todos)



José Manuel  
Redondo López

Twitter

Instagram



José Manuel  
Redondo López

# COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

- Hay una serie de empresas que trabajan de “**aspiradoras de datos**” (como Kirby 😊)

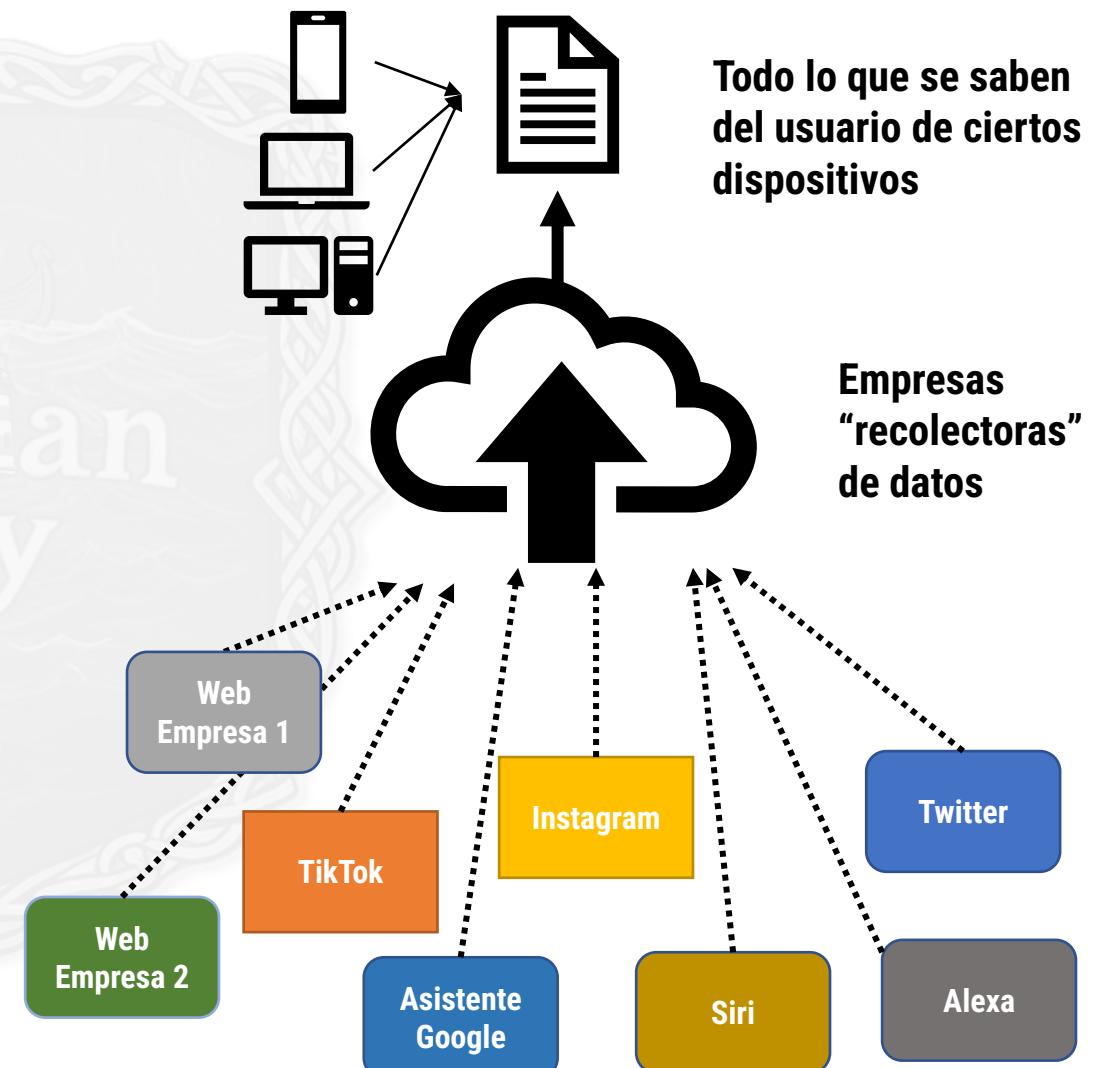
- Se les suele llamar “data brokers”
- A esta venta de datos se la llama “data capitalism”

- Pagan por **sacar datos de DONDE SEA**

- Participas en un concurso, te suscribes a algo, usas un descuento, canjeas un vale...
- Cualquiera de esas acciones genera datos que reciben y tratan de asociarlos a ti

- **¿Pero cómo?** Ahí está el truco, **TODAS** las empresas les **VENDEN** esos datos

- Y luego los “cruzan”...y con eso ¡**SABEN UN MONTÓN DE COSAS DE TI!**
- Y esos “perfils engordados” luego **se compran por mucho dinero** para hacer campañas publicitarias



# COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

- *¿Y cómo saben que a mí me gustan las figuras prehistóricas ultra-realistas?*

- Yo navego a webs donde se anuncian y hacen reviews
- Esas webs tienen “sondas” de Meta, la dueña de Instagram
  - Que **mandan información de lo que miro** vinculada a mi y a mi teléfono
- Ahora abro la aplicación de Instagram en él teléfono
  - Y **Meta** sabe que al usuario del teléfono cuyo ID es X le gustan las figuras prehistóricas por su actividad web
  - Así que ya sabe **qué anuncios mostrarme y qué cuentas recomendarme** (todas están “etiquetadas”)
- Y si navego a webs con publicidad insertada por **Meta...**
  - Ya sabe de que temática mostrarme los anuncios
- **¡Todo juntando datos míos de distintos sitios!**
- Esto ocurre constantemente y es un mercado que **genera una BARBARIDAD de dinero** 💰💷💹💵💴

Las webs a las que navego...



the\_rounded\_man [Editar perfil](#)

363 publicaciones 458 seguidores 524 seguidos

Jose Manuel Redondo López  
'Kakashi'. I publish research and teaching stuff in my web  
[www.researchgate.net/profile/Jose\\_Redondo8](http://www.researchgate.net/profile/Jose_Redondo8)

Kakashi Ayuda com...

Las cosas que posteo en RRSS...

# COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

## ● Pero... ¡hay más, mucho más!

- Yo **sigo a cuentas** de marcas de estas figuras, y faveo / retwitteo cosas que me gustan
  - Y de gente que habla sobre sus nuevos lanzamientos, hacen críticas de ellos...
- Y me gustan **sólo de ciertas marcas**, porque es fácil saberlo si analizas lo que hago
- Y como lo hago en mi Twitter / Instagram... ellos tienen estos datos (¡son tuyos!)

## ● ¿Qué anuncios me van a poner entonces?

- De figuras prehistóricas
- Y sólo de las marcas que más me gustan

## ● Pero no es necesariamente “malo”, ¿sabéis?

- Así me entero de las novedades y a veces compro...
- ¡La marca de figuras **ha pagado a la red social** para colocar esos anuncios “inteligentes”!
- Y así... ganan dinero (porque se hace con todo el mundo en todo el mundo ☺)

## ● Esta “**publicidad dirigida a cada persona individual**” funciona **MUY BIEN**

- Genera muchos beneficios y las marcas lo saben ¡este es el imperio que rige Internet hoy en día! 😊

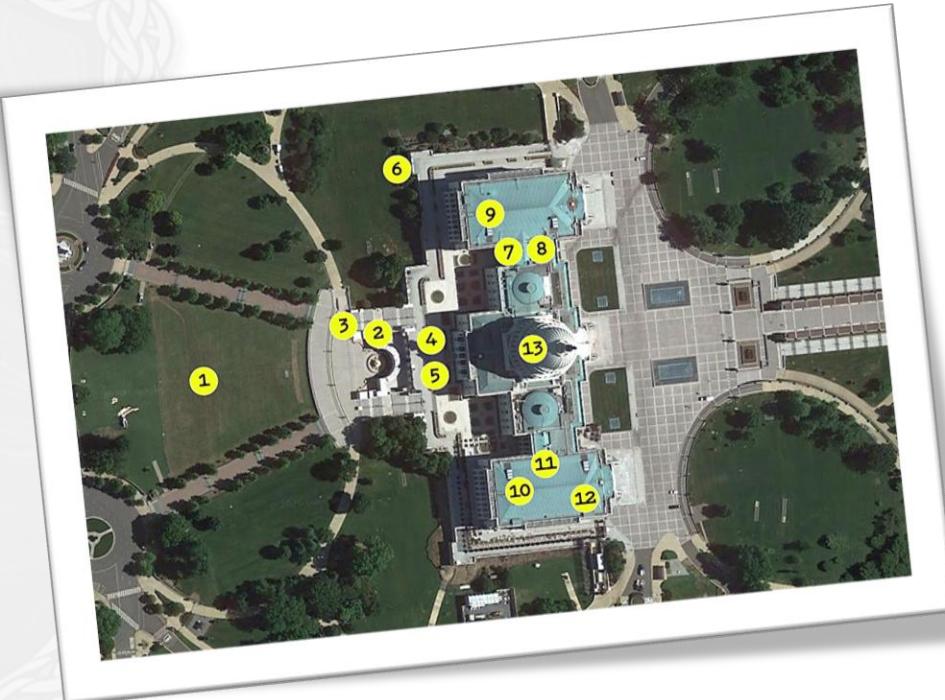




José Manuel  
Redondo López

# COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

- ¿Te parece alucinante? Espera...
- Antes he dicho que pueden saber tu **geolocalización** (dónde estás en el mundo)
  - Pero también saben la de **TODOS** los móviles...
  - Y con eso, por increíble que parezca, pueden saber qué teléfonos están regularmente cerca de mi
- Y si es en una casa, en un colegio, en un gimnasio...porque...**¡Google Maps!** ☺
  - Es decir, ¡pueden reconstruir todo mi entorno social y mis rutinas!
  - Familia, amigos, compañeros de clase...



Esta imagen es real, y corresponde a personas durante el asalto al capitolio según sus móviles. ¡Supieron por dónde se movían en todo momento! ¿Cómo creías que los asistentes saben cosas como "tu casa", "tu instituto", etc.?

# COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

- Y con eso, las RRSS empezarán a mostrarme a mí anuncios de cosas que le interesan a “mis panas”
  - Sí, ya sé que lo que les interesa a tus colegas no tiene por qué interesarte a ti...
  - Y gente que me stalkee sabe por dónde me muevo, lo que me gusta, mis rutinas, mis colegas...
    - ¡Depende de cuanto posteé!
- Pero...igual así un día hablo de ello con alguien de mi entorno al que **SÍ LE INTERESA**
  - ¡Y le hago “publi” gratis!
  - Is this... ¿*publicidad subliminal?*
  - ¡**NO!** Pero...a lo mejor te conviertes en “embajador” de una marca inconscientemente ¡está todo calculado!





José Manuel  
Redondo López

# COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

## ● Pero ¿creéis que solo pasa en las redes sociales?

- ¡NO! ¡Prácticamente cualquier web con anuncios lo hace!
- ¿No te aparecen en las RRSS “post promocionados”?
- ¿De dónde crees que salen? ¡Ahora lo sabes!

## ● ¿Y esta movida de espionaje bruto no le importa a nadie?

- Pues en realidad, parece que no...
- Tiene nombres “guays” para que se vea como algo “cool”: “Targeted marketing”, “Smart Ads”

## ● Es una herramienta para servir publicidad buenísima...¿pero te has parado a pensar qué más se podría hacer con esa información?

- En malas manos, se puede usar para cosas **MUY TURBIAS** (lo dejo a tu imaginación)
- **¿Tu teléfono (y sus apps) son tu propio “gran hermano”?**

Así que no...NO ES “GRATIS” como parece ☺



TAG Heuer @TAGHeuer

Next #CR7Time contest is coming soon! Follow @TagHeuer to get a chance to win exclusive #TagHeuer bags and wallets! [pic.twitter.com/FAN9JjxUT0](http://pic.twitter.com/FAN9JjxUT0)

TAG Heuer

Promocionado



A alguien de mi entorno le gustan los relojes Tag Heuer (yo no soy ☺)



José Manuel  
Redondo López

# ¿CÓMO SÉ LO QUE SABEN DE MI SIN FUNDIRME EL TARRO?

- Leer los “papiros legales” de las RRSS es muy aburrido
  - Aparte que sin formación en leyes te vas a enterar de poco...
- Por suerte hay páginas que te los describen “para personas”
  - Ej.: <https://tosdr.org/es>
- Hay muchos más servicios que las RRSS
  - Entra y lee (y horrorízate 💀)

The screenshot shows the homepage of **Terms of Service Didn't Read**. The main headline reads: "He leído y estoy de acuerdo con los Términos" es la mayor mentira en la web. Juntos, podemos cambiar eso. Below this, there's a search bar and a navigation menu with links like PRESENTADO EN, Le Monde, Zeit Online, WIRED, strategy-business, Dating News, Waka, and a link to Buscar.

Two service profiles are displayed side-by-side:

- Facebook:** Grade E
  - Facebook almacena tus datos tanto si tienes una cuenta como si no.
  - El servicio puede leer tus mensajes privados.
  - Este servicio puede ver el historial de tu navegador.
  - El contenido borrado no está realmente borrado.
  - Este servicio conserva los registros de los usuarios durante un período de tiempo indefinido.
- Amazon:** Grade E
  - Las cookies de tercero.
  - Las condiciones de privacidad del usuario.
  - Este servicio le rastrea en otros sitios web.
  - El servicio puede leer tus mensajes privados.
  - Este servicio puede ver el historial de tu navegador.
  - Este servicio conserva los registros de los usuarios durante un período de tiempo indefinido.

A red arrow points from the text "Este servicio puede ver el historial de tu navegador" in the Amazon profile to the corresponding section in the list below.

The list continues with several more items for both services, each with a "Ver detalles" button:

- Facebook:
  - Este servicio conserva los registros de los usuarios durante un período de tiempo indefinido.
  - La aplicación necesaria para este servicio requiere amplios permisos del dispositivo.
  - Este servicio puede recopilar, utilizar y compartir datos de localización.
  - Este servicio puede conservar los datos personales después de una solicitud de supresión por intereses comerciales u obligaciones legales.
  - El servicio recoge muchos tipos diferentes de datos personales.
  - Seguimiento mediante cookies de terceros para publicidad.
  - Este servicio le rastrea en otros sitios web.
  - Este servicio puede utilizar sus datos personales con fines de marketing.
  - El servicio puede utilizar píxeles de seguimiento, balizas web, huellas digitales del navegador y/o huellas digitales del dispositivo de los usuarios.
  - Este servicio recopila información sobre usted a través de terceros.
- Amazon:
  - Este servicio conserva los registros de los usuarios durante un período de tiempo indefinido.
  - La aplicación necesaria para este servicio requiere amplios permisos del dispositivo.
  - Este servicio puede recopilar, utilizar y compartir datos de localización.
  - Este servicio puede conservar los datos personales después de una solicitud de supresión por intereses comerciales u obligaciones legales.
  - El servicio recoge muchos tipos diferentes de datos personales.
  - Seguimiento mediante cookies de terceros para publicidad.
  - Este servicio le rastrea en otros sitios web.
  - Este servicio puede utilizar sus datos personales con fines de marketing.
  - El servicio puede utilizar píxeles de seguimiento, balizas web, huellas digitales del navegador y/o huellas digitales del dispositivo de los usuarios.
  - Este servicio recopila información sobre usted a través de terceros.



# No seas adicto a la bronca y al conflicto

Máquinas de odio sociales



# EL CONFLICTO Y LAS RRSS

- Para sacar información, las RRSS quiere que **interacciones**

- Vamos, que “escribas cosas” para extraer esos datos tan 💰💰 de ti

- Para ello, los algoritmos de las RRSS **fomentan el conflicto**

- Te dejan ver mensajes de **gente que opina de manera contraria** a ti
  - O son gente muy polémica 😠
- Todo **con tal de que interactúes** con ellos y “escribas cosas”
- Si un influencer cobra por “visitas” e “interacciones” **le da igual que sean positivas o negativas** 💸 💳
- **Más preguntas**
  - Muchos crean flames para cobrar así... 😞

- ¡Están diseñadas para cabrearte y “comerte la cabeza”!

- **No hagas RT, comentes ni compartas “basuras”, bloquea y denuncia**
- ¡Hacerles “casito” es bueno para ellos! *¿No me crees?*
  - <https://www.newtral.es/algoritmo-twitter-como-funciona-marcelino-madrigal/20210525/>
  - <https://www.newtral.es/opinion-discurso-ira-online-echo-marcelino-madrigal-redes-sociales/20210614/>



En serio, esto no merece la pena,  
por muchas ganas que te den...  
**be water, my friend.** No  
interacciones, no compartas,  
denuncia y bloquea, como buen  
Jedi 😊



José Manuel  
Redondo López

# LA POLÉMICA GENERA “ENGAGEMENT” EN RRSS

## ● Cobrar por interacción en muchas RRSS hace proliferar contenidos “discutibles”

- Si le unes equipos o herramientas de moderación insuficientes, la RRSS se degrada
- La parte social queda en un segundo plano, y **solo queda la parte económica**

Hola buenas, hoy vamos a ver el origen una de las tradiciones más bonitas del verano

Vamos a tomar el fresco

[Abro hilo]



El perfecto **imbécil** de Jota Pe Hernández no tiene ninguna prueba en contra de la vicepresidenta Francia Márquez. Nuevamente este mamarracho quedó en ridículo como siempre.



Hilos extra-largos (muchos hechos con IA) que se repiten cada X tiempo. Al menos algunos son interesantes...

Faltosidades, flames, racistadas y salvajadas varias, muchas de ellas denunciables (lo veremos luego)

Reply this tweet with your most **unpopular opinion** of Dragon Ball



Generación de polémicas intencionadamente y “sealioning”: <https://es.wikipedia.org/wiki/Sealioning>



José Manuel  
Redondo López

# LA POLÉMICA GENERA “ENGAGEMENT” EN RRSS

● Si alguien te provoca en RRSS seguramente quiere generar conflicto para que le des views

● Relájate y no caigas en tu juego

- **No eres realmente anónimo:** Si le amenazas o dices alguna barbaridad, te puede caer una buena 🕵️
- **No seas troll,** te puede costar la cuenta 🦹
- **Toréales de otra forma:** Puedes usar la IA para contraargumentar 🐂
  - Si te dice algo que no sabes, úsala para informarte rápidamente y rebatirle
    - Pídele a la IA directamente que le rebata 😊
    - Pero cuidado por que la IA a veces **se inventa cosas** 🤖
  - Si quieres decirle algo heavy, pídele a la IA que te lo “endulce”
    - ¡Eres un señor/señora, no te rebajas a los plebeyos!

¿Puedes reescribirme esta frase de manera que no resulte tan agresiva? "Eres un desgraciado sin ética y unos valores morales de mierda que no es digno de..."

◆ Claro, aquí tienes algunas opciones para reescribir esa frase de manera menos agresiva, enfocándose en la crítica del comportamiento y la idoneidad para el puesto:

Opciones enfocadas en el comportamiento y la ética profesional:

- "Considero que algunas de sus acciones recientes plantean serias dudas sobre su ética profesional y su adecuación para este puesto."
- "Me preocupa la falta de ética demostrada en ciertas situaciones, lo cual cuestiona su idoneidad para las responsabilidades que conlleva este cargo."
- "Desde mi punto de vista, su comportamiento en algunos aspectos ha sido cuestionable éticamente y no se alinea con los valores que considero importantes para esta posición."
- "Creo que es necesario reflexionar sobre si sus principios y su conducta son compatibles con la ética y los valores requeridos para este puesto."

La IA te puede hacer hablar mejor que Cervantes. Eso les confundirá 😎

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



## ● Asegúrate de haber entendido lo siguiente

- *Cómo una red social cualquiera saca partido de todo lo que hagas en ella, aunque no pagues dinero directamente*
- *Que cuanto más compartas en una red social más beneficio le reportas, de manera directa o indirecta, gracias al mundo de la publicidad*
- *Que lo que pones en una RRSS puede usarse en tu contra, especialmente por gente que te stalkee y sepa lo que haces o a dónde vas*
- *Que las cosas que ves en las redes sociales están influenciadas por tus gustos y preferencias, tanto para sugerirte contenido como para fomentar interacciones, aunque sea basándose en la polémica*
- *Que interaccionar, aunque sea para criticar, beneficia al que pone el contenido polémico*



# ¿CÓMO ME “ENFRENTO” A UNA RED SOCIAL?

¿Qué debo tener en cuenta cuando estoy en una?



# ¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

## ● En este bloque te voy a enseñar a dar respuesta a estas preguntas...

- *¿Te da miedo entrar en una red social por la de cosas que hay?*
  - No te preocupes, yo te enseño una estrategia para entrar con menos riesgo
- *¿Te has parado a pensar que estar en una red social no deja de ser algo similar a estar en la calle, y que se aplican las mismas normas?*
  - ¿Hablarías con un desconocido? Pues en las redes social tampoco...
  - ¿Harías amistad con gente que no conoces, o sólo con gente que sean amistades o populares? Pues aquí es lo mismo...
- Y también voy a tratar de explicarte que tu perfil en las redes sociales eres “**tú en Internet**” para bien y para mal
  - Y que el hecho de que te **suplanten** puede ser un verdadero problema
  - Así que tienes que evitarlo y también te voy a explicar cómo
  - Lo que incluye cuidar también tu imagen personal
- Y por supuesto **evitar riesgos comunes** a través de redes sociales
  - Y de los que podrías ser víctima solo por el hecho de estar ahí



# CONSEJOS GENERALES PARA VIVIR (MÁS) TRANQUILO/A: CUENTA

- Tienes que cuidar de tus cuentas en RRSS como cualquier otra cuenta ❤️
  - La imagen muestra las claves para cuidar de cualquier cuenta 🔒
- Mejor usa (si te deja) el navegador que su app dedicada
  - Así recogerá menos datos sobre ti (menos no es cero, pero algo es algo...)
  - Ej.: En lugar de instalarte la app de Twitter, navega a <https://x.com/>



**CONSEJOS DE SEGURIDAD EN REDES SOCIALES**

- 1 CREA CONTRASEÑAS SEGURAS**  
Las contraseñas son el primer filtro de acceso a tus redes sociales. Mejor utiliza contraseñas robustas, que sean difíciles de descifrar.  

- 2 USA LA DOBLE AUTENTICACIÓN**  
De esta forma sumas una capa extra de seguridad para acceder a tus redes a la vez que verificas tu identidad por otra vía.  

- 3 DESACTIVA LA GEOLOCALIZACIÓN**  
Dejarán de llegarte anuncios de tu zona pero también no sabrán donde estás en cada instante.  

- 4 CONFIGURA TU PRIVACIDAD**  
Revisa bien todas las opciones de privacidad de las que dispones en las redes en las que estés. Decide con quién quieras compartir tu contenido, asigna roles, etc.  

- 5 SENTIDO COMÚN**  
Publicar cualquier tipo de información confidencial, como cuentas de correo privadas, documentos identificativos, etc. es un peligro en Redes Sociales  


Más información en [dinahosting.com/blog](https://dinahosting.com/blog)

 dinahosting



José Manuel  
Redondo López

# CONSEJOS GENERALES PARA VIVIR (MÁS) TRANQUILO/A: CONTENIDO

- La realidad ya es bastante chunga como para encima leer basura por Internet 😭
- Usa las opciones de cada red social para no ver lo que no quieres ver 🙅
  - Podrán saber de ti hasta tu talla de camisetas, pero al menos aún controlas en gran medida que NO quieres ver
- Cuidado también con lo que posteas 🤫
  - Y/o a quién lo posteas (no es lo mismo hacerlo en general que a un grupo privado que tengas)
  - Tampoco quieres que haya gente que vea o averigüe cosas que no quieres que se vean / intuyan

 <b>BLOQUEAR</b> Puedes bloquear cualquier cuenta de forma instantánea. Al hacerlo esa cuenta no podrá ver tus tuits o contactarte.	 <b>Top consejos de seguridad en Twitter</b>	 <b>LOCALIZACIÓN</b> Selecciona si quieres incluir o no la localización en cada tuit.
 <b>SILENCIAR</b> Silencia cuentas, palabras o conversaciones si no estás interesad@ en ver estos tuits.	 <b>FILTRO DE CALIDAD</b> Filtrá las notificaciones que recibes para evitar ver respuestas o menciones de ciertos tipos de cuentas.	 <b>ETIQUETADO DE FOTOS</b> Escoge entre permitir que cualquiera, solo amigos o nadie te etiquete en fotos.
 <b>REPORTAR</b> Reporta una cuenta o un tuit siempre que creas que se están violando las Reglas de Twitter o los Términos y Condiciones.	 <b>DESCUBRIR</b> Tus contactos pueden encontrarte en Twitter utilizando tu dirección de correo electrónico o número de teléfono.	 <b>PROTEGER</b> Tienes el control sobre tu experiencia, ya que cada vez que alguien quiera seguirte, tendrás la opción de aceptar o declinar.

8 reglas generales para andar en RRSS. Fuente:  
[https://blog.x.com/es\\_es/topics/company/2018/Seguridad](https://blog.x.com/es_es/topics/company/2018/Seguridad)



José Manuel  
Redondo López

# CONSEJOS GENERALES PARA VIVIR (MÁS) TRANQUILO/A: AYUDA

- Tienes derecho a tu privacidad e intimidad SIEMPRE
- Pero si tienes un problema online, **no te lo comas solo** 😳
  - Estos son consejos que les dan a tus padres
    - Que pueden estar más perdidos que tú con estas cosas...
    - ¡Seguramente no “pilotan” tanto como tú!
    - Pero no quiere decir que no te puedan ayudar
  - Un consejo solo sirve parcialmente ante un problema real, necesitas **apoyo**
    - Más de esto en el **P-74 “Atalaya”**
- Si tienes un problema, pídeles ayuda
  - Demuéstrales que **pueden confiar en ti y haz equipo con ellos** ante los problemas 🤝

**8 TiPS PARA USAR REDES SOCIALES**

ESTRATEGIAS DE PROTECCIÓN EN LÍNEA QUE DEBEMOS USAR CON NUESTROS HIJ@S.

- 1 ES MEJOR COMPARTIR MENOS QUE MÁS: cuando compartís información sensible, no sabés quiénes pueden acceder a ésta o qué usos pueden darle
- 2 PENSAR ANTES DE COMPARTIR: todo lo que publicás en red, se convierte en parte de tu huella digital y es casi imposible de borrar
- 3 NO HACER A OTROS LO QUE NO QUERÉS QUE TE HAGAN: debés respetar a los demás y no publicar fotografías o comentarios que sean ofensivos o burlistas
- 4 MANTENER PRIVADO LO PRIVADO: debés restringir los permisos de acceso a tu perfil, modificando la configuración automática
- 5 RECORDAR QUE NO ES UN CONCURSO DE POPULARIDAD: tu red de contactos debe estar compuesta por personas confiables, no por “amigos” desconocidos
- 6 SER CREATIV@ CON LAS CONTRASEÑAS: debés tener un mínimo de 8 caracteres y mezclar letras, números y símbolos especiales
- 7 HACERSE EL DIFÍCIL DE ENCONTRAR: hay que desactivar los servicios de geolocalización que comparten automáticamente nuestra posición
- 8 TENER CUIDADO: debés aplicar las mismas reglas de seguridad que usás en el mundo real y recordar que detrás de cada dispositivo, hay una persona

ACOMPAÑALOS EN CADA ETAPA

NIÑAS Y NIÑOS PEQUEÑOS	PRE-ADOLESCENTES	ADOLESCENTES
Mantene a mano. Aunque tus hijos e hijas quieran y puedan usar las tecnologías con más independencia, debés establecer los límites de uso apropiado.	Establecé las reglas del juego. Hablá con tus hijos e hijas sobre lo que hacen, leen y ven en red. Compartí con ell@s sus expectativas sobre qué es y no es apropiado.	

Crianza TECNOLÓGICA

FUNDACIÓN paniamor

f /FUNDACIONPANIAMOR-COSTARICA

A medida que te hagas mayor tendrás más libertades y el rol de tu familia será más de apoyo y ayuda que de poner restricciones

# ¿QUÉ TENGO QUE SABER CUÁNDO ESTOY EN UNA RED SOCIAL?

## ● Lo primero es **USAR LA CABEZA** y **PENSAR**

- Ya viste las movidas de los pros y contras que te conté al principio
- ¿VAS A DEJAR QUE TE ENGAÑEN? ¡**NUNCA!**

## ● Te doy consejos de qué hacer en distintas situaciones

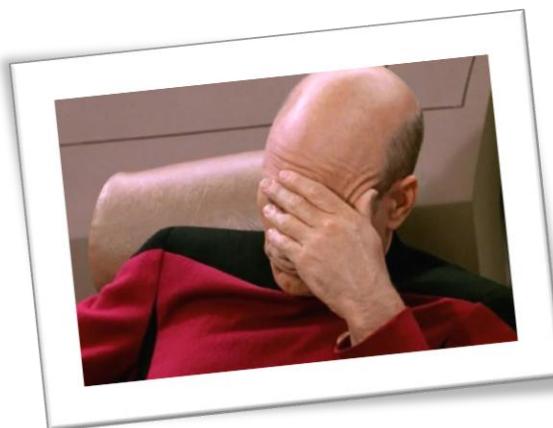
- **¿Te dan Información que “huele rara”?**. Contrástala (fact check)
  - Opiniones / noticias (ojo, que también las hay falsas) demasiado “burras”
    - <https://maldita.es/malditobulo/>
  - Usa **TU** criterio y toma **TUS** decisiones
  - Cuando termines de analizarlo, si aún tienes dudas consulta a tu familia/profesores y explícales lo que has visto
    - Y cómo “te lo has currado” 🤦 (¡seguramente aprendan ellos de ti ahora!)
- **¿Te piden que compres algo? CUIDADO**
  - A un influencer podría haberle **pagado** para promocionar que compres cosas, juegues a sus juegos...
    - Y simplemente “venderlo” sin haber probado nada de lo que vende...
  - *¿Realmente las necesitas? ¿no estás haciendo trampa? ¿de verdad quieres pagar aún más dinero por el juego?*



# ¿QUÉ TENGO QUE SABER CUÁNDO ESTOY EN UNA RED SOCIAL?

- **¿Hay “red flags”?** Oh sí, estos, por ejemplo
  - **Nunca juegues con cosas que no tienes** (apuestas, compras in-game ... todo lo que requiera dinero tuyo o de tu familia)
    - **Sí, eso incluye micro-transacciones, loot boxes, gachas, cromos del FIFA, etc. (aunque te lo diga tu influencer favorito)**
    - ¡Quieren que gastéis (y les regaléis) dinero a las compañías de videojuegos! (¡y ya habéis pagado por él!), pero... ¡controla!
  - **Nunca mandes fotos ni datos personales de cualquier clase a nadie** (direcciones, DNIs, nºs de tarjetas de crédito...) da igual la excusa
    - Es abrir la puerta a un montón de estafas (ver **M-31 “Segura”**)
  - **¿Aún así te has equivocado / te han engañado?** Lo siento ☹
    - Si lo has pensado antes lo has hecho bien, **es aprendizaje**
    - ¡Para la próxima te espero pedazo de  !
- **¿Tienes dudas? En seguridad siempre tenemos un dicho**

**Si dudas o sospechas, la única respuesta segura es decir NO**



Si te engañan, que te hunda la moral un tiempo es normal (es humano), pero no te dejes vencer por eso. Hay estafadores muy buenos, la idea es convertirse en alguien más listo que ellos

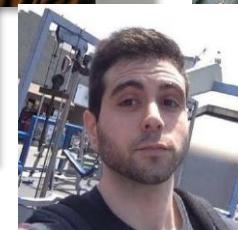
# ¿CÓMO ENTRO EN UNA RED SOCIAL?

## ● Empieza restringiendo quién puede añadirte

- Y añadiendo tú a quién **VERDADERAMENTE** conozcas
  - Déjate de cuentas “raras”, desconocidas... stop “ninjas” 
  - Tus compañeros de clase, tus amigos, tu gente, tu cole, tu equipo de deportes, influencers conocidos que hablen de lo que te interesa... ¡anda que no hay gente interesante!

## ● “Ábrete al mundo” a medida que pilles confianza y te familiarices

- O tus contactos te recomiendan gente buena y de confianza...
- **Pero NUNCA aceptes NADA de desconocidos**



## ● Controla para quién publicas las cosas

- Todo el mundo, grupos concretos, “mejores amigos”...
- ¡Todas las redes sociales tienen opciones para esto!
- Tienes que analizarlas y dominarlas como un pro ☺

## ● **Ojo con los mensajes directos:** ¡Asegúrate de que se los mandas a quien de verdad quieres y no los aceptes de desconocidos! ☺



# Configurar una red social

No es “crear una cuenta y ya” precisamente...



# SOBRE TU CUENTA



José Manuel  
Redondo López

## ● Lo primero que tienes que hacer es tener **una contraseña decente**

- ¿Te sientes *hakin bestia*? ¡Puedes ir más allá activando un 2FA!
  - ¡Usa tu propio teléfono para que solo tú puedas entrar a tus cuentas de cualquier servicio! 
- **Aquí te lo explican:**
  - <https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras/autenticacion-de-dos-factores>

## ● Y luego tratar tu perfil, tus datos, tu localización (desde dónde publicas), etc. adecuadamente

- Es decir, **echar un rato en configurarlas bien**
- Os voy a dar algunos ejemplos en redes sociales conocidas
- ¡Pero que sepáis que **TODAS tienen opciones parecidas!**
  - Así que... ¡invierte un tiempo en buscarlas para estar más seguro!

## Crea tu contraseña segura

### PASO A PASO

#### PASO 1

Pensar una frase  
Puede tener significado para nosotros o simplemente unir 2 o 3 palabras al azar, pero que nadie más conozca. La longitud mínima recomendada es de 10 caracteres.



Mi cuenta segura

#### PASO 2

Alternar mayúsculas y minúsculas  
Unímos las palabras y resaltamos las iniciales con mayúsculas.



MiCuentaSegura

#### PASO 3

Sustituir letras por números  
Un truco es intercambiar algunas letras por cifras, como "o" por 0, "i" por 1, "e" por 3 o "a" por 4.



M1Cu3nt4S3gur4

#### PASO 4

Añadir caracteres especiales  
Solo queda incluir algún símbolo (~ ! @ # \$ % ^ & \* - + | \ \ ( ) { } [ ] ; : ; < > . ? , ! ).



M1Cu3nt4S3gur4!

#### PASO 5

Personalizar la clave para cada servicio  
Podemos utilizar las dos primeras letras del servicio y una las ponemos al principio y otra al final de la clave, ambas en mayúsculas. Ejemplo: si el servicio se llama "Mailbook", usaremos la M y la A.



MM1Cu3nt4S3gur4!A  
¡Y listo! Así de sencillo hemos creado nuestra contraseña robusta, segura y fácil de recordar.



Y como medida de seguridad extra, sigue estos consejos y los ciberdelincuentes no tendrán nada que hacer:

Utiliza gestores de contraseñas para controlar todas tus claves.

No repitas las mismas contraseñas en distintas cuentas.

Cambia las cada cierto tiempo (3 meses).

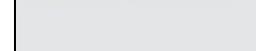
No las compartas con nadie, ni amigos ni familiares.

Utiliza la verificación en dos pasos siempre que sea posible.

Configura tu móvil para que, no se muestren los caracteres que pulsas.



Recuerda que tienes a tu disposición la Línea de Ayuda en Ciberseguridad de INCIBE, 017, gratuita y confidencial, para cualquier duda relacionada con la ciberseguridad.



[www.incibe.es](http://www.incibe.es) | [www.osi.es](http://www.osi.es)



Oficina de Seguridad del Internauta

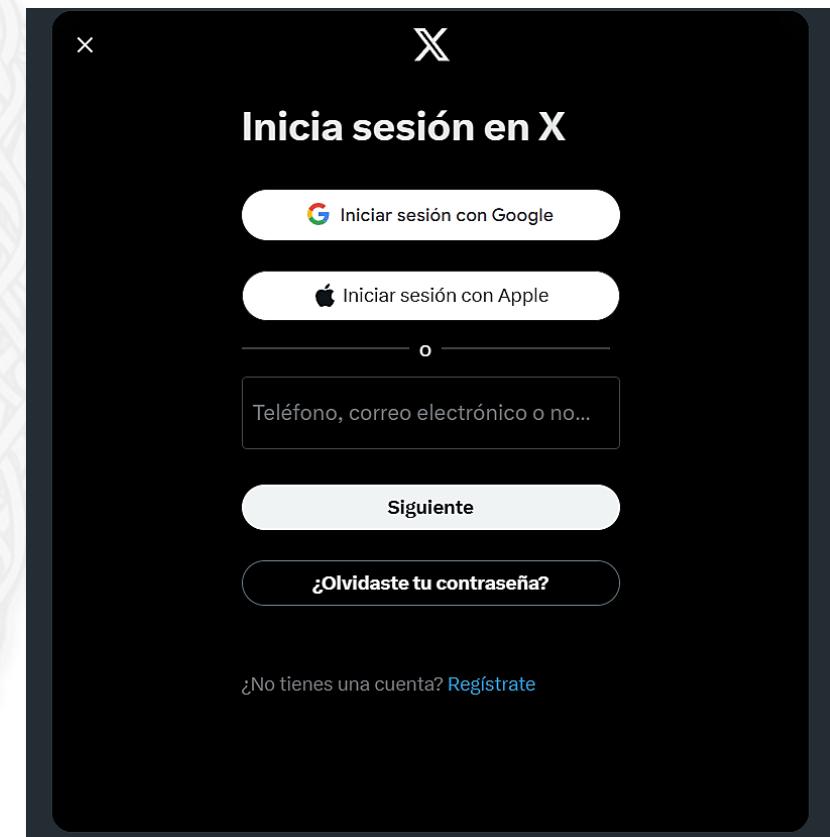
# COMO HACERSE UNA CUENTA NUEVA

- Muchas RRSS permiten usar una cuenta que tengas en otro servicio, y es mejor por varias razones

- No tienes que recordar otro usuario y contraseña
- **¿Se filtran datos de cuentas de la RRSS?** No es tu problema
  - Ej.: Usar Google para darte de alta en Twitter **NO le da** tu contraseña de Google a Twitter
  - Google verifica que eres tú dentro de la propia Google y le dice a Twitter: "Ok, es fulanito, déjale entrar en su cuenta"
- **¿Tienes que cambiar contraseñas?** Hazlo solo en un sitio para cambiarlas todas
- **¿Ya tienes Google, etc. abierto?** Entras directamente en la RRSS
- **¿Tienes 2FA en Google o similar?** Lo tienes en la RRSS también

- Hay más razones, míralo en este artículo

- En general, es **aplicable a cualquier cuenta en cualquier servicio**
- <https://www.incibe.es/ciudadania/blog/registrarte-con-tu-cuenta-de-google-facebook-o-twitter-ventajas-e>



Una cuenta para entrar a todas :P. En caso de robo, los sistemas de recuperación de Google, Apple, etc. suelen ser mejores que los de las RRSS al uso

# ¿POR QUÉ CONFIGURAR LAS CUENTAS DE RRSS?



José Manuel  
Redondo López

- Tristemente, estar en una red social te hace objetivo de muchos tipos de fraudes
  - Muchos usuarios en una red social no son reales, sino bots
  - Están ahí para escribir mensajes falsos y sacar algún beneficio
  - Desinformación, estafas, troleo...
  - El **M-31 “Segura”** y el **“Nautilus”** profundizan en ello
- Muchas veces usando la información que tú mismo/a das
  - Ej.: Robando tus fotos, audios, videos (y así entrenar IAs para hacerte deepfakes)
- Configurando bien tu RRSS puedes parar muchos de estos problemas

Fraudes hay de muchos tipos, desde falsas ofertas de empleo, préstamos falsos, promociones de viaje que no llevan a ningún lado, anuncios de alquileres o venta de productos y viviendas que acaban en decepción.

En la OSI, canal especializado en ciudadanos de INCIBE, encontrarás más información sobre todos ellos, además de recursos para ayudarte a identificarlos y prevenirlos.

[www.incibe.es](http://www.incibe.es) | [www.osi.es](http://www.osi.es)

GOBiERNO DE ESPAÑA  
VICEREJERÍA DEL GOBIERNO  
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL  
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN Y DIFUSIÓN ALÍPJICA  
**incibe**  
INSTITUTO NACIONAL DE CIBERSEGURIDAD  
017  
**osi** Oficina de Seguridad del Internauta

@INCIBE @osiseguridad

## Aprende a reconocer fraudes en redes sociales y WhatsApp

En nuestras redes sociales y aplicaciones de mensajería instantánea, como WhatsApp, son comunes los fraudes y estafas. Por eso, debemos aprender a reconocerlos y evitarlos:

- 1 Concursos y promociones falsos:**  
¡He ganado un premio sin haber participado!
  - Si para recibirlo debo:
    - Compartirlo con mis contactos.
    - Rellenar un formulario con mis datos personales.
    - Efectuar un pago o suscripción a un servicio de pago.
    - Aceptar unas bases legales confusas o que se contradicen.
  - Más información en "Sorteos y premios online, un reclamo para hacerse con nuestros datos".
- 2 Secuestro de WhatsApp:**  
Me han robado mi cuenta de WhatsApp.
  - Inesperadamente:
    - He recibido un código de verificación de la app por SMS para configurar la cuenta en un nuevo dispositivo.
    - Un usuario me ha solicitado el código bajo alguna excusa.
  - Más información en "¡Socorro, me han secuestrado WhatsApp!".
- 3 Cuentas falsas:**  
¿Perfiles de empresas o famosos demasiado parecidos en una red social?
  - Análisis si:
    - Existen dos o más cuentas con un nombre similar y la misma descripción e imágenes.
    - El perfil no cuenta con la insignia de verificación de la cuenta (check).
    - Comparte enlaces a webs desconocidas o que no tienen nada que ver con la empresa.
    - Manda mensajes genéricos solicitando apoyo económico a sus seguidores.
  - Más información en "Suplantación de identidad y secuestro de cuentas: ¿cómo actuar?".
- 4 Sextorsión y amores en línea:**  
Buscando pareja encontré un perfil fraudulento.
  - Se caracteriza por:
    - Utilizar perfiles abiertos, con fotografías de personas atractivas.
    - Usar fotos robadas de otras cuentas privadas o públicas en Internet.
    - Compartir los mismos gustos, aficiones, etc.
    - Pedir ayuda económica bajo algún pretexto.
    - Solicitar imágenes íntimas o vídeos explícitos.
  - Más información en "Amor online: ¡Que no te den sapo por príncipe azul!".
- 5 Anuncios de tiendas fraudulentas:**  
He visto un anuncio que es un chollo.
  - Pistas:
    - Se difunden en redes sociales con promociones muy atractivas.
    - Promocionan productos de marcas muy conocidas.
    - La URL y estética de la tienda anunciada no tiene nada que ver con la original.
    - Las imágenes y descripciones de los productos están poco cuidadas (poca calidad y mala redacción).
    - Proporcionan escasa información, o es inexistente, sobre quién es la empresa y cómo contactar con ella.
    - No aceptan **métodos de pago seguros**, facilitan un formulario para introducir todos los datos de tu tarjeta, sin ninguna garantía de seguridad.
  - Más información en "Tiendas online fraudulentas".



# PRIVACIDAD

- **Alguna gente dice que la privacidad no es importante**

- Dicen que “no son delincuentes y no tienen nada que ocultar”

- **Esto es falso: Tu falta de privacidad puede ser usada en tu contra**

- Ej.: *¿Qué pasa si alguien te suplanta en un grupo que tienes con tus amigos/as?*
- Es imposible calcular todos los riesgos
- Por lo que puedes tener un problema si no la cuidas en cualquier momento

- **Tus pensamientos, fotos, etc. son tuyos,**

- ¡No dudes en protegerlos en cualquier RRSS!

The infographic features a woman holding a padlock and a key, standing within concentric circles. It includes logos for incibe\_ (Instituto Nacional de Ciberseguridad) and OSi (Oficina de Seguridad del Internauta). The main text reads: "Tu privacidad sí importa, ¡protégela!" (Your privacy does matter, protect it!). Below the text are six icons with corresponding tips:

- Protege la información almacenada en tus cuentas usando contraseñas seguras y distintas para cada servicio online.
- Activa la autenticación en dos pasos para dotar de mayor seguridad el acceso a tus cuentas online.
- Limita la información que compartes en redes sociales u otros canales para prevenir el robo y suplantación de identidad.
- Lee las políticas de privacidad de las webs en las que estás registrado para conocer cómo protegerán tus datos y qué uso harán de ellos.
- Cierra siempre la sesión cuando termines de hacer uso de un servicio en dispositivos compartidos o públicos.
- Revisa qué permisos concedes a las aplicaciones que tienes instaladas.

#OSIconsejo  
[www.incibe.es/ciudadania](http://www.incibe.es/ciudadania)



# REPUTACIÓN

- La privacidad va de la mano con tu **reputación online** 😞
- Si algo no lo dirías/harías en persona, no lo digas/hagas en RRSS 🤡
  - La culpa **siempre es de quien acosa**, extorsiona, etc.
  - Pero las consecuencias chungas de primeras **te las llevas tú** 😞
- Como dijimos antes, en la RRSS se busca “guerra”: No caigas en la trampa
- Cuidado con lo que dices, o con lo que le dicen a la gente de tu entorno
  - Es importante **combatir el ciberbullying**: Mira la P-74 “Atalaya”
  - ¡Tú puedes ayudar a quien lo necesita!

The infographic is titled "¿Cómo cuido mi reputación online?" and is produced by incibe (Instituto Nacional de Ciberseguridad) and OSi (Oficina de Seguridad del Internauta). It features a woman in an orange jacket holding a smartphone, looking at five circular icons representing different steps to manage online reputation:

- Indaga sobre ti en motores de búsqueda.** (Search engines) Description: Encuentras contenido que no te gusta, elimínalo si tienes permisos para ello. En caso contrario, solicita su eliminación a la plataforma donde está publicado.
- Piensa antes de publicar contenido en Internet.** (Thinking before posting) Description: si puede malinterpretarse, disgustar y ofender a otros usuarios si no se conoce el contexto.
- Interactúa de forma positiva en línea.** (Positive interaction) Description: Respeta las opiniones de los demás y evita discusiones innecesarias que perjudiquen tu imagen.
- Utiliza las opciones de privacidad.** (Privacy options) Description: Utiliza las opciones de privacidad que proporcionan las redes sociales y otros sitios web para controlar quién puede ver lo que publicas.
- Si alguien publica algo negativo sobre ti,** (Negative content) Description: trata de resolver el problema de manera privada y cordial para solicitar su retirada. Si no atiende a tus peticiones, solicita a la plataforma su eliminación.

#OSIconsejo  
[www.incibe.es/ciudadania](http://www.incibe.es/ciudadania)



# OK, PERO...¿CÓMO LO HAGO?

- Por suerte para nosotros, el INCIBE tiene guías fáciles de seguir

- ¡Para todas las RRSS!
- <https://www.incibe.es/ciudadania/tematicas/priva/cidad/configuraciones-redes-sociales>

- Te incluimos aquí unas imágenes resumen

- Y luego usaremos Twitter/X como ejemplo de por qué ciertas configuraciones son importantes
- Así puedes buscar **opciones parecidas en otras RRSS** que tengas

The infographic is titled "No dejes que X (Twitter) te delate, configura tu privacidad". It features the logos of INCIBE (Instituto Nacional de Ciberseguridad) and OSi (Oficina de Seguridad del Internauta). A woman in an orange sweater is shown holding a smartphone displaying the Twitter app's privacy settings menu. The menu includes sections like "Privacidad y seguridad", "Tu actividad en Twitter", "Audiencia y etiquetas", "Tus Tweets", "Contenido que ves", "Silenciar y bloquear", "Mensajes directos", "Espacios", and "Visibilidad y contactos". A large orange padlock icon is overlaid on the phone screen. To the right, four steps are outlined:

- **Abre la aplicación.** (Open the application.)
- **Accede al menú principal** pulsando sobre la imagen de tu perfil. (Access the main menu by tapping on your profile picture.)
- A continuación, dirígete al apartado **"Configuración y privacidad"**. (Next, go to the "Configuration and Privacy" section.)
- Una vez ahí, desde el apartado **"Privacidad y seguridad"** podrás configurar cuestiones como:
  - **Controlar** quien puede ver y responder a tus tuits.
  - **Bloquear y silenciar** palabras, usuarios, listas, notificaciones, etc.

At the bottom, there is a thumbs-up icon, the hashtag #OSIconsejo, and the website www.incibe.es/ciudadania.



José Manuel  
Redondo López

# OK, PERO...¿CÓMO LO HAGO?

incibe\_ 017 OSI  
INSTITUTO NACIONAL DE CIBERSEGURIDAD Oficina de Seguridad del Internauta

## ¿Cómo protejo mi privacidad en TikTok?



Entra en tu perfil y haz clic en las tres rayas.

Accede a 'Ajustes y privacidad'.

Revisa dentro de 'Privacidad' cuestiones relevantes como:

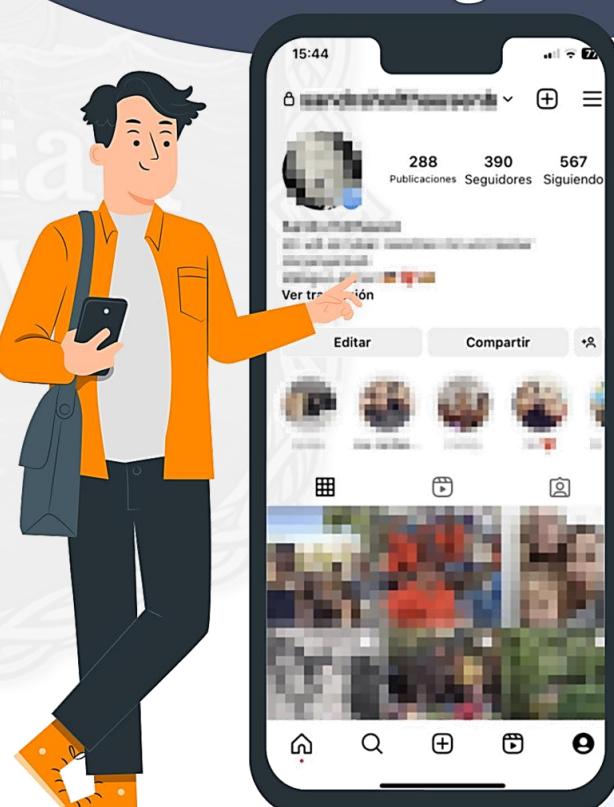
- Si la cuenta es privada.
- Si estás compartiendo tu ubicación.
- Quién puede enviarte mensajes.
- Usuarios bloqueados.

### Ajustes y privacidad



¡Configura la aplicación y ten bajo control tu información!

#OSIconsejo  
[www.incibe.es/ciudadania](http://www.incibe.es/ciudadania)



## Configura tu privacidad de Instagram en 5 pasos

incibe\_ 017 OSI  
INSTITUTO NACIONAL DE CIBERSEGURIDAD Oficina de Seguridad del Internauta

Abre la aplicación de Instagram

Entra en tu perfil

Pulsa en las tres líneas horizontales de arriba a la derecha.

Dirígete a 'Configuración y privacidad'.

A continuación, podrás:

Revisar la configuración de la cuenta: datos personales, contraseña, permisos así como las preferencias de los anuncios.

Establecer quién puede ver tus contenidos.

1. Privacidad de la cuenta.  
2. Bloquear cuentas de usuarios.  
3. Ocultar historias y directos a usuarios concretos.

Indicar cómo pueden interactuar contigo los demás.

1. Bloquear comentarios, quién puede etiquetarte, etc.

#OSIconsejo

[www.incibe.es/ciudadania](http://www.incibe.es/ciudadania)

Pasos a seguir en iPhone. En dispositivos Android, en el paso 4 habrá que seleccionar 'Configuración' y después 'Privacidad' para encontrar las distintas opciones.



José Manuel  
Redondo López

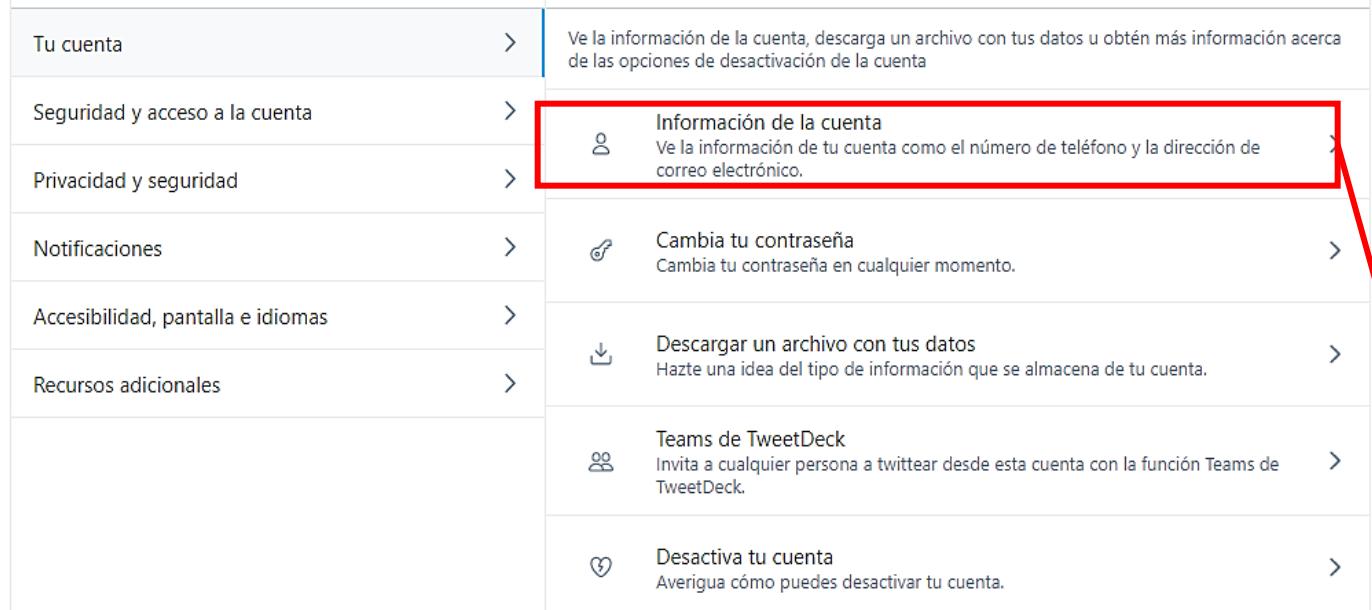
# EJEMPLO DE OPCIONES DE UNA RED SOCIAL: TWITTER/X

The image shows a mobile screenshot of the Twitter/X navigation menu. On the left, there's a vertical sidebar with options like 'Solicitudes de seguimiento' (20+), 'Temas', 'Momentos', 'Boletines informativos', 'Twitter Ads', 'Analytics', 'Configuración y privacidad' (which is highlighted with a red box and has a red arrow pointing to it), 'Centro de ayuda', 'Mostrar', and 'Atajos de teclado'. The main content area has two sections: 'Configuración' (also highlighted with a red box) and 'Privacidad y seguridad'. The 'Configuración' section contains links for 'Tu cuenta', 'Seguridad y acceso a la cuenta', 'Privacidad y seguridad', 'Notificaciones', 'Accesibilidad, pantalla e idiomas', and 'Recursos adicionales'. The 'Privacidad y seguridad' section contains links for 'Tu actividad en Twitter' (with sub-links for 'Audiencia y etiquetas', 'Tus Tweets', 'Contenido que ves', 'Silenciar y bloquear', 'Mensajes Directos', and 'Visibilidad y contactos').

Configuración	
Tu cuenta	>
Seguridad y acceso a la cuenta	>
Privacidad y seguridad	>
Notificaciones	>
Accesibilidad, pantalla e idiomas	>
Recursos adicionales	>

Privacidad y seguridad	
Administra qué información ves y compartes en Twitter.	
<b>Tu actividad en Twitter</b>	
Audiencia y etiquetas	>
Tus Tweets	>
Contenido que ves	>
Silenciar y bloquear	>
Mensajes Directos	>
Visibilidad y contactos	>

# ¡PROTEGE TU CUENTA! (SOBRE TODO AL PRINCIPIO)



Tu cuenta > Ve la información de la cuenta, descarga un archivo con tus datos u obtén más información acerca de las opciones de desactivación de la cuenta

Seguridad y acceso a la cuenta > **Información de la cuenta** (highlighted with a red box)  
Ve la información de tu cuenta como el número de teléfono y la dirección de correo electrónico.

Privacidad y seguridad >

Notificaciones > Cambia tu contraseña  
Cambia tu contraseña en cualquier momento.

Accesibilidad, pantalla e idiomas > Descargar un archivo con tus datos  
Hazte una idea del tipo de información que se almacena de tu cuenta.

Recursos adicionales > Teams de TweetDeck  
Invita a cualquier persona a twittear desde esta cuenta con la función Teams de TweetDeck.

Desactiva tu cuenta  
Averigua cómo puedes desactivar tu cuenta.

**Esto es el “tick” azul, pero solo se lo dan a famosos, a empresas (tick amarillo) o a quienes pagan**



← **Información de la cuenta**

Nombre de usuario  
@The\_Rounded\_Man

Teléfono

Correo electrónico (highlighted with a blue bar)  
Verificado  
No. Solicitar verificación

Tweets protegidos  
 Sí (highlighted with a red box)

**Superimportante, esto hace que solo quien te siga (y tú aceptes primero) vea lo que publicas**

**¡Búscalos en todas tus RRSS!**



José Manuel  
Redondo López

# ¡NO DES DEMASIADA INFORMACIÓN Y VIGILA TU CUENTA!

**Configuración**

- Tu cuenta >
- Seguridad y acceso a la cuenta** > **Aplicaciones y sesiones** >
- Privacidad y seguridad >
- Notificaciones >
- Accesibilidad, pantalla e idiomas >
- Recursos adicionales >

**Seguridad y acceso a la cuenta**

Administra la seguridad de tu cuenta y lleva un control de su uso, incluidas las aplicaciones que conectaste a ella.

**Seguridad**  
Administra la seguridad de tu cuenta.

**Aplicaciones y sesiones**  
Consulta la información sobre cuándo iniciaste sesión en tu cuenta y las aplicaciones que conectaste a ella.

**¿Sospechas que alguien te entra en la cuenta? Aquí puedes ver desde dónde se entró últimamente...**

**¡Revísalo a menudo por si hay algo sospechoso!**

**Configuración**

- Tu cuenta >
- Seguridad y acceso a la cuenta** > **Agregar información de ubicación a tus Tweets** >
- Privacidad y seguridad >
- Notificaciones >
- Accesibilidad, pantalla e idiomas >
- Recursos adicionales >

**Tus Tweets**

Administra la información asociada a tus Tweets.

Marcar el contenido multimedia que twitteas para indicar que contiene material que puede herir la sensibilidad de algunas personas

Si activas esta opción, las imágenes y los videos que twittees se marcarán como delicados para las personas que no deseen ver ese tipo de contenido. [Más información](#)

**Entra aquí y DESACTIVA la ubicación para tus tweets**

**¡A nadie le interesa saber desde donde posteas! (demasiada información a la que dar mal uso)**

# ¿No te interesa cierto contenido? ¡PUES NO LO VEAS!

Configuración	Privacidad y seguridad
Tu cuenta	Administra qué información ves y compartes en Twitter.
Seguridad y acceso a la cuenta	
Privacidad y seguridad	<b>Audiencia y etiquetas</b> Administra qué información permite que vean otras personas en Twitter.
Notificaciones	
Accesibilidad, pantalla e idiomas	
Recursos adicionales	<a href="#">Contenido que ves</a> Decide qué ver en Twitter en función de los temas e intereses de tu preferencia.  <a href="#">Silenciar y bloquear</a> Administra las cuentas, palabras y notificaciones que silenciaste o bloqueaste.

Aquí puedes bloquear o silenciar gente (más de eso después)

¡Pero lo más importante es que si estás harto de un TT o tema, puedes silenciar palabras y no volverán a salirte más mensajes que las contengan!

## Contenido que ves

Decide qué ver en Twitter en función de los temas e intereses de tu preferencia.

Mostrar contenido multimedia que pueda contener material delicado

Temas

Intereses

Configuración de Explorar

Configuración de búsqueda

Indica lo que te interesa y así tu red te mostrará cosas más interesantes...

¡También puedes bloquear videos o imágenes catalogadas como ofensivas (hay gente que se cree muy graciosa 😞)

## Configuración

Tu cuenta	Administra las cuentas, palabras y notificaciones...
Seguridad y acceso a la cuenta	
Privacidad y seguridad	<a href="#">Cuentas bloqueadas</a> <a href="#">Cuentas silenciadas</a> <a href="#">Palabras silenciadas</a>
Notificaciones	
Accesibilidad, pantalla e idiomas	
Recursos adicionales	



José Manuel  
Redondo López

# ¡EN INSTAGRAM HAY OPCIONES MUY SIMILARES!

Privacidad de la cuenta

**Cuenta privada**  
Si tu cuenta es privada, solo las personas que apruebes podrán ver tus fotos y vídeos en Instagram. Esto no afectará a tus seguidores actuales.

Estado de actividad

**Mostrar estado de actividad**  
Permite que las cuentas que sigues y las personas a las que has enviado mensajes puedan ver la última vez que has estado activo en las aplicaciones de Instagram. Si desactivas esta opción, no podrás ver el estado de actividad de otras cuentas.

Compartir las historias

**Permitir compartir**  
Permite que las personas comparten tu historia como mensajes.

Comentarios

[Editar configuración de los comentarios](#)

**¡Merece MUCHO la pena dedicar un rato a leer opciones de privacidad y seguridad y activarlas en TODAS tus redes sociales!**

**¡Hay cosas muy útiles que seguramente no conocías!**



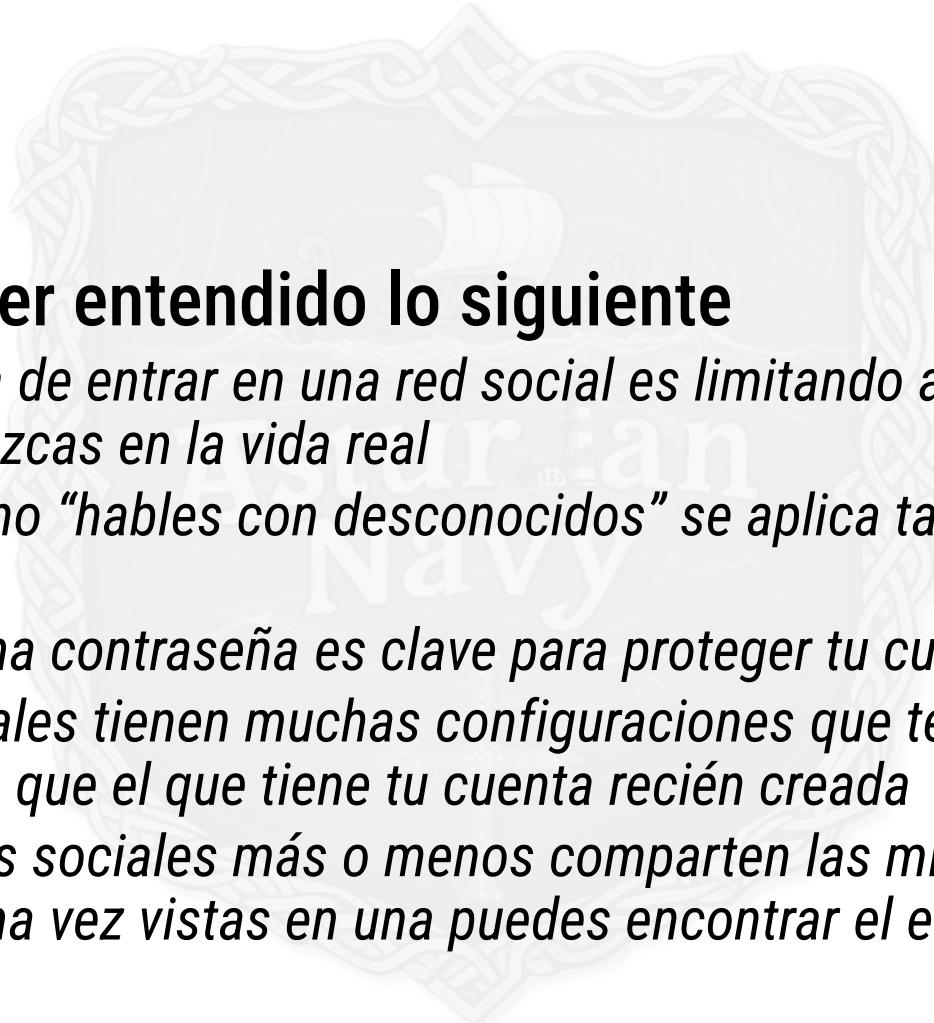
José Manuel  
Redondo López

# ¿Y EN TIKTOK?

The image consists of three screenshots of the TikTok mobile application. The first screenshot shows the user's profile page with a placeholder profile picture, 0 videos, 0 following, 0 fans, and 0 hearts. It includes a red box around the 'Edit Profile' button and another around the 'No bio yet' section. The second screenshot shows the 'Privacy and Settings' menu with various options like Digital Wellbeing, Live Photo, General Settings, Help Center, Terms of Use, Privacy Policy (which is highlighted with a red box), Copyright Poli, Report a Problem, Clear Cache, and Log Out. The third screenshot shows the 'Privacy and Safety' settings screen under 'Discoverability', which includes 'Allow Others to Find Me' and 'Private Account' (both highlighted with red boxes). It also shows sections for Personalization and Safety, with specific settings for who can comment, react, duet, message, download, and block.

Aunque...TikTok es una red que ahora mismo está rodeada de polémicas (tratamiento de tus datos, privacidad...)

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



## ● Asegúrate de haber entendido lo siguiente

- Que la mejor forma de entrar en una red social es limitando al principio tu cuenta solo a personas que conozcas en la vida real
- Que el consejo de no "hables con desconocidos" se aplica tanto en la calle como en las redes sociales
- Que tener una buena contraseña es clave para proteger tu cuenta en una red social
- Que las redes sociales tienen muchas configuraciones que te permiten dejarla en un estado mucho más seguro que el que tiene tu cuenta recién creada
- Que todas las redes sociales más o menos comparten las mismas opciones de privacidad y seguridad, y que una vez vistas en una puedes encontrar el equivalente en las demás



## Precauciones usando una red social

Cosas que no debes hacer o debes tener especial cuidado



# RIESGOS GENERALES DE LAS RRSS



José Manuel  
Redondo López

- Ya se que eres libre de hacer lo que quieras

- Pero tampoco es plan de lanzarse a lo loco...
- O podrías tener hermanos/as menores que necesiten tu ayuda

- Voy a hablarte en general de los 10 riesgos más frecuentes de las RRSS

- Si quieres saber más, te recomiendo leer la **P-74 “Atalaya”** y la **“A-71 Juan Sebastián Elcano”**

## 1. CIBERACOSO



El ciberacoso es el acoso que se desarrolla a través de los canales digitales. En concreto las redes sociales son uno de los canales más utilizados junto a las aplicaciones de juegos

## 2. SEXTING



El sexting (sex and texting) consiste en el intercambio, envío o reenvío de contenido audiovisual erótico a través de aplicaciones de mensajería o mensajes privados en plataformas sociales



José Manuel  
Redondo López

# RIESGOS GENERALES DE LAS RRSS



## 3. SEXTORSIÓN

La sextorsión consiste en la extorsión y chantaje a una persona utilizando los contenidos enviados durante el sexting o afirmando tener posesión de ellos. Los fines con los que se realizan pueden ser muy diversos, pero en líneas generales son para exigir que se continúen enviando imágenes y contenido sexuales como medio de coacción o para conseguir dinero.



## 4. GROOMING

El grooming es el peligro que existe para niños y adolescentes que interactúan con adultos cuyo objetivo es ganarse su confianza con fines sexuales. Para conseguirlo pueden hacerse pasar por otra persona más joven, ofrecer regalos, etc.



# RIESGOS GENERALES DE LAS RRSS

## 5. RETOS PELIGROSOS (CHALLENGES)



Estos últimos pueden llegar a poner en peligro a la persona que los realiza o afectar a terceros por tratarse de acciones delictivas. Además de estas consecuencias existen otros aspectos psicológicos a tener en cuenta como ansiedad, depresión, dependencia y trastornos del sueño

## 6. CONTENIDO INAPROPiado



Las redes sociales pueden ser el punto de acceso consciente o inconsciente donde niños y jóvenes vean contenido sexual o violento. Entre ellos se puede encontrar vandalismo, pornografía, racismo, etc.



# RIESGOS GENERALES DE LAS RRSS



## 7. SUPLANTACIÓN DE LA IDENTIDAD DIGITAL

Al robarse una cuenta en redes sociales perdiendo el control total de ella y de las publicaciones o acciones que se realizan.

O falsificando el perfil, más común ante cuentas abiertas, ya que es más fácil sustraer fotos y contactos que se usarán posteriormente para crear un perfil falso con la misma apariencia que el verdadero, pero gestionado por un delincuente



## 8. FAKE NEWS

La problemática de las fake news a través de las redes sociales es la facilidad de difusión y en el caso de los menores puede ser más efectiva por su grado de desprotección. Ellos mismos pueden convertirse en altavoces del engaño que puede tener diferentes grados



# RIESGOS GENERALES DE LAS RRSS



## 9. ACCESO A DISCURSOS DE ODIO

Su definición puede ser compleja, pero se refiere a cualquier mensaje o contenido que incita a actos de discriminación o violencia por motivos de odio racial u orientación sexual, entre otros



## 10. ADICCIÓN A LAS REDES SOCIALES

El uso de estas tecnologías en edades tempranas genera adicción y consecuencias como: falta de sueño, negación de la realidad y conflictos familiares. Su continuidad en el tiempo genera efectos negativos



José Manuel  
Redondo López

# ASPECTOS POSITIVOS Y NEGATIVOS DE LAS RRSS

- Como te decía al principio, cualquier red social tiene aspectos positivos y negativos

- Ten presentes ambos si te planteas seguir o entrar en una

- Cada red tiene los suyos

- Twitter/X por ejemplo tiene **más anuncios y discursos de odio** de distintos tipos que otras redes sociales
  - LinkedIn tiene demasiado contenido de “auto-promoción” y gente con discursos tóxicos de **hiperproductividad**
    - <https://www.reddit.com/r/LinkedInLunatics/>
  - Facebook cada vez está más plagado de **contenido malicioso** (estafas, fake news...) pensado para personas mayores de 40

- ¿Encaja tu perfil en una red concreta?

- Piénsalo antes de meterte en ella

- ¿Estas en una red te está haciendo daño sicológico?

- Quizá sea hora de **priorizar tu bienestar**





# ASPECTOS POSITIVOS Y NEGATIVOS DE LAS RRSS

## ● Pero esta presentación está pensada para gente joven

- Y, de todas las redes, TikTok es en la que debes tener (aún) más cuidado
- Debido a que tiene un nº comparativamente alto de usuarios “**no recomendables**”

## ● Ten mucho cuidado si hablas con gente que realmente no debes identificar

- Hay un buen nº de casos de “**depredadores**” que van a por gente de tu edad
  - O para enseñarte fotos que NO quieres ver
- **Evita, denuncia, bloquea**
  - *¿Cómo?* Esto es para padres, pero le puedes sacar partido tú también
  - <https://www.incibe.es/menores/familias/control-parental/tiktok>



The infographic is titled "TikTok" and features a question "¿CUÁLES SON LOS RIESGOS?" (What are the risks?). It lists several categories of risks:

- EXPOSICIÓN DE DATOS PERSONALES**
  - No te filmes con **uniforme** o escudo del colegio (o del club)
  - No compartas tu **ubicación** (ojo también con tu "escenografía")
  - Revisá periódicamente tu configuración de **privacidad**
- ACCIDENTES**
  - No aceptes **retos ni desafíos** que te pongan en peligro a vos o a otros.
- CONTACTO CON DESCONOCIDOS**
  - No todos son quienes dicen ser. Es muy fácil **mentir** en internet.
- HUMILLACIÓN Y MALTRATO**
  - No **critiques** los videos de los demás.
  - No les hagas caso a los que hagan críticas con mala onda.
- ADICCIÓN**
  - Regulá el **tiempo** de uso. Si no podés, pedí ayuda para limitarlo.
- ACOSO**
  - Si te sentís acosado, **decilo**. Nadie puede resolverlo solo.

At the bottom, it includes the website [www.libresdebullying.com.ar](http://www.libresdebullying.com.ar) and the logo for "libresdebullying" which includes the text "EQUIPO DE DIAGNÓSTICO, PREVENCIÓN E INTERVENCIÓN".



José Manuel  
Redondo López

# ¿QUÉ COSAS TENGO QUE VIGILAR CUANTO ESTOY EN UNA RRSS?

## ● Como te comentaba antes, estar en RRSS te somete a nuevos peligros (mira la imagen)

- Todos están en todas las RRSS

## ● Pero algunos son más frecuentes en unas que en otras

- La de **bulos** conspiranóicos para mayores que hay en Facebook mete miedo (recuerda: algunas personas se creen eso...)
- Algunos **challenges** de Insta son muy peligrosos
  - También en TikTok 😞
- Cuidado con las **funas** (hacerlas (¡es bullying!, P-74 “Atalaya”) y que te las hagan) y con quedarte “enganchado”
  - No solo a la red, hay mucho **juego online encubierto** (o a la vista)
- ...

## ● Es necesario que sepas lo que son y tengas bien entrenado tu “sentido arácnido”

### Top 10 de los principales peligros de las redes sociales para los jóvenes

	Problemas para la privacidad
	Suplantación de identidad
	Adicción a las RRSS
	Ciberbullying
	Contacto con desconocidos que pueden ser peligrosos
	Grooming
	Sexting
	Sextorsión
	Fake news y la distorsión de la realidad
	Challenge o retos muy peligrosos, en ocasiones delictivos

Fuente: <https://protecciondatos-lopd.com/empresas/peligros-redes-sociales/>



José Manuel  
Redondo López

# APLICACIONES QUE SE INSTALAN EN TUS RRSS

## ● ¿Este tipo de aplicaciones “graciosas” te suena?

- Son simpáticas y tienen funcionalidades interesantes, pero...
- ...¡Algunas veces resultan ser timos!
- **¡Lo mismo pasa con algunos anuncios en RRSS!**

## ● Quieren que hagas clic y acceder a tu cuenta para...

- Mostrarte **publicidad** (¡que jeta!) 🔈
- Postear como su fueras tú, es decir, **suplantarte** (¡impostor!) 👤
- **Borrarte** mensajes (¡lo que faltaba!) 😵 😵
- ¡O robarte la cuenta! (Oh, oh...) 😠

## ● El daño que pueden hacer depende de los permisos que les concedas



¿Quien visita tu perfil?

Paso 1 de 4

Te gustaría saber quien visita tu perfil de facebook?, sigue estos simples y rápidos pasos y podrás usar esta aplicación ya mismo.

WHO VISITS YOUR TWITTER PROFILE?

- CLICK HERE -

Last visits to your Twitter profile - WORKING NOW !!  
Last visits to your Twitter profile - WORKING NOW !!

Find out your profile visitors for free

Continue with Facebook



José Manuel  
Redondo López

# APLICACIONES QUE FUNCIONAN CON TU CUENTA DE RRSS

## ● Tu cuenta es tuya

- **No la cedas a nadie... ¡ni a nada!**
- Lo mejor es **NO** instalarse estas aplicaciones
- Si ya lo has hecho
  - Vete a las opciones y busca el apartado de aplicaciones
  - Una vez allí, elimínala o quítale permisos
  - ¡Todas las RRSS tienen una opción así!

¡Está intentando instalarse en tu cuenta de Twitter!

twitter

Authorize Seesmic Web to use your account?

This application **will be able to**:

- Read Tweets from your timeline.
- See who you follow, and follow new people.
- Update your profile.
- Post Tweets on your behalf.
- Access your direct messages.

This application **will not be able to**:

- See your Twitter password.

You can revoke access to any application at any time from the [Applications tab](#) of your Settings page. By authorizing an application you continue to operate under [Twitter's Terms of Service](#). In particular, some usage information will be shared back with Twitter. For more, see our [Privacy Policy](#).

## ● Lo mismo pasa con los anuncios

- Mejor **no hagas clic** en ninguno
- Te pueden llevar a páginas de fraudes o que te instalen algo automáticamente
  - Y ya no te digo si te piden que te lo instales tú
- **No te instales cosas de cualquier sitio**, ¡que es lo que buscan para liártela!
- **Mira bien antes de hacer clic**: Algunos anuncios son muy buenos haciéndose pasar por publicaciones

Instagram

Edit Profile

Change Password

Authorized Applications

Email and SMS

Manage Contacts

Privacy and Security

Buffer

Production environment client for Buffer

Permissions

Access your basic information Your media & profile info

Revoke Access

WordPress.com

Display your latest Instagram photos on your WordPress.com site.

Permissions

Access your basic information Your media & profile info

Revoke Access

¿No sabes qué hace aquí o no te interesa?  
Cárgatela!

# ¡ALGUIEN HA POSTEADO UNA BURRADA!



José Manuel  
Redondo López

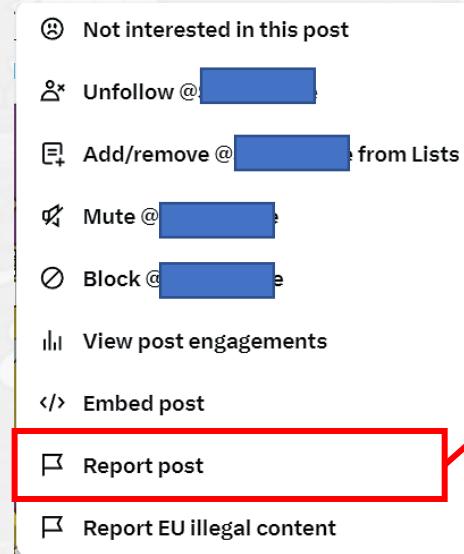
## ● ¿Alguien ha posteado una burrada, algo ofensivo o similar? 🤦‍♂️

- ¡Tú puedes ayudar a “limpiar” la red!
- Se puede **denunciar un mensaje** alegando una razón ⚡
- La red social te pregunta **por qué crees que es ofensivo**
  - Luego analiza tú denuncia
  - Si hay más gente que ha hecho lo mismo y/o es verdad, puede borrar el mensaje
  - ¡O suspender / cancelar la cuenta!

## ● Así se auto-regulan sus contenidos

## ● Siempre es anónimo

- ¡Nadie sabrá que le has denunciado!



Cada RRSS tiene sus normas y “contenidos prohibidos”, pero en general acaban más o menos siendo estos en todas

x Gathering info

### What type of issue are you reporting?

Why are we asking this?

Hate

Slurs, Racist or sexist stereotypes, Dehumanization, Incitement of fear or discrimination, Hateful references, Hateful symbols & logos

Abuse & Harassment

Insults, Unwanted Sexual Content & Graphic Objectification, Unwanted NSFW & Graphic Content, Violent Event Denial, Targeted Harassment and Inciting Harassment

Violent Speech

Violent Threats, Wish of Harm, Glorification of Violence, Incitement of Violence, Coded Incitement of Violence

Child Safety

Child sexual exploitation, grooming, physical child abuse, underage user

Privacy

Sharing private information, threatening to share/expose private information, sharing non-consensual intimate images, sharing images of me that I don't want on the platform

Spam

Fake engagement, scams, fake accounts, malicious links

Suicide or self-harm

Encouraging, promoting, providing instructions or sharing strategies for self-harm.

Sensitive or disturbing media

Graphic Content, Gratuitous Gore, Adult Nudity & Sexual Behavior, Violent Sexual Conduct, Bestiality & Necrophilia, Media depicting a deceased individual

Impersonation

Pretending to be someone else, including non-compliant parody/fan accounts

Violent & hateful entities

Violent extremism and terrorism, hate groups & networks

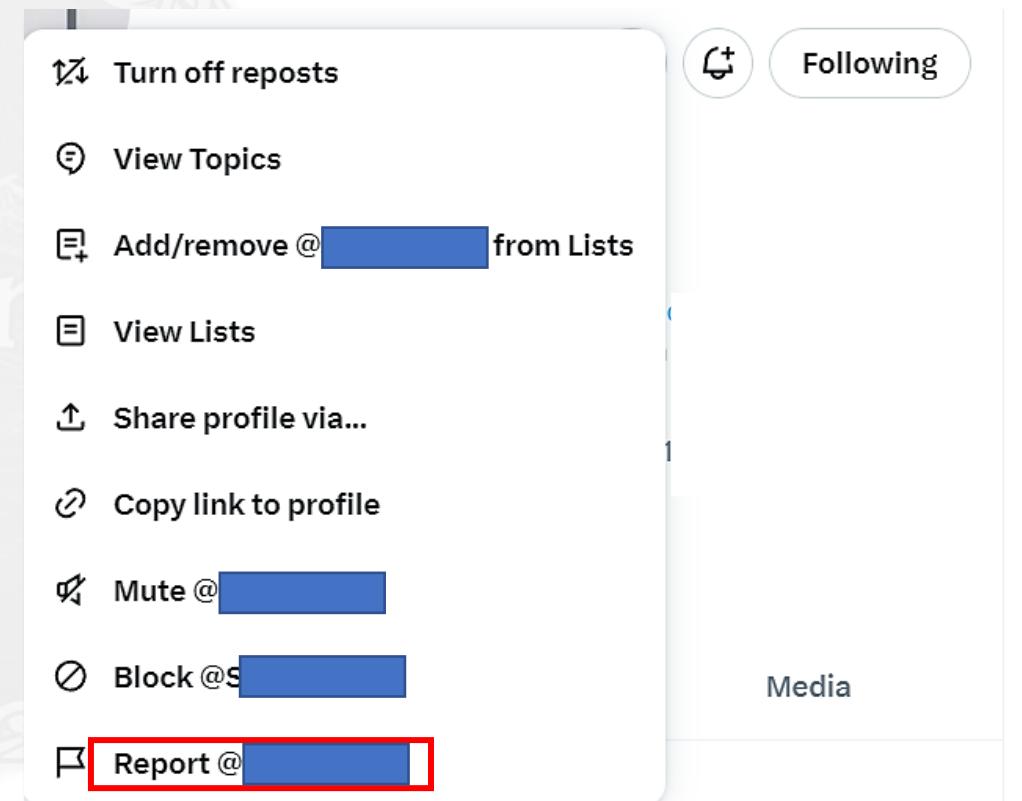
[Next](#)



José Manuel  
Redondo López

# ¡UNA CUENTA SOLO POSTEA BURRADAS!

- ¿Ves que *una cuenta solo postea funas, beef, mal rollo, amenazas, burradas, estafas / mensajes automáticos / engaños / etc.*?
  - No un mensaje o unos pocos: **TODO lo que hace es así**
- Se puede hacer lo mismo: **denunciar una cuenta completa**
- Nuevamente te preguntará una razón
  - Que suelen ser las mismas que a la hora de denunciar un post, como en el caso anterior
  - Y si hay varias denuncias / comprueban que es cierto, ¡adiós cuenta troll!
  - La suspensión puede ser temporal o total



Bloquear a un troll está bien, pero **¿denunciarlo y que le tiren la cuenta por tóxico/cafre?** Otro rollo ☺

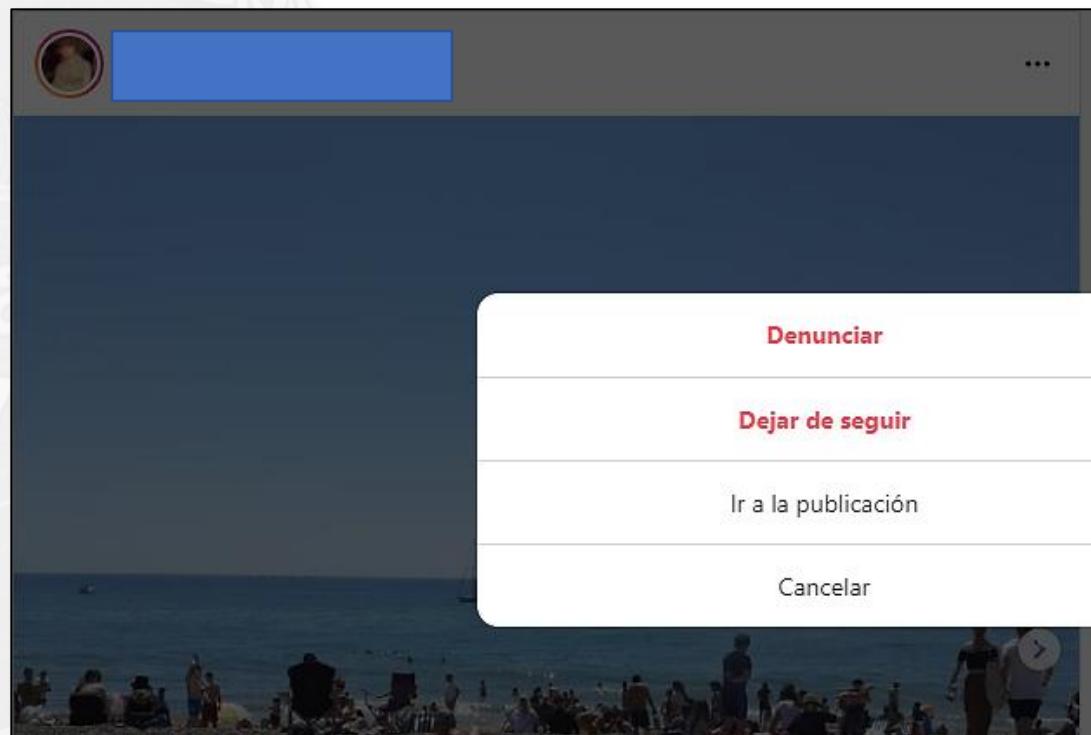
# ¿ESTO SE PUEDE HACER EN TODAS? ¡SÍ!

## ● Instagram u otras redes usan este sistema de auto-regulación

- Haciendo esto ayudas a “limpiar” la RRSS de trolls
- Tampoco desesperes si la RRSS no te hace caso
  - Les interesa tener usuarios porque da dinero
  - Algunas (Ej.: Twitter/X) tienen una moderación muy mejorable en la actualidad (2025)
- Pero a fuerza de denunciar burradas normalmente acaban cediendo

## ● Recuerda: Las denuncias son anónimas en la mayoría de las redes sociales

- ¡Pero no denuncies “por los loles” o puedes acabar tú eliminado!
  - Las denuncias masivas hacen que tu cuenta pierda visibilidad en muchas RRSS
- ¡Asegúrate de tener una razón!



- Dejar de seguir: Alguien que no quieres ver, pero no quieres que sepa que ya no le ves
- Bloquear: Alguien que no quieres ver, y quieres que sepa que te ha ofendido/hecho daño, etc.
- Denunciar: Alguien tan burro que no quieres que nadie más vea sus barbaridades (diciendo a la red cuáles son)



José Manuel  
Redondo López

# SI USAS UN PC COMPARTIDO...

- Si usas un PC de un colega / colegio, no dejes trazas en él de lo que navegas

- Tienes dos opciones

- Usa siempre **navegación privada**
- **Borra los datos almacenados**
  - El INCIBE te cuenta cómo:  
<https://www.incibe.es/ciudadania/temáticas/navegacion>



Lo último que quieras es dejar tu cuenta abierta en el navegador de un colega o en el del colegio. Puede pasar de todo...



José Manuel  
Redondo López

# MOVIDAS QUE ME PUEDEN PASAR

- Algunas cosas que te pueden pasar las cubre este curso
- Otras son muy delicadas y necesitan expandirse en cursos aparte

- Suplantación: “A-71 Juan Sebastián Elcano”
- Adicciones: “A-71 Juan Sebastián Elcano”
- Ciberbullying: P-74 “Atalaya”
- Desconocidos peligrosos: P-74 “Atalaya”
- Grooming, Sexting y Sextorsión: P-74 “Atalaya”
- Fake news y desinformación: “A-71 Juan Sebastián Elcano”
- Challenges: “A-71 Juan Sebastián Elcano”

- ¿No te gusta mi contenido? Ok 😞, pero no te enfrentes a esto solo/a, por favor

- Busca en Google lo que te pasa y añádele “INCIBE”
- Ellos tienen mucha información que te puede ayudar
- O llama al teléfono gratuito 017

## Top 10 de los principales peligros de las redes sociales para los jóvenes

	Problemas para la privacidad
	Suplantación de identidad
	Adicción a las RRSS
	Ciberbullying
	Contacto con desconocidos que pueden ser peligrosos
	Grooming
	Sexting
	Sextorsión
	Fake news y la distorsión de la realidad
	Challenge o retos muy peligrosos, en ocasiones delictivos



José Manuel  
Redondo López

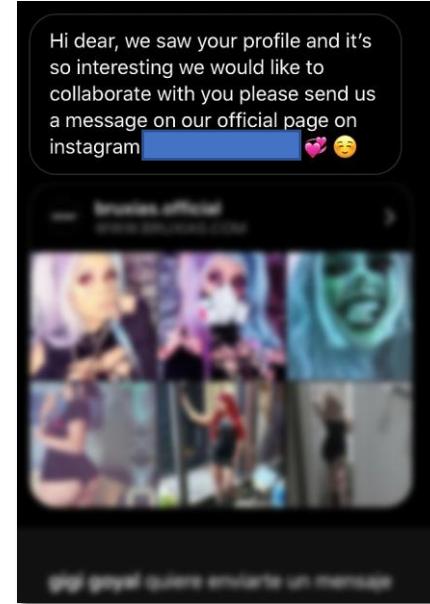
# MOVIDAS QUE ME PUEDEN PASAR: TIMOS Y ESTAFAS

## ● Desgraciadamente las redes sociales están llenas de intentos de timos y estafas...y debes tener cuidado

- Cuentas falsas, anuncios, mensajes privados... ¿qué persiguen?
  - **TU DINERO** (o el de tu familia)
    - Dar datos bancarios para que te hagan una transferencia por algún concepto
    - Comprar productos o servicios que sean timos, falsos o no hagan lo que prometen
    - Esquemas tipo piramidal y otras formas similares de estafa
  - **TUS DATOS PERSONALES**: Como parte de supuestas colaboraciones, pago por un producto o servicio...
  - **TUS LIKES / FOLLOWS**
  - **¡TU CUENTA DE USUARIO ENTERA!**: Para cometer más estafas ¡en tu nombre!
- *¿Quieres ver un testimonio de alguien que lo ha visto en Instagram/Bookstagram?*
  - <https://www.youtube.com/watch?v=0OAXfk1x5-s>

## ● Tengo un YouTube sobre estafas

- <https://www.youtube.com/@j.m.redondo8618/featured>
- Y los cursos **M-31 “Segura” y “Nautilus”**



**TENED CUIDADO CON LOS PERFILES FALSOS**

Han comenzado a aparecer numerosas cuentas falsas que solo buscan estafar al pedir datos bancarios con la excusa de que habéis ganado un sorteo.

Este perfil es el único oficial, y todos los sorteos se anuncian públicamente. NUNCA solicitaremos datos bancarios.

»» PUCK

# DENUNCIAR A LA POLICÍA / GUARDIA CIVIL



José Manuel  
Redondo López

- Y si ya tienes un problema...hablar con tu familia y **DENUNCIAR**
- Por ejemplo, en la página de la policía hay opciones para denunciar online
  - Y una batería de preguntas que te pueden guiar en casos comunes
- También puedes informar de muchas cosas que veas en RRSS o en Internet en general
  - [https://www.policia.es/\\_es/colabora\\_informar.php?strTipo=CGSCP#](https://www.policia.es/_es/colabora_informar.php?strTipo=CGSCP#)
- ¡Están para ayudarte!

Denuncias

## DENUNCIAR

Recuerde llevar a comisaría cualquier documentación de identificación personal, D.N.I., PASAPORTE, NIE, etc., listado de los objetos sustraídos, si es posible con el número de serie, modelo, marca, IMEI (en el caso de los teléfonos móviles), cualquier característica que pueda servir para identificarlo, así como vídeos grabados de las cámaras de seguridad, si dispone de ellos.

DÓNDE Y CÓMO DENUNCIAR

Siempre puedes acudir a cualquier comisaría, abiertas las 24 horas del día, los 7 días de la semana.

Ver dependencias policiales

Consejos de seguridad.

Programa Colectivos Ciudadanos

Comercio Seguro

Consejos en la vivienda

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



## ● Asegúrate de haber entendido lo siguiente

- Que *estar en redes sociales tiene en una serie de peligros, y que ciertas redes son más propensas que otras a ciertos tipos de ellos*
- Los *principales riesgos a los que te enfrentas en las redes sociales*
- Que *las aplicaciones que se pueden instalar asociadas a redes sociales pueden usarse para robarte tu cuenta, y que no debes instalar cualquier cosa, aunque te la recomiende un amigo*
- Que *el mecanismo de denuncia es tu principal defensa contra la aparición de contenidos o personas que sean ofensivos*
- Que *las redes sociales son uno de los principales canales de distribución de estafas*
- Dónde *debes denunciar todas las estafas o contenido dañino que te encuentres*



# ¿QUÉ PASA CON MI INFORMACIÓN EN UNA RRSS?

Lo que tienes que saber cuando subes cosas



# ¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

## ● En este bloque te voy a enseñar a responder a estas preguntas...

- *¿Alguna vez te has planteado qué pasa con todas las cosas que subes en una red social?*
  - Pues yo te lo voy a explicar en esta sección
  - Y con lo mismo que puedes aplicarlo a tu información, también puedes estudiar la que suben los demás...
- *¿Te has parado a pensar que una simple foto de un lugar puede usarse para mucho más?*
  - Pues hasta te voy a poner un ejemplo de eso
  - Y de qué cosas no deberías nunca subir para que las vea todo el mundo
  - Además de otra serie de trucos para que estés más seguro
  - *¿Te molan estos temas? Consulta el curso “**Santísima Trinidad**”*
- Finalizando con una serie de trucos para **identificar trolls, mentirosos** y otro tipo de gente no recomendable
  - Y así te puedas defender contra ellos



# “SI LO SUBES A UNA RED SOCIAL, DEJA DE SER TUYO”

## ● Eso que se dice de que cuando subes algo a una RRSS "deja de ser tuyo" es más complicado de lo que parece

- Es cierto que al subir contenido a redes sociales **cedes ciertos derechos** 🤝
- Pero **no** significa que pierdas la propiedad intelectual del mismo 🧠

## ● Hay que tener en cuenta

- **Los términos de servicio y condiciones de uso** 🤝 : Al crear una cuenta en una RRSS, los aceptas
  - Vimos antes cómo leerlos sin que te explote la cabeza, ¿recuerdas?
  - Suelen incluir una sección que da a la red social una licencia no exclusiva, mundial y gratuita
  - Para **usar, reproducir, modificar, distribuir y mostrar** el contenido que subes
- **El alcance de la licencia** 📄 : La licencia que concedes no es una “barra libre”
  - La RRSS **no puede usar tu contenido para lo que le de la gana**
  - Solo para lo que declare en sus términos de servicio
    - Ej.: Mostrarlo a otros usuarios, mejorar sus servicios, promocionar la plataforma...
- **Que sigues teniendo la propiedad intelectual**: Eres el dueño de los derechos de autor de tu contenido
  - Tienes el derecho exclusivo de **reproducir, distribuir, modificar y crear obras derivadas** de tu contenido

# “SI LO SUBES A UNA RED SOCIAL, DEJA DE SER TUYO”

- **Limitaciones a tus derechos:** Debes tener en cuenta que los hay y cuáles son
  - Por ejemplo, no puedes usar tu contenido para **infringir los derechos de autor de otros**
  - O, por ejemplo, podrías **no tener la opción de eliminarlo** de la red social una vez que lo has subido

## ● Recomendaciones si vas a subir obras originales tuyas o contenido muy personal

- **Lee los términos de servicio** y condiciones de uso antes de crear una cuenta
  - Ya sé que es un rollo, pero vimos antes páginas que te los resumen...
- **Comprueba la configuración de privacidad** de tu cuenta para controlar quién puede ver tu contenido
  - Lo vimos en una sección anterior
- Marca tu contenido como con **derechos de autor** si lo deseas (y la RRSS tiene esa opción)
  - O ponle una **marca de agua** tuya propia
- **Ten cuidado al compartir contenido de terceros**, y siempre cita la fuente
- **Guarda copias de tu contenido** en un lugar seguro
  - Te pueden cerrar la cuenta, y con ello perderías acceso a todo lo que has subido
- Y recuerda que **alguien podría usar tu propio contenido contra ti** si no cuidas lo que subes
  - Veamos este último aspecto a continuación

# ¿QUÉ PASA CON LAS FOTOS QUE SUBIMOS?

- Esto va más allá de lo que ya hablamos de la publicidad dirigida y marketing
  - Lo que subes puede dar información a otras personas que lo leen...**a veces demasiada** 😱
- Especialmente fotos o videos (se sacan fotogramas de ellos)...
  - Con ellos puedes hacer **búsqueda inversa** -> obtener el sitio **dónde se hizo** la foto
    - O **preguntarle a una IA** de dónde es la foto, últimamente es muy común
  - Si posteas muchas fotos, con eso pueden saber tus **rutas habituales** (dónde vives, colegio, gimnasio,...) -> **tus costumbres**
  - Si posteas con quien estás -> **amigos** -> **grupos** -> **tu clase**
- ¡Analiza lo que subes como el profesor Layton! 🕵
  - Mira todo con “ojos de hacker”
  - Esto es una rama de la ciberseguridad **muy potente**
    - El OSINT, del que te hablo en el “**Santísima Trinidad**”
  - ¿No me crees? Espera que te enseño unas muestras...





# BÚSQUEDA INVERSA EN GOOGLE

¡Esto vale para cualquier imagen sospechosa!: persona, producto, piso, calle, ...  
¡ASÍ PODEMOS DETECTAR PERFILES FALSOS! (Catfishing)

¡Puedes “Recortar” cualquier imagen de la pantalla con la herramienta “Recortes” de Windows!



Imagen de perfil recortada  
Y “sospechosa”

Aparece un artículo con esa imagen más completa escrita por Mike Pompeo (ex-Secretario de Estado de EEUU)

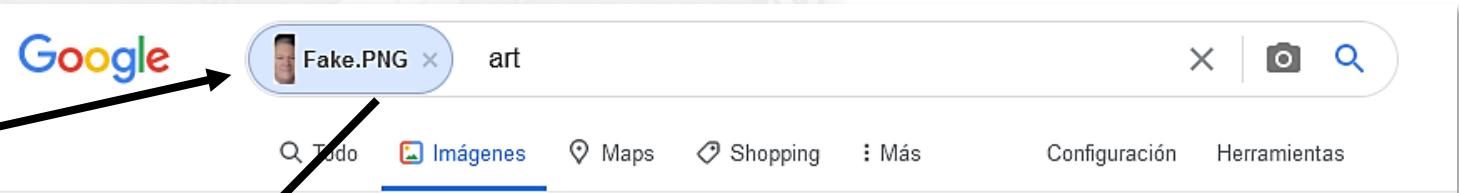
Sanciones en Siria - Prisionero en Argentina



150 × 150 - 30 jul. 2020 - Por Michael R. Pompeo, Secretario de Estado de Estados Unidos de América Hoy, el Departamento de Estado y el Departamento del Tesoro ...

<https://www.osi.es/es/actualidad/blog/2018/06/06/detectando-fraudes-me-suena-esta-foto>

La guardamos en un fichero, y arrastramos y soltamos el fichero en la búsqueda de Google



Efectivamente, es él y la imagen del perfil es **FALSA**



# IMÁGENES QUE DICEN SER DE ALGO... PERO ES MENTIRA



"Chilling with the bros in the mountain"

Tamaño de imagen:  
1116 × 513  
No se ha encontrado esta imagen en otros tamaños.

Posible búsqueda relacionada: [tree](#)

## Búsqueda en Google Images

[en.wikipedia.org › wiki › Tree](#) Traducir esta página  
[Tree - Wikipedia](#)  
In botany, a **tree** is a perennial plant with an elongated stem, or trunk, supporting branches and leaves in most species. In some usages, the definition of a **tree** ...

[en.wikipedia.org › wiki › Tree\\_\(da...\)](#) Traducir esta página  
[Tree \(data structure\) - Wikipedia](#)  
In computer science, a **tree** is a widely used abstract data type that simulates a hierarchical **tree** structure, with a root value and subtrees of children with a parent ...

Imágenes visualmente similares

¡La foto!



**Todo es mentira, es una casa de un estudio de arquitectura. Esto es más frecuente de lo que te crees en páginas de alquileres de pisos. ¡Díselo a tus padres!**

- Cualquier imagen de una web que te resulte sospechosa admite este tratamiento
- ¿Encuentras imágenes falsas? No te fíes de esa web



José Manuel  
Redondo López

# ¡MIRA COMO DISFRUTO EN ESTE SITIO!...MMM ¿SEGURO?



**"De vacaciones por la sierra de Andalucía"**

https://www.turismoasturias.es › rutas › senderismo › ru... ▾

## Ruta del Cares. Rutas en Asturias - Turismo Asturias

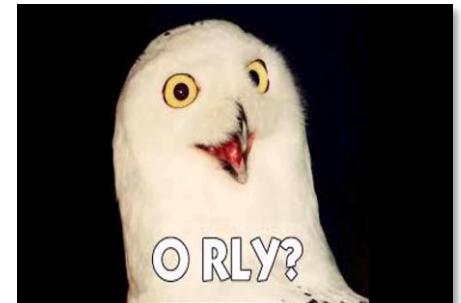
Ruta del Cares. Rutas en Asturias ... A pie 6 h. 15 min. ... Hacer la ruta, Poncebos-Caín ida y vuelta, supone caminar unos 22 km, distancia que no es apta para ...

https://www.escapadarural.com › ... › Planes › Rutas ▾

## Todo lo que necesitas saber para hacer la Ruta del Cares

12 jul 2016 — Longitud: 12 km (24 km ida y vuelta). · Duración: 6 horas aproximadamente. · Dificultad: medi.a · Desnivel: Prácticamente llano todo el recorrido, ...

🕒 Imágenes visualmente similares





José Manuel  
Redondo López

# ¡MIRA COMO DISFRUTO EN ESTE SITIO!...MMM ¿SEGURO?



**“¡De vacaciones por Toledo!”**

[https://buendiatours.com › guías › casco-antiguo](https://buendiatours.com/guías/casco-antiguo) ▾  
**Casco antiguo de Oviedo | Buendía Tours**  
Casco antiguo de Oviedo. El casco antiguo, o el "Oviedo antiguo" como se le llama en la ciudad, es la ciudad medieval que estaba dentro de la ...

[https://asturias.com › el-casco-histórico-de-oviedo](https://asturias.com/el-casco-histórico-de-oviedo) ▾  
**El casco histórico de Oviedo. Qué ver en Oviedo Asturias ...**  
4 feb 2021 — La vamos dejando a nuestra derecha y tomamos la calle Magdalena camino ya de El Fontán, plaza emblemática del Oviedo Antiguo que se ha ...

Imágenes visualmente similares



**¡Te saca hasta las imágenes similares del sitio! (lo cual te da aún más contexto para “investigar”)**

# IMÁGENES QUE DICEN MÁS DE LO QUE PARECE...

## • Este método no es infalible

- Pero probar a ver qué pasa no está mal... ☺

## • Como os decía, si se publican varias imágenes, se puede llegar a “triangular” a la persona

- Averiguar su rutina, gustos, aficiones, rutas... (hay gente que postea su vida)
- Incluso muchas veces la propia persona geolocaliza la imagen, así que no hace falta investigar nada
- Por eso todo este tema de “**cuidado con lo que se publica**” ☺



“Vistas desde mi casa”

Aproximadamente 299 resultados (1,08 segundos)



Tamaño de imagen:  
1200 × 900

Buscar esta imagen en otros tamaños:  
[Todos los tamaños](#) - [Pequeño](#) - [Mediano](#) - [Grande](#)

Possible búsqueda relacionada: [puertollano españa](#)

Ups...ahora ya  
saben dónde  
vives...



# IMÁGENES QUE DICEN MÁS DE LO QUE PARECE...

- Google Earth puede hacer magia...



La foto anterior se ha hecho por esta zona

# ¿QUÉ ES LO QUE NUNCA DEBEMOS SUBIR?

## ● Nunca subas

- **Billetes de tren, avión:** con la numeración pueden saber demasiado
- **Tarjetas de crédito o nºs de cuenta** (compras fraudulentas)
- **El ID de una avión o medio de transporte grande** (¡pueden saber tu ruta exacta!)
- **Cosas demasiado personales /** que alguien pueda usar en tu contra
- **Si te vas de casa / vacaciones**, etc... (casas deshabitadas)
  - A posteriori lo que quieras. ¿Mientras estás? ¡NO!
- ...

Piensa “**como un malo**” y responde la siguiente pregunta  
¿**Cómo podría usar yo esto que voy a subir para el mal?**

**Si tienes una respuesta, NO lo hagas (y, sino sabes, pregunta a tu familia / profesores)**

Fuente: <https://www.incibe.es/ciudadania/formacion/infografias/7-datos-que-nunca-debes-compartir-en-internet>



# ¿QUÉ ES LO QUE NUNCA DEBEMOS SUBIR?

## ● ¿Crees que esto solo aplica a menores?

- ¡No! También a cualquier mayor de edad
- Por temas personales, laborales, etc.

## ● Los de “cierta generación” son quizá los que más problemas dan en ese sentido

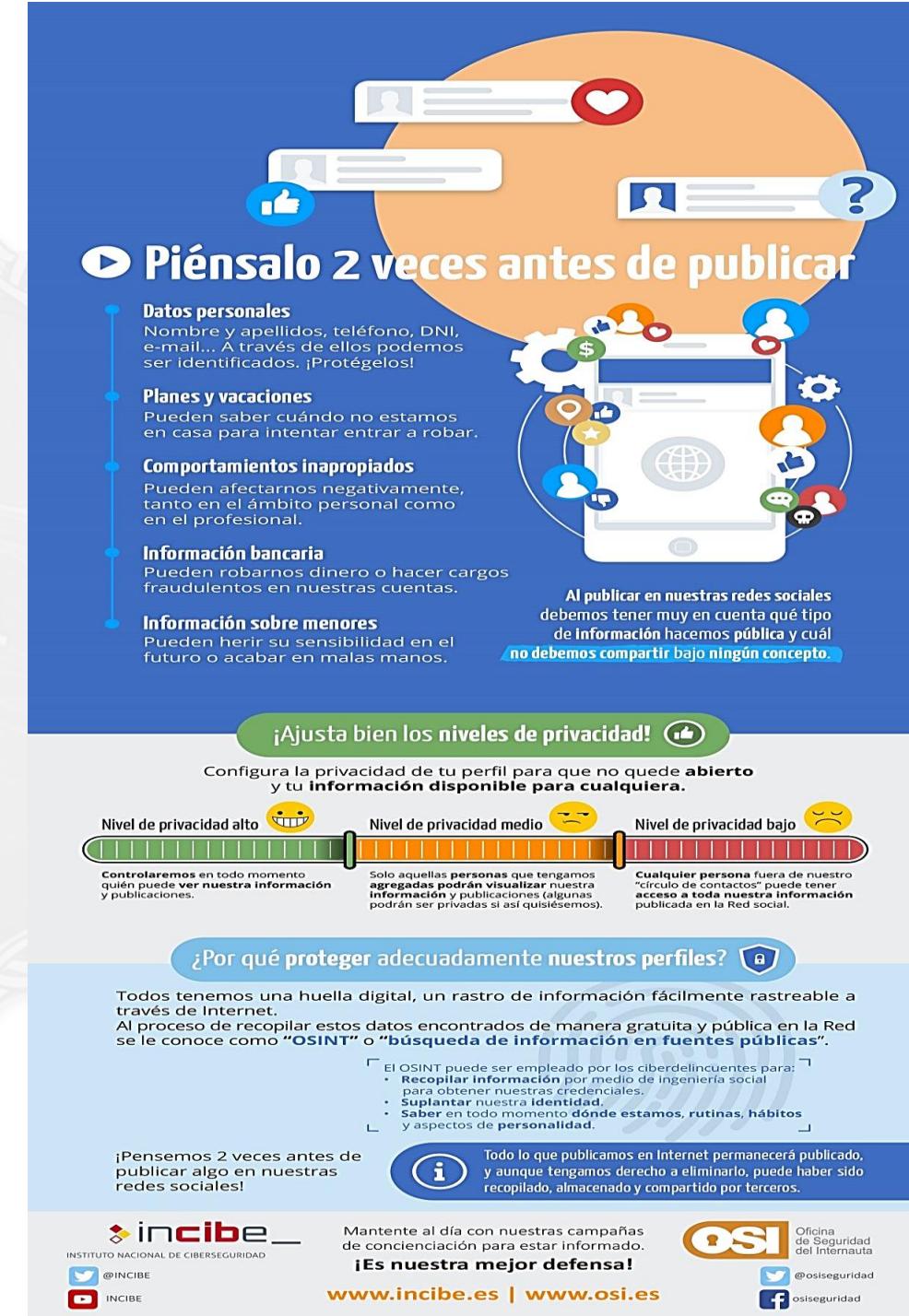
- ¡Les encanta postear de todo, sin entender las consecuencias!
- Y es una generación poco sospechosa de ser menor 🙄 🙄

## ● ¡Pon sentido común en tu casa y edúcales!

## ● Este video de Sarina Abdullah sobre el tema es muy revelador

- <https://www.youtube.com/watch?v=35caskf6YJg>

Fuente: <https://www.incibe.es/ciudadania/formacion/infografias/piensalo-2-veces>





José Manuel  
Redondo López

# EJEMPLO: BILLETE DE AVIÓN



Cuándo te vas, dónde te vas, cómo te vas...



# NºS DE VEHÍCULOS DE TRANSPORTE

- Saber el identificador de un avión y el día aproximado de un viaje da mucha información a quien quiera saberla 

- Hay páginas que la muestran toda ...¡gratis!
- ¡Sabrán todo de tu viaje! ¡Hasta si llegaste tarde!

- Otros medios de transporte pueden tener el mismo problema

- Así que **¡no lo hagas!**

- Otras cosas que **nunca debes postear**

- Fotos de tu DNI (suplantación)
- Tus tarjetas (compras ilegales)
- Entradas de conciertos (geolocalización, falsificación)
- ...



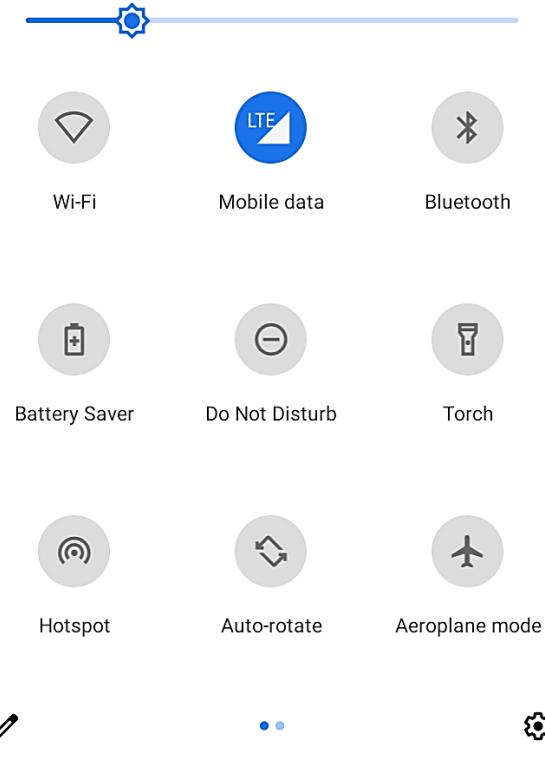


José Manuel  
Redondo López

# ¿Y QUÉ MÁS PUEDO HACER?

## ● Se un usuario **ACTIVO** de tu teléfono

- **Desactiva lo que no uses** (datos cuando uses Wifi, Bluetooth si no lo usas, tu posición si estás en casa, etc.)
  - Es ecológico 😊 (ahorras batería)
- Evita problemas que pueden llevar a que “se filtren” cosas



## ● Dile a tu familia donde vas a estar, por si acaso

- Lo que vas a hacer, depende ya de ti 😊
- Mejor que sepan donde buscarte, ¿no?
- ¡Confiar en alguien estas cosas es una buena forma de evitar problemas!

## ● Usa las redes sociales vía navegador web mejor que usando su app (si te dejan)

- **Recuerda:** Se filtran menos datos tuyos de esta forma, ¡créeme!
- *¿Por qué crees que te insisten tanto en que te la instales?* 😠



José Manuel  
Redondo López

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



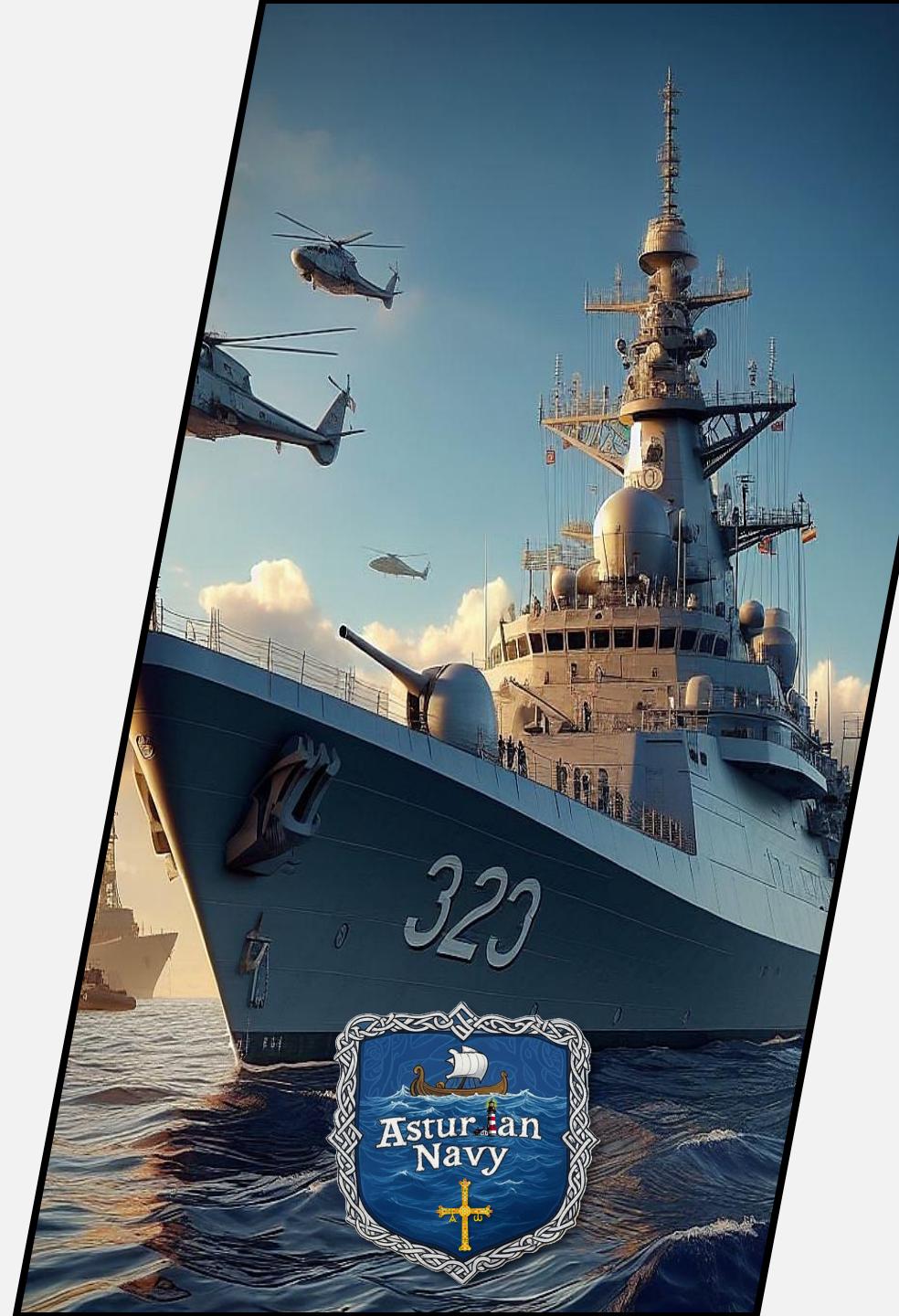
## ● Asegúrate de haber entendido lo siguiente

- Que una vez que subes algo a una red social deja de ser 100% tuyo
- El peligro que tiene subir ciertas cosas a las redes sociales, por la información que pueden sacar de ellas
- Y que hay toda una rama de la ciberseguridad que se usa para sacar información de las cosas que otras personas suben en Internet, el OSINT
- Que hay que mantener una serie de medidas de “higiene” a la hora de manejar tanto las redes sociales como tus teléfonos móviles



## 😢 La persona detrás de una cuenta de una red social

¿Se pueden averiguar cosas, aunque la cuenta no refleje una identidad real?



# ¿Y QUÉ HAGO CON LOS TROLLS?

## ● En las redes sociales hay bots o trolls

- **Es un hecho**, no algo cuestionable
- La forma más rápida de intentar averiguar si una cuenta es falsa es la búsqueda en Google Images de la foto de perfil que vimos en la presentación anterior
  - *¿Es la imagen de otra persona? ¿de un catálogo?* **CUENTA FALSA**
- El problema es que ahora **muchas son generadas por IA**, y no se pueden distinguir de esta forma

## ● Por otro lado, si alguien así te está acosando, lo mejor es **denunciarlo a la policía** en caso de que cometa un delito

- **Si publica fotos de sitios y lugares** (o fotogramas de un video), una búsqueda de imágenes saca fotos visualmente similares...que podrían ser del mismo sitio y estar geolocalizadas
  - Lo vimos antes
- Con ello, averiguarás más o menos por dónde vive o por dónde pasa
- Y probablemente así sepas más fácilmente quién puede ser (**datos para la denuncia**)
- No obstante, esto es más frecuente usarlo **para detectar fraudes**

# TÉCNICAS BÁSICAS PARA IDENTIFICAR “TROLLS”

## ● ¿Y si esto no funciona?

- A veces en la **información extendida pública** de la cuenta aparece el identificador original que se usó para crearla
  - Que puede ser el nombre real de la persona (que luego cambió por otro anónimo)
- **El mismo id de usuario**  se puede usar en distintas redes sociales / foros / perfiles de juegos
  - Y en algún sitio de ellos puede aparecer su nombre real (mención de un amigo, foto...)
  - Lo veremos en la siguiente hoja
- **El nombre de su web personal** (si tiene) puede delatarlo
- **Averiguarlo por lo que escribe:** Provocar que diga un dato que poca gente sepa
  - Deducción detectivesca over 9000 😊
- **Con quién se relaciona:** ¿hay confianza con alguno de sus allegados? Pregunta
- **A quien le da/no le da like:** Muchos se dan like a si mismo cuando postean con otra cuenta “pública”
  - Si critica a una persona mucho, no descartes que sea él mismo (para desviar la atención)
  - Si defiende a ultranza a otra persona aparentemente sin relación, es probable que estés a ante una “cuenta B” de esa persona (muchos streamers famosos lo hacen 😊)
- O también puedes identificarlo por **cómo se comporta...**



José Manuel  
Redondo López

# EL IDENTIFICADOR DE UNA RED SOCIAL PUEDE DECIR MUCHO

## ● El identificador que alguien usa en las redes sociales puede ser delator

- Puede usar el mismo en muchas redes distintas, unas protegidas y otras no
- Puede tener alguna página registrada con ese pseudónimo

## ● Hay webs que averiguan esta información por ti

- <https://namechk.com/>
- <https://www.namecheckr.com/>

En rojo tienes las redes sociales donde hay registrado alguien con el pseudónimo que he puesto. ¿Será la misma persona en todas? 😱

### Usernames

Facebook	YouTube	Twitter	Blogger	Twitch	TikTok
Shopify	Reddit	Ebay	Wordpress	Pinterest	Yelp
Slack	Github	Basecamp	Tumblr	Flickr	Pandora

Show more



De verdad que parece una tontería, pero pasa más a menudo de lo que crees. La gente tiende a usar el mismo pseudónimo en distintos sitios, y lo hace con él en algunos...

# IDENTIFICANDO CUENTAS FALSAS / BOTS POR COMPORTAMIENTO

- Es cierto que hoy en día en las redes sociales hay muchas fake news y muchas cuentas encargadas de propagarlas
- ¿Cómo las identifico?
  - **SENTIDO COMÚN**: Si dice cosas que parecen inverosímiles, es son mentira 😊
  - **Múltiples mentiras 🍞** : Si a la cuenta le han “pillado” en varias mentiras, raro será que mentir / manipular constantemente no sea uno de sus objetivos
    - Aparte de hacerles “fact check”, también pueden quedar “retratados” en los comentarios
  - **Es una cuenta con “comportamientos extraños” 🕵️** : Solo son indicios de sospecha, no quiere decir que todas las cuentas que hagan algo así lo sean (puede haber una razón legítima para hacerlo)
    - Ha **cambiado frecuentemente de nombre** (*¿por qué? ¿hizo algo grave con su antiguo nombre?*)
    - **Borra muchos mensajes** (*¿tiene frecuentes “pilladas”?*)
    - Hace “limpias” de seguidores arbitrarias, dirigidas a un tipo de seguidor, o contrarios a su opinión (*¿es que elimina las críticas/“pilladas” que le hacen?*)
- Veamos ejemplos de ello en Twitter (nadie la llama X 😊)

# CAMBIOS DE NOMBRE

- Se pueden descubrir con una búsqueda en Twitter/X sencilla
- El procedimiento de búsqueda es
  - **to:<nombre de cuenta> until:<año>-12-31**
    - <año> es el año de creación de la cuenta
  - Ejemplo, dado que el presidente de España en 2024 creó su cuenta en 2009, se haría:
    - **to:sanchezcastejon until:2009-12-31**
  - Pulsamos en “Más Reciente”
  - Si no sale ningún resultado, cambiamos al año siguiente y repetimos el proceso
- En los resultados vemos que las respuestas están dirigidas al mismo id. de usuario
  - El presidente no ha cambiado de nombre



A screenshot of a Twitter search results page. The search bar at the top contains the query `to:sanchezcastejon until:2009-12-31`. Below the search bar, there are tabs for **Destacado**, **Más reciente** (which is selected), **Personas**, **Fotos**, and **Videos**. The results show four tweets from different users:

- Ramón Ramón** (@ramonramon) - 29 sept. 2009: En respuesta a @sanchezcastejon @sanchezcastejon felicidades por esa nueva responsabilidad, te deseo muchos éxitos y progresos.
- Jorge Martínez** (@jorgermp) - 18 sept. 2009: En respuesta a @sanchezcastejon @sanchezcastejon en un zip?
- Jose Vicente Espino** (@JoseviEspino) - 18 sept. 2009: En respuesta a @sanchezcastejon @sanchezcastejon Ánimo amigo!!!
- Jose Vicente Espino** (@JoseviEspino) - 15 sept. 2009: En respuesta a @sanchezcastejon @sanchezcastejon Espero que tengas mucha suerte y éxito en tu nueva etapa. Estoy seguro que darás todo por nuestros valores. Un abrazo



José Manuel  
Redondo López

# CAMBIOS DE NOMBRE

- En cambio, este usuario sí que ha cambiado de identificador
  - Aunque esto por sí solo no quiere decir nada
  - ¡Mucha gente lo hace!
- Es un dato a tener en cuenta nada más...
  - Pero ahora sabes cómo averiguarlo con una búsqueda
- Es más sospechoso si los cambios son frecuentes cuando se va recorriendo el “historial” de la cuenta

**Roberto Benito** @robertobenito · 21 dic. 2011  
En respuesta a @javiernegre10  
@javiernegre No sé yo si Rajoy va a confiar a Gallardón la gestión del alto el fuego de ETA.

**Roberto Benito** @robertobenito · 21 dic. 2011  
En respuesta a @javiernegre10  
@javiernegre No se me ocurre un nombre en el PP con un perfil más parecido al de Chacón.

**Marcos Iriarte** @MarcosIriarte · 21 dic. 2011  
En respuesta a @javiernegre10  
@javiernegre Le tiene cariño porque le vio crecer...

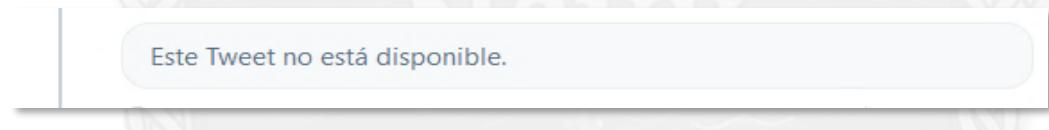
**Manuel Regalado** @titoregalado7 · 20 dic. 2011  
En respuesta a @javiernegre10  
@javiernegre Hombre, el inefable Javi Negre! Muy bien, tío. Currando un poquillo. Mán arriba a las seis. Abrazo. Q tal tú x el norte?

**@javiernegre10 antes era @javiernegre. Se ha cambiado de nombre por algún motivo, al menos 1 vez**

# BORRADO DE TWEETS

- Si un usuario ha borrado tweets o no se puede comprobar fácilmente haciendo clic en sus respuestas para verlas en detalle

- Como, por ejemplo, las obtenidas en el proceso anterior
- Si existe una respuesta a un tweet, pero al entrar a ella vemos esto:



Este Tweet no está disponible.

- Implica que **el usuario ha borrado ese tweet**
- *¿Tiene muchos tweets borrados? Sospecha*
  - Implicaría que puede haber dicho cosas falsas / por las que le han denunciado / desmentidas y ha tenido que borrarlas
  - Si son muchos casos, es un potencial mentiroso habitual...

# TEMÁTICAS

- Si en lugar de to: usamos from: (from:<nombre de cuenta> until:<año>-12-31 veremos los tweets hechos por la cuenta, no las respuestas que tuvieron

- Si hacemos un recorrido histórico por ellos, podemos ver si la temática de estos ha cambiado, o la forma de expresarse
- @norcoreano por ejemplo ha pasado de ser una cuenta de humor a una cuenta con fuerte contenido de crítica política
- ¡Ojo! Eso no es malo, es un hecho a considerar por si es útil para alguna investigación nada más



from:norcoreano until:2011-12-31

	Destacado	Más reciente	Personas	Fotos	Videos
1	 Kim Jong-un @norcoreano · 30 dic. 2011	A ver si nos enteramos, aquí no prohibimos internet, lo que prohibimos es acercarse a la frontera y para pillar Wifi hay que acercarse.	6	2	
2	 Kim Jong-un @norcoreano · 30 dic. 2011	La libertad es el opio del pueblo.	22	4	
3	 Kim Jong-un @norcoreano · 30 dic. 2011	He convocado las primeras oposiciones de 2012, 10 plazas de funcionario para rascarme la espalda.	7	0	
4	 Kim Jong-un @norcoreano · 30 dic. 2011	Si el pueblo no come es culpa mía, si se muere gente también, a ver si va a ser culpa mía que tengan cara de chinorris...	1	5	

from:norcoreano until:2019-12-31

	Destacado	Más reciente	Personas	Fotos	Videos
1	 Kim Jong-un @norcoreano · 30 dic. 2019	Si Cristina Pedroche quiere vestirse de otro año de mamarracha para llamar la atención, está en su derecho y nosotros no somos nadie para criticarla.	38	246	1 mil
2	 Kim Jong-un @norcoreano · 28 dic. 2019	Hoy es el Día de los Inocentes, felicidades a todos los que casi en 2020 siguen creyendo en Dios, en el horóscopo y en el marxismo-leninismo.	73	811	2,7 mil
3	 Kim Jong-un @norcoreano · 27 dic. 2019	Si León se independiza, espero que su himno nacional sea Hakuna Matata.	31	423	1,6 mil
4	 Kim Jong-un @norcoreano · 27 dic. 2019	Tomándome una caña en una terraza al sol en plena Navidad. Esto es lo que quiere quitarnos Greta Thunberg.	27	753	2,7 mil



José Manuel  
Redondo López

# ¿ES UNA CUENTA SOSPECHOSA ENTONCES?

## ● Por tanto

- Si nos encontramos con una cuenta de usuario que ha tenido **varios cambios de nombre**
- Cada vez que cambia de nombre “**muta**”
  - Habla de noticias de distintas ideologías, apoya posturas contrapuestas, se le descubren diferentes bulos...
  - Hay personas que son una especie de “**ciber-mercenarios**” de opiniones: ¡a cambio de dinero hablan bien de lo que les digan!
- Y además **borra muchos tweets** (probablemente por cada cambio de nombre borre un buen puñado de ellos)
- Entonces...



# Y AHORA DAROS CUENTA DE UN DETALLE...

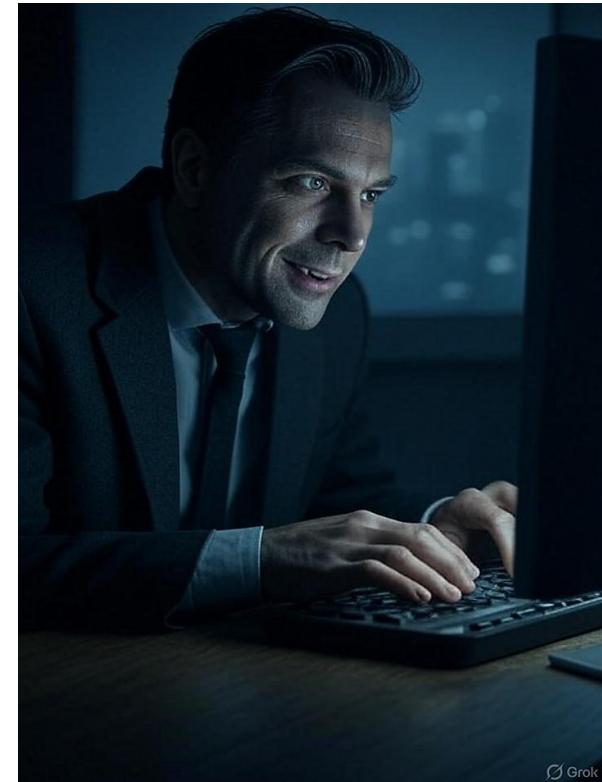
## ● **CUIDADO con las redes sociales**

- **Se clonian perfiles** con fotos con fines ilegales / destrucción de reputación
- **Recuerda:** Si publicas tu foto en sitios, **se podrían identificar esos sitios**
  - Dónde vives, por dónde paras, con quién andas...
  - Aunque no estén geolocalizadas
  - Facilitas la vida a posibles ciber-acosadores... ☹

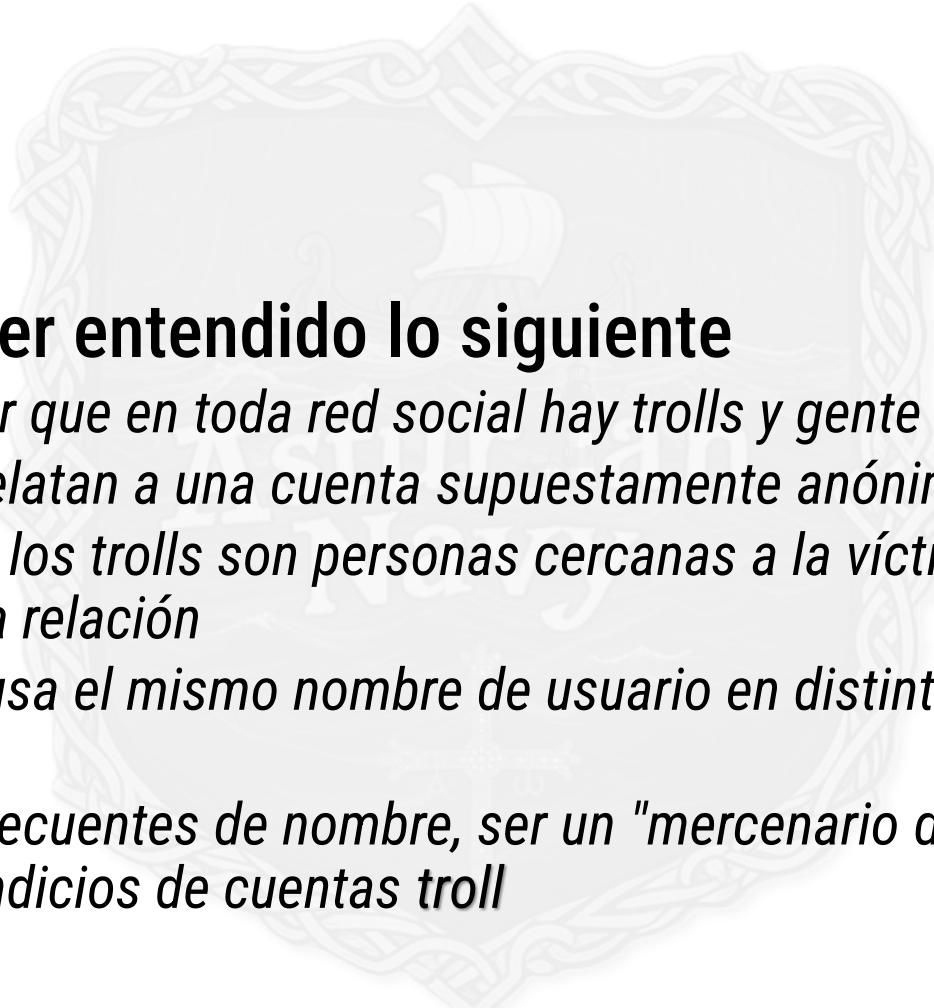
## ● **Si mientes, también pueden pillarte (¡acabamos de verlo!)**

## ● **Y, si cometes un delito, VAN A PILLARTE**

- La policía puede, tras una denuncia, acceder a muchos más datos que tú
- Pidiéndolos a redes sociales / proveedores de Internet:
  - Tu IP (**F-83 “Numancia”**), horas de conexión...
- **Solución: ¡NO COMETAS DELITOS!**



# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



## ● Asegúrate de haber entendido lo siguiente

- Que *hay que asumir que en toda red social hay trolls y gente aburrida que solo va a hacer daño*
- Los *indicios que delatan a una cuenta supuestamente anónima*
- Que *muchas veces los trolls son personas cercanas a la víctima, y es fácil que digan algo que les delate dada esa relación*
- Que *muchá gente usa el mismo nombre de usuario en distintas redes, y no en todas es igual de anónimo*
- Que *los cambios frecuentes de nombre, ser un "mercenario de temáticas" y el borrado frecuente de mensajes son indicios de cuentas troll*



# PRECIOS EN LA DARK WEB DE LOS DATOS QUE NOS ROBAN

¿A cuánto el kilo de dato privado?





José Manuel  
Redondo López

# ¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

## ● En este bloque te voy a enseñar...

- *¿Nunca te has planteado por qué hay tanto robo de datos privados y de cuentas en internet?*
- Pues en esta sección vas a ver que **hay un mercado para ello** y que hay gente que compra, aunque sea ilegal
- Así que, como fin de esta presentación, te voy a enseñar un estudio
  - Dónde vas a ver **los precios que tiene determinada información robada**
  - En la web oscura (**dark net o dark web**)
  - Que es donde se venden estas cosas...
- Así que, de nuevo, ten cuidado con tu actividad y lo que compartes en redes sociales...
  - Tu información y otros datos es una mercancía que alguien puede estar interesado en comprar para hacer diferentes delitos



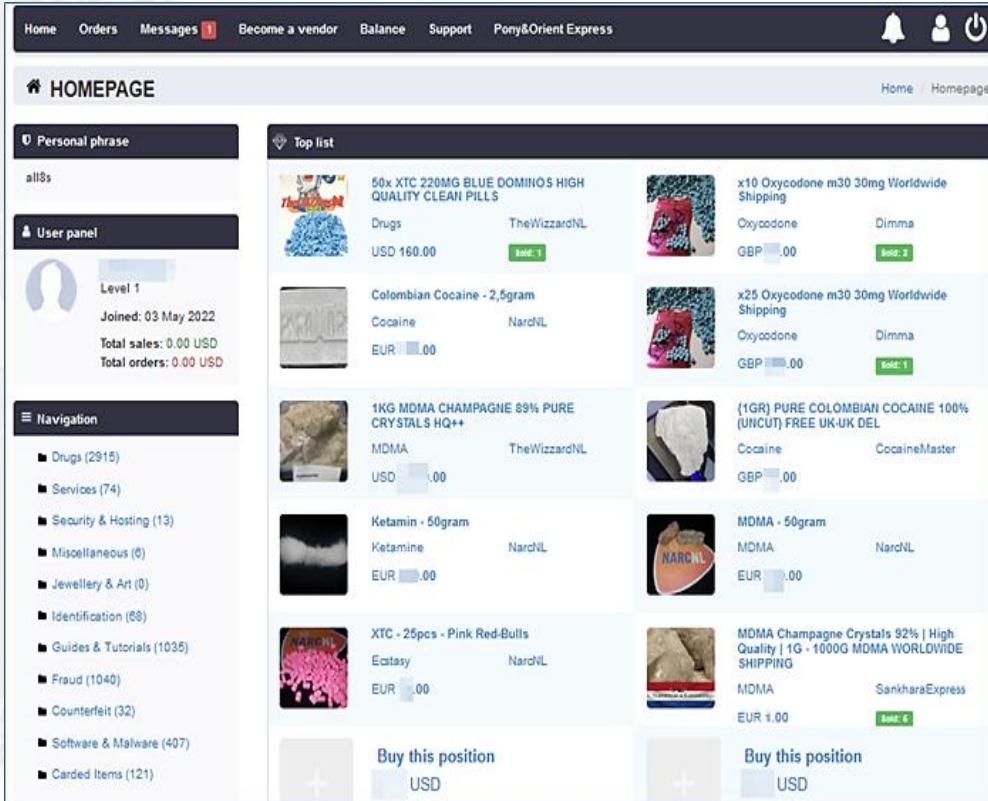
# PRECIOS EN LA DARK WEB DE LO QUE NOS ROBAN

- La dark web 🌐 es una parte de Internet donde uno puede ser más anónimo y solo puedes acceder con un navegador especial
  - Te cuento más en la F-83 “Numancia”
- Debido al anonimato, hay tiendas de cosas / servicios ilegales 😱
  - Aunque se cierran muchas, en general hay cada vez más
  - ¿Qué venden? Drogas, medicinas ilegales, sicarios, material robado y... ¡tus datos! 💀 ❤️ 🧛‍♂️ 🦉 🐣 🕊
  - En esos mercados valen dinero y por eso se roban
- Es una realidad y que no algo que vaya a desaparecer
  - Los delincuentes roban datos porque su venta les es rentable
    - El comercio ilegal de datos es un negocio floreciente y que pone en peligro a cualquiera
  - Existen investigaciones recientes acerca del tipo de cosas que se venden en él y sus precios
  - Vamos a usar como base: <https://www.privacyaffairs.com/dark-web-price-index-2023/>

# PRECIOS EN LA DARK WEB DE LO QUE NOS ROBAN

- Este informe reveló que en la dark web...

- No hay un líder claro del mercado: El cierre de muchos sitios “grandes” dio lugar a muchos más “pequeños”, pero que duran poco tiempo
  - La oferta no ha disminuido, se reparte más
  - El objetivo es ser más difíciles de “pillar”
    - Desaparecen en unos pocos meses
    - Ser pequeño llama menos la atención
    - Es una especie de “guerra de guerrillas”
- Telegram en lugar de sitios web:** Telegram se ha convertido en un canal importante para facilitar la venta de datos personales robados
  - Existen muchos canales para eso...con MUCHOS usuarios
  - También se usa para anunciar la creación de nuevos sitios de venta de servicios y cosas robadas



Item	Category	Seller	Price
50x XTC 220MG BLUE DOMINOS HIGH QUALITY CLEAN PILLS	Drugs	TheWizzardNL	USD 160.00
Colombian Cocaine - 2,5gram	Cocaine	NarcNL	EUR 100.00
1KG MDMA CHAMPAGNE 89% PURE CRYSTALS HQ++	MDMA	TheWizzardNL	USD 100.00
Ketamin - 50gram	Ketamine	NarcNL	EUR 100.00
XTC - 25pcs - Pink Red-Bulls	Ectasy	NarcNL	EUR 100.00
x10 Oxycodone m30 30mg Worldwide Shipping	Oxycodone	Dimma	GBP 100.00
x25 Oxycodone m30 30mg Worldwide Shipping	Oxycodone	Dimma	GBP 100.00
(1GR) PURE COLOMBIAN COCAINE 100% (UNCUT) FREE UK-UK DEL	Cocaine	CocaineMaster	GBP 100.00
MDMA - 50gram	MDMA	NarcNL	EUR 100.00
MDMA Champagne Crystals 92%   High Quality   1G - 1000G MDMA WORLDWIDE SHIPPING	MDMA	SankharaExpress	EUR 1.00

Son páginas web “típicas” (aparentemente), solo que venden de todo. Insisto: DE TODO: Fuente: <https://telefonicatech.com/blog/dark-markets-mercado-negro-en-internet>

# TARJETAS DE CRÉDITO

- Tarjetas de crédito  clonadas o robadas, con los datos del titular de la tarjeta

## ● Consejos

- Nunca dejes tu tarjeta en manos de nadie, ni siquiera temporalmente
  - *¿Vas a pagar algo?* El **terminal siempre a la vista** (díselo a tus padres)
- No metas la tarjeta en sitios/webs “raras”, **hay mejores alternativas**
  - *¿Tienda no conocida?* No metas tu tarjeta de crédito “normal”
  - Más en “**A-71 Juan Sebastián Elcano**”
- En diciembre de 2022, había unos **7,5 millones de tarjetas de crédito en la dark web**

Credit Card CVV BALANCED \$9500-\$29000 FOR WORLDWIDE USE



Sold by: ROCKO  
Product Type: Digital  
Payment: Escrow  
Coins: BTC XMR

Quantity: 1

Add to Cart

1 sold, ∞ in stock

\$14.99

0.00066735 BTC  
0.1005173 XMR

Pagar con criptomonedas facilita hacer pagos anónimos. Ten en cuenta que se trata de un mercado del crimen...

# TARJETAS DE CRÉDITO: PRECIOS

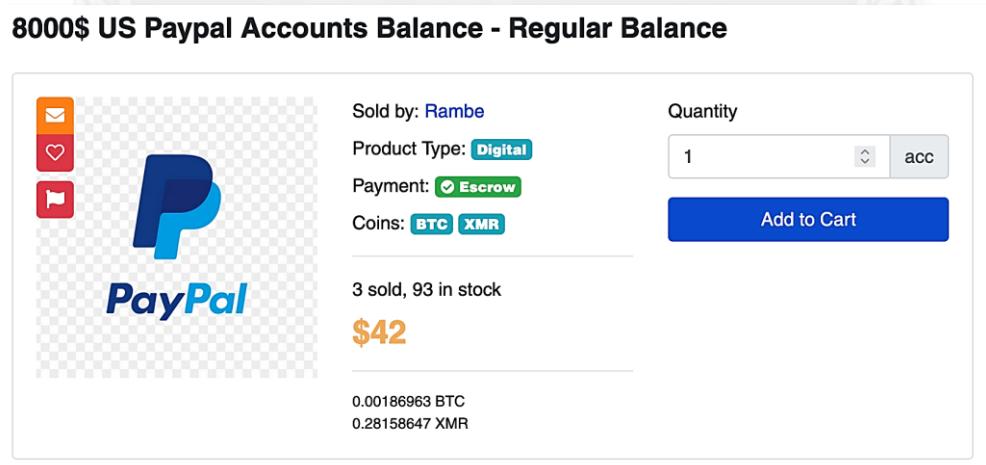
- Estos son ejemplos de precios de tarjetas de crédito
  - Incluso con cierto saldo en la cuenta asociada
- Todas con el código CVV para poder usarlas en compras online
- Como puedes ver, el precio permite hacer una compra grande
  - Por mucho menos de lo que vale la tarjeta
- Hay tarjetas robadas de todos los países

<i>Credit card details, account balance up to 5,000</i>	\$110
<i>Card.com hacked account</i>	\$75
<i>Credit card details, account balance up to 1,000</i>	\$70
<i>Stolen online banking logins, minimum 2,000 on account</i>	\$60
<i>United Arab Emirates credit card with CVV</i>	\$35
<i>Stolen online banking logins, minimum 100 on account</i>	\$40
<i>TDBank hacked account</i>	\$30
<i>Canada hacked credit card details with CVV</i>	\$30
<i>Australia hacked credit card details w/ CVV</i>	\$23
<i>Israel hacked credit card details with CVV</i>	\$20
<i>Spain hacked credit card details with CVV</i>	\$20
<i>UK hacked credit card details with CVV</i>	\$20
<i>Cloned American Express with PIN</i>	\$20
<i>Cloned Mastercard with PIN</i>	\$20
<i>Cloned VISA with PIN</i>	\$20
<i>USA hacked credit card details with CVV</i>	\$15
<i>Hacked (Global) credit card details with CVV</i>	\$10
<i>Walmart account with credit card attached</i>	\$5

Fuente: Investigación de precios en la dark web de Privacy Affairs  
[\(https://www.privacyaffairs.com/dark-web-price-index-2023/\)](https://www.privacyaffairs.com/dark-web-price-index-2023/)

# CUENTAS EN SERVICIOS DE PROCESAMIENTO DE PAGOS ONLINE

- Cuentas en servicios de pagos desde móvil, procesadores de pago, etc.
- Son cada vez más populares en estos mercados
  - Al dar más oportunidades de robar datos personales e información financiera de las personas
  - El tipo de cuenta más común **es la de PayPal**
- Debido a que hay tantos servicios de este tipo disponibles, su precio es bajo
  - Es más caro y complejo transferir dinero desde una cuenta pirateada
- Consejos
  - **Protege MUY bien tu cuenta** de PayPal o similar (como lo visto aquí, buena password, 2FA...)



Prácticamente hacemos casi todas las compras online, por lo que como mínimo deberíamos tener un 2FA activo en cada cuenta que tengamos en este tipo de servicios. Ya vemos que es una mercancía a la venta muy común...

# CUENTAS EN SERVICIOS DE PAGO: PRECIOS



## ● Este tipo de cuentas tienen mucha variedad de precios

- En bancos suelen ser más caras, en función del tamaño del banco
- Los servicios de pago suelen ser más baratos
  - Probablemente al ser cuentas que duran bastante menos tiempo

## ● Llama la atención la compra de transferencias desde cuentas de PayPal robadas

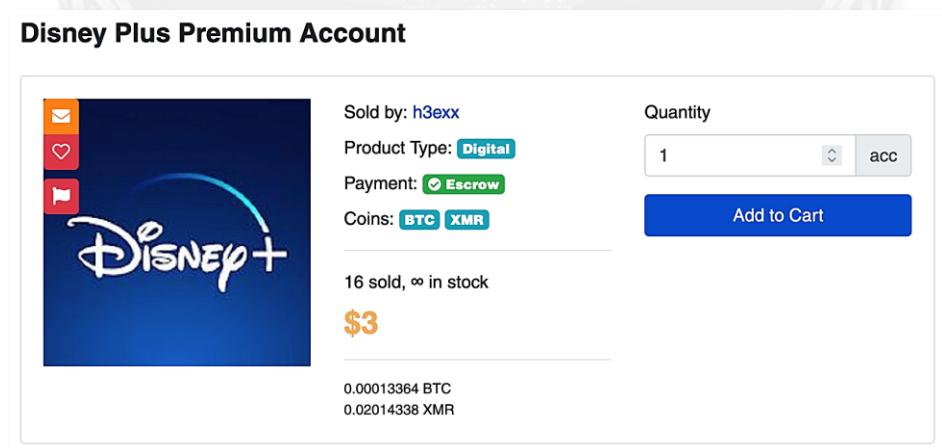
- Se usan para timos en ventas

Fuente: Investigación de precios en la dark web de Privacy Affairs (<https://www.privacyaffairs.com/dark-web-price-index-2023/>)

ING bank account logins (verified account)	\$4,255
HSBC UK Business account	\$4,200
Switzerland online banking login	\$2,200
Barclays online banking login	\$2,100
Santander personal bank account	\$1,800
Revolut verified account (UK, USA)	\$1,600
Verified Stripe account with payment gateway	\$1,200
Cashapp verified account	\$860
Stolen UK fully verified Skrill account details	\$610
Chase Bank login	\$500
Hacked Weststein Card account	\$500
Hacked TransferGo account	\$500
Payoneer verified account	\$200
CitiBank verified account	\$200
Wells Fargo banking login	\$150
Chime Bank account login	\$125
50 Hacked PayPal account logins	\$120
Hacked PerfectMoney account	\$100
Luno Account together with a balance of \$5,000	\$80
Bluebird Bank account login	\$75
Go2Bank hacked account	\$60
Huntington bank account login	\$60
PayPal transfer from stolen account, \$8,000+ balances	\$54
Hacked Western Union Account	\$39
Western Union transfer from stolen account, \$1,000+ balances	\$32
Bank of America account login	\$30
PayPal transfer from stolen account, \$1,000 – \$3,000 balances	\$30
Suntrust Bank account	\$30
PayPal transfers from stolen account, \$100-\$1,000 balance	\$25
CBA Random Bank login	\$25
PayPal transfer from stolen account, \$5,000+ balances	\$22
Stolen PayPal account details, no balance	\$15
Movo.Cash Login	\$11
Stolen PayPal account details, minimum \$1,000 balances	\$10
Stolen PayPal account details, minimum \$100 balances	\$10

# SERVICIOS EN INTERNET Y CUENTAS DE ENTRETENIMIENTO

- Las cuentas de RRSS robadas se usan para propagar estafas o desinformación
  - Con una cuenta que sea menos sospechosa (al ser de alguien real)
- También se ofrecen accesos a servicios de suscripción (Ej.: Netflix, Disney+...)
  - A precios más baratos que una suscripción estándar
    - Pero a riesgo de que el robo sea descubierto y se cancele sin previo aviso, claro
  - Se suelen adquirir para ver contenido gratis en regiones diferentes a las del comprador
    - Esto normalmente se puede hacer legalmente vía VPN (Ej.: ProtonVPN, F-83 “Numancia”)



Venta de una cuenta premium al servicio de streaming Disney+

# SERVICIOS EN INTERNET Y CUENTAS DE ENTRETENIMIENTO: PRECIOS

- A nivel de redes sociales se venden tanto cuentas como seguidores
- El precio es muy bajo
  - Especialmente el de seguidores...
- Permiten hacer creer que cuentas son más importantes de lo que lo son realmente
  - Es compra de cuentas bot
- Por ello, todo lo que veamos en redes sociales hay que asumir que es falso

<i>Hacked Gmail account</i>	\$60
<i>Hacked Facebook account</i>	\$25
<i>Hacked Instagram account</i>	\$25
<i>Hacked Twitter account</i>	\$20
<i>Twitter retweets x 1000</i>	\$10
<i>LinkedIn company page followers x 1000</i>	\$5
<i>Instagram followers x 1000</i>	\$2
<i>Pinterest followers x 1000</i>	\$2
<i>Twitch followers x 1000</i>	\$2
<i>Instagram likes x 1000</i>	\$2
<i>Spotify followers x 1000</i>	\$1
<i>Soundcloud plays x 1000</i>	\$1

Fuente: Investigación de precios en la dark web de Privacy Affairs (<https://www.privacyaffairs.com/dark-web-price-index-2023/>)

# SERVICIOS EN INTERNET Y CUENTAS DE ENTRETENIMIENTO: PRECIOS

- Prácticamente se venden cuentas de cualquier clase de servicio
  - Streaming, casinos, deportes...
- Los precios no suelen ser muy altos
- Mientras el dueño original siga pagando, el ladrón puede disfrutar del servicio por un precio ridículo
  - La prohibición de compartir cuentas de algunos servicios de streaming puede detectar estos robos

<i>AirBNB.com verified account</i>	\$300
<i>Bet365 account</i>	\$35
<i>Uber driver hacked account</i>	\$30
<i>US eBay account</i>	\$20
<i>Netflix account, 1-year subscription</i>	\$20
<i>Uber hacked account</i>	\$12
<i>Spotify hacked account</i>	\$10
<i>Hacked Alaskaair account</i>	\$10
<i>NBA League Pass</i>	\$8
<i>Kaspersky account</i>	\$7
<i>Various adult site accounts</i>	\$6
<i>Canva Pro yearly</i>	\$5
<i>Disney Plus hacked account</i>	\$3
<i>CNBC Pro</i>	\$3
<i>Hulu</i>	\$3
<i>HBO</i>	\$2
<i>Orange TV</i>	\$2
<i>Netflix 4K 1 year</i>	\$1

Fuente: Investigación de precios en la dark web de Privacy Affairs (<https://www.privacyaffairs.com/dark-web-price-index-2023/>)

# DOCUMENTOS DIGITALES DE VARIOS TIPOS

## ● Aquí podemos encontrar dos categorías

- **Escaneos de documentos personales** (auténticos o falsificados) 
  - Se suelen usar para **hacerse pasar por alguien real** en Internet
    - *¿Estas negociando con alguien comprar algo por WhatsApp y te manda una foto de su DNI para que te fíes?*  
Replantéate lo que estás haciendo
    - **No se compra nada ni por WhatsApp ni por RRSS:** Son estafas fijo
  - También para abrir cuentas a nombre de otros en distintos sitios
    - Sitios webs de citas, pornográficos, de criptomonedas, casinos...
    - Ya no solo es una pérdida económica, sino también **reputacional**
  - **Es algo que caerá en desuso:** La IA ya permite generar documentos creíbles de quien sea
- **Plantillas de identificación y facturas de servicios** 
  - Los compradores pueden modificar estas plantillas con cualquier detalle que necesiten
  - Con información real y algo de experiencia, se puede crear fácilmente una colección de documentos falsos de aspecto auténtico
  - Infectarlos con malware que actúe cuando se abra
  - Se pueden usar en **cualquier clase de estafa** (especialmente spear phishing), suplantación o contratación de bienes (por ejemplo, alquileres)

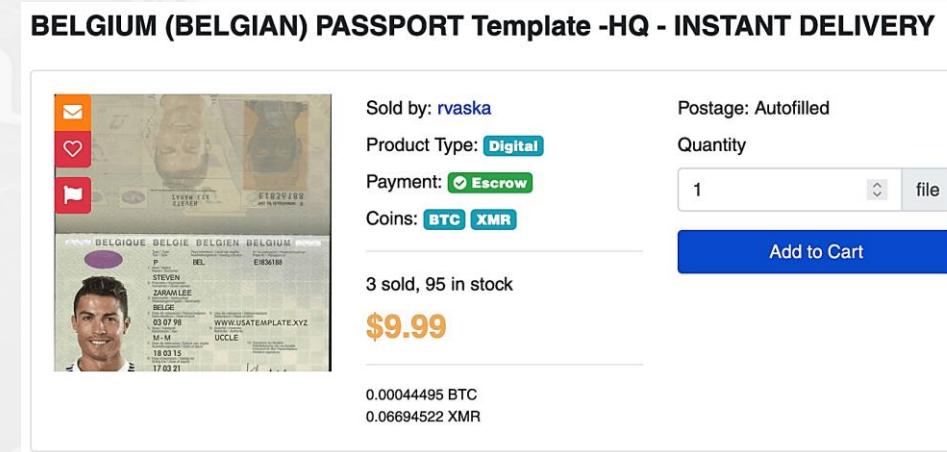
# DOCUMENTOS DIGITALES DE VARIOS TIPOS

- Una variante son los escaneos de documentos que incluyen un **selfie** con su propietario

- Son como las plantillas vistas, pero con ese dato adicional
- Lo suelen pedir en varios servicios para **verificación de identidad**

- Últimamente se piden videos cortos en lugar de escaneos por ese motivo

- Ej.: En YouTube
- Pero con IA se puede hacer esto también...



Plantilla para crearse un escaneo de un pasaporte belga. Con un poco de **Photoshop**, se puede crear uno que parezca auténtico a nombre de quien sea

# DOCUMENTOS DIGITALES: PRECIOS



José Manuel  
Redondo López

- La fabricación de documentos falsos en formato digital es un negocio popular
  - Muchos servicios piden copia o escaneo de un documento original
  - Así tienen un modelo fiable del que partir
- Con estas copias es posible suplantar a personas en muchos casos
  - Para usar a la hora de hacer gestiones, contratar servicios...
- Los hay de todos los países

<i>Alberta CA driver's License (scan)</i>	\$140
<i>USA selfie with holding ID</i>	\$110
<i>Forged WalMart prescription Rx labels</i>	\$100
<i>Russian passport scan</i>	\$80
<i>New York driver's license</i>	\$60
<i>USA passport scans</i>	\$50
<i>NSW (Australia) driver's license</i>	\$40
<i>Custom drivers' license</i>	\$35
<i>Minnesota driver's license</i>	\$22
<i>UK passport template</i>	\$22
<i>Germany passport template</i>	\$22
<i>New Hampshire drivers license template</i>	\$20
<i>Utility bill templates</i>	\$15
<i>Belgian passport template</i>	\$10
<i>UK utility bill templates</i>	\$10
<i>US business cheque templates</i>	\$8

Fuente: Investigación de precios en la dark web de Privacy Affairs  
(<https://www.privacyaffairs.com/dark-web-price-index-2023/>)

# DOCUMENTOS FÍSICOS DE VARIOS TIPOS: DINERO

## ● El dinero falso es un artículo muy común y fácil de encontrar



- Las monedas más demandadas son el euro, la libra esterlina y los dólares de Canadá, Australia y EEUU
- Algunos ofrecen hasta garantía de que pueden pasar una prueba de verificación por rayos UV

## ● Los billetes falsos de alta calidad suelen costar un 30% ciento de su valor nominal

- Imagina la de barbaridades que se pueden hacer con esto



**“Colar” billetes falsos no solo permite al delincuente comprar lo que sea, sino perjudicar a un tercero que acabe recibiéndolo como cambio. Fuente:**  
[https://www.lasexta.com/programas/mas-vale-tarde/como-identificar-billetes-falsos\\_2024030665e8ba58d3310300012e5ac4.html](https://www.lasexta.com/programas/mas-vale-tarde/como-identificar-billetes-falsos_2024030665e8ba58d3310300012e5ac4.html)



José Manuel  
Redondo López

# DOCUMENTOS FÍSICOS DE VARIOS TIPOS

## ● Los compradores también pueden obtener documentos físicos en la dark web

- **Falsificados:** Debido a la dificultad de falsificarlos por todas las medidas de seguridad que tienen, **son los artículos más caros** normalmente
- **Robados:** A su propietario original
  - Si el propietario ha denunciado el robo el comprador podría ser “cazado” fácilmente

**Carte d identite francaise cni FULL SECU**

Sold by: FreshID  
Product Type: **Physical**  
Payment:  Escrow  Multisig  
Coins: **BTC** **XMR**  
Ships from: FRA  
Ships to: EU  
Shipping Option  
FRANCE SUIVI - 3 days - \$5  
Quantity  
1  
Add to Cart  
Buy with Multisig

Un DNI francés falsificado, supuestamente que pasa todas las medidas de seguridad (si te fías del delincuente)



José Manuel  
Redondo López

# DOCUMENTOS FÍSICOS DE VARIOS TIPOS: PRECIOS

- Si existe un mercado para documentos digitales, también lo hay para físicos
- Con esto cualquier delincuente puede suplantar a quien desee en cualquier parte del mundo
  - ¿Entiendes por qué no debes enviarle tu DNI a nadie?
- Los precios son más elevados que las copias digitales
  - En función de lo que cueste hacer la falsificación (o el robo)

<i>Maltese Passport</i>	\$4,000
<i>French Passport</i>	\$3,000
<i>Netherlands Passport</i>	\$3,000
<i>Various European Union passports</i>	\$3,000
<i>Poland Passport</i>	\$2,500
<i>EU drivers' license</i>	\$2,000
<i>Lithuanian passport</i>	\$1,800
<i>European Union National ID (avg.)</i>	\$1,700
<i>Poland ID card</i>	\$1,700
<i>France drivers' license</i>	\$1,500
<i>Romania drivers' license</i>	\$1,450
<i>Latvian National ID</i>	\$1,300
<i>Fake US Green Card</i>	\$450
<i>Delaware ID</i>	\$200
<i>Indiana ID</i>	\$200
<i>Montana ID</i>	\$200
<i>Nevada ID</i>	\$200
<i>Texas ID</i>	\$200
<i>New Jersey drivers license</i>	\$200
<i>Louisiana ID</i>	\$200
<i>Utah ID</i>	\$200
<i>US driver's license (avg.)</i>	\$150

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



## ● Asegúrate de haber entendido lo siguiente

- Que muchas de las cosas que se puedan subir a internet tienen valor para alguien, especialmente vinculado con el crimen
- Que existe todo un mercado de cuentas, identificaciones, etc. robadas, que incluso fluctúa en función de la oferta y la demanda
  - ¿Para qué crees que se usa este tipo de información?
- Las ventajas que tiene para un delincuente hacerse pasar por otras personas con cosas que les ha robado, además de la ganancia que puede obtener poniéndolas a la venta
- Que algunos de estos elementos casi se venden en packs por un precio realmente bajo
- Debido a lo anterior, entiendes cómo se hacen los *review bombing* o los ataques de bots en redes sociales



## MÁS INFORMACIÓN...

Para saber más...



# REFERENCIAS

- Como has visto, esta presentación forma parte de un proyecto de formación pensado para gente joven
  - Y/o sin conocimientos previos
- Si te gusta “el cacharreo”, tengo más cosas para ti
  - Si quieres saber más cosas “de hacker” sin instalar nada y requiriendo conocimientos técnicos mínimos, puedes echarle un ojo a **S-74 “Tramontana”**
  - Si quieres tener tus propios “mini-ordenadores” emulados para tus cosas, la **R-11 “Príncipe de Asturias”** te gustará
  - *¿Tienes un colega en problemas?* Creo que puedes ayudarle con la **P-74 “Atalaya”**
  - *¿Te flipa que haya gente así de mala por la red?* Te cuento como engañan a los demás en la **M-31 “Segura”**
  - *¿Te vienes arriba porque esto te mola?* Prueba alguna del **Rango 3 ;)**
- Quien sabe...a lo mejor esto te gusta y ¡en el futuro tú des charlas como esta! ☺



José Manuel  
Redondo López

# REFERENCIAS

## ● Otros enlaces interesantes

- **Redes sociales:** <https://www.incibe.es/node/53247>
- **Estar a la última en fraudes:** <https://www.incibe.es/ciudadania/tags/Redes%20sociales>
- **Más consejos para ti:** <https://www.incibe.es/ciudadania/redes-sociales>
- **Y también para tus padres**
  - <https://www.incibe.es/menores/recursos/redes-sociales-en-la-adolescencia>
  - <https://www.incibe.es/menores/tematicas>



# SOBREVIVIENDO EN LAS REDES SOCIALES

