

CUANDO EL OBJETIVO DE UN CIBERATAQUE ES UN SER HUMANO



Hablemos de ciberbullying y
otras lacras



JOSÉ MANUEL REDONDO LÓPEZ

PROYECTO "P-74 'ATALAYA'" v1.21



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

¡BIENVENIDO!

- En este curso vamos a tratar de ver aspectos de ciberseguridad más humanos que técnicos
 - Es decir, donde las víctimas **son personas**, y no máquinas
- No creas que por eso es menos importante
 - De hecho, **lo es más**
 - Lo primero que hay que proteger en un sistema son las personas que forman parte de él
- Vamos a ver qué medidas podemos tomar para ello
- Todo ello como parte de la infraestructura de la iniciativa “Cobra Kali”



La iniciativa
“Cobra Kali” por
José Manuel
Redondo López



Investigar Redes Sociales

Técnicas de investigación para RRSS

F-31 “Descubierta”



Virtualización Básica

Creación y uso de máquinas virtuales

R-11 “Príncipe de Asturias”

Rango 1
(Marinero)



Investigación de Webs

Detección de webs problemáticas

S-64 “Narval”



Entendiendo la Mente del Crimen

Mentes criminales y engaño

M-31 “Segura”



Ataques contra Personas

Ciberacoso

P-74 “Atalaya”

Rango 2
(Marinero de Primera)



Ciberseguridad General

Ciberseguridad general para el día a día

F-74 “Asturias”



Crime-spotting

Ejemplos de fraudes reales para concienciación

“Nautilus”



Vigilancia de Redes

Entendiendo cómo funcionan las redes modernas

F-83 “Numancia”

Rango 3
(Cabo)



Y si el cuerpo te pide marcha... ☺



La iniciativa
"Cobra Kali" por
José Manuel Redondo
López



Introducción a la Ciberdefensa Personal

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



Ciberdefensa Personal Avanzada

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



Seguridad de Redes

Threat hunting
TBA. L-52 "Castilla"

Administración Segura de SO

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

Identificación y Análisis de Vulnerabilidades en Web

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



Protección de Servidores Web

Seguridad de infraestructuras para startups
Guías INCIBE, F-103 "Blas de Lezo"



Defensa contra el Cibercrimen

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



Rango 1
(Sargento)



Innovación e Investigación en Ciberdefensa

Avances e innovación en ciberdefensa (Nivel C2)
Proyecto UNIDIGITAL. "BPM P-51 'Asturias'"

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, Guías INCIBE,
Microcreencias. D-73 y C-
33 "Blas de Lezo"



Rango 2
(Suboficial Mayor)



Rango 3
(Capitán de Fragata)



Desarrollo Seguro de Software

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



Rango 4
(Almirante)



José Manuel
Redondo López

¿Y TODO EL RESTO DE MATERIAL?

- Durante este curso se hará mención a otros cursos complementarios que te regalo y que forman parte de la misma iniciativa
- Puedes encontrarlos todos aquí:
 - [https://github.com/jose-r-lopez/Formacion_-Seguridad_Joven/wiki/Contenidos-de-la-Iniciativa-%22Cobra-Kali%22-\(Capacitaci%C3%B3n-B%C3%A1sica\)](https://github.com/jose-r-lopez/Formacion_-Seguridad_Joven/wiki/Contenidos-de-la-Iniciativa-%22Cobra-Kali%22-(Capacitaci%C3%B3n-B%C3%A1sica))
- También tengo pensado en el futuro subir videos explicando cada curso en mi canal de YouTube
 - <https://www.youtube.com/@JoseRedondo-dj7xk>



ÍNDICE

- **El complejo problema del bullying en la sociedad**
- **La actitud general contra el bullying y el acoso**
- **Uso de redes sociales**
 - Afectados por el bullying: un espectro amplio
 - Mecanismos de ciberdefensa personal
 - Acoso avanzado en redes sociales
 - Sextorsión
- **Aplicaciones de Mensajería**
 - Narcisistas
 - Acoso académico
 - Cuando el ataque viene de un conocido
- **Conclusiones**

¿QUÉ VAMOS A VER EN ESTE BLOQUE?



● En la primera sección veremos...

- **Qué es** el bullying o acoso y como de grave es el problema
- Las **consecuencias** que tiene ser acosado
- Por qué mucha **gente "senior"** no entiende estos problemas
- Las **relaciones de poder asimétricas**
 - Y por qué son un caldo de cultivo para abusos de todo tipo

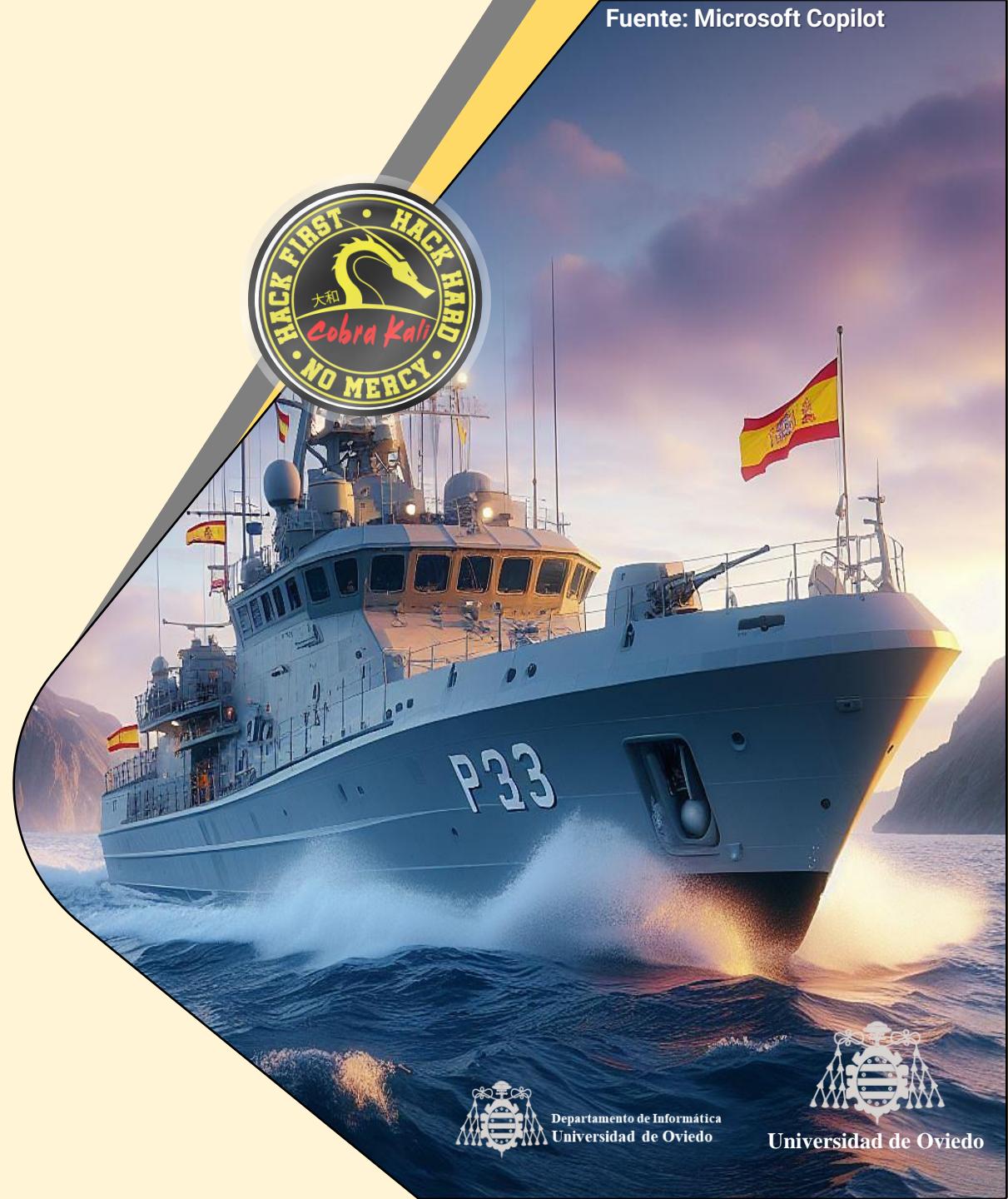
● Y en la segunda...

- Que el **bullying** no es solo cosa de la víctima: **es necesario la proactividad**
- Como se puede uno "aliar" contra el **bullying** sin ser víctima: **bloqueo y denuncia**

[< Ir al Índice](#)

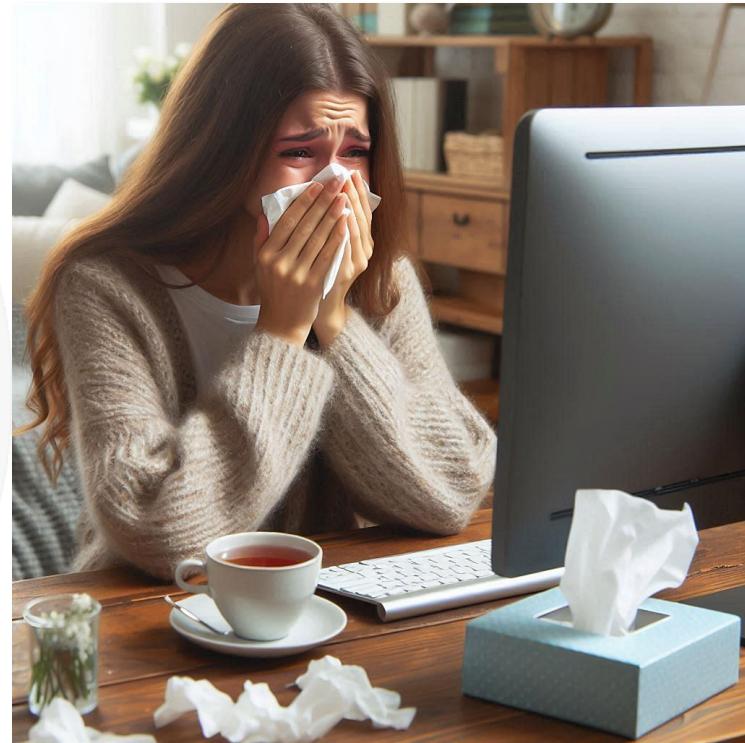
EL COMPLEJO PROBLEMA DEL BULLYING EN LA SOCIEDAD

¿Es grave? Y si lo es, ¿Por qué aún hay gente que lo niega?



¿Es GRAVE?

- El ciberacoso o **cyberbullying** es un problema creciente a nivel mundial
- En España, un 6,9% de los estudiantes afirmó haber sufrido ciberacoso durante los últimos dos meses,
 - Según datos de Unicef actualizados en diciembre de 2021
- Segundo un estudio de Unicef de 2017, un 12% de los jóvenes consideraba haber sufrido ciberacoso durante los últimos 12 meses
 - Esta cifra aumenta conforme los jóvenes entran en la adolescencia, llegando hasta una diferencia de 7 puntos porcentuales entre los 9 y los 16 años
 - **Fuente:** <https://www.epdata.es/datos/cibercriminalidad-ciberbullying-datos-estadisticas/291>



No tienes por qué aguantar esto. Por favor, pide ayuda

¿Es GRAVE? SÍ

- *¿Y en otros países?* Esta igual o peor

- Por ejemplo, en Perú...

- 6 de cada 10 niños, niñas y adolescentes aseguraron haber sufrido ciberbullying
 - Según un informe reciente
- Según su Ministerio de Educación, los casos de ciberbullying registrados en 2023 duplican a los del 2022
- **Fuentes:**
 - <https://www.infobae.com/peru/2023/09/01/un-61-de-escolares-revela-haber-sido-victima-de-ciberbullying-y-un-91-de-padres-cree-que-esto-no-ocurre/>
 - <https://diariocorreo.pe/peru/ciberbullying-61-de-ninas-ninos-y-adolescentes-peruanos-lo-ha-vivido-noticia/>

El ciberacoso es un problema muy serio que afecta a jóvenes de todo el mundo
NO, NO ESTÁS SOLO

¿QUÉ CONSECUENCIAS TIENE PARA LA VÍCTIMA?

● Consecuencias psicológicas

- Daño a la **autoestima**, sensación perenne de culpa
- Dificultad para relacionarse con los demás, **fobia social**
- **Depresión** y **Desconfianza** hacia cualquier persona
- **Aislamiento**
- **Alteraciones** en el sueño y trastornos alimenticios

● Consecuencias físicas

- Cuando el acoso se extiende al mundo físico, y la víctima sufre algún tipo de agresión del acosador
- También incluyen las **autolesiones**

● Consecuencias sexuales

- Cuando se trata de un ciberacoso de carácter sexual, la sextorsión o el grooming
- Tengo un monográfico del grooming en: <https://github.com/jose-r-lopez/Fraudes-y-Timos/blob/main/Case%20Files/T1E34.%20Grooming%20y%20ataques%20a%20la%20infancia.pdf?raw=true>

● Cada persona vive el ciberacoso de una forma diferente y cada situación es única

- Las secuelas varían dependiendo del perfil de la víctima, del tipo de acoso y del apoyo recibido
- **No hay acoso mejor ni peor, cada uno lo vive de forma distinta**

Fuentes:

- <https://www.syneidis.com/es/problem-cyberbullying-consequences/>
- <https://www.iberdrola.com/compromiso-social/que-es-ciberacoso-como-prevenir>

¿No te parece lo suficientemente grave para poner medios contra él?

¿CUÁL ES EL DISCURSO TRADICIONAL SOBRE EL BULLYING QUE SE HACÍA EN EL PASADO?

- *¿Por qué crees que una parte más “señor” de la sociedad no entiende estos problemas?*

- **Se debe al discurso tradicional sobre el acoso**
- **Violencia en la educación:** En la antigüedad, la violencia estaba implícita en el método educativo (“la letra con sangre entra”)
 - Que la violencia física era necesaria para educar era algo totalmente **validado y aceptado**
- **Es algo escolar:** Se entendía como un acto en el que un chico o chica o un grupo de ellos someten a maltrato a un compañero
 - Pero que **quedaba en la escuela**
 - En la actualidad, con las redes sociales, **esto ya no es así** (acoso 24/7/365)



Sí, probablemente te cuenten que ellos en clase eran unos héroes y que nada de lo que te pasa ahora ocurría antes. Es mentira, lo siento. Más bien se tapaba. Y de lo que no se habla...

¿CUÁL ES EL DISCURSO TRADICIONAL SOBRE EL BULLYING QUE SE HACÍA EN EL PASADO?

- **Características del bullying:** Se entendía como una práctica de superioridad del agresor
 - Transmitida por la sumisión o el temor del individuo acosado
 - Las formas más comunes eran agresiones, amenazas, insultos, juegos sucios, trampas, apodos, etc.
 - Con las redes sociales esto **se ha transformado en una nueva dimensión** de tortura intensa e intensiva
- **Consecuencias del bullying:** Se trataba como una fase necesaria para “hacerse más duro”
 - Y parte de la “educación para ser un adulto fuerte”...
- **Llamada a la acción:** El discurso tradicional sobre el bullying también incluía su **minimización**
 - “son cosas de niños”, “ya se les pasará”....



La vida real no es una escuela militar chunga, aunque algunos se empeñen en decirlo constantemente...

CUIDADO CON CAER EN RELACIONES ASIMÉTRICAS DE PODER

- Relaciones donde un miembro tiene excesiva autoridad, influencia o control

- Son un caldo de cultivo habitual de desequilibrio, **abuso, dependencia o frustración**
- Se conocen casos entre **docentes y estudiantes, padres e hijos o jefes y empleados**
 - Uno de los miembros debe tener más autoridad por el puesto que ocupa
 - Pero eso **no le da derecho a acosar o abusar** de ninguna forma del otro
- O **parejas** donde uno de los miembros **decide todo** por el otro

- No hay respeto, comunicación ni cooperación

- “*Quien bien te quiere te hará sufrir*” **NO**



No se aguantan gritos de nadie, por mucho que sea tu jefe, lo quieras, dependas de él para algo... Tú NO eres un punching ball

¿CÓMO SABER SI ESTÁS EN UNA?

- Debes identificar signos que indican que hay un desequilibrio entre las partes
- ¿Qué signos son? Por ejemplo...
 - Nunca puedes decir que no a peticiones de esa pareja, amigo/a, jefe, etc.
 - Temes a las consecuencias, sean o no físicas (ver [Narcisistas](#))
 - Excusas constantemente el mal comportamiento de la otra persona
 - “Es que el/ella es así”, “Es que ya sabes cómo es”, “Es mejor hacerlo como dice o se pone pesado/a”...
 - De hecho, asumes eso como algo normal
 - Sientes que estás “caminando sobre cáscaras de huevo” todo el tiempo
 - Tratando de evitar conflictos o críticas con el otro miembro de la relación
 - Te sientes atrapado o impotente, sin poder expresar tus opiniones, deseos o necesidades.
- Pero es un abuso, y puede generarte las mismas consecuencias que ya vimos

¿QUÉ HACER EN GENERAL SI ESTÁS EN UNA?

- Salir de una relación asimétrica de poder no es fácil, pero tampoco imposible
- Debes identificar si estás en una situación de desequilibrio y si te está afectando
 - **Busca ayuda profesional y no dejes que esto “medre”**: cuanto más tiempo pase, peor
- Si es algo en el plano personal
 - Recupera tu autoestima, tu autonomía, tu identidad, tu confianza y seguridad en ti mismo
 - Haz cosas que te gusten **A TI**, que te hagan sentir bien y que te permitan expresarte
- **Si es algo laboral:** Contacta con un sindicato para saber y ejercer tus derechos
- **Si es algo universitario/escolar:** Contacta con las unidades adecuadas de la Universidad / Centro de estudios
 - Ej.: Defensoría universitaria (<https://defensora.uniovi.es/>), unidad de igualdad (<https://igualdad.uniovi.es/>)
 - Y lee el reglamento para conocer tus derechos y protocolos de actuación
- **Recuerda que NADIE tiene derecho a manipularte, controlarte o hacerte daño**

¿QUÉ HACER EN GENERAL SI ESTÁS EN UNA?



José Manuel
Redondo López

● Más información

- Relación asimétrica: qué es y señales para detectarla
 - <https://www.lavanguardia.com/vivo/sexo/20201124/49674501543/relacion-asimetrica-problemas-pareja.html>
- Relaciones simétricas y asimétricas
 - <https://www.psicologialflexible.com/es/relaciones-simetricas-asimetricas/>
- Asimetría de poder en las relaciones: Cuando uno de los dos decide todo
 - https://www.clarin.com/entremujeres/pareja/asimetria-poder-relaciones-decide_0_Hy455b_ib.html
- El poder y las relaciones asimétricas
 - <https://prezi.com/n4nw0nctafts/el-poder-y-las-relaciones-asimetricas/>

No todas tienen un componente amoroso, pero muchas sí...Fuente:

https://www.incibe.es/sites/default/files/contenidos/materiales/Campanas/relacion_e_internet_entregable.pdf

¿TENGO UNA RELACIÓN SALUDABLE CON MI PAREJA A TRAVÉS DE INTERNET?

¿TE AGOBIA ESCRIBIÉNDOTE DEMASIADOS MENSAJES?

¿TE EXIGE QUE LE DIGAS DÓNDE ESTÁS Y QUÉ HACES A CADA MOMENTO?

¿SE MOLESTA SI NO CONTESTAS RÁPIDAMENTE A SUS MENSAJES?

¿SE MOLESTA SI VE QUE ESTÁS EN LÍNEA, PERO NO LE HABLAS?

¿TE EXIGE QUE LE DES TUS CONTRASEÑAS DE REDES SOCIALES?

¿SE ENFADA SI ACEPTAS UNA SOLICITUD DE AMISTAD DE OTRA PERSONA?

¿CRITICA TU FORMA DE VESTIR O ACTUAR EN LAS FOTOS QUE PUBLICAS?

¿UTILIZA UN LENGUAJE AGRESIVO U OFENSIVO?

¿TE EXIGE QUE LE ENVÍES IMÁGENES O VÍDEOS ÍNTIMOS?

¿TE HACE SENTIR MAL CON SUS MENSAJES O SUS PUBLICACIONES SOBRE TI?

Cualquiera de estas conductas se considera **cibercontrol**: no es una muestra de afecto, sino todo lo contrario. Nadie tiene derecho a controlarte, ni hacerte sentir mal, tampoco en Internet.

Ante cualquiera de **estas situaciones**, ahora o en el futuro, **no lo dudes**:

 Habla con esa persona, con asertividad, muéstrale tu desagrado y no lo consientas.

 Pide consejo a una persona adulta de confianza y cuéntale lo que está ocurriendo.

Puedes **solicitar ayuda a profesionales** llamando a la Línea de Ayuda en **Ciberseguridad de INCIBE** para determinar si hay un problema, y en ese caso resolverlo.



Asegúrate de que el móvil e Internet son una parte positiva en vuestra relación. Recuerda, ante todo **respeto**.

¿CÓMO SABER SI LO HAS ENTENDIDO TODO? RESPONDE ESTO

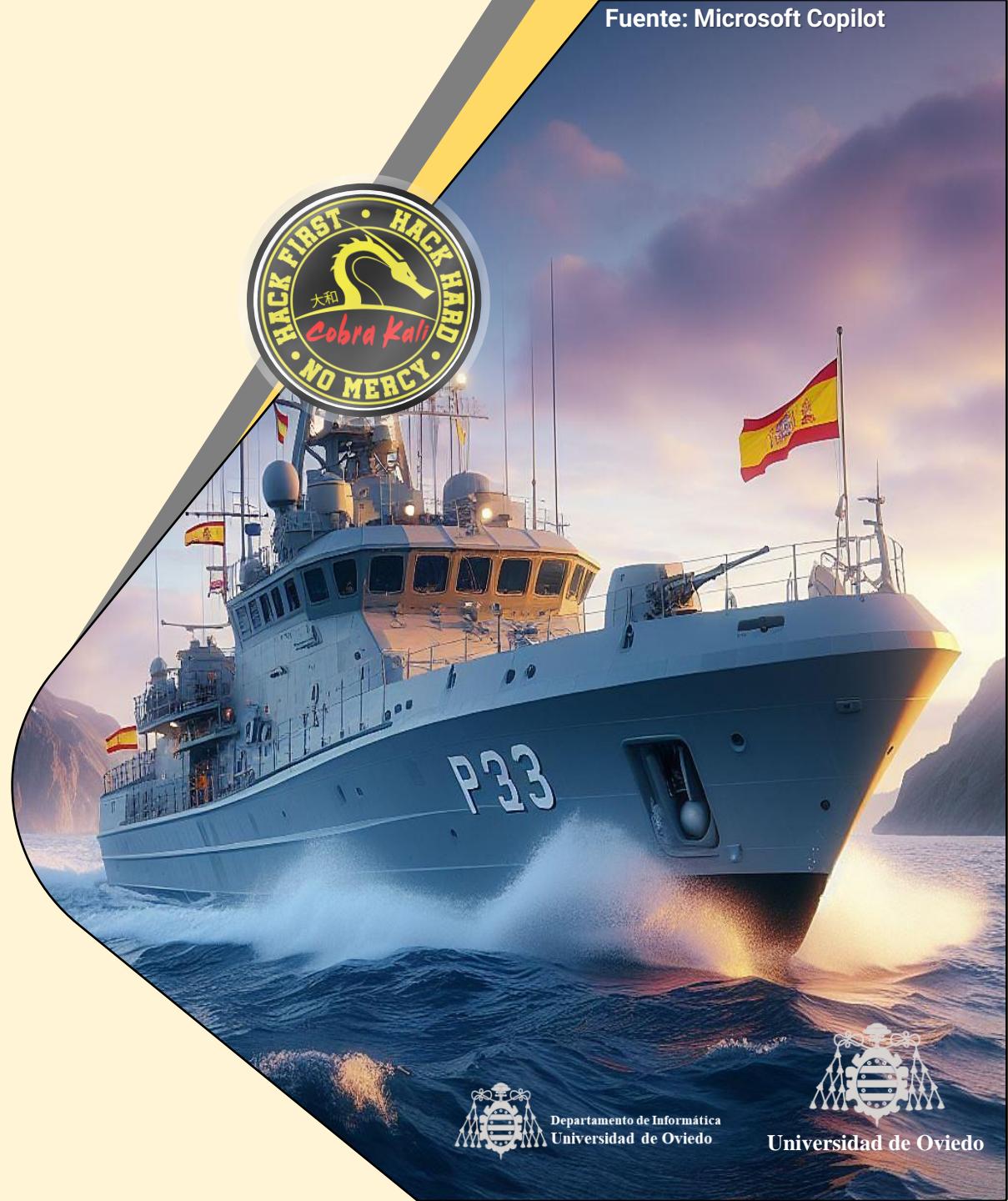
?

- *¿Entiendes que las consecuencias del acoso son tan graves que no prestarle atención (tanto si eres víctima como conocido) es un terrible error?*
- *¿Tienes alguna "idea antigua" del acoso implantada en tu subconsciente?*
 - *¿Comprendes por qué es errónea y no te deja ayudar a quienes tienen estos problemas?*
- *¿Comprendes lo peligrosa que es una relación asimétrica de poder y como se produce cuando hay abuso de autoridad?*
- *¿Entiendes qué cosas no debes tolerar en entornos donde haya una persona con autoridad sobre otras, ya que entonces se "weaponiza" esa autoridad contra ti?*
- *¿Entiendes por qué y cómo debes actuar si te encuentras en una relación asimétrica de cualquier tipo?*

[< Ir al Índice](#)

⚔️ LA ACTITUD GENERAL CONTRA EL CIBERBULLYING Y EL ACOSO

Qué postura general debes tomar,
independientemente de otras consideraciones



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

ANTES DE EMPEZAR...HABLEMOS DE UNA POSTURA GENERAL

- Vamos a hablar del **bullying** tocando varios casos concretos y desde diferentes perspectivas (menores, adultos, entornos...)
- Sin importar las indicaciones específicas que demos, recuerda este mandamiento:
Hay que ser proactivo y colaborar en su erradicación, no mirar a otro lado
 - El que ataca es el culpable y quien debe sufrir las consecuencias, nunca el atacado
- Se traduce en dos términos: **denuncia y bloquea**
- Sin la colaboración de todos, Internet puede convertirse en un lugar muy hostil

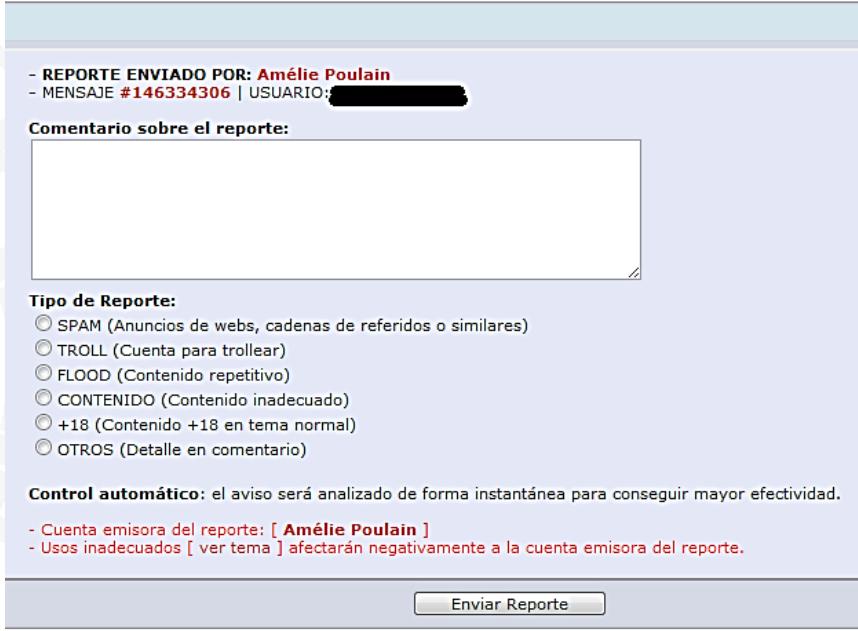
BLOQUEA Y DENUNCIA TODA ACTIVIDAD QUE TE RESULTE SOSPECHOSA

- **Motivo:** Es importante que te acostumbres a **denunciar** cualquier actividad sospechosa

- Gracias a eso se mantiene una red más segura para todos
- En la mayoría de las plataformas las denuncias **son anónimas**

- **Solución:** Sé proactivo en cómo tratas contenidos que creas que son maliciosos

- Si, por ejemplo, detectas un mensaje que podría ser un **timo**, no te limites a borrarlo
 - **Informa a la plataforma** de que es un posible mensaje malicioso
- Si ves a alguien en una cuenta de una red social escribir **algo perjudicial**, tampoco te limites a bloquearlo
 - Estudia las opciones que tienes para **reportar el mensaje** como algo malicioso (luego veremos ejemplos concretos)
- En general, antes de bloquear algo, **contribuye a la comunidad**
 - Informando a la plataforma del contenido perjudicial



The screenshot shows a reporting form. At the top, it displays the reporter's information: "REPORTE ENVIADO POR: Amélie Poulain" and "MENSAJE #146334306 | USUARIO: [REDACTED]". Below this is a text area labeled "Comentario sobre el reporte:" which is currently empty. Underneath is a section titled "Tipo de Reporte:" with several radio button options:

- SPAM (Anuncios de webs, cadenas de referidos o similares)
- TROLL (Cuenta para trolllear)
- FLOOD (Contenido repetitivo)
- CONTENIDO (Contenido inadecuado)
- +18 (Contenido +18 en tema normal)
- OTROS (Detalle en comentario)

At the bottom, there is a note about automatic control: "Control automático: el aviso será analizado de forma instantánea para conseguir mayor efectividad." followed by two links: "Cuenta emisora del reporte: [Amélie Poulain]" and "Usos inadecuados [ver tema] afectarán negativamente a la cuenta emisora del reporte." A "Enviar Reporte" button is located at the very bottom right.

Muchos foros de Internet tienen su sistema para informar de contenidos inadecuados, no sólo redes sociales

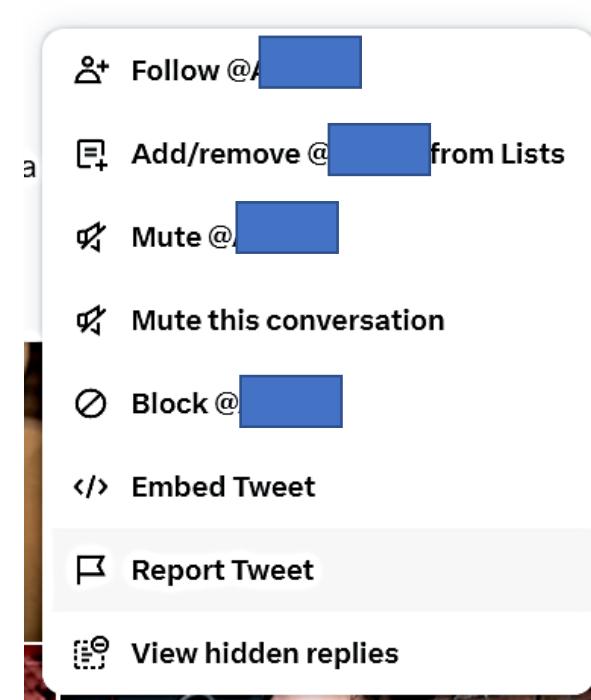
BLOQUEA Y DENUNCIA TODA CUENTA QUE TE RESULTE SOSPECHOSA

● **Motivo:** Como dijimos, mantener una actitud proactiva con los contenidos maliciosos es de importancia capital

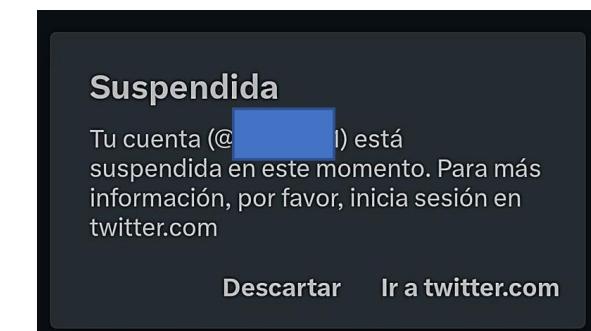
- Esto es de especial relevancia cuando estamos en redes sociales
- La cantidad de cuentas falsas o perjudiciales que puede haber en una red social es demasiado elevada como para no actuar

● **Solución:** Cuando estés en una red social estudia bien los mecanismos para reportar mensajes maliciosos y úsalos

- Muchas redes sociales te permiten **especificar exactamente** qué tipo de contenido crees que es perjudicial
 - **Engaños, ciberacoso, suplantación, influir en elecciones...**
 - Informa correctamente del tipo de contenido que has visto
 - La **acumulación de informes negativos** bloqueará la cuenta
 - Temporal o permanentemente, según la gravedad de lo dicho
- **No se debe confiar solo en el equipo de moderación** de una red social
 - No pueden procesar todos los mensajes de este tipo que se encuentran



Página para reportar un Tweet



DENUNCIA PREVENTIVA DE INFORMACIÓN PRIVADA

- **Motivo:** Mientras navegas quizá te encuentres con información privada

- O **indicios** de algún delito **por accidente**
- O cosas que perjudiquen a 3^{as} personas
- O **seas víctima de un delito o acoso**

- **Solución:** Busca las herramientas que los cuerpos policiales poseen para la denuncia de determinados contenidos delictivos en internet

- En caso de duda, **pide asesoría** a un profesional acerca de cómo hacerlo
- **No intentes** quitar el contenido o “atacarlo” tú mismo, ya que entonces podrías incurrir en un delito
- Hazlo aquí:

https://www.policia.es/_es/colabora_informar.php?strTipo=CGPJDT#

Portal web de la Policía Nacional

ES Español DIRECCIÓN GENERAL DE LA POLICÍA

Gobierno de España Ministerio del Interior UE 23 POLICIA NACIONAL

INICIO DENUNCIAS COLABORA COMUNICACIÓN TU POLICIA EXTRANJERÍA FONDOS EUROPEOS SEDE ELECTRÓNICA

DEPENDENCIAS BUSCAR CONTACTA DNI ELECTRÓNICO CITA PREVIA DNI Y PASAPORTE

Contacta CONSEJOS MUJER TRATA BUSCADOS DESAPARECIDOS

SELECCIONA LA ESPECIALIDAD

Concreta la especialidad a la que quieres informar

Selección del área policial Selección de la especialidad

Pornografía infantil	Redes sociales	Amenazas y extorsiones	Fraudes en Internet
Comunicación de información sobre páginas web, publicaciones o cualquier situación que ponga en peligro al menor en el uso de las nuevas tecnologías (Ciber-bullying, Grooming, Sexting).	Comunicación de cualquier actividad ilegal a través del uso de las Redes Sociales (Facebook, Twitter, Youtube, foros, newgroups, etc).	Comunicación de delitos de amenazas, extorsiones, calumnias o injurias cometidos a través de las Tecnologías de la Información y la Comunicación.	Comunicación sobre uso fraudulento de tarjetas de crédito en Internet, fraudes en subastas y comercio electrónico, estafas en la red.
Seleccionar	Seleccionar	Seleccionar	Seleccionar
Seguridad lógica	Antipiratería	Fraudes uso telecommunicaciones	Otra información
Seguridad lógica, virus, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidad o sustracción de cuentas de correo electrónico.	Comunicación de delitos contra la propiedad intelectual de programas de ordenador, música y productos cinematográficos o contra la propiedad industrial, uso indebido de señales de video.	Comunicación de delitos cometidos utilizando cualquier sistema de telecomunicación, fraudes telefónicos en sistemas de telefonía fija o móvil.	Para comunicaciones no recogidas en los epígrafes anteriores.
Seleccionar	Seleccionar	Seleccionar	Seleccionar

La policía tiene opciones para denunciar una gran cantidad de delitos online

¿CÓMO SABER SI LO HAS ENTENDIDO TODO? RESPONDE ESTO

?

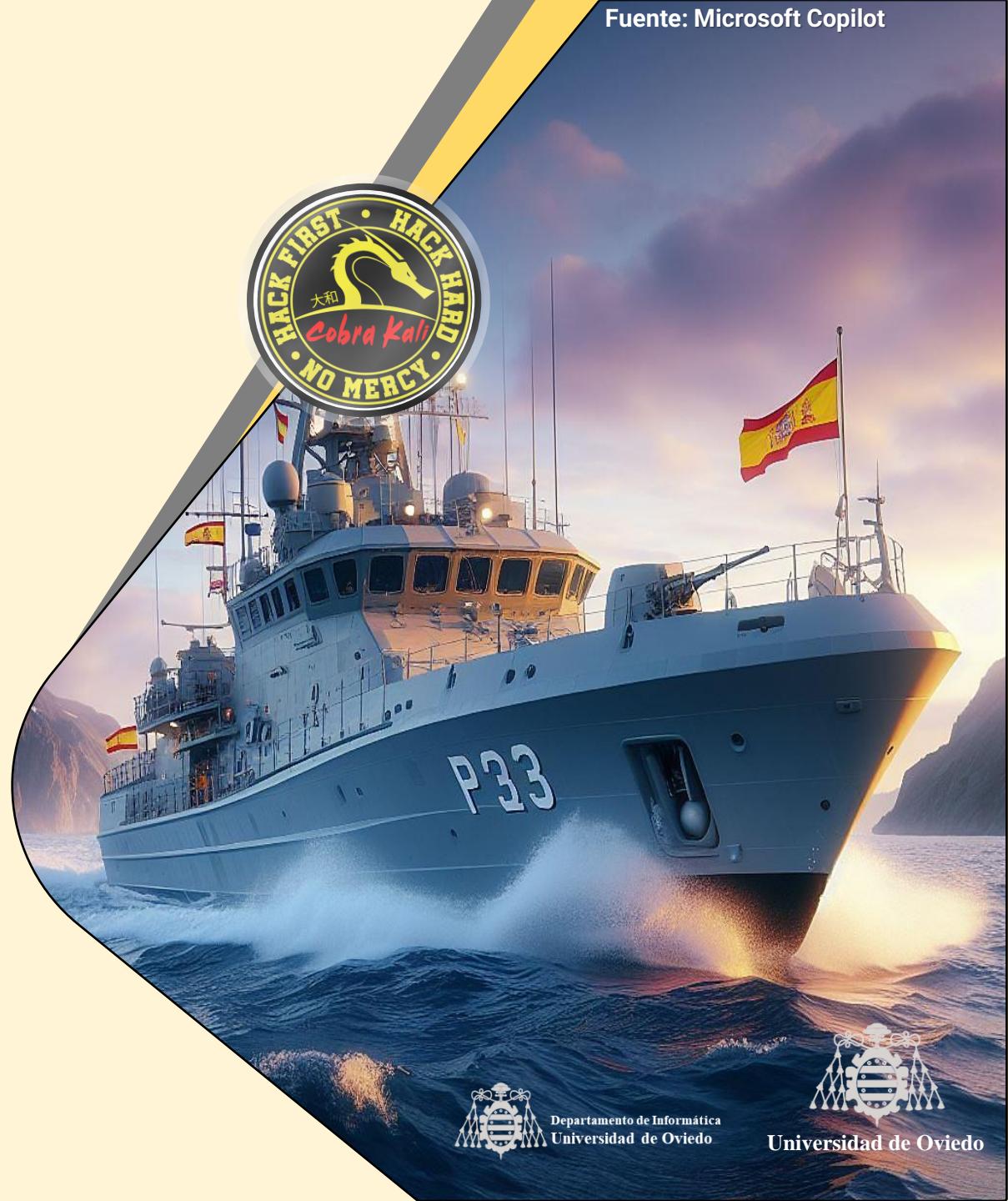
- *¿Entiendes que "mirar para otro lado" nunca es una solución?*
- *¿Has entendido que existen mecanismos de denuncia y bloqueo en foros / redes sociales /etc. que puedes usar contra abusadores/as o estafadores/as?*
 - *¿Y que estos son anónimos, por lo que no te "juegas" nada?*
- *¿Entiendes que ante la certeza de está viendo un delito en la red, tienes sitios en los que denunciarlo para poder pararlo a tiempo?*

< Ir al Índice



USO DE REDES SOCIALES

Compartir está bien, pero hay que hacerlo con cabeza



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

¿QUÉ VAMOS A VER EN ESTE BLOQUE?

● En la primera sección veremos...

- Que ser víctima de acoso **nunca es culpa tuya**
- Cómo **evitar dar "munición"** a un acosador...y a los estafadores
- **Cómo actuar** ante casos de acoso, ya sea con menores o no menores

● En la segunda...

- **Normas mínimas** para actuar y protegerte ante acoso (o estafas) en redes sociales
- La importancia de **certificar los mensajes** si quieres denunciar

● En la tercera...

- Técnicas y tácticas de acoso por redes sociales **más avanzadas**
- Cómo estas técnicas son **más sutiles**, pero igual de devastadoras

● Y, finalmente, en la cuarta...

- Las terribles **consecuencias de la sextorsión**
- Formas de **evitar ser víctima** de este tipo de acoso



EL USO RESPONSABLE DE RRSS EVITA PROBLEMAS

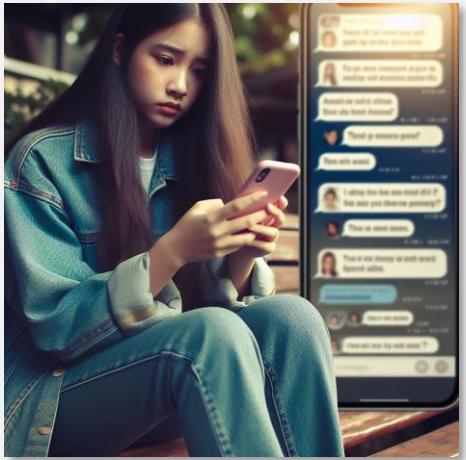
- Ten claro una cosa: **el culpable de un delito es siempre el delincuente**
- Si alguien decide ir contra ti, nunca va a ser culpa tuya
 - Alguien ha decidido, libre y conscientemente, cometer un acto para hacerte daño y potencialmente delictivo: **no hay justificación ni excusa que valga**
 - Nadie puede alegar que no sabía, no era consciente...ninguna persona normal hace eso por desconocimiento: **saben que es un delito o dañino y lo hacen**
 - No te lo mereces, no te lo has ganado, no te ha pasado por hacer, vestir, decir...**NO: Nadie tiene derecho ni justificación para hacerle daño a otra persona**
- Pero, por favor, controla y recapacita bien sobre lo que publicas...
 - Evita en lo posible darles “munición”
 - Porque, si no lo haces, entonces pones más fácil el ser víctima de **acoso...y de estafas**

¿REALMENTE COMPARTIMOS TANTO EN RRSS COMO PARA ESO?

- Obviamente no todos lo hacemos, pero es un problema grave a nivel mundial
- Hay videos de concienciación del problema verdaderamente preocupantes
 - Mira y analiza el video de Sarina Abdullah
 - *¿Es tu caso? ¿Hay algo que te quieras replantear (o borrar) de tus RRSS después de verlo?*
 - <https://www.youtube.com/watch?v=35caskf6YJg>
 - Otra fuente:
https://www.linkedin.com/posts/derechoinformatico_informaci%C3%B3n-activity-7022952957579079680-4A5N/
 - Más videos de concienciación similares
 - <https://www.youtube.com/watch?v=yrjT8m0hcKU>
 - <https://www.youtube.com/watch?v=j-tFoYNHi1w>



El video de concienciación de Sarina Abullah es muy bueno y efectivo para abrir los ojos a gente que no cree que esto sea para tanto. Es muy buena idea verlo y distribuirlo a quien creas que lo necesita ☺



Afectados por el bullying: un espectro amplio

Como responder ante estos casos según el afectado



LAS PERSPECTIVAS A LA HORA DE LIDIAR CON EL BULLYING

● El bullying es cosa de todos, aunque tu no seas víctima de él

- El bullying no se queda solo en la víctima (así se pensaba antes, ¿recuerdas?)
- Una víctima no necesita sentirse sola: **necesita apoyo y ayuda de sus amigos y familiares**
 - Mirar para otro lado no soluciona ningún problema



● Además, en tu entorno puedes tener personas menores a cargo

- Hermanos, primos...
- O las podrás tener en el futuro (👦 👩)
- Ellos también pueden tener problemas de esta clase, principalmente escolares
 - Y, en ese caso, puedes ocupar un rol de "protector"

Los verdaderos héroes no llevan capa, sacan la cara por los necesitados

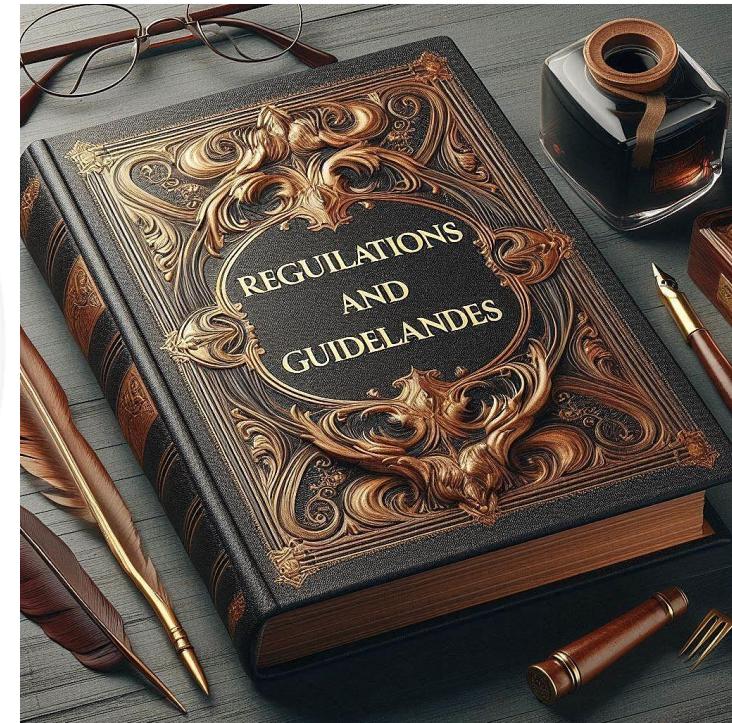
● Hablemos de todas estas perspectivas

MECANISMOS DE ACTUACIÓN FRENTES AL BULLYING EN RRSS

-  **Motivo:** El bullying en RRSS es muy peligroso por la posibilidad de que lo haga gente conocida desde cuentas anónimas
 - El acoso puede ser **constante y muy dañino** para la víctima
-  **Solución:** Estudia los protocolos de actuación ante casos de **bullying**
 - Es necesario para asesorar a la víctima
 - **¿Eres tú?** Pide ayuda aquí
 - <https://www.incibe.es/menores/ayuda#:~:text=Puedes%20ponerte%20en%20contacto%20con,los%20365%20d%C3%A1as%20del%20a%C3%B1o.>
 - **¿Eres un familiar?** Aquí tienes materiales de ayuda
 - <https://www.incibe.es/menores/tematicas/ciberacoso>
 - <https://www.incibe.es/menores/tags/Bullying>
 - **En caso de menores de edad, al no estar en edad penal, es más complejo**
 - Enumeraremos posibles formas de actuar según la **AEPAE**: <https://aepae.es/protocolo-de-actuacion>
 - Esto es una guía general, debes **consultar el correspondiente a tu comunidad autónoma**

MECANISMOS DE ACTUACIÓN FREnte AL BULLYING EN RRSS

- En caso de mayores de edad / alumnos de universidad es un delito
- Como vimos, es necesario **consultar el reglamento disciplinario**, de convivencia o similar
 - Ej. (Universidad de Oviedo):
https://secretaria.uniovi.es/c/document_library/get_file?uuid=394c7515-0812-4c23-ac09-4849b43614d6&groupId=952290
- **Informar a la víctima de sus derechos** a través de este
 - Lugares a los que puede acudir, procedimientos de actuación y recopilación de evidencias...
 - Recordar al alumnado que, al no ser menores, **sus actos pueden repercutirles en problemas legales serios**
 - Si el reglamento no aplica o cubre el caso, es necesario que la víctima **denuncie ante las autoridades**



Hay algo en algún reglamento que te ayudará. Hay que dar con ello...

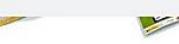
PROCEDIMIENTO DE ACTUACIÓN POR BULLYING Y OTROS PROBLEMAS

- **Motivo:** El ciberacoso es una lacra muy grave que debe atajarse lo antes posible
 - Por las consecuencias tan terribles para las víctimas
- **Solución:** Si has detectado un caso de ciberacoso en menores...
 - Busca el **protocolo de tu comunidad**
 - Para proceder a parar el problema lo antes posible y denunciarlo si es preciso
 - Cuanto más tiempo tarde, más envalentonará el acosador y se puede agravar el problema
 - Pero hay **más variantes de problemas online**
 - Tenemos que buscar información sobre cómo tratarlos
 - <https://www.tepongounreto.org/2022/07/lineas-de-ayuda-dirigidas-a-infancia-y-adolescencia-para-denunciar-o-solicitar-ayuda-ante-el-ciberacoso-y-otros-riesgos-online/>
 - <https://www.incibe.es/menores/>

is4k INTERNET SEGURA FOR KIDS

INCIBE INCIBE-CERT CIUDADANIA MENORES EMPRESAS EVENTOS ESPAÑA DIGITAL 2026

Blog Educadores Familias Jóvenes Te ayudamos Recursos Juegos Temáticas Hotline



Guía control parental
Guía de herramientas de control parental, de utilidad para reducir riesgos a medida que el menor aprende a...



Guía infancia
Guía de uso seguro y responsable de Internet para profesionales de servicios de protección a la infancia.



Guía de RRSS
Guía de seguridad en redes sociales para comprender por qué les gustan tanto a los jóvenes.



Guía de mediación
Guía de mediación parental para la educación en seguridad y responsabilidad digital de tus hijos.



Guía de juguetes
La guía de juguetes conectados está formada por 7 fichas que recogen las principales recomendaciones para las...



Guía de Privacidad
La guía está formada por 18 fichas que recogen los principales riesgos a los que nos exponemos al hacer uso de Internet.



Herramientas control parental
Catálogo de herramientas de control parental con información, capturas de pantalla e instrucciones



Preguntas frecuentes
¿Tienes alguna duda respecto de la seguridad de los menores en Internet? ¿Te preocupa que puedan estar en...

El INCIBE tiene manuales para todo lo que necesites aprender del mundo online, de forma gratuita

PROCEDIMIENTO DE ACTUACIÓN POR BULLYING Y OTROS PROBLEMAS

● ¿Y qué hacer si no es exactamente acoso, sino otro problema online?

- Es difícil estar al día...
- Pero si es necesario saber **dónde acudir a buscar información**
- En la web anterior vimos formación sobre determinados problemas

● El INCIBE tiene también un **apartado de preguntas y respuestas para problemas varios con menores**

- <https://www.incibe.es/menores/ayuda/preguntas-frecuentes>
- Es muy importante consultarla para saber qué hacer si estamos en el caso que contempla alguna de estas preguntas

¿Tu hijo está asustado por un reto viral?

Está raro, ¿cómo puedo saber si tiene algún problema online?

Está sufriendo ciberacoso, ¿cómo puedo actuar?

Ha compartido una foto desnudo, ¿qué puedo hacer?

Está enganchado en Internet, ¿cómo le puedo ayudar?

¿Cómo puedo saber lo que hace en Internet?

Está hablando con desconocidos por Internet, ¿qué puedo hacer?

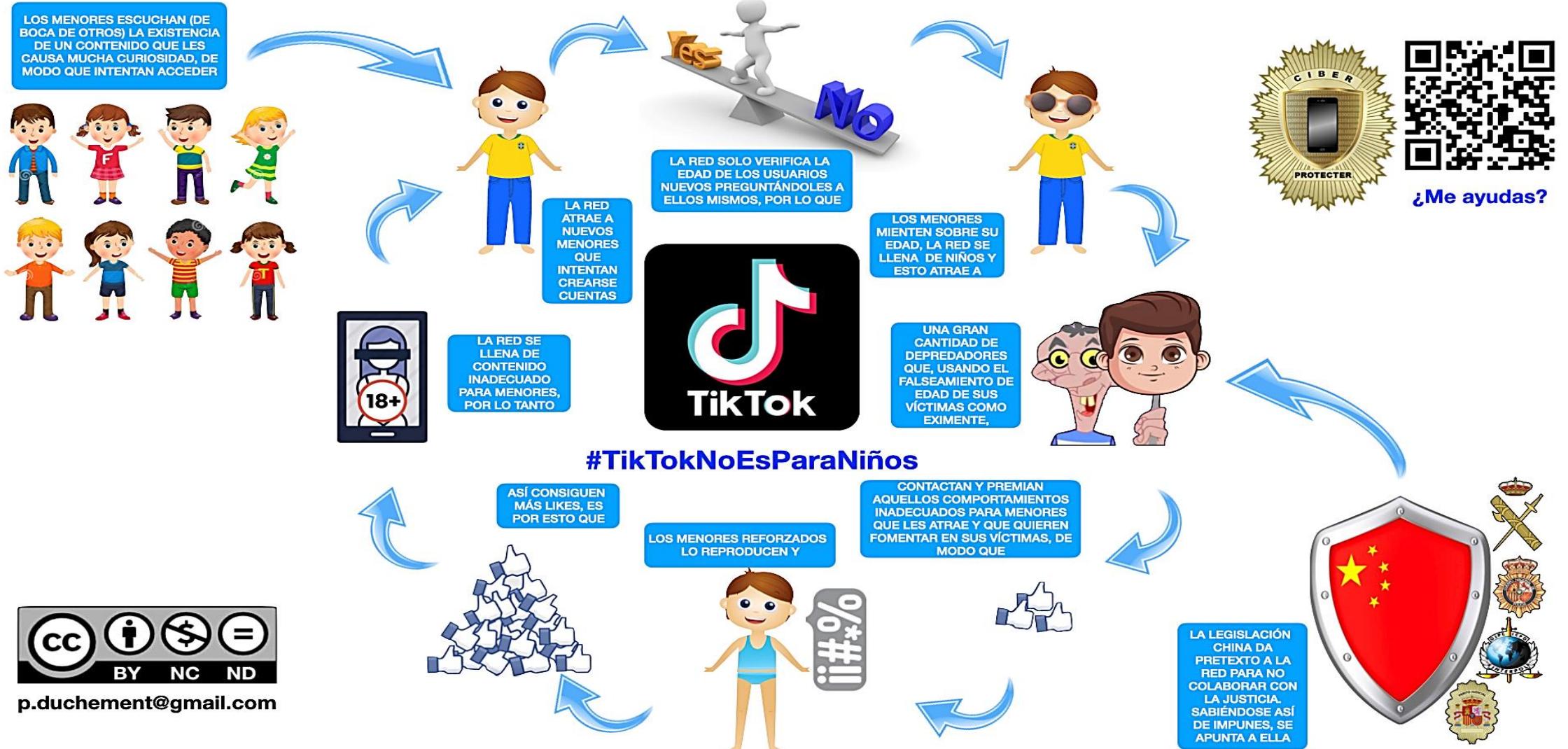
Se está interesando por temas de riesgo como perder peso, ideas extremistas, grupos violentos, ¿cómo le puedo ayudar?

Se hacen pasar por mi hijo o hija en las redes sociales, ¿cómo puedo actuar?

Merece la pena echarle un ojo a la página de preguntas del INCIBE, porque están todas las más frecuentes e importantes

PROCEDIMIENTO DE ACTUACIÓN POR BULLYING Y OTROS PROBLEMAS

- TikTok es una red especialmente problemática en este sentido, ¡cuidado!



MECANISMOS CONTRA EL BULLYING EN RRSS CON MENORES

- En caso de que la víctima sea menor (hijo, familiar...), es bueno conocer cómo actuar para ayudarle

- El bullying a través de medios electrónicos es muy común: **para mí es parte de la ciberseguridad**

- Veamos el protocolo general de la AEPAE mencionado antes

1. **Establecer una vigilancia “pasiva” en redes sociales**

- Una de las primeras medidas es **vigilar lo que hace y lo que le dicen**
 - Desde otra cuenta que creemos para nosotros en la misma red social, salvo que sea contenido público
 - Idealmente pasando desapercibido...
- Pero tendremos problemas si **establece su cuenta como privada**
 - Tendríamos que hacer que nos permita seguirlo, pero entonces cohibiremos sus interacciones
 - O si tiene **grupos ocultos de contactos** con los que comparte solo determinados contenidos
 - No obstante, la vigilancia “desde lejos” en la medida de lo posible puede detectar muchos problemas

2. **Hacer vigilancia activa y permanente en la vida real**

- Siempre ante **posibles señales que puedan alertarnos** de que se está produciendo acoso
- Disminución del rendimiento escolar, pérdida o robo de material escolar, cambios de humor repentinos, temor a ir a clase, insomnio, lesiones físicas...

MECANISMOS CONTRA EL BULLYING EN RRSS CON MENORES: CUANDO EL ORIGEN ESTÁ EN LA ESCUELA

3. Establecer y fomentar un clima de confianza

- Para que puedan **comentarnos cualquier problema** que tengan abiertamente
- Dedicarle tiempo a **interesarte cómo le ha ido el día** y en el colegio
- Poner límites en su comportamiento diario y **asignales tareas** para fomentar responsabilidad y autoestima
 - Felicitándoles cuando las cumplan y explicándoles las consecuencias de no cumplirlas
 - El refuerzo positivo fomenta la confianza y que nos puedan contar cosas abiertamente
- **Enséñales a mostrar sus sentimientos sin temor** y a expresarse de una **manera asertiva**
 - Decir claramente lo que les gusta y no les gusta, sin uso de la violencia

4. Conocer el posible origen de los problemas

- Es demasiado frecuente que los casos de bullying por RRSS **se originen en algo que pasó en la escuela**
- No importa qué, **nada justifica el acoso** (es una excusa para el bully)
- En ese caso los **bullies** son sus propios compañeros de clase
 - Y el acoso ocurre tanto en redes sociales como en el centro escolar
 - La víctima no puede "escapar" y se ve sometido potencialmente a **acoso 24/7**
- Por ello daremos unas recomendaciones a tomar en relación al centro escolar

MECANISMOS CONTRA EL BULLYING EN RRSS CON MENORES: CUANDO EL ORIGEN ESTÁ EN LA ESCUELA

5. Vigilancia escolar ante incidentes

- Pide una tutoría para ver que ha ocurrido con el menor si descubres que ha habido problemas en el colegio
- Comprueba que el episodio **es puntual** (maltrato verbal, físico o psicológico), y **no vuelve a producirse**
 - Un episodio aislado es “normal”, especialmente con niños/as pequeños
 - **El problema es si se cronifica**
- Anima al menor para que no permita que vuelvan a producirse estos episodios puntuales y a **que los ponga en conocimiento del profesorado y los cuente al llegar a casa**
- **Dale herramientas de defensa personal verbal y física**
 - CUIDADO: Eso no implica enseñarle a pegar y a abusar del atacante
- Hazle saber **que puede contar contigo** y que vas a estar siempre con el/ella para ayudarle



MECANISMOS CONTRA EL BULLYING EN RRSS CON MENORES: CUANDO EL ORIGEN ESTÁ EN LA ESCUELA

6. Acciones a tomar por la familia cuando el incidente no es puntual

- Habla con el/ella y **recopila toda la información posible**
 - Qué está ocurriendo, desde cuando ocurre, donde ocurre, y quien o quienes están acosando...
- Con esta información haz una **cronología de los hechos**
- Adjúntale, si los hubiese, **partes de lesiones**, o **informes médicos** del psicólogo y/o psiquiatra
 - Que el menor haya necesitado a consecuencia del maltrato
 - Esto deja más clara la importancia del problema
- Ahora es cuando debes **pedir urgentemente una reunión con el tutor o tutora del menor**
 - Para poner en su conocimiento todos los hechos y aportar la documentación
- Y pedirle al centro escolar que **haga una investigación** de los hechos denunciados y que proteja al menor
- Concierta una **segunda cita** a la semana siguiente, para informarte



La familia tiene que arropar a un niño acosado

MECANISMOS CONTRA EL BULLYING EN RRSS CON MENORES: CUANDO EL ORIGEN ESTÁ EN LA ESCUELA

7. Acciones a tomar por el centro cuando el incidente ya no es puntual

- En esta **segunda reunión**, el colegio tiene la obligación de **informar de las medidas de protección** que se han puesto en marcha
 - También de las medidas sancionadoras activadas, si fuera el caso
- El centro debe mostrarte el **protocolo de actuación oficial** que tiene que abrir obligatoriamente
 - El protocolo de actuación **NO** es confidencial para las familias implicadas
- En una **tercera reunión** la familia debe transmitir al centro la satisfacción o desaprobación del proceso
 - Tras valorar la evolución de la situación de la víctima
 - Debe primar la protección de la víctima y la sanción educativa
- En el caso de que **la situación persista**, se debe acudir con toda la documentación a **inspección educativa**
- **Si no se arreglase la situación**, hay que interponer una **denuncia por vía civil y/o vía penal**



El profesorado debe ponerse de parte del acosado, nunca del acosador

¿CÓMO SABER SI LO HAS ENTENDIDO TODO? RESPONDE ESTO

?

- *¿Tienes claro que la víctima nunca tiene la culpa del delito, y que es el delincuente el que ha decidido delinquir?*
- *¿Tienes claro también que nada que la víctima lleve puesto, haga, etc. justifica un delito?*
- *¿Eres consciente de que compartir demasiada información en la red puede atraer por igual a estafadores/as y acosadores/as?*
- *¿Entiendes que proteger a una víctima indefensa de acoso es posible y la forma correcta de proceder?*
- *¿Entiendes cómo actuar en caso de acoso escolar a menores y los pasos a seguir?*
 - *¿Comprendes que estos pasos implican un seguimiento de cerca y continuo del caso y no simplemente una acción puntual?*



Mecanismos de ciberdefensa personal

No dejes al bully entrar en tu vida a través de tus redes sociales



No ACEPTAR NUNCA MENSAJES PRIVADOS DE DESCONOCIDOS

● **Motivo:** Los mensajes que nos envían desconocidos en redes sociales son casi siempre intentos de inicio de estafas

- Salvo que haya un interés particular en ti por tu actividad o por algo que hayas dicho, **es muy raro** que un desconocido se ponga en contacto contigo
- Estos mensajes privados **empezarán de forma amable** para ir “liándote” y luego pasar al objetivo concreto que pretende el estafador
- **Pero así también empiezan muchos acosos:** en este caso “liarte” es para que reveles información que luego puedan usar contra ti

● **Solución:** Bloquea inmediatamente cualquier mensaje que te envíe un desconocido por internet

- Mejor aún, configura tu RRSS para **no permitir mensajes de desconocidos**
- **Más información**
 - <https://www.lavanguardia.com/tecnologia/20210204/6218135/evita-spam-instagram.html>
 - <https://maldita.es/timo/bulo/20220609/mensajes-privados-instagram-hackeo-cuentas/>

←  Toreau

Hoy

Encantado de conocerlo.
Mi novia quiere conocer
un hombre maduro y
tranquilo. Actualmente es
soltera y le gusta viajar,
los libros, los deportes y la
comida. Si es un hombre
maduro mayor de 28 años,
si desea conocer, agregue
el WhatsApp de mi novia:
wa.me/60192143152

4:09 p. m.

**Sin comentarios... (pero
cuidado, que los hay
mucho mejores)**

No ACEPTAR NUNCA MENSAJES PRIVADOS DE DESCONOCIDOS

- Hay una gran cantidad de fraudes que empiezan de esta forma, ten cuidado
 - En cualquier red social
 - En la imagen ves un robo de cuenta típico
 - Pero recuerda: **muchos acosos empiezan también de esta forma**



La cantidad de mensajes privados con fraudes que llegan hoy en día en las redes sociales es demencial 😱. Pues ahora súmale si es un conocido tratando de sonsacarte cosas para luego extorsionarte, por ejemplo

QUÉ HACER SI NOS METEN EN LISTAS CONTRA NUESTRA VOLUNTAD

- **重要原因:** A veces en RRSS nos sale una notificación de que alguien nos acaba de incluir en una lista o grupo
 - Muchas veces es algo **inocuo** y se trata de alguno de nuestros contactos clasificando los suyos
 - Pero muchas veces esto se hace para luego **usar ese grupo para escribir mensajes** que estén relacionados con alguna clase de **estafa**
- **Solución:** Si te notifican que has sido añadido a algún grupo de usuarios sin tu consentimiento salte de él ya
 - Si ves que es algo fraudulento, **denuncia al grupo o a su creador**
 - Debería haber una opción en tus RRSS para hacer ambas cosas
 - También opciones para que nadie pueda meterte en ningún grupo **sin tu consentimiento**



Alguien sin mediar aviso me añadió a una lista mientras usaba Twitter: Era un timo. Es muy común

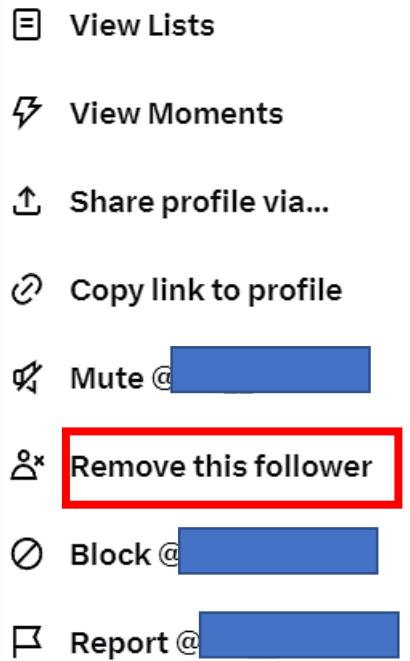
SOFT BLOCKS EN REDES SOCIALES

• **Motivo:** A veces seguimos a una persona cuyo contenido nos molesta, pero no queremos bloquearla directamente

- El principal motivo es que **los bloqueos son visibles** para la otra persona, y se puede enfadar
 - Lo que necesitamos es que esa persona **nos deje de seguir**
- Siempre podemos dejar de seguirlo nosotros, pero *¿Cómo conseguir que sea él el que lo haga también?*

• **Solución:** Investiga si la RRSS tiene un mecanismo de "soft block"

- De forma que tu cuenta y la de la otra persona **ya no os sigáis mutuamente**
- A veces la opción existe directamente
 - Otras veces se consigue con un truco (Ej.: bloquear y desbloquear a la persona de seguido)
- Siempre le podrás echar la culpa a un fallo de la red social ☺



"Soft blocks" en Twitter. Otras redes tienen mecanismos parecidos

CADENAS DE “HATE”

- En ciertas redes sociales (ejem...Twitter*...ejem) es mucho más probable que algo que digas te genere una cadena de “hate”
- Lo que se traduce en
 - **Insultos** por parte de muchos desconocidos
 - **Seguimiento masivo de bots**: Persiguen “tumbar” la cuenta a base de reportes o por tener un perfil sospechoso
 - **Reportes masivos** organizados por grupos
- Lo único que realmente se puede hacer es ponerte “candado” (cuenta privada)
 - Y esperar a que pase el “chaparrón” (sí, se olvida todo en unos días)
 - O desactivar la cuenta (tienes 30 días para volver, pero consulta porque depende de la red social y cambia a veces)



*Asúmelo, nadie le llama X. Bueno sí, igual Elon Musk...pero seguro que la llama Twitter en la intimidad ☺

CERTIFICACIÓN DE MENSAJES DE RRSS

• **Motivo:** A veces debes certificar un mensaje de una RRSS

- Para usarlo por ejemplo **en un proceso judicial**
- Hay empresas que te ofrecen este servicio
 - Incluso gratuitamente para usos esporádicos

• **Solución:** Certifica los mensajes que quieras usar como prueba judicial

- **Egarante** (<https://www.egarante.com/>) lo permite
 - <https://twitter.com/RubenSanchezTW/status/1206898976496267264?s=20>
- **Para certificar por ejemplo un tweet** debes
 - Enviar un correo a websigned@egarante.com
 - En el asunto pones la URL del tweet
 - Recibirás un correo con **la certificación en PDF**
 - Funciona también para Facebook
 - Y otras redes que puedan verse vía web
 - Hasta **2 gratis al día**
 - Esto evitaría que su borrado sirva al autor para eludir que prospere una causa judicial contra él



CERTIFICACIÓN DE MENSAJES DE RRSS



eG Web

eGarante te proporciona una prueba del contenido de una web o de una red social en un momento determinado.

Certificamos:

- La url a la que accedemos.
- El contenido realizando una captura de pantalla que incluye los enlaces existentes en la página
- La fecha y hora a la cual accedimos a la página.
- Informamos del hecho de que lo hacemos desde unos servidores no manipulables por el interesado

[Ampliar información](#)[Contratar](#)

eG Mail

Te proporcionamos una prueba de los correos electrónicos que envías desde tu cuenta de email. Certificamos:

- Envío
- Contenido incluyendo adjuntos
- Destinatarios
- Fecha indubitable de certificación
- Entrega al servidor de correo del destinatario de una copia idéntica del mensaje original

[Ampliar información](#)[Contratar](#)

eG Doc

Somos testigos de la entrega de los documentos que envías y también de la aceptación del destinatario. Certificamos:

- Envío
- Documento
- Destinatario
- Entrega del documento al servidor de correo electrónico del destinatario
- Respuesta del destinatario
- Fecha indubitable de envío y respuesta
- Dirección IP de la respuesta
- Identificación del destinatario mediante PIN enviado a su email o móvil

[Ampliar información](#)[Contratar](#)

eG Webtrack

Hacemos un seguimiento certificado de las páginas web que nos indiques, tuyas o de terceros durante un periodo de tiempo.

Certificamos:

- La url a la que accedemos
- El contenido realizando una captura de pantalla incluyendo los enlaces existentes en la página
- La fecha y hora a la cual accedimos a la página
- Informando del hecho de que lo hacemos desde unos servidores no manipulables por el interesado en un momento del tiempo aleatorio
- Adicionalmente emitiremos un certificado resumen del proceso.

[Ampliar información](#)[Contratar](#)

eG Inbox

Te ofrecemos un buzón de correo electrónico nuevo en el que certificamos todos tus correos enviados y recibidos sin que tengas que preocuparte por nada. Certificamos:

- Envío o recepción
- Contenido incluyendo adjuntos
- Destinatarios y emisor
- Fecha indubitable de certificación
- Entrega del mensaje original al servidor de correo del destinatario
- Además te daremos un resumen de los correos enviados y recibidos al final de cada mes.

[Ampliar información](#)[Contratar](#)

Esta empresa tiene una gran variedad de servicio para recabar evidencias si las necesitas

¿CÓMO SABER SI LO HAS ENTENDIDO TODO? RESPONDE ESTO

?

- *¿Comprendes que aceptar mensajes de desconocidos es realmente equivalente a entablar conversaciones con desconocidos por la calle a nivel de peligrosidad?*
- *¿Entiendes por qué no debes aceptar que te introduzcan en listas contra tu voluntad?*
- *¿Comprendes que para no "quedar mal" el soft block muchas veces es mejor opción que el "block" normal?*
 - Siempre le puedes echar la culpa a un "error informático" de la plataforma ☺
- *¿Entiendes la terrible situación de acoso de las "cadenas de hate", que son ataques organizados, y que para aguantarlos debes "blindarte"?*
- *¿Comprendes lo que debes hacer en caso de tener que denunciar a alguien por algo que te ha dicho en RRSS?*



Lo último que un acosado necesita es sentirse solo. Fuente: Bing Chat AI

Acoso avanzado en redes sociales

Cuando el delincuente va con todo y las defensas no sirven...y esta vez ya no hablo solo de menores



RECONOCER Y PREVENIR EL ACOSO AVANZADO EN REDES SOCIALES

• **Motivo:** Las redes sociales en la actualidad son herramientas de acoso que pueden ser terribles

- El acoso puede alcanzar **niveles de sofisticación muy elevados**
- Si no estamos preparados para entender estas dinámicas de acoso moderno, es probable que no seamos capaces de verlo hasta que sea tarde

• **Solución:** Aprende las dinámicas de acoso actuales para que puedas identificarlas y ayudar a las personas acosadas

- Estas dinámicas se asocian más a jóvenes, pero **también se dan en adultos**
 - Te sorprendería la de patrones que te voy a describir que se reproducen en gente "senior"
- Las personas acosadas **suelen esconderlo**: desesperación, vergüenza, amenaza...
 - Solo nos enteraremos cuando la situación explota (**intento autolítico**) o por desesperación
- Aunque tengas confianza con la persona acosada, la probabilidad de que te lo cuente todo **es baja**
 - El acoso va asociado a una "**ley del silencio**"
 - Es decir, el entorno no habla del acoso hasta que es evidente o pasa algo
 - La **fama o reputación** de un centro de estudios o de un grupo de investigación es muy importante
 - Suele ponerse por encima del bienestar individual

RECONOCER Y PREVENIR EL ACOSO AVANZADO EN REDES SOCIALES



José Manuel
Redondo López

● El acoso se manifiesta de la siguiente forma

- Al acosado **se le hace el vacío**
 - Por estar de acuerdo, por miedo a ser un acosado más o para no implicarse por miedo a las consecuencias
- Una persona acosada a la que nadie habla se desespera y **puede caer en dinámicas destructivas**
 - Las personas más jóvenes tienen menos recursos para resistirse a un intento autolítico



El acoso por aislamiento puede ser devastador. Si supervisas a alguno, es necesario observar para ayudar y prevenir. Fuente: Microsoft Copilot

Reconoce el CIBERACOSO ESCOLAR a tiempo



¿Cómo afecta a mis alumnos/as?

Tu papel es clave. Implicate en su detección y resolución.



El 16%

de los menores españoles afirma haber sufrido ciberacoso a través de Internet.



1 de cada 5
admite haber acosado a un compañero/a.

*Datos pertenecientes al informe EU Kids Online 2020.

¿Cómo lo identifico?

Ahora el acoso escolar o ciberbullying también se produce en las redes sociales y otros espacios de comunicación en línea.



Debo prestar atención a...

Cambios de conducta y/o actitudes ofensivas hacia un menor.

Burlas continuadas o bromas de mal gusto.

Nuevas amistades o aislamiento social evidente

Modificación de estatus, liderazgo o popularidad.

Rechazo de la tecnología, el uso de Internet o las redes sociales.

Reacciono ante el ciberacoso

Muestro mi rechazo firme ante burlas, bromas o ataques entre alumnos/as.

Si escucho comentarios sobre una actividad negativa en las redes sociales, converso con ellos/as al respecto y aclaro la veracidad de los hechos.

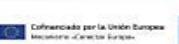
Ofrezco un espacio de comunicación seguro, donde puedan contarme sus dudas o problemas en la Red.

Les transmito cómo actuar contra el ciberacoso en Internet: bloquear y reportar está en sus manos.

Me coordino con los equipos de convivencia y orientación para dar una respuesta eficaz.

Hablo a mis alumnos/as de los servicios de ayuda existentes, como la Línea de Ayuda en Ciberseguridad de INCIBE, 017.

www.is4k.es/ciberacoso



RECONOCER Y PREVENIR EL ACOSO AVANZADO EN REDES SOCIALES

● Sobre los grupos de redes sociales y de mensajería

- El **volumen de mensajes** de estos grupos puede ser altísimo
 - Leérselos todos para detectar que alguien está acosando a otros es muy complicado
 - Esto es especialmente cierto en **grupos “para hacer trabajos” de estudiantes**
- El acoso por “**aislamiento virtual**” en esos grupos
 - **Nunca se contesta** a peticiones de determinadas personas (los acosados)
 - Es un “vacío virtual” que se une al físico
 - Hay ciertas personas a las **que todos contestan**, dan su aprobación u opinión
 - Lo que contrasta con lo anterior y contribuye al aislamiento
 - Un acosado **no suele interpretar este aislamiento como acoso**,
 - Por lo que no lo cuenta
 - Esta es la razón principal por la que te louento yo...
 - El acosado **se siente muy mal y se sigue encerrando en sí mismo**
 - Pensando que es su problema porque nadie le habla
 - Sin detectar que es víctima del maltrato



Los grupos de mensajería a veces son un auténtico sumidero de lo peor de la humanidad...

RECONOCER Y PREVENIR EL ACOSO AVANZADO EN REDES SOCIALES

● El acoso por “bromas”, contestaciones “faltosas” (Ej.: falacias ad hominem), etc.

- La “ley del silencio” **se complementa** con bromas de mal gusto, desacreditaciones
 - O ignorar mensajes que el acosado ha dicho y solo validar cuando lo dice otro (aunque sea el mismo)
- **Los acosadores ya habrán hecho el “trabajo” de arruinar la reputación del acosado**
 - El acosador por lo que tendrá a mucha gente a su favor (probablemente sea narcisista)
 - Nadie quiere hablar con “el/la rarito/a”
- Estos mensajes además suelen borrarse periódicamente para no dejar rastro

● El acoso específico por redes sociales

- Recortar fotos del acosado para hacer “memes” y “bromas” de pésimo gusto
- Hacer reels de Instagram con contenido vejatorio que no quedan registrados (**caducan rápidamente**)

● Respeto a los protocolos anti-acoso

- Muchos quedan simplemente en “papel mojado”
- **La mediación** que se ofrece suele no ser efectiva y se queda en meras palabras
 - Un problema tan grave rara vez se puede arreglar así
- **La culpa de un acoso nunca es del acosado**, y **el acoso está MUY PRESENTE** en nuestro entorno

SOBRE LA SUBIDA DE FOTOS DE PERSONAS A LAS REDES

- **重要原因:** No debes subir fotos de personas a las redes sociales sin su consentimiento (especialmente grave en menores)
 - No sabes en qué situación se encuentran ni las consecuencias que les pueden traer
 - **Huella digital:** Cada foto que se sube a Internet deja una huella digital
 - Que puede ser difícil de eliminar
 - Puede tener consecuencias a largo plazo
 - Las fotos pueden seguir accesibles mucho tiempo (Ej.: Wayback Machine)
- **Riesgos psicológicos:** Las personas pueden sentirse incómodas o avergonzadas si se comparten detalles íntimos de su vida
 - Lo que también puede ser otra forma de acoso avanzado
- **Efectos legales:** Compartir fotos en las redes sociales puede atentar el **derecho a la intimidad**
 - *¿Has pensado que pasaría si compartes la foto de alguien que está en una situación de maltrato conyugal?*
- **Ciberacoso:** Las fotos pueden ser utilizadas por ciberacosadores
- **Uso indebido de las imágenes:** Potenciado por el uso de la IA actual
 - Suplantación de identidad, uso indebido de las imágenes (falsificaciones, porno deep fake, **sextrusión**...)

SOBRE LA SUBIDA DE FOTOS DE PERSONAS A LAS REDES

- **Solución:** Pide permiso antes de subir una foto de nadie a una red social

- Por las consecuencias que puede llegar a tener para algunos de los que aparecen en ellas
 - <https://twitter.com/DerechodelaRed/status/1689895503025012736?s=20>
- **Video explicativo sobre menores**
 - <https://twitter.com/i/status/1689895503025012736>
- **Influencer que explica los peligros del sharenting**
 - <https://x.com/MellamanSil>



Por favor, piensa en las consecuencias de subir fotos de tus hijos en RRSS (el “sharenting”). Nunca las subas de otro, y recuerda que el mundo está lleno de degenerados y las aplicaciones de las IAs dan verdadero miedo 😊

¿CÓMO SABER SI LO HAS ENTENDIDO TODO? RESPONDE ESTO



- *¿Entiendes que una víctima de acoso avanzado va a tender a ocultarlo por defecto?*
- *¿Comprendes que el entorno del acosador, aunque sea consciente del problema, no habla del mismo para no implicarse?*
- *¿Eres consciente de que una técnica de acoso típica es el "aislamiento virtual" motivado por la mala prensa que el acosador propaga del acosado?*
 - *¿Entiendes que si eres partícipe de este tipo de prácticas sin conocer la historia de "la otra parte", en el fondo eres cómplice del acoso?*
- *¿Entiendes que una broma entre partes en la que una de las partes no se ríe (o lo hace visiblemente forzado/a), no es una broma?*
 - *¿Has entendido que hacer memes de un tercero sin consentimiento es una forma de acoso?*
- *¿Entiendes que nunca debes compartir fotos de alguien sin consentimiento?*



Un afectado por sextorsión necesita el apoyo de su entorno para evitar males mayores. Fuente: Bing Chat AI

Sextorsión

Cuando el acoso se vuelve personal



EL PROBLEMA DE LA SEXTORSIÓN

-  **Motivo:** Tipo de extorsión donde un delincuente obliga a la víctima a proporcionarle materiales / favores sexuales o dinero
 - Bajo amenaza de distribuir material confidencial de la víctima, que también podría ser de tipo sexual
 - Es una forma de explotación sexual en la cual una persona es inducida o chantajeada con imágenes o videos de sí misma desnuda o realizando actos sexuales
 - Si recibes material gráfico así y lo difundes, **es un delito**
 - https://www.elconfidencial.com/tecnologia/2019-05-29/sextorsión-suicidio-mujer-video-sexual-delitos-acoso_2041114/
 - La víctima es coaccionada para
 - Tener relaciones sexuales con alguien
 - Entregar más imágenes eróticas o pornográficas, dinero o alguna otra contrapartida
 - Bajo la amenaza de difundir las imágenes originales si no accede a las exigencias del extorsionador
 - Es importante tener en cuenta que este tipo de delito **puede tener graves consecuencias psicológicas** para las víctimas y puede ser especialmente dañino
 - Especialmente para los adolescentes y los jóvenes, pero en realidad para todo el mundo
 - <https://www.elmundo.es/madrid/2019/05/28/5ced493efddff0758b48fb.html>
 - <https://cnnespanol.cnn.com/2023/05/13/gavin-guffey-suicidio-estafa-de-sextorsión-ley-trax/>

EL PROBLEMA DE LA SEXTORSIÓN

- Para que te des cuenta de las consecuencias puedes ver un caso real
 - <https://twitter.com/Maylenchan/status/1693591787695173785?s=20>
 - Se trata de una estafa que se origina pidiendo nudes (fotos de la víctima desnuda para hacer sexting)
- Ocurrió de esta forma
 - Una víctima conoce a alguien (el delincuente) a través de una aplicación de citas
 - Tras un tiempo de contacto, pasa a hacer llamadas con el delincuente
 - En un momento dado, el supuesto interés amoroso le pidió que se desnudase, y la víctima accedió
 - Poco tiempo después **empezó a recibir intentos de extorsión desde perfiles falsos**
 - Para no revelar esos nudes a su entorno
 - Con la desesperación, la víctima **cedió a la extorsión** y les ingresó dinero
 - Pero le pidieron más (son delincuentes, ¿crees que van a tener palabra?)
 - Al final, enviaron esas fotos igualmente
 - La víctima fue a la policía, que consideró el caso poca gravedad y le dieron cita para más adelante
 - La víctima se suicidó porque su estado mental no le permitió aguantar la presión

EL PROBLEMA DE LA SEXTORSIÓN



José Manuel
Redondo López

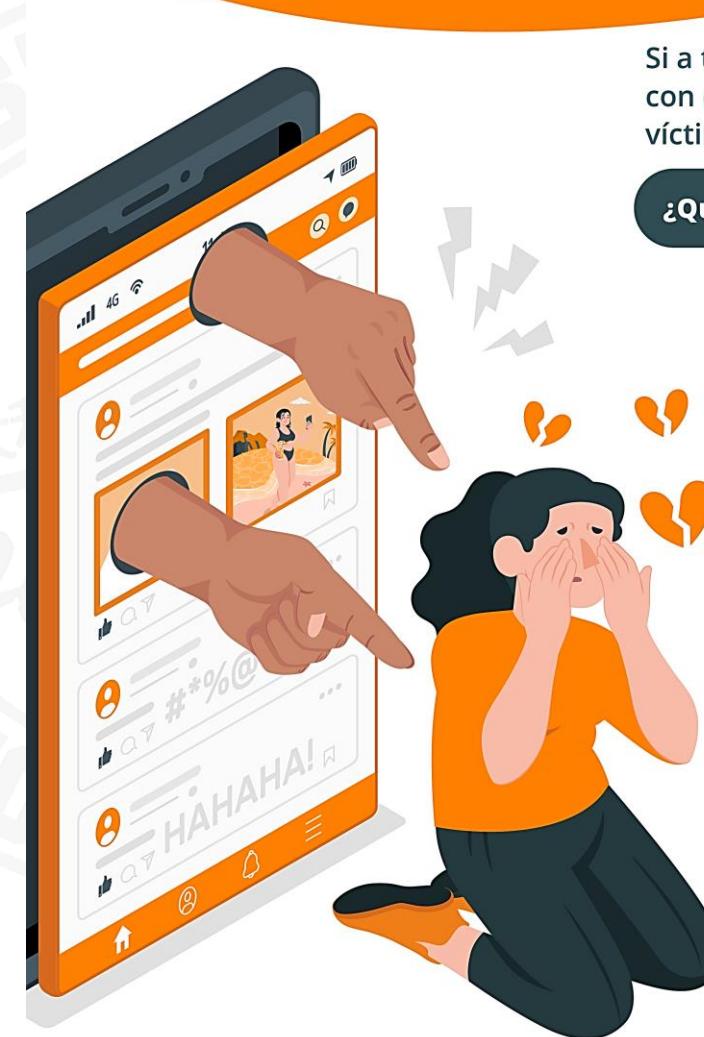
Sextorsión: El chantaje de las imágenes comprometidas

- **Recuerda: Si compartes algo pierdes el control de lo mismo**

- Medita los usos que pueden hacer de lo que compartes con alguien, aunque parezca de confianza

- **¿Necesitas más información?**

- <https://www.incibe.es/aprendecer/seguridad/sextorsion>
- <https://www.incibe.es/node/486964>



Si a través de un email o mensaje te amenazan con exponer fotos íntimas tuyas, estás siendo víctima de sextorsión.

¿Qué debes hacer si te ves en una situación así?

-  No cedas al chantaje, si lo haces, es probable que te sigan amenazando.
-  Cortar el contacto con el extorsionador.
-  Captura y guarda las pruebas de chantaje para denunciarlo ante FCSE (Fuerzas y Cuerpos de Seguridad del Estado).

Y si envías imágenes o videos comprometidos tuyos... no te juzgues. Simplemente ten en cuenta los riesgos a los que te expones realizando este tipo de contenido, si llega a caer en malas manos.

#OSIconsejo

incibe.es/ciudadania

EL PROBLEMA DE LA SEXTORSIÓN

● **Solución:** Entiende la gravedad de estos delitos y cómo actuar contra ellos

- Se trata de un ataque que sufren ambos géneros, y **no importa la edad ni la condición social**
- La forma de conseguir videos o fotos para comenzar la extorsión varía
- **Creándolo a partir de una foto real de la víctima e IAs (porno deepfake)**
 - Todo lo que el delincuente tiene de la víctima es falso, pero teme la reacción de su entorno si se distribuye
 - <https://elpais.com/tecnologia/2023-09-18/de-rosalia-al-instituto-la-inteligencia-artificial-generaliza-la-creacion-de-imagenes-pornograficas-no-consentidas.html>
 - <https://elpais.com/tecnologia/2023-09-21/todos-podemos-ser-victimas-y-los-danos-son-irreparables-como-los-deepfakes-han-inundado-el-planeta.html>
- **Por ingeniería social en aplicaciones de citas:** Personas con las que “ligas” y que te mandan su móvil privado para seguir la conversación (**eliminando la supervisión de la aplicación de citas**)
 - La persona actúa/habla de forma extraña (hay bots conversacionales orientados a este fin)
 - El móvil es extranjero, pero te dice que vive en España
 - Nunca envía audios (aunque con los deepfakes de voz esto no es una razón de desconfianza válida)
 - Te solicita intercambiar fotos sugerentes o videos (**sexting**)
 - Los tuyos serán reales, los de el/ella...no (robados, porno deepfake...)

EL PROBLEMA DE LA SEXTORSIÓN



José Manuel
Redondo López

• Fotos temporales

- Instagram, WhatsApp, Snapchat o Telegram permitan enviar fotos temporales
- Pero la otra persona las puede guardar igualmente (**¡no te fíes!**)
 - Grabar pantalla a través del ordenador, con otro dispositivo...

• Tras una extorsión inicial

- Quizás el delincuente sabe algo comprometido de ti, ha conseguido acceso a alguna foto (o se la han enviado) o pide más para “comprar” su silencio
- El silencio no se compra, solo se alquila por un tiempo:** Te tiene en su poder y volverá a hacerlo
 - Si no tiene escrúpulos para hacerlo la primera vez, nada le impedirá hacerlo más veces

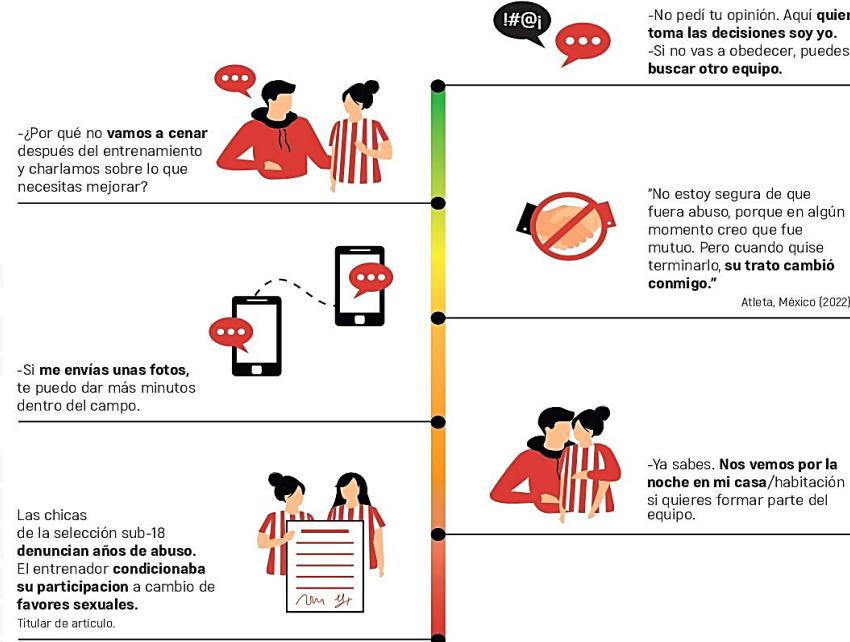
• Robo de cuentas y dispositivos

- Si no nos protegemos, podrían infectar nuestro móvil o PC y acceder a sus fotos
- O incluso acceder a su cámara

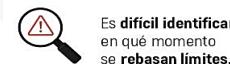
¿ACOSO? ¿ABUSO? ¿CORRUPCIÓN?

O SIMPLEMENTE CONDUCTAS DEPORTIVAS NORMALIZADAS

¿HAS VISTO O TE HA PASADO ALGO DE ESTO?



LA EXTORSIÓN SEXUAL TIENE MUCHOS MATICES



Es difícil identificar en qué momento se rebasan límites.



I#@ Dando pie a culturas de abuso encubierto.



El deporte es un esfuerzo mutuo por alcanzar la excelencia y no tiene porqué implicar abusos.

DENUNCIA CUALQUIER CONDUCTA QUE SOBREPASE LOS LÍMITES DE TU CONSENTIMIENTO EN: aterpe@athletic-club.eus

*Fuente: "Sextortion in Sport. An International Examination on this Silent abuse of Power" Whitney Bragagnolo y Yanet Lezama

Aunque es para el mundo del deporte, se puede aplicar a otros perfectamente. Fuente:
<https://www.athletic-club.eus/noticias/2022/11/25/aterpe-conciencia-contra-la-sextorsion-en-el-deporte>

EL PROBLEMA DE LA SEXTORSIÓN: QUÉ HACER



José Manuel
Redondo López

- **No envíes NADA comprometido a NADIE por RRSS**
 - Ni, por supuesto, por cualquier otro medio
- **Si el afectado es un menor, habla con ellos e infórmales de este grave problema**
 - Con los datos que damos en esta presentación y más que encuentres similares
 - Hazles saber que no están solos y que pueden contar contigo
- **Navega de forma segura**
 - Descargando solo cosas de lugares de confianza
 - Accediendo a sitios con buena reputación y con plugins de protección
 - Vigilando lo que publicamos
 - Controlando estrictamente a quien le permitimos acceder a nuestro contenido en RRSS / mensajería

Sextorsión

La sextorsión es un tipo de extorsión sexual en la que la persona que sufre el chantaje, normalmente por aplicaciones de mensajería instantánea o redes sociales, es amenazada con una o varias imágenes de sí misma (fotografías o videos) desnuda o realizando actos sexuales. Este chantaje puede tener como finalidad dominar la voluntad de la víctima, obtener dinero y/o victimizarla sexualmente.

¿Cómo evitar la sextorsión?

- Protégete**
Tapa las cámaras de tus dispositivos digitales cuando no los estés usando y no permitas que se graben videoconferencias.
- Actualízate**
Ten actualizadas tus aplicaciones en el teléfono móvil y los antivirus/antimalware de todos tus dispositivos digitales. Activa las opciones necesarias para protegerte.
- Cuida tu imagen**
No compartas imágenes íntimas a través de redes sociales, aplicaciones de mensajería instantánea, etc. Piensa que una vez que la envías, la pierdes para siempre.
- Contraseñas**
No compartas tus contraseñas. Haz que estas sean seguras y cámbialas cada cierto tiempo. Si tu expareja tiene tus contraseñas, debes cambiarlas de inmediato.
- Cifra tu información**
Aprende a cifrar la información de tus dispositivos por si te los roban y/o quieren hackear tus cuentas.

¿Qué hago si sufro sextorsión?

- No borres nada!** Guarda todas las pruebas de las que dispongas: mensajes, imágenes, conversaciones, etc.
- Presenta una denuncia** en la policía explicando todo lo que ha ocurrido y aportando todas las pruebas de las que dispongas.
- Si lo necesitas**, busca ayuda psicológica profesional que te ayude a superar lo que te ha ocurrido.

reA
Asociación para el avance de las personas con discapacidad intelectual y desarrollo

www.asociacionrea.org

Subvencionado por la Junta de Castilla y León con cargo a la asignación tributaria del IRPF

Servicios Sociales de Castilla y León

Fuente: <https://www.asociacionrea.org/que-es-la-sextorsion/>

EL PROBLEMA DE LA SEXTORSIÓN: EL SEXTING



José Manuel
Redondo López

- **Para evitar problemas no lo practiques**
 - Pero no te puedo decir lo que debes o no hacer...
- **Asegúrate de cumplir con estas precauciones**
 - Que no se te pueda identificar
 - NUNCA muestres tu cara
 - Un cuerpo sin cara es muy difícilmente reconocible
 - Nunca muestres algo que te pueda identificar (lunares, heridas, cicatrices, tatuajes, joyas)
 - Hazle OSINT a tu interlocutor
 - Ej.: Búsqueda inversa de su imagen a ver si es de stock



Consejos para prevenir la SEXTORSIÓN

The infographic is divided into two main sections: 'SEXTING' and 'SEXTORSIÓN'. It lists 10 tips, each accompanied by a small icon:

- SEXTING**:
 - Evita hacerte fotografías de contenido Sexual (Icon: camera)
 - No Envíes contenido a personas desconocidas (Icon: speech bubble)
 - Cuida tu imagen en internet (Icon: person)
 - No cedas al chantaje (Icon: dollar sign)
 - Elimina malware. (Icon: shield)
 - Cambia tus contraseñas (Icon: lock)
 - No confundas relaciones sentimentales, de amistad, etc. (Icon: heart)
- SEXTORSIÓN**:
 - Intercambio, difusión o publicación de fotografías y videos de carácter sexual, grabados por el remitente haciendo uso de dispositivos informáticos" (Icon: speech bubble)
 - Chantaje al que es sometida una persona por parte de otra que emplea contenidos de carácter sexual para obtener algún beneficio de la víctima, amenazando con su publicación (Icon: speech bubble)
 - Evita imágenes con tu rostro (Icon: face)
 - Borra el contenido sexual de tu móvil (Icon: smartphone)

Si eres víctima de Sextorsión, no lo dudes, DENUNCIALO

No cedas al chantaje. Denuncia.

Fuente: <https://lucasrojas.com/blog/sexting-y-sextorsion-denuncia/>

EL PROBLEMA DE LA SEXTORSIÓN: EL SEXTING

● Si ya te están extorsionando...

- Recopila todas las pruebas que puedas
- Llama al INCIBE (017) para pedir consejo
- Denuncia ante la Policía o la Guardia Civil
- Denuncia la cuenta en la red social, bloquéala y prepárate para lo peor

● ¿Por qué digo lo de prepararse para lo peor?

- Porque nunca te aconsejo pagar (recuerda el caso anterior)
- Hay varios motivos para ello
 - El delincuente se puede estar “marcando un farol” (ver imágenes)
 - Te va a seguir extorsionando
 - Si has pagado la 1^a vez sabe que “te tiene” y va a seguir exprimiendo
 - Si ve que no cedes, muchas veces lo dejan porque no van a sacar beneficio y pierden el tiempo (caso anterior)

 incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

 protege
tuempresa

Es posible que no me conozca y verosimilmente Se está preguntando por qué recibe este e-mail, ¿cierto?

Soy un hacker que descifró su e-mail y aparatos hace unos meses.

No trate de hacer estar en contacto con me o encuentrame, es imposible, desde que para ti envié un correo electrónico desde SU cuenta hackeada.

Configuré malware en el sitio de videos para adultos (porno) y comprendo que visitó este sitio web para pasaste bien (usted sabe a qué {me refiero|quiero decir}).

Mientras estar via estos videos, su navegador de Internet puso en marcha a funcionar como un RDP (mando a distancia) con un registrador de teclas que me dio acceso a su pantalla y cámara web.

Después de eso, mi programa de software obtuvo toda la información.

Usted ingresó las contraseñas en los sitios web que visitó y yo las intercepté.

Claro está, puede cambiarlos, o ya los ha cambiado.

Pero no importa, mi malware lo actualiza todo el tiempo.

Que hice.

Hice una copia de seguridad del dispositivo. De todos los archivos y contactos.

Hice un video de doble pantalla. 1^a parte muestra el video que usted estaba viendo (tiene buen gusto, jaja...), y la segunda parte muestra la grabación de su cámara web.

¿Qué es exactamente lo que tiene que hacer?

Está bien, en mi opinión, 1000€ es un precio justo para nuestro pequeño secreto. Realizará el pago por medio de bitcoins (si no lo sabe, busque “cómo adquirir bitcoin” en Google).

Mi dirección de billetera bitcoin:

1AXTd7o7BRufoJ4a3xnuHgNjNkECz5ZZYB

(Es distingue MAYÚSCULAS y minúsculas, por lo tanto copiarlo y pegarlo.)

Importante:

Tiene cuarenta y ocho horas por hacer el pago. (Yo tengo un pixel único en este correo electrónico, y en este instante sé que ha leido este e-mail).

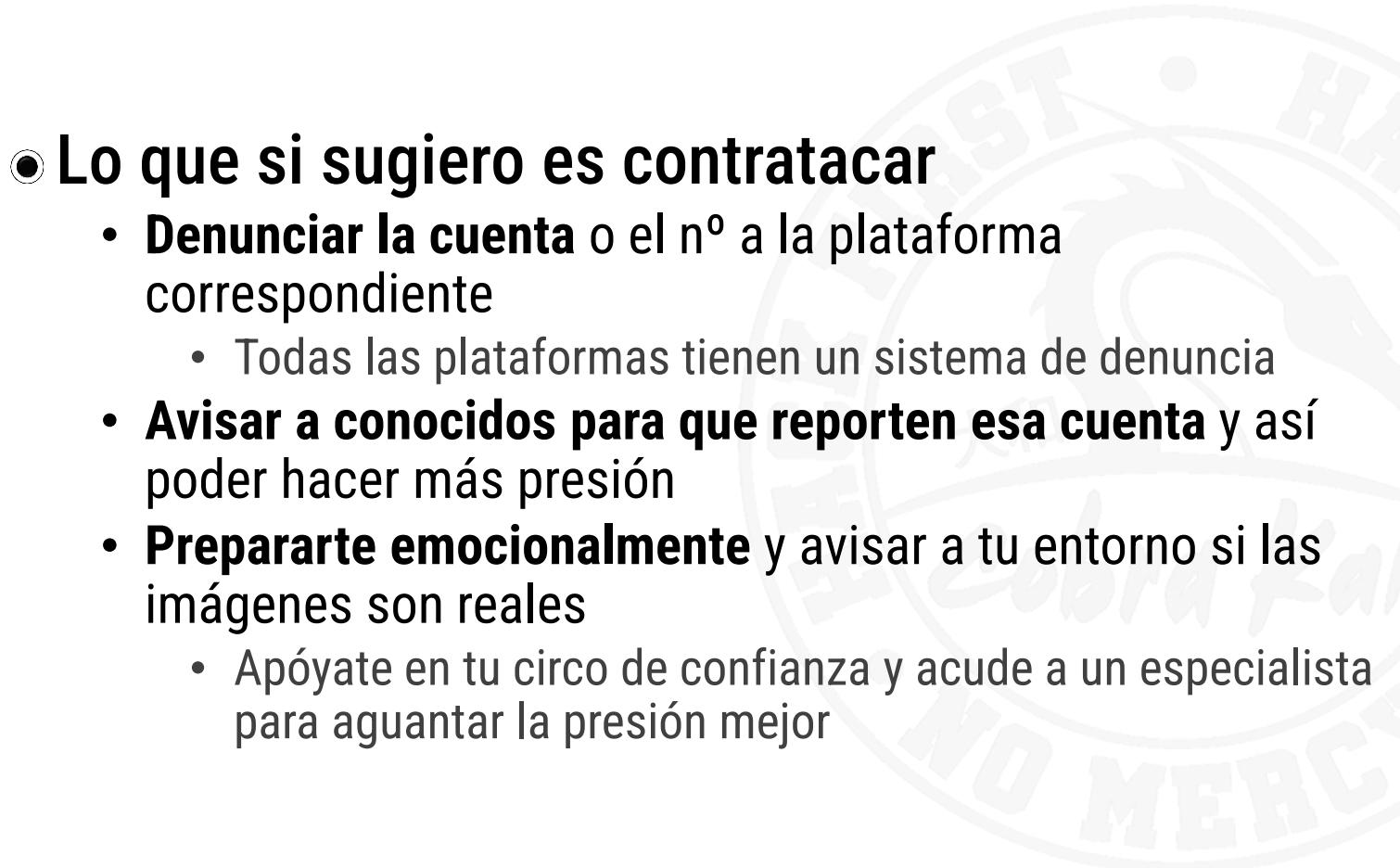
Para rastrear la lectura de un mensaje y las acciones en él, uso un pixel de Facebook. Gracias a ellos. (Cualquier cosa que se usa para las autoridades puede ayudarnos.)

Si no recibo el dinero, indudablemente voy a enviar su video a todos sus contactos, incluidos familia, compañeros de trabajo, etc.

EL PROBLEMA DE LA SEXTORSIÓN



José Manuel
Redondo López



● Lo que si sugiero es contrataracar

- **Denunciar la cuenta o el nº a la plataforma correspondiente**
 - Todas las plataformas tienen un sistema de denuncia
- **Avisar a conocidos para que reporten esa cuenta y así poder hacer más presión**
- **Prepararte emocionalmente y avisar a tu entorno si las imágenes son reales**
 - Apóyate en tu círculo de confianza y acude a un especialista para aguantar la presión mejor

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege
tu empresa

Su dispositivo ha sido pirateado por piratas informáticos.
¡Lea con urgencia las instrucciones!

¡Hola!

Soy un hacker que tiene acceso a su sistema operativo.
También tengo pleno acceso a su cuenta.

Llevo observándole desde hace unos meses.
Su equipo se infectó con un malware cuando visitó un sitio web para adulto.
Se lo explicaré mejor por si no está familiarizado con este tema.
El troyano me da acceso y control total sobre el ordenador o cualquier otro dispositivo.
Esto significa que puedo ver todo lo que aparece en su pantalla y encender la cámara y el micrófono sin que usted se de cuenta.

También tengo acceso a todos sus contactos y mensajes.

¿Por qué su antivirus no detecta el malware?
Respuesta: mi malware dirige el controlador y actualiza sus firmas cada 4 horas para que el antivirus se mantenga en silencio.

He grabado un vídeo en el que sale usted satisfaciéndose en la parte izquierda de la pantalla y en la parte derecha se puede ver el vídeo que está mirando.
Con un solo clic puedo enviar este vídeo a todos sus contactos de correo electrónico y de las redes sociales.
También puedo publicar el acceso en todos sus mensajes de correos electrónico y de messenger.

Si quiere evitarlo,
transfiera 1000 \$ a mi dirección bitcoin (si no sabe cómo hacerlo, escriba en Google: "Comprar bitcoins").

Mi dirección bitcoin (monedero de bitcoin) es: 13rjBXxXXXXXxxxxxXXXXxxXXXXXX

Una vez que haya recibido el pago, borraré el vídeo y no volverá a saber nada de mí.
Le doy 50 horas (más de 2 días) para pagar.
Cuando lea esta carta recibiré un aviso y el temporizador se pondrá en marcha.

Presentar una denuncia no tiene sentido porque este correo electrónico no puede ser rastreado, al igual que mi dirección bitcoin.
Yo no cometo errores.

Si descubro que ha compartido este mensaje con alguien más, el vídeo se distribuirá inmediatamente.

¡Un saludo!

www.incibe.es/protege-tu-empresa

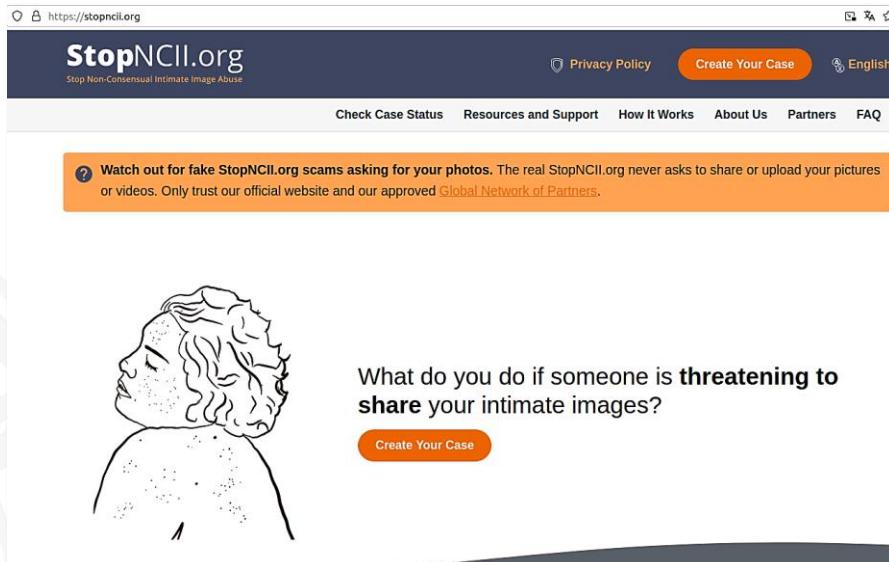
EL PROBLEMA DE LA SEXTORSIÓN

● Pedir ayuda a organizaciones que se dedican a eliminar tu información

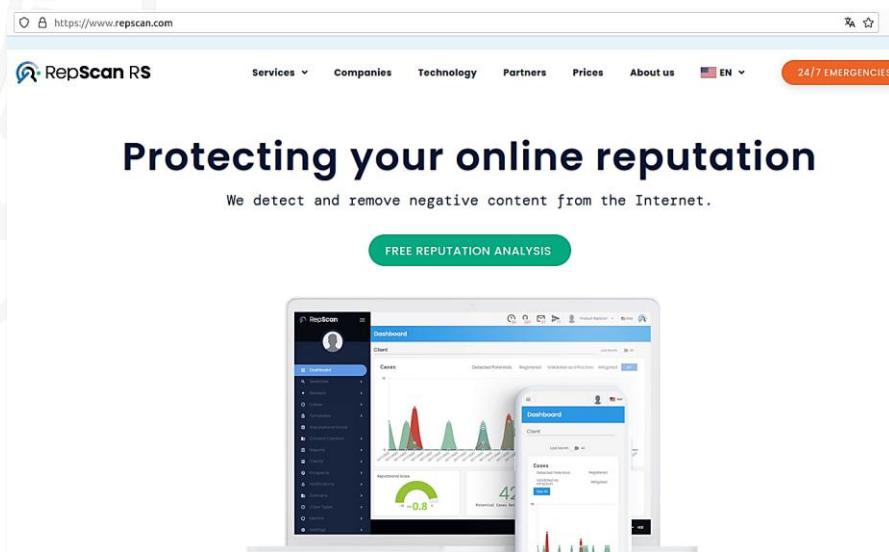
- Existen organizaciones que ayudan a las personas que han sufrido este tipo de ataques. Ej.:
 - <http://stopncii.org>
 - <http://repscan.com> (con programa gratis para personas sin recursos)
- Comprueba no obstante si funcionan en España
 - Una con sede española: <https://eliminalia.com/>

● Usa tu derecho al olvido en internet

- **Contacta con la AEPD** para usar su canal prioritario u otros servicios para eliminar tu información
- **Más información**
 - <https://www.aepd.es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido>



The screenshot shows the homepage of StopNCII.org. At the top, there is a navigation bar with links for 'Privacy Policy', 'Create Your Case', and 'English'. Below the header, a prominent orange banner warns users about fake scams asking for photos, stating: 'Watch out for fake StopNCII.org scams asking for your photos. The real StopNCII.org never asks to share or upload your pictures or videos. Only trust our official website and our approved Global Network of Partners.' To the right of the banner is a stylized line drawing of a person's head and shoulders. Below the drawing, a text box asks: 'What do you do if someone is threatening to share your intimate images?' with a 'Create Your Case' button.



The screenshot shows the homepage of RepScan RS. The top navigation bar includes links for 'Services', 'Companies', 'Technology', 'Partners', 'Prices', 'About us', and a language selector for 'EN'. A large headline reads 'Protecting your online reputation' with the subtext 'We detect and remove negative content from the Internet.' Below the headline is a green button labeled 'FREE REPUTATION ANALYSIS'. The main area features a large dashboard with various charts and graphs, and a mobile phone icon showing a similar interface.

¿CÓMO SABER SI LO HAS ENTENDIDO TODO? RESPONDE ESTO

?

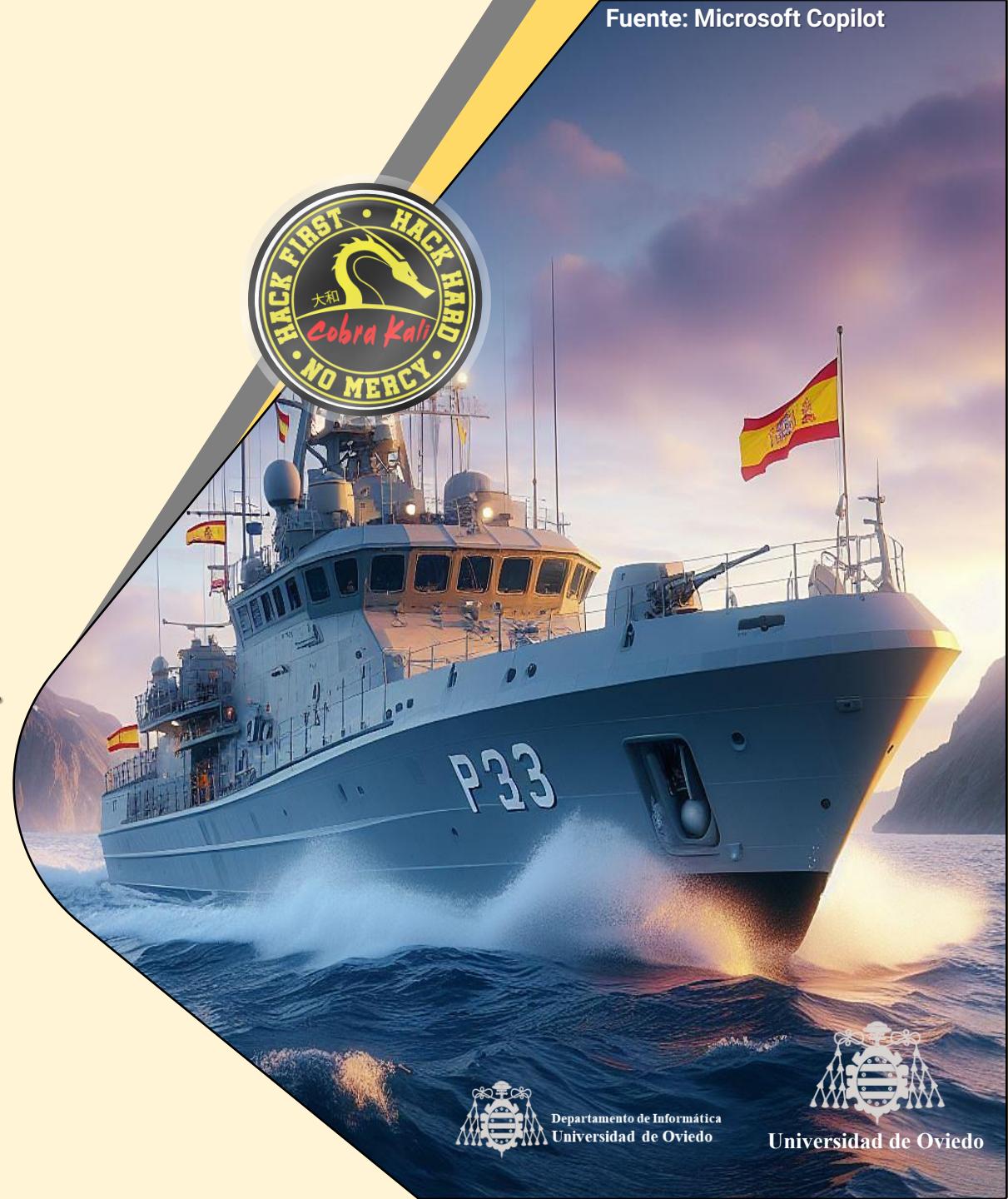
- *¿Entiendes qué es en esencia la sextorsión, y como es una forma de acoso devastadora?*
- *¿Comprendes las distintas tácticas que el delincuente tiene para conseguir el material para extorsionar?*
- *¿Entiendes bien lo que debes hacer y lo que no para que nadie use esta forma de acoso sobre ti?*
- *¿Y especialmente si acostumbras a hacer sexting?*
- *¿Entiendes qué medidas puedes tomar contra el/la delincuente si eres víctima de sextorsión?*

[< Ir al Índice](#)

APLICACIONES DE MENSAJERÍA

Personales: WhatsApp, Telegram, Signal, Messenger...

Profesionales: Teams, Slack, Google Meet...



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

¿QUÉ VAMOS A VER EN ESTE BLOQUE?

- Que el acoso por RRSS, mensajería y email son muy similares
- En la primera sección veremos...
 - El perfil de un **narcisista** como acusador destructivo del que debemos defendernos
 - Como **responder a un narcisista** cuando no puedes cortar relación con el/ella
- En la segunda sección...
 - Qué es y en que consiste el **acoso académico**
 - Formas de **identificar** este tipo de acoso
 - **Qué hacer** ante él
- Y en la tercera sección...
 - Porque la **usurpación de un perfil** conocido puede ser la antesala de un acoso
 - El motivo por el que debes sospechas de **peticiones "raras"** de conocidos



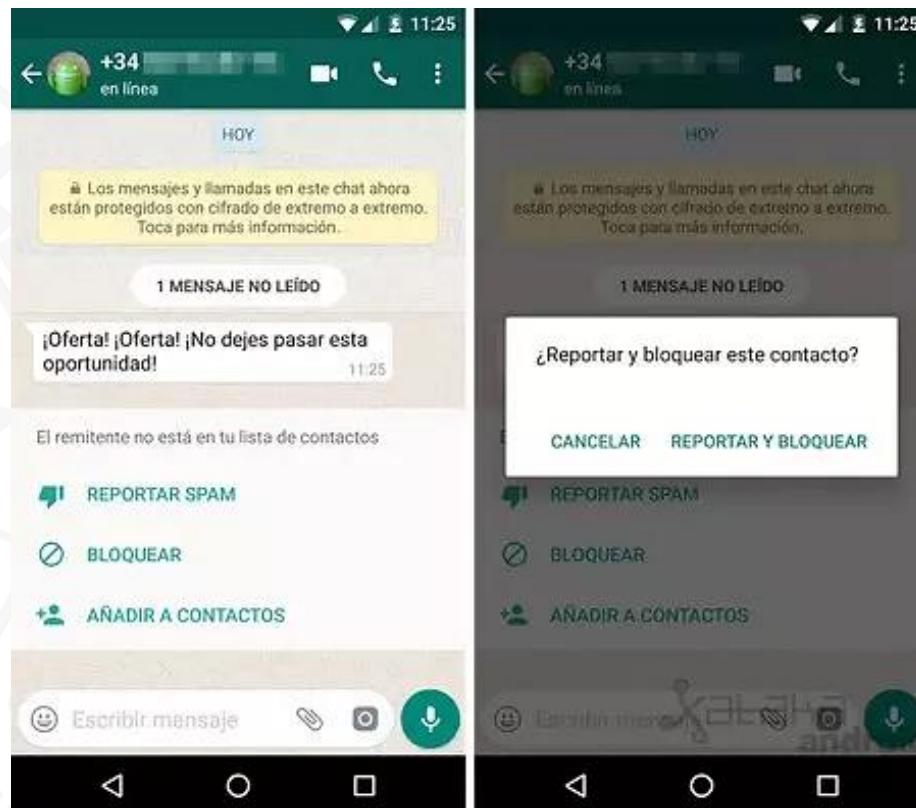
PARALELISMOS CON EL EMAIL Y RRSS

● **Motivo:** Hay un paralelismo entre el email, las RRSS y las aplicaciones de mensajería

- La mayoría de las aplicaciones de mensajería cuentan con las **mismas opciones de defensa** que los emails, y conviene usarlas
- Se pueden hacer sobre **usuarios y grupos** de usuarios

● **Solución:** Cuando te llegue un mensaje sospechoso debes hacer lo dicho anteriormente

- **Reportar al emisor** como spam
- **Informa del contenido del mensaje** en donde la aplicación de mensajería indique
 - Depende de cada plataforma
- **Bloquear al emisor** para que nunca más pueda volver a contactar con nosotros



Fuente: <https://www.xatakandroid.com/tutoriales/como-denunciar-a-un-usuario-o-grupo-de-whatsapp-por-spam>

MECANISMOS DE ACTUACIÓN CONTRA EL BULLYING EN MENSAJERÍA

-  **Motivo:** El bullying por mensajería y el de RRSS es similar
 - La principal diferencia es que **el atacante suele ser más fácilmente identifiable**
 - Conseguir una cuenta falsa en una aplicación de mensajería no es tan sencillo como en una RRSS...
 - El volumen de **bullys** normalmente es menor que en una RRSS (no así el daño)
 - En cambio, también **es más fácil de que la víctima lo oculte**
 - Borra los mensajes ofensivos por vergüenza, amenazas, etc.
 - El autor de los mensajes borra los mensajes ofensivos tras asegurarse de que la víctima los ha leído
-  **Solución:** Si es un menor, nuevamente, aplica el protocolo de la AEPAE visto con RRSS
 - Fomenta la confianza y haz que el/la afectado/a te hable de estos problemas
 - Mantente vigilante ante cambios de comportamiento o intentos de usar el móvil a escondidas, por si fuera indicio de este tipo de ataques
 - **Más información:** <https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo>



Narcisistas

Acoso íntimo, cercano, personal y muy difícil de detectar



*Imagen generada por Microsoft Copilot



IDENTIFICA LOS ENGAÑOS DE CONTACTOS NARCISISTAS

● 📖 Motivo: Los narcisistas son personas incapaces de ver el mundo más allá de sus intereses

- <https://es.wikipedia.org/wiki/Narcisismo>
- Tienen **muy bajos niveles de empatía**
 - O la tienen, en el sentido de entender los sentimientos de los demás, pero los “**weaponiza**”
 - Saben cómo se sienten sus víctimas, y usan ese conocimiento en su contra (manipulación)
- Necesitan una **atención y admiración excesiva**
- **Generan relaciones conflictivas** y por ello **dañan** a quienes se vinculan con él/ella
- Exhiben **personalidad arrogante, envidiosa, intolerante, soberbia o sin inhibiciones**
- Debido a ello, **son un perfil peligroso** si te los encuentras en aplicaciones de mensajería / RRSS, etc.



● 🔨 Solución: Aprender a reconocerlos para no vincularte con ellos

- Sus engaños pueden hacerte mucho **daño sicológico**, afectar a tu autoestima, etc.
- En la siguiente página te doy algunos indicios para hacerlo
 - **Más información:** <https://www.gq.com.mx/estilo-de-vida/articulo/como-identificar-a-un-narcisista-por-mensajes-de-texto>

IDENTIFICA LOS ENGAÑOS DE CONTACTOS NARCISISTAS

● Un/a narcisista en una red social o aplicación de mensajería...

- **Te escribe cuando quiere:** Piensa solo en sus intereses, sin considerar tus tiempos o límites
 - Puede enviar muchos mensajes de pronto, sin considerar si estas ocupado/a, la hora del día, lo que estés haciendo, etc.
- **Solo buscará que te concentres en él/ella en el momento que quiera, para generar dependencia**
 - Debes estar pendiente del momento en el que escriba para responder rápido
 - Y generarte ansiedad por tener muchos mensajes pidiendo atención urgente
- **No responde a tus mensajes:** Si no demanda atención, puede dejarte en visto o responder cuando quiera, pasado mucho tiempo
 - Aunque seas tú quien necesite ayuda de alguna clase (**no reciprocidad**)
 - Otra táctica es **responder a los mensajes de otros mucho más rápidamente que a los tuyos**
 - Especialmente cuando puedas ver que lo hace claramente (**mostrar desprecio**)
 - Lo hace para que **dudes de tu importancia** en el contexto de la relación con el (**ninguneo**)



IDENTIFICA LOS ENGAÑOS DE CONTACTOS NARCISISTAS

- **Uso de herramientas de control:** Necesidad de saber lo que haces, de que apruebe tus decisiones antes de hacerlas, de que supervise todo lo que hagas “por tu bien”, etc.
- **Dependencia de su humor:** Puede mostrarse amable e interesado/a cuando necesita algo
 - Para pasar a ser borde y distante cuando lo consiga
 - Son personas de tono o interés muy variable (**no sabes a lo que atenerte con el/ella**)
- **Te mantiene en suspense:** Escribe un mensaje interesante para luego desaparecer mucho tiempo
 - El objetivo es provocarte **inestabilidad emocional**
 - Ej.: Ofrecer una idea o plan muy interesante pero luego olvidarse de ella o no mostrar interés alguno cuando aceptas
 - Es un mecanismo para **generar vulnerabilidad**
 - Y comprobar que sigues siendo alguien manipulable y a su disposición
- Aquí hay **ejemplos de mensajes tipo de narcisistas** que puedes usar como guía
 - https://twitter.com/rosky_wolf/status/1653311576508645377
- Si crees que estás en un caso así con alguien con el que tengas un vínculo fuerte que es difícil de romper, **acude a un especialista que te ayude a manejar la situación**

ESTRATEGIAS Y TÁCTICAS DE RESPUESTAS A NARCISISTAS

-  **Motivo:** Ahora tenemos herramientas para detectar narcisistas
 - ¿Pero qué pasa si tenemos que responderles obligatoriamente?
-  **Solución:** Usa métodos documentados de respuesta a narcisistas
 - **Acude siempre primero, si te es posible, a un profesional para pedir consejo**
 - Si no puedes, estas técnicas que te enumero están documentadas aquí
 - <https://es.wikihow.com/responder-los-mensajes-de-texto-de-una-persona-narcisista>
 - **Dejarlo en “visto”** si no nos hace una pregunta que debamos contestar (**odian que les ignoren**)
 - Usar **respuestas con “sí” y “no”** para responder siempre que puedas
 - Para dificultar que pueda usar **tus respuestas como arma** posteriormente
 - “Pero no dijiste qué...”, “Pues aquí yo entendí...”, “Claro, es que como escribes mal...”
 - Al responder, **deja claros tus límites**
 - Trabajo que vas a hacer, horas de reunión permitidas...
 - **Comparte tus propias experiencias** si te envía un mensaje de texto sobre un recuerdo
 - Es una estrategia de **manipulación**, probablemente intente alterar los hechos en su beneficio
 - Cuenta tú **tu versión**, así no es tan fácil alterar los hechos

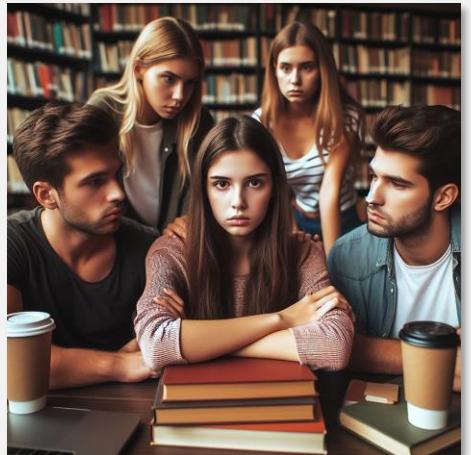
ESTRATEGIAS Y TÁCTICAS DE RESPUESTAS A NARCISISTAS

- Halaga a esa persona **si necesitas un favor** o que haga algo obligatoriamente
 - Aunque siempre es mejor pedírselo a otra persona (aunque a veces no queda más remedio...)
 - Necesitan sentirse el centro de atención
- Di que tienes un nuevo “**sistema de apoyo**” (amigos, trabajo, pareja...)
 - En caso de que el narcisista intente retomar el contacto contigo
 - Su intención es que dependas de él para todo, pero si ya no hace falta...
- Responde a sus preocupaciones con **amabilidad e integridad**
 - Las respuestas violentas le dan combustible para **dañar tu reputación**
- **Aliéntalo a buscar ayuda profesional** en caso de que no pueda contar contigo
 - Aunque prepárate si no reacciona bien a esto...
- Si te escribe un mensaje que te altera, **no respondas en el momento, “en caliente” (busca alterarte)**
 - Tómate tu tiempo para pensar una estrategia y calmarte, aunque es difícil en una aplicación de mensajería
 - Es buena idea **quitar la confirmación de lectura** en estos casos
- **Háblalo con otras personas** antes de responder a un mensaje
 - Es bueno tener otras perspectivas, si conocen el problema

¿CÓMO SABER SI LO HAS ENTENDIDO TODO? RESPONDE ESTO



- *¿Entiendes en qué medida el acoso por aplicaciones de mensajería es similar a otro tipo de medios y en qué se diferencia?*
- *¿Comprendes que una de las formas de acoso más peligrosas para la víctima son mensajes vejatorios que el delincuente borra una vez leídos?*
- *¿Entiendes las pautas para identificar a un o una narcisista?*
- *¿Comprendes las principales técnicas de manipulación por mensajería de un/a narcisista?*
- *¿Entiendes la importancia de acudir a un profesional para lidiar con las consecuencias de ser víctima de un narcisista?*
- *¿Comprendes que las víctimas suelen estar mucho tiempo en ese problema y por qué les cuesta mucho salir de él?*
- *¿Entiendes las pautas de respuesta ante peticiones de un narcisista si no puedes cortar contacto con él?*



Acoso académico

Acoso entre miembros de una institución académica distinto al acoso escolar



*Imagen generada por Microsoft Copilot



EL ACOSO ACADÉMICO

- **Motivo:** El acoso del personal académico se presenta especialmente en lugares de educación superior

- Como universidades, centros de investigación...
- Se cree que es común, pero no ha sido investigado con la misma atención que otros tipos de acoso
- Es un proceso **de larga duración**, físico o psicológico
- Es una **conducta individual o de grupo**, dirigido hacia y contra otro individuo que no puede defenderse
 - Hay **conciencia y deseo** de lastimar, herir, amenazar, etc. poniendo a la víctima bajo un estrés elevado
- Se ha agravado por el **uso de aplicaciones de mensajería como vehículo de acoso** constante



La categoría académica no da derecho a nadie a faltarte al respeto, gritarte, insultarte, etc. No aguantes eso, porque estarás a merced de alguien que no te valora en absoluto (sino no te haría la vida imposible)

EL ACOSO ACADÉMICO

● 🔨 Solución: Denuncia alguno de los posibles tipos de acoso que puedes sufrir

- **Amenazas, humillación pública**, acusaciones como falta de esfuerzo y menosprecio
- Amenazas al estatus social con **burlas y sobrenombres**
- **Aislamiento, ocultar información clave e impedir oportunidades académicas** o profesionales
- **Exceso de trabajo**, interrupciones innecesarias al trabajo que se está desarrollando
- **Desestabilización**, como no dar el crédito debido o que quiten a personas de su posición de autoridad
 - “*Todo lo aprueba por pura suerte*”
 - “*Seguro que conoce a alguien que le hace el trabajo*”
 - “*Regala sus asignaturas*”
 - “*Es un mal profesional*”
 - “*Todo lo que ha conseguido es gracias a esta otra persona*”
 - ... (si algo de esto te suena, o alguna similar, vete a la defensoría universitaria u órgano equivalente)

EL ACOSO ACADÉMICO

● Características del acoso académico

- Los **acosadores** suelen ser **personas en posiciones de poder** o de “posición protegida”
- Los que pueden identificarlo y prevenirlo muchas veces **no han recibido formación** para ello
 - Es el motivo principal de crear este apartado
- Las **víctimas** suelen ser profesores **de categorías más bajas** (o estudiantes)
 - Ejs.: https://twitter.com/joven_profesor, <https://twitter.com/seacaboacademia>
- **El acoso moral** es el tipo de acoso académico más frecuente
- Para una víctima **es difícil presentar una reclamación** por la naturaleza descentralizada de las instituciones académicas
 - Es más frecuente ver denuncias anónimas por aplicaciones de mensajería o redes sociales

● El acoso cambia en función de la escala, PDI o PAS

- **En el caso de PDI**, se suele dar porque el que lo causa fija objetivos y normas arbitrarios o asfixiantes al acosado
- **En el caso de PAS**, se hace mediante una medición y revisión de rendimientos y logros irreal

EL ACOSO ACADÉMICO

● Indicios de acoso académico

- Un **nivel socioeconómico superior** por parte del acosador
 - Se auto-posiciona en una situación de **superioridad** respecto al acosado
 - El acosado es visto como una persona más débil e inferior, que debe someterse a los designios del acosador **si desea prosperar** en su carrera académica
- **Abusos sexuales**, como, por ejemplo
 - Envío de mensajes, imágenes/ videos insinuantes y/o de carácter sexual, bromas sobre la condición sexual
- **Críticas continuas** sobre la vida privada de una persona
- **Agresiones físicas o verbales, difusión de rumores falsos** o comentarios vejatorios
- **Impedir a la víctima que hable** con otras personas, o prohibirle realizar ciertas acciones
- **Sobrecargar a la víctima con trabajo** que no le corresponde
 - Disfrazándolo de “ayuda” o “contribución” al grupo y con consecuencias veladas si no se hace
- **Dirigirse de forma ofensiva** a los compañeros u otras personas del entorno universitario

● Más información

- <https://www.elperiodico.com/es/sociedad/20230522/abusos-acoso-universidad-departamentos-podridos-87710750>
- <https://ciberintocables.com/acoso-universidades-espanolas/>

EL ACOSO ACADÉMICO

- La ley de convivencia universitaria estatal no permite ese tipo de casos
 - <https://www.boe.es/buscar/act.php?id=BOE-A-2022-2978>
- Cada Universidad tiene su propio reglamento de convivencia y actuación
- No tienes ninguna necesidad de aguantar ese tipo de abusos
 - Te pueden hacer un daño psicológico muy grave
- Como vimos, acude a figuras como el **Defensor Universitario** o similar en caso de que te veas en ese tipo de problemas
- **Ponte en manos de un terapeuta para paliar las consecuencias sicológicas**

Artículo 3. Normas de Convivencia.

1. Con el fin de favorecer el entendimiento, la convivencia pacífica y el pleno respeto de los valores democráticos, los derechos fundamentales y las libertades públicas en el ámbito universitario, las universidades públicas y privadas aprobarán sus propias Normas de Convivencia, que serán de obligado cumplimiento para todos los miembros de la comunidad universitaria, tanto respecto de sus actuaciones individuales, como colectivas.
2. Las Normas de Convivencia de las universidades públicas y privadas promoverán:
 - a) El respeto a la diversidad y la tolerancia, la igualdad, la inclusión y la adopción de medidas de acción positiva en favor de los colectivos vulnerables;
 - b) la libertad de expresión, el derecho de reunión y asociación, la libertad de enseñanza y la libertad de cátedra;
 - c) la eliminación de toda forma de violencia, discriminación, o **acoso** sexual, por razón de sexo, orientación sexual, identidad o expresión de género, características sexuales, origen nacional, pertenencia a grupo étnico, discapacidad, edad, estado de salud, clase social, religión o convicciones, lengua, o cualquier otra condición o circunstancia personal o social;
 - d) la transparencia en el desarrollo de la actividad académica;
 - e) la utilización y conservación de los bienes y recursos de la universidad de acuerdo con su función de servicio público;
 - f) el respeto de los espacios comunes, incluidos los de naturaleza digital;
 - g) la utilización del nombre y los símbolos universitarios de acuerdo con los protocolos establecidos.

Extracto de la ley de convivencia universitaria

¿CÓMO SABER SI LO HAS ENTENDIDO TODO? RESPONDE ESTO

?

- *¿Entiendes qué es el acoso académico y sus características particulares?*
- *¿Comprendes por qué se conocen numerosos casos de este tipo de prácticas en la Universidad en general y qué los fomenta?*
- *¿Entiendes los síntomas principales de ser víctima de un acoso académico?*
- *¿Comprendes que las universidades tienen órganos, reglamentos y formas de denunciar estas prácticas y de dejar evidencia de las mismas?*



Cuando el ataque viene de un conocido

Cuando el ataque viene de una cuenta de un “mutual”

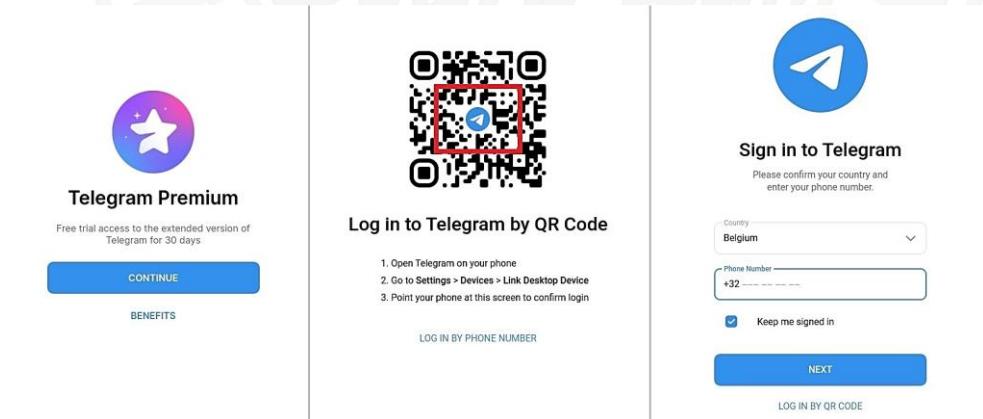


ROBO DE CUENTAS Y PERFILES PARA ACOSAR

-  **Motivo:** Uno de los medios más frecuentes para fomentar el acoso es el robo de perfiles de Instagram o similares
 - Los delincuentes roban cuentas y **buscan víctimas entre todos sus contactos**
 - Intentan **sacar información privada de cualquiera** de ellos usando la identidad de la cuenta robada
 - Mismamente imágenes para sextorsión, como vimos antes
 - Una vez conseguido, ejecutan el tipo de acoso que buscan
 - Exactamente **lo mismo pasa con perfiles de aplicaciones de mensajería** como Telegram
-  **Solución:** Extrema las precauciones si uno de tus contactos se comporta de forma extraña, pide cosas que no te ha pedido nunca o comprometidas
 - También se roban también cuentas bien valoradas en tiendas de segunda mano para estafas
 - Mira este ejemplo ilustrativo: <https://www.kaspersky.es/blog/telegram-takeover-contest/28438/>
 - Te llega un mensaje de uno de tus contactos **con un enlace y un “anzuelo”**: invitación para participar en una votación, concurso, regalo, una solicitud para firmar una petición colectiva, etc.
 - Estas **páginas falsas**, cuyo enlace siempre viene acortado, tienen siempre algo en común: la necesidad de autenticarse a través de Telegram (con un código QR, introduciendo tu nº de teléfono...)

ROBO DE CUENTAS Y PERFILES PARA ACOSAR

- Si das tu número de teléfono, el atacante inicia sesión en tu cuenta de Telegram desde un nuevo dispositivo
- Si tienes 2FA, Telegram requiere tu confirmación y te envía un código de verificación a tu teléfono u ordenador donde ya esté autorizado
 - **Siempre debes tener 2FA activo**
 - Si caes en el pretexto que la página te dé, e introduces este código, te habrán robado la cuenta
- Con un código QR, es aún más sencillo: Ni siquiera necesita un código de verificación
 - Este código se usa para **conectar un dispositivo adicional** o una sesión web a tu cuenta
 - Por tanto, si escaneas este código según las instrucciones, los atacantes iniciarán sesión automáticamente en tu cuenta y tomarán su control



Da igual el pretexto, si algo te pide volver a autenticarte en Telegram, desconfía de ello automáticamente

ROBO DE CUENTAS Y PERFILES PARA ACOSAR

● Además del acoso a tus contactos, estos robos se usan para algo más

- Tu cuenta tiene datos que podrían usarse en otros delitos
- A través de la **versión de escritorio de Telegram**, los delincuentes pueden exportar tu lista de contactos
 - Y datos personales, historial de chat o archivos que hayas cargado y recibido **con información confidencial**
 - **Puede ser el inicio de una sextorsión o robo de información privada de tus investigaciones / artículos**
- Los secuestradores también podrían llamarte y ofrecerte la devolución de tu cuenta a cambio de dinero (**extorsión**)

● Si ya eres víctima de la estafa, todavía hay esperanza si actúas rápido

- Podrás recuperar el control de tu cuenta en **Ajustes -> Dispositivos** y la opción “**Cerrar todas las demás sesiones**”

← Privacidad y seguridad		← Dispositivos	
Seguridad			
Código de bloqueo		Este dispositivo	
Verificación en dos pasos		Desactivada	Telegram Android 7.3.1 Xiaomi Redmi 7A, Android 9 P (28) 201.210.55.93 – Caracas, Venezuela
Sesiones activas		en línea	
Controla tus sesiones en otros dispositivos.		Cerrar todas las demás sesiones	
		Sale de todos los dispositivos, excepto este.	
Eliminar mi cuenta			
Si estoy fuera		6 meses	Sesiones activas
			Escanear código QR
Si no estás en línea al menos una vez durante este período, tu cuenta se eliminará junto con todos tus mensajes y contactos.			
Bots y sitios web			
Eliminar información de pago y envío		Telegram Web 0.7.0 Chrome, Windows 201.210.55.93 – Caracas, Venezuela	
		12:17 PM	
Sesión iniciada con Telegram			
Sitios web en los que iniciaste sesión con Telegram.			
Toca en una sesión para cerrarla.			

Como cerrar todas las sesiones abiertas de Telegram. Fuente:
<https://www.lavanguardia.com/andro4all/telegram/como-ver-sesiones-abiertas-telegram-como-cerrarlas>

BLOQUEO, REPORTE Y DIVULGACIÓN DE CUENTAS

-  **Motivo:** Antes vimos que bloquear y reportar contactos en aplicaciones de mensajería era la respuesta adecuada
 - Pero no debemos dejarlo ahí: tenemos que **informar también a nuestro entorno** de los usuarios que os están intentando estafar
 - En una aplicación de mensajería los usuarios tienen una relación más personal con nosotros
-  **Solución:** Reporta, bloquea e informa rápidamente a tu entorno de usuarios fraudulentos, especialmente en estos casos
 - Te han intentado estafar y **sospechas que es por formar parte de un grupo**: El resto de los miembros recibirán la misma estafa seguramente tarde o temprano
 - Recibes un **mensaje extraño de un miembro de un grupo** o compañero de trabajo: un más que probable indicio de una cuenta intervenida
 - **En caso de que sea Teams u otro chat corporativo, avisa al responsable de informática de tu Universidad**
 - Es un posible indicio de filtración de datos de cuentas de compañeros
 - Nuevamente, **dar la alarma** es muy importante para mantener la seguridad de todos

¿CÓMO SABER SI LO HAS ENTENDIDO TODO? RESPONDE ESTO



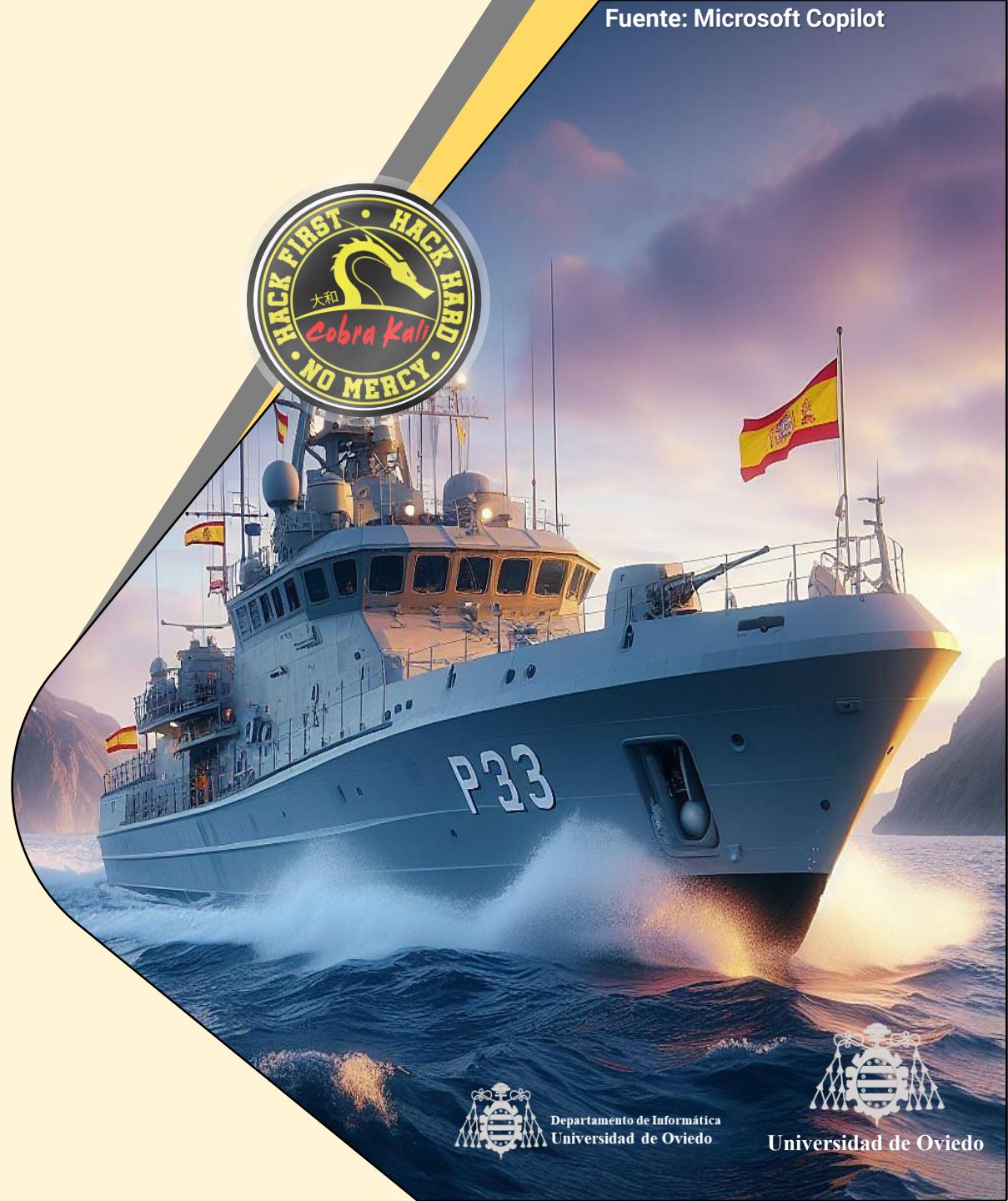
- *¿Entiendes por qué el robo de cuentas es una de las formas más efectivas de iniciar estafas...y acosos?*
- *¿Entiendes en qué sentido la divulgación de cuentas comprometidas o con estafas es un medio más efectivo de pelear contra estos problemas en entornos de amistad y familiares?*
- *¿Y que, en este sentido, el bloqueo y la denuncia, aun siendo necesarios, no son todo lo que puedes hacer?*

< Ir al Índice



CONCLUSIONES

Para finalizar la charla...



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

CONCLUSIONES

● Algunos consejos generales contra acoso en general

- No contestes a las provocaciones, **bloquéalas**
- **Compórtate con educación en la red:** no hagas a los demás lo que no quieras que te hagan a ti
- Si te acosan, **abandona la conexión** y pide ayuda si es necesario
- **Nunca facilites datos personales**
- **Busca apoyo y vías de escape:** Desconéctate y dedícate a estar con tu gente o a hacer otras cosas
- Encuentra otras personas que **compartan tus mismos valores e intereses**
- **Comparte tus sentimientos** acerca de la intimidación y el acoso

● Recuerda que puedes buscar ayuda profesional si te sientes acosado en línea

- No estás solo y hay recursos disponibles para ayudarte

RECURSOS

- **10 Consejos básicos contra el ciberbullying**
 - <https://www.ciberbullying.com/cyberbullying/diez-consejos-basicos-contra-el-ciberbullying/>
- **Consejos para jóvenes para enfrentarse al cyberbullying**
 - <https://lamenteesmaravillosa.com/consejos-para-jovenes-para-enfrentarse-al-cyberbullying/>
- **Cómo actuar ante el ciberbullying: Guía 2021 para víctimas de acoso**
 - <https://www.giztab.com/ciberbullying-como-evitarlo-consejos-ciber-acoso/>
- **Ciberacoso: Qué es y cómo detenerlo**
 - <https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo>
- **Redes sociales y salud mental: Una relación complicada**
 - <https://www.giztab.com/redes-sociales-y-salud-mental/>

RECURSOS: INCIBE

- El INCIBE tiene también recursos específicos contra esta lacra
 - <https://www.incibe.es/menores/tematicas/ciberacoso>
 - <https://www.incibe.es/aprendeciberseguridad/cyberbullying>
- ¡El 017 también puede ayudarte en estos casos! ¡Llama para pedir ayuda!



TU AYUDA EN CIBERSEGURIDAD

Servicio gratuito y confidencial, disponible de 08:00 am a 11:00 pm los 365 días del año.

CONTACTANDO

017

WhatsApp 900 116 117

Telegram @INCIBE017

Formulario web

Atención presencial

Financiado por la Unión Europea NextGenerationEU

Gobierno de España MINISTERIO DE TRANSFORMACIÓN DIGITAL

PROGRAMA DE RECONSTRUCCIÓN Y TRANSFORMACIÓN ALTAZUL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

RECURSOS: TELÉFONO / CHAT DE LA ESPERANZA

- Otro recurso es el teléfono de la esperanza
- Si estás en una situación muy mala, aquí hay quien te escuche
 - Gente buena, preparada y dispuesta a escuchar y aportar soluciones
- Con atención telefónica 24h al día, 7 días a la semana
 - Y ahora con **chat**, para cubrir a más gente
 - Con horario ampliado y atención en fin de semana



Teléfono de la esperanza
telefonodelaesperanza.org

CHAT DE AYUDA PARA JÓVENES Y ADOLESCENTES EN SITUACIÓN DE CRISIS EMOCIONAL, CONDUCTA SUICIDA O AUTOLESIONES

CHAT DE LA ESPERANZA



DE LUNES A DOMINGO
DE 18:00H A 00:00H
(DE 17:00 A 23:00 EN CANARIAS)

ESTAMOS LAS 24H EN EL TELÉFONO DE ATENCIÓN EN CRISIS 717 003 717
BUSCA TU SEDE MÁS CERCANA EN TELEFONODELAESPERANZA.ORG/CONTACTO

¡ESPACIO SEGURO Y SIN JUICIOS!

ANÓNIMO Y CONFIDENCIAL

DIRIGIDO A JÓVENES

ACCESIBLE A PERSONAS CON DIFICULTADES AUDITIVAS O DEL HABLA

ENCUÉNTRALO DESCARGANDO CONÉCTATE.SOCIAL

¡ESPACIO SEGURO Y SIN JUICIOS!

ANÓNIMO Y CONFIDENCIAL

DIRIGIDO A JÓVENES

ACCESIBLE A PERSONAS CON DIFICULTADES AUDITIVAS O DEL HABLA

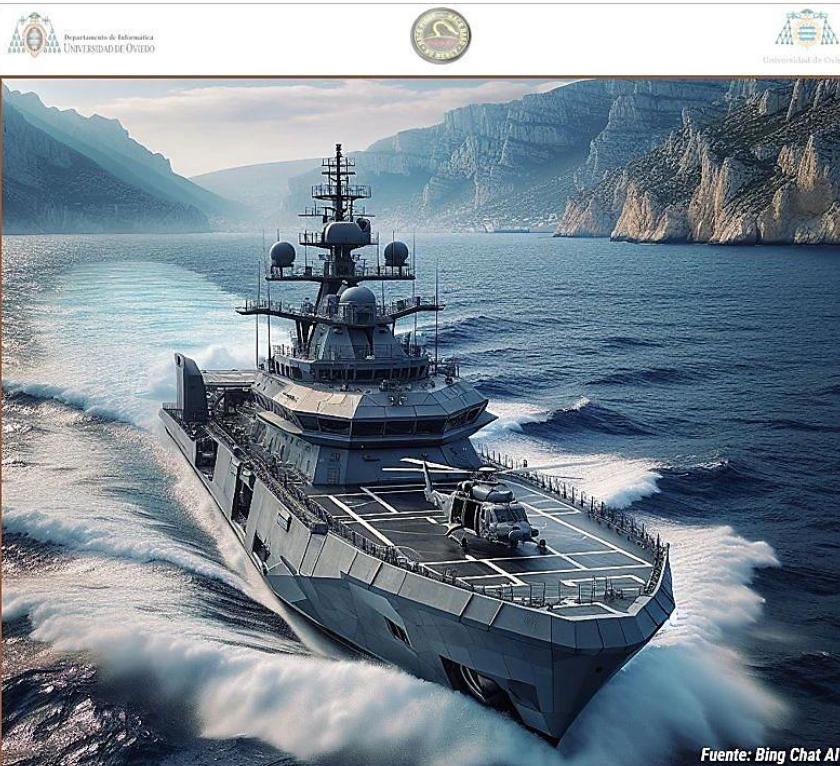
ENCUÉNTRALO DESCARGANDO CONÉCTATE.SOCIAL



¿Y TÚ? ¿TIENES MÁS MATERIALES?

- Yo tengo un canal de YouTube donde hablo de fraudes, y de vez en cuando se tocan temas cercanos al acoso y al bullying
 - <https://www.youtube.com/@j.m.redondo8618/featured>
- En 2024 se liberó por OCW SSI v4.0 (<https://ocw.uniovi.es/course/view.php?id=98>)
 - Incluye una documentación de **iniciación al OSINT**
 - Que puede servir para entender **las técnicas que usan los delincuentes avanzados** para acosar desde el anonimato
 - Y para encontrar información de sus víctimas
 - Es un tema **muy técnico**...pero que te abrirá los ojos en cuanto a lo peligrosas que son estas prácticas



Fuente: Bing Chat AI

INTRODUCCIÓN AL OSINT

DEPARTAMENTO DE INFORMÁTICA. UNIVERSIDAD DE OVIEDO

Técnicas de Investigación con Fuentes Abiertas | 2023 – 2024 (V1.5 "A-21 'Poseidón' Lite")

José Manuel Redondo López



CUANDO EL OBJETIVO DE UN CIBERATAQUE ES UN SER HUMANO



*Imagen generada por Microsoft Copilot