Ciudadanía e identidad digital

Juan José de Haro Ollé

Ministerio
de Educación
y Formación Profesional

Ciudadanía e identidad digital

Juan José de Haro Ollé

Catálogo de publicaciones del Ministerio: https://sede.educacion.gob.es/publiventa/inicio.action

Catálogo general de publicaciones oficiales: https://cpage.mpr.gob.es/

Autor
Juan José de Haro Ollé

MINISTERIO DE EDUCACIÓN
Y FORMACIÓN PROFESIONAL
Instituto Nacional de Tecnologías
Educativas y de Formación del Profesorado

Edita:
© SECRETARÍA GENERAL TÉCNICA
Subdirección General de Atención al Ciudadano, Documentación y Publicaciones

Edición 2020

NIPO (línea): 847-20-109-5

Índice

Seguridad y privacidad en Internet 5
Ciudadanía e identidad digital 5
Introducción 5
El uso de internet 5
Ciudadanía digital 6
Identidad digital 9
Identidad y ciudadanía 9
Los menores como ciudadanos digitales 10
Elementos de la ciudadanía digital 10
Acceso digital 10
Etiqueta digital 12
Comunicación digital 17
Alfabetización digital 18
Responsabilidad y derechos 20
Seguridad física y psicológica 20
Seguridad como autoprotección 23
Ética en el mundo digital 25
Ética en lo digital e Internet Justo 25
La falta de ética 26
¿Qué podemos hacer? 29
Identidad, reputación y huella digital 37

Habilidades y competencias del ciudadano digital 41
Desarrollo evolutivo y socioemocional en el ámbito digital 41
Las TIC y los adolescentes 41
La importancia de las redes sociales 43
Comunicación y colaboración en redes sociales 47
Formación y colaboración en las redes sociales 47
Plataformas sociales 47
Comunicación y colaboración 49
Engaños en la web 61
Introducción 65
Bulos 65
Estafas por pagos anticipados 67
Phishing 69
Posverdad 71
Derechos de autor y licencias 74
Los problemas del copyright 74
Creative Commons 74
Buscadores de recursos abiertos 75
Recursos Educativos Abiertos (REA) 78

La construcción de nuestra identidad digital 81
Privacidad y navegación segura 81
Introducción 81
Contraseñas 82
Inicio de sesión en dos pasos 82
Configuración del navegador 83
Inicio de sesión en el dispositivo 89
Sesión de Google en el navegador 89
Consejos para la navegación segura 92

Riesgos de Internet 94
Grooming 95
Ciberbullying escolar 98
Sexting y sextorsión 104
Juegos peligrosos 107
Pautas para la protección de datos en centros educativos 118
Introducción 118
Aplicaciones usadas en clase 119
Temas de interés para el profesorado 120
Protección de datos del centro 122

Seguridad y privacidad en Internet

Ciudadanía e identidad digital

Introducción

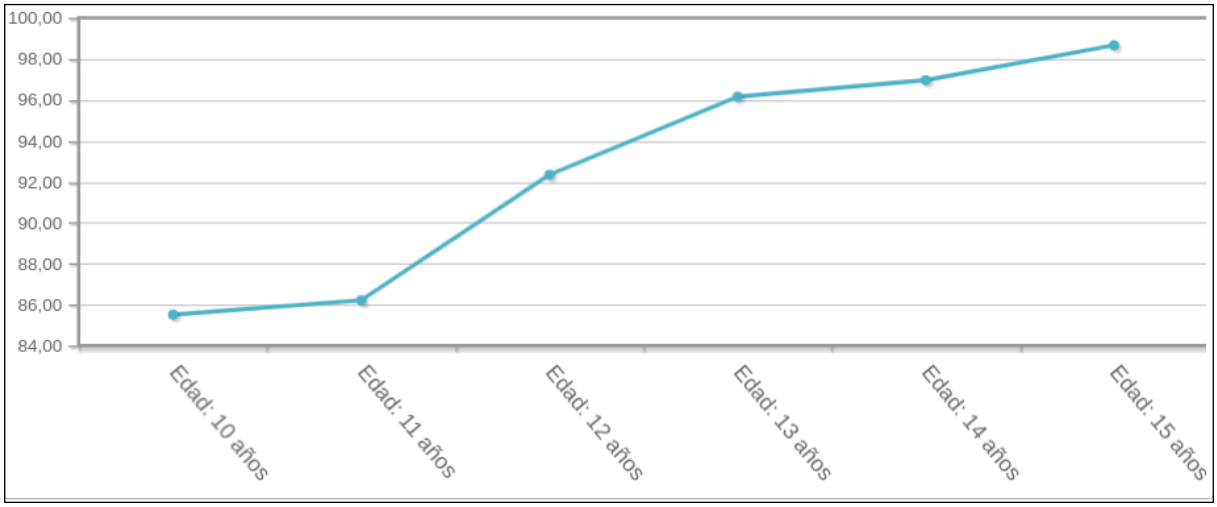
Ya hace tiempo que Internet dejó de ser una novedad, lo que en un principio se identificaba con páginas web estáticas ha evolucionado hacia el estado que tenemos en la actualidad. La Red se ha difuminado en una serie de servicios, herramientas y utilidades de las que no siempre somos conscientes del todo. La extrema generalización de la comunicación digital hace que, lo que antes era privado, ahora cada vez tenga menos probabilidades de serlo y, sin siquiera sospecharlo, nuestra información puede llegar muy lejos, incluso a personas a las que no conocemos y con las que siquiera nos relacionamos. La tecnología ha sufrido cambios espectaculares en los últimos años, la interconexión entre la gente se ha visto incrementada a medida que el tiempo pasa. Nuestra actividad digital no ha dejado de aumentar y el flujo de información se pierde muchas veces por lugares que no podemos controlar. Además, la edad en la que los niños empiezan a disponer de un teléfono con conexión a Internet va disminuyendo con el tiempo. Estos son algunos de los motivos por los que es tan importante la educación, ya que los niños tienen acceso a Internet desde muy pequeños y deben saber desenvolverse en este ámbito. Igual que se enseña cuándo se debe cruzar la calle y cuándo no, también tienen que saber qué se puede hacer y qué no en Internet.

Por lo tanto, existe una nueva responsabilidad que ha aparecido en siglo XXI: la de **saber ser ciudadano digital.**

El uso de internet

Según datos del INE[1], aproximadamente el 86 % de la población española de 16 a 74 años está conectada a Internet. Esta cifra se eleva hasta el 98 % si atendemos a la franja de edad de los 16 a los 24 años, y entre los 10 y 15 años el uso de Internet es del 93 %, es decir, la mayoría de los jóvenes están conectados. El siguiente gráfico, también del INE[2], nos indica el uso de Internet en 2018 desglosado por edades de este sector de la población:

Figura 1:
Jóvenes con conexión a Internet. INE. Instituto Nacional de Estadística. Resumen de datos de niños de 10 a 15 años.



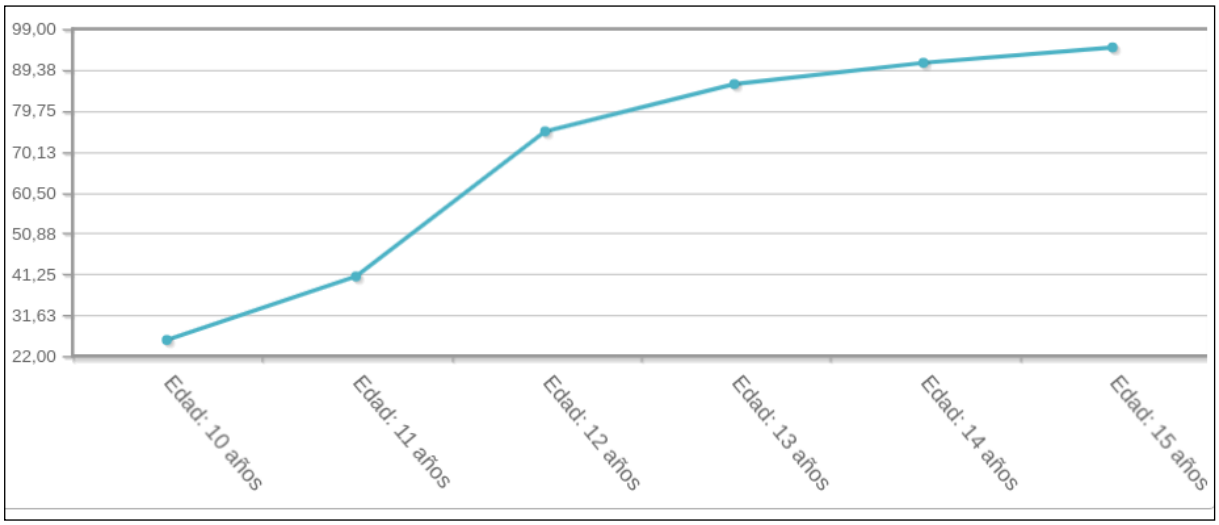
Nota 1: Tomado de *Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares, Sexo, edad, hábitat, tamaño del hogar, ingresos mensuales netos del hogar, Total Niños (10-15 años).* [Gráfico] por INE, 2018 [Página web] https://www.ine.es/jaxi/Datos.htm?path=/t25/p450/base_2011/a2018/l0/&file=01005.px#!tabs-grafico. Todos los derechos reservados

1 https://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528782&p=1254735110672&pagename=ProductosYServicios%2FPYSLayout

2 https://www.ine.es/jaxi/Tabla.htm?path=/t25/p450/base_2011/a2018/l0/&file=01005.px

En estas mismas edades, el uso de móvil es del 70 % (de 10 a 15 años) y del 99 % para los 15 años. En la siguiente gráfica lo vemos detallado por edades:

Figura 2:
Jóvenes de 10 a 15 años que disponen de teléfono móvil.



Nota 2: Tomado de *Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares, Sexo, edad, hábitat, tamaño del hogar, ingresos mensuales netos del hogar, Total Niños (10-15 años).* [Gráfico] por INE, 2018 [Página web] https://www.ine.es/jaxi/Datos.htm?path=/t25/p450/base_2011/a2018/l0/&file=01005.px#!tabs-grafico. Todos los derechos reservados

Estos datos nos dan una idea de hasta qué punto la tecnología está presente en la vida de niños y adolescentes. En ausencia de una educación en este sentido, no es de extrañar que se produzcan problemas como el ciberacoso, la suplantación de personalidad o el *sexting*, entre otros.

Además, no solo se producen en menores, sino que también afectan a determinados adultos que actúan muchas veces con desconocimiento o tienen un bajo nivel de preocupación por el tema de la veracidad, la privacidad y la reputación digital, lo que les lleva a cometer errores que pueden llegar a ser muy graves. Recuérdese el caso del linchamiento a los falsos secuestradores[3] de niños en Colombia, una noticia falsa difundida a través de WhatsApp que terminó con la muerte de un inocente y la agresión de dos más. La falta de un mínimo **razonamiento crítico** ante muchas de las informaciones que nos llegan hace necesaria una reflexión sobre nuestro comportamiento con respecto a Internet.

Ciudadanía digital

De las muchas definiciones que existen sobre el concepto ***ciudadano digital*** nos parece especialmente útil la proporcionada por Edith González en el artículo «Formación Ciudadana [digital], una nueva materia para el currículum escolar»:[4]

> «Un ciudadano digital es aquella persona que utiliza tecnología de la información para mejorar su participación en la sociedad, la política y el gobierno, o sea, los que utilizan Internet regularmente y con efectividad».

Así pues, la ciudadanía digital supone el conocimiento y la aplicación de la cultura y los valores sociales en el mundo de las tecnologías de la información y la comunicación. Y, por lo tanto, esto lleva a la aplicación de un código de conducta y ético en Internet.

Además, esta autora puntualiza lo siguiente:

3 https://www.24horas.cl/internacional/una-noticia-falsa-difundida-por-whatsapp-termino-con-un-hombre-muerto-por-linchamiento-en-colombi-2848599

4 http://formacionib.org/noticias/?Formacion-Ciudadana-digital-una-nueva-materia-para-elcurriculum-escolar

Son sinónimos o términos relacionados a "ciudadano digital": ciberciudadano, netizen, y e-ciudadano, quien

- Usa intensivamente la tecnología de la información.
- Puede tener su propio blog o sitio web.
- Utiliza de forma intensiva las redes sociales.
- Participa en sitios periodísticos.
- Tiene activa participación en el comercio electrónico.
- Usa sitios de organizaciones privadas, como bancos, y públicas, estatales, provinciales y/o municipales.

El concepto *ciudadano digital* lleva al nacimiento de una serie de ámbitos en los cuales se desenvuelve de forma habitual. Ribble, Bailey y Ross (2004) en Digital Citizenship[5] identifican nueve áreas relacionadas con la ciudadanía digital:

- **Etiqueta**: normas de conducta o formas de proceder en los medios electrónicos.
- **Comunicación**: intercambio electrónico de información.
- **Educación**: el proceso de enseñanza y aprendizaje sobre la tecnología, así como el uso de esta.
- **Acceso**: plena participación electrónica en la sociedad.
- **Comercio**: compra y venta electrónica de bienes.
- **Responsabilidad**: responsabilidad electrónica por acciones y hechos.
- **Derechos**: las libertades extendidas a todos en un mundo digital.
- **Seguridad**: bienestar físico en un mundo de tecnología digital.
- **Seguridad como autoprotección**: precauciones electrónicas para garantizar la seguridad.

La finalidad de esta publicación digital es tratar estos puntos, que, de un modo u otro, se verán reflejados a través de sus diferentes capítulos.

En la figura 3 de la página siguiente se recoge, a modo de resumen, una infografía propia sobre los nuevos ámbitos del ciudadano digital.

5 https://files.eric.ed.gov/fulltext/EJ695788.pdf

Figura 3:
Los nuevos ámbitos del ciudadano digital.

Nota 3: Adaptado de *Digital citizenship: Addressing appropriate technology behavior*, Ribble, M. S., Bailey, G. D., & Ross, T. W. (2004). Learning & Leading with technology, 32(1),

Identidad digital

La identidad digital es **todo aquello que nos identifica en Internet y, por tanto, nos define**. A medida que utilizamos diferentes herramientas, redes sociales o sistemas de mensajería, cada uno de nosotros va dejando una huella que es visible por cualquiera con acceso a un buscador o a nuestros perfiles en redes.

Este rastro lo forman los comentarios que realizamos en páginas web (por ejemplo, al valorar un producto que hemos comprado), los mensajes escritos en redes sociales como Twitter o Facebook, las fotos y los comentarios en aplicaciones como Instagram y un largo etcétera.

Como hemos dicho anteriormente, la mayoría de todo aquello que realizamos a través de los medios digitales deja alguna huella reconocible y rastreable por otros. En el mundo analógico —aquel que discurre al margen de las redes— esta huella que dejamos también nos define y caracteriza como personas. Cuando hablamos, escribimos o simplemente salimos cada día a la misma hora de casa, estamos dando información a los demás. Información que podrán captar (o no) de primera mano dependiendo de la atención que pongan o del interés que tengan por nosotros.

Esta realidad de nuestros actos suele definirnos tal como somos a no ser que estemos actuando o mintiendo por sistema en aquello que hacemos y decimos. Esta segunda posibilidad es mucho más frecuente en el mundo digital que en el analógico. El hecho de que podemos controlar fácilmente aquello que los demás ven de nosotros hace que se puedan dar casos de perfiles falsos o, siendo verdaderos, perfiles que ofrecen una imagen diferente a la realidad. Esta es la base para muchos de los engaños que encontraremos en las redes sociales y contra los cuales hemos de estar prevenidos los adultos y, muy especialmente, los menores.

Identidad y ciudadanía

Llegados a este punto nos podemos preguntar: ¿Qué relación existe entre la identidad y la ciudadanía digital? ¿Debemos ocultarnos en Internet de forma que no haya ningún vínculo entre nuestra vida real y la virtual?

Algunas personas optan por pasar totalmente desapercibidas y se niegan a tener perfiles en las redes sociales, tampoco utilizan ningún programa de mensajería y, en algunos casos, no disponen tan siquiera de teléfono móvil. Es verdad que todas las opciones son lícitas, pero, de cara a la pertenencia a la sociedad en la que vivimos, quizás no sea lo más indicado. Del mismo modo que una persona puede decidir no leer la correspondencia en papel que le llega hasta su buzón, tenga el origen que tenga (por ejemplo, una multa de tráfico o el pago de un impuesto), también puede hacer lo mismo en el mundo digital. Sin embargo, aparte de los problemas personales que le pueda ocasionar el vivir en la era pre-Internet, **como individuos pertenecientes a una sociedad tenemos el derecho y el deber de participar en ella** como miembros plenos.

El uso razonable de los mecanismos digitales que nos ofrece la sociedad debe contribuir a hacer de esta un lugar mejor. No es únicamente una forma de estar mejor informados o de obtener un beneficio particular de algún tipo, sino que la ciudadanía digital debe permitirnos **participar de forma activa en el desarrollo y mejora social**.

A nivel local, hay mecanismos de intervención en el desarrollo de nuestro barrio o ciudad —tales como las aplicaciones para dispositivos móviles que ponen en contacto a los **vecinos del barrio**— que permiten no solo estar al tanto de los problemas que tiene nuestro entorno más cercano, sino también aportar ideas, sugerencias o información útil para los que nos rodean (léase, por ejemplo, el artículo «Los móviles logran potenciar las relaciones vecinales en Barcelona»).[6]

También existen aplicaciones y servicios que actúan a nivel más general y que nos permiten interactuar en un entorno más amplio como ayuntamientos, comunidades autónomas y a nivel estatal. Podemos encontrar algunas de ellas en este artículo: «Las 10 mejores apps para promover la participación ciudadana en España y Latinoamérica».[7] Y en la página Aplicaciones de la Administración General del Estado[8] podemos encontrar algunas aplicaciones oficiales del Gobierno de España.

6 https://www.elperiodico.com/es/barcelona/20181216/tecnologia-logra-potenciar-relaciones-ayudas-vecinales-barcelona-7202783

7 https://www.compromisoempresarial.com/transparencia/2016/01/las-10-mejores-apps-para-promover-la-participacion-ciudadana/

8 https://administracion.gob.es/pag_Home/atencionCiudadana/app_age.html

Un ejemplo es la web change.org[9] permite hacer visibles las **causas de los ciudadanos** y los grupos que deseen dar visibilidad a sus peticiones, normalmente relacionadas con los derechos humanos (para saber más: https://es.wikipedia.org/wiki/Change.org en Wikipedia)[10]. Gracias a servicios como este podemos apoyar determinadas causas que consideramos justas y necesarias.

O bien, el **micromecenazgo**, también denominado ***crowdfunding*** o financiación colectiva, es otro aspecto, esta vez económico, muy relacionado con el concepto de ciudadanía digital. Además, permite a los particulares apoyar económicamente, con pequeñas aportaciones, proyectos tecnológicos, humanitarios y de otros tipos. Pueden verse algunas de las plataformas más importantes de este tipo en este artículo sobre micromecenazgo de la Wikipedia.[11] En estos otros dos artículos se pueden ver algunos casos exitosos de micromecenazgo: «Micromecenazgo en la era digital para empresas que buscan destacarse en el mercado»,[12] y «¿Qué es el 'crowdfunding' o micromecenazgo?».[13]

Así pues, vemos que ejercer la ciudadanía de forma responsable puede conllevar también la realización de estas y otras acciones que implican necesariamente el uso de una **identidad digital**. Identidad que debemos cuidar y proteger, pero no esconder si deseamos ejercer nuestros derechos en el mundo actual.

Los menores como ciudadanos digitales

La práctica totalidad de nuestros alumnos utiliza Internet y dispone de un teléfono móvil. Para ellos **la identidad digital es algo de lo que no pueden huir,** ya que la actividad que realizan a través de Internet es, por lo general, muy activa y con frecuencia de riesgo, ya que muchas veces suben fotos y vídeos personales sin ningún tipo de filtro ni reflexión.

Es necesario que los menores se hagan responsables de su pertenencia al mundo digital, donde todos tenemos también una forma de comportarnos y donde nuestros actos, como en el mundo real, pueden tener importantes consecuencias. En definitiva, deben ser **ciudadanos digitales responsables** que hacen un **uso racional y útil de Internet**, tanto para sí mismos como para la sociedad, que **evitan las situaciones de riesgo y son capaces de ayudar a otros**. El uso responsable de Internet no es un acto individual y aislado, sino que tiene repercusiones en muchas otras personas y, a diferencia del mundo analógico, estas repercusiones tienen un alcance mucho mayor, más rápido y en personas que pueden estar muy alejadas físicamente de nosotros. **Se trata, por lo tanto, de un nuevo ecosistema social que es necesario aprender a manejar y gestionar.**

Elementos de la ciudadanía digital

El documento Digital Citizenship[14] ha establecido unos elementos propios del ciudadano digital que hoy en día se toman como básicos para todos.

Acceso digital

El simple hecho de estar leyendo esto ya indica que se está en posesión de un **acceso digital**. Es lo que podríamos llamar un «**principio antrópico digital**» que nos puede hacer creer que el acceso es universal. Nos movemos por él y podemos tener la falsa idea de que así es para todos, pero no siempre lo es.

Precisamente el hecho de que más del 90 % de los jóvenes esté conectado hace que aquellos que no lo están puedan sufrir las consecuencias de su ausencia como la **falta de comunicación con los compañeros, el grupo de estudio o la dificultad para obtener información**. Se debe tener especial cuidado con aquellos que, por motivos económicos o de otro tipo, no dispongan de un acceso fácil a la Red, aun siendo una minoría.

9 https://www.change.org/

10 https://es.wikipedia.org/wiki/Change.org

11 https://es.wikipedia.org/wiki/Micromecenazgo#Plataformas_de_Crowdfunding

12 https://destinonegocio.com/co/negocio-por-internet-co/micromecenazgo-digital-para-empresas/

13 https://www.elperiodico.com/es/hablemos-de-futuro/20180725/que-es-crowdfunding-o-micromecenazgo-6953695

14 https://files.eric.ed.gov/fulltext/EJ695788.pdf

Otro aspecto a tener en cuenta es el dispositivo que se utiliza. No es lo mismo estudiar una presentación de clase o un texto electrónico desde la pantalla de un pequeño móvil que desde una tableta o un ordenador. En cierto sentido **no disponer de un dispositivo adecuado es equivalente a no disponer del acceso** a Internet, ya que para trabajar es necesario poder hacerlo con comodidad y durante períodos prolongados. Con un móvil lo único que conseguiremos es resolver dudas puntuales, pues su incomodidad hará que se reduzca también el tiempo de consulta.

Además, aunque el alumno disponga de un ordenador o una tableta donde poder trabajar cómodamente, perderá una gran parte de su eficacia si el profesorado no es capaz de adaptar sus clases a los nuevos tiempos. Aprender a manejar lo digital no es solo recibir consejos o clases sobre este tema, sino, sobre todo, usarlo en el día a día, con normalidad y no de modo exclusivo. A veces, por efecto de lo nuevo y la ilusión del profesorado, se cae en el extremo contrario y todo se hace a través de medios electrónicos, muchas veces forzando las herramientas y la metodología empleada sin causa que lo justifique. Un buen aprendizaje consistirá, sin duda, en el uso equilibrado y se debe evitar todo lo que sea exclusivamente analógico o exclusivamente digital.

Asimismo, el acceso a la nueva tecnología se puede ver impedido, en más de una ocasión, por la dotación escasa de los centros, donde el material es ya antiguo o se encuentra obsoleto; por las normas excesivamente restrictivas para su uso; o por la forma poco eficiente en la que hay que hacerlo. Estos factores echan para atrás a más de un profesor que usaría los medios, pero no lo hace por la dificultad que supone.

Así pues, los equipos directivos de los centros educativos deben poner especial atención tanto en la formación de sus profesores como en la accesibilidad de los medios que disponen. Ideas y proyectos magníficos pueden fracasar por una planificación pobre o defectuosa.

La facilitación del acceso a Internet de los menores tiene tanto una dimensión particular, en cuanto a los dispositivos que usa a nivel personal, como una educativa, respecto a los medios que ponemos a su disposición en las aulas. Para que los pequeños puedan convertirse en ciudadanos digitales con efectividad **debemos comprometernos y asegurarnos de que nadie queda fuera del acceso digital**.

Estrategias

Estrategias en la escuela

– Localizar en el aula a los alumnos que tienen dificultades en el acceso a Internet en su casa, especialmente la presencia o ausencia de:

  - Wifi.
  - Ordenador.
  - Tableta.
  - Teléfono inteligente.
  - Acceso a datos o solo wifi en el teléfono inteligente.

– Facilitar el uso de la tecnología a aquellos que carezcan de ella, por ejemplo, haciendo trabajos en parejas en las que uno de los miembros tiene acceso total y otro que carece de él o disponiendo de espacios con acceso a la wifi en la escuela.

Estrategias en la familia

- Valorar cuándo es el momento de disponer de un ordenador para el trabajo escolar, lo que sucederá, normalmente, en los últimos cursos de Primaria.
- Valorar cuándo es el momento de disponer de un teléfono móvil con conexión a Internet. Sería conveniente esperar a la ESO. Valorar también la necesidad de tener acceso a Internet mediante datos o solo mediante wifi.
- Antes de gastar el dinero en un dispositivo caro, valorar si nuestro hijo tiene lo que necesita para su trabajo escolar. Es preferible un ordenador portátil a uno de sobremesa, así lo podrá llevar a casa de los amigos o al colegio cuando lo necesite. La tableta puede ser útil cuando ya se dispone de un ordenador en casa, permite realizar muchas de las cosas que se pueden hacer con el ordenador, sin embargo, no todas y de forma menos eficiente. El móvil no sustituye al ordenador o la tableta, su uso no es práctico durante mucho tiempo, aunque sí lo es para poder estudiar o repasar en cualquier momento y lugar.

Etiqueta digital

La **etiqueta digital (o netiqueta) es el conjunto de normas de comportamiento general en Internet**. La Red tiene sus peculiaridades en cuanto a la comunicación entre personas, eso hace que tenga también unas normas especialmente adaptadas a la convivencia. Podemos destacar los siguientes factores como determinantes de estas reglas:

1. Los **tiempos de respuesta** son extraordinariamente cortos.
2. **Anonimato**. La posibilidad de crear perfiles falsos con nombres inventados hace que muchas veces se pueda actuar sin que el otro sepa quién es realmente.
3. **Alexitimia digital.** De forma similar a como sucede con el trastorno mental llamado *alexitimia* —que dificulta el captar y expresar emociones y sentimientos—, la comunicación a través de medios digitales muchas veces también carece de esa capacidad. Cuando la comunicación es textual se pierde totalmente la capacidad de expresar sentimientos a partir de la corporalidad como los movimientos y gestos de las manos o la expresión de la cara.
4. **Interculturalidad**. Por primera vez en la historia de la humanidad es posible la conversación simultánea desde lugares opuestos de la Tierra. Eso hace que puedan confluir en una misma conversación —ya sea de Twitter, Instagram, Facebook, Telegram o WhatsApp— **personas de culturas distintas, con formas distintas de interpretar las palabras y los sucesos cotidianos,** con otras con las que estamos acostumbrados a convivir diariamente.

La netiqueta aparece como un medio de regular la comunicación, sobre todo la textual, y como un modo de evitar los malentendidos con el fin de evitar ofender o molestar a otros. En los inicios de Internet se hicieron muy populares las listas de correo[15] y los grupos de noticias[16], en los que eran frecuentes las peleas y los enfados. Entonces se hizo evidente la necesidad de unas normas que habría que seguir si se quería que el sistema de comunicación fuese útil. Estas varían de un servicio a otro, pero podemos sugerir algunas que deberían ser seguidas la mayoría de las veces, si no todas.

Muchas veces se mezclan las normas de seguridad con las de comportamiento, cuando en realidad son cosas totalmente diferentes. A continuación, se expone una selección de normas básicas de conducta que nos ayudará a ser un mejor ciudadano digital.

15 https://es.wikipedia.org/wiki/Lista_de_correo_electrónico

16 https://es.wikipedia.org/wiki/Grupo_de_noticias

Normas de conducta

- Nunca debemos olvidar que **al otro lado hay un ser humano**, es importante no herir sus sentimientos, ponerse en el lugar de la otra persona y preguntarse si desearíamos que nos traten como lo hacemos con ella. Los alumnos deben tener muy claro que el hecho de no ver en ese momento a la persona a la que escriben no significa que lo que digan va a causar menos impacto sobre ella.
- Internet no es un mercado libre de productos gratuitos. Lo que es ilegal en el mundo real, también lo es en Internet. Al igual que no enseñamos a nuestros alumnos a robar en las tiendas, sino todo lo contrario, del mismo modo debemos enseñarles a usar responsablemente los recursos de la Red, con el fin de evitar las descargas ilegales o el uso de ciertos trucos para no pagar servicios que son de pago. **La honradez y la responsabilidad** han de ser nuestra forma de conducta tanto dentro como fuera de la Red. Es necesaria la educación activa en este campo para que el respeto por los demás sea el hilo conductor.
- Se debe cuidar el **estilo con el que escribimos**, muchas veces será lo único que los otros percibirán de nosotros:

    - Vigilar la **ortografía**, especialmente en los mensajes enviados con el móvil, la tendencia es a acortar los mensajes con abreviaturas y a prescindir de los acentos.
    - Evitar escribir con **mayúsculas**. LAS MAYÚSCULAS SE UTILIZAN PARA GRITAR.

- Hay que ayudar a mantener los **debates sanos y en un tono educativo**. Debemos evitar las provocaciones y participar activamente para que no se produzcan.
- Los mensajes de **correo** que enviemos deben ir precedidos de un **saludo** y una **despedida** al final del mismo.
- El **asunto** de los mensajes de correo electrónico debe reflejar el motivo de lo que enviemos. Si mandamos un mensaje por correo a nuestros alumnos para que traigan determinado material a clase, es mejor un asunto del tipo «Material para la clase de biología» que algo menos descriptivo como «Biología».
- Cuando recibamos un mensaje de correo al que debamos responder, se considera un **plazo razonable de respuesta** hacerlo entre 24 y 48 horas después de recibirlo. Desgraciadamente esto no se aplica a los programas de mensajería como WhatsApp o Telegram, donde el plazo es mucho menor, del orden de 1 a 3 horas como mucho. En un contexto educativo deberemos valorar los tiempos de respuesta de forma particular. Responder a un mensaje que nos manda un alumno dos días después de hacerlo no tiene sentido, ya que lo habremos visto con antelación.
- **No reenviar mensajes** a no ser que sea necesario. Vivimos en la época del reenvío de mensajes porque nos parecen graciosos, simpáticos o «por si acaso» lo que dicen es verdad. La realidad es que uno de los motivos de cansancio en la comunicación electrónica es la afluencia masiva y continua de mensajes intrascendentes, falsos y que no aportan nada. Si reenviamos algo, que sea porque es necesario que el que lo reciba lea ese mensaje. Evitemos los mensajes de tipo cadena y, sobre todo, aquellos que dicen que hay que reenviarlos al mayor número de personas.
- Antes de enviar un mensaje en una red social o en un grupo de mensajería, **debemos pensarlo dos veces**, pues llegará inmediatamente a sus destinatarios y, aunque podemos borrarlos si nos arrepentimos, casi con seguridad ya habrá sido leído por más de uno. Lo mismo sucede con los vídeos e imágenes. Procuremos no enviar **material gráfico** que pueda ofender o del que nos podamos arrepentir más adelante. Una buena guía es pensar si colocaría esas imágenes en el tablón de anuncios de clase o de la escuela. Debemos recordar que **lo que se coloca en la Red, se queda en la Red**. Una vez que un texto o una imagen abandona nuestro ordenador, tableta o teléfono móvil, ya no tenemos más control sobre él, aunque nos parezca lo contrario.
- En los grupos y las redes sociales debemos tener mucho cuidado con el **sentido del humor**: lo que nos parece gracioso o normal a otros les puede parecer ofensivo o ridículo. Este es uno de los mayores motivos de desencuentro y enfrentamiento *online:* los malentendidos derivados de un uso diferente del lenguaje y su interpretación.

- En situaciones informales, al escribir en redes sociales podemos utilizar los **emoticonos** para reforzar los sentimientos que queremos transmitir. Como ya se ha indicado, uno de los problemas de la comunicación textual es la interpretación del tono con el que se está hablando.
- Nunca debemos crear perfiles falsos o que den una idea contraria de lo que somos.

Figura 4:
Etiqueta digital

Nota 4: Elaboración propia

Netiqueta en la escuela

Además de la netiqueta de carácter general y que todos deberíamos intentar respetar, hay ciertas normas que debemos aplicar nosotros mismos como docentes y ellos como alumnos, ya que son exclusivas del ecosistema docente en el que nos movemos a diario.

Docentes

- **Respetar los tiempos de trabajo y descanso de los alumnos**. A no ser que esté pactado con anterioridad, no se debe enviar trabajo por sorpresa a casa a través de los medios digitales. La posibilidad de contactar con los alumnos fuera de clase ha hecho que en los últimos tiempos algunos profesores puedan llegar a abusar de esta situación. Por ejemplo, sin previo aviso, un lunes por la tarde enviar un trabajo para entregar el martes. Es muy posible que no estén pendientes de nosotros o, si lo están, quizás no podrán dedicar las horas que les quedan para hacerlo, debido a que tienen otras obligaciones extraescolares.
  Estas situaciones crean frustración en los alumnos y rechazo por parte de las familias que ven cómo el profesor interfiere en sus horarios. Si enviamos tareas a los alumnos que tendrán que realizar en casa, deberemos **avisar siempre con antelación** para que el alumnado pueda prepararse y organizar su tiempo.
- En la **corrección de trabajos *online***, hay que tratar de **enviar siempre una retroalimentación** al alumno, es decir, algún comentario, anotación o aclaración que, preferiblemente de forma **positiva**, ayude al alumno en su aprendizaje.
- **Pactar con los alumnos la forma que tienen de comunicarse con nosotros fuera del horario escolar**, si es que así lo queremos. Debemos darles una forma para que nos puedan hacer preguntas de la materia (correo, programa de mensajería que usemos con ellos, mensajes a través del servicio educativo que tengamos en nuestro centro, etc.) o, por el contrario, dejar bien claro que no deben hacerlo.

Alumnos

- Mantener la **buena educación** también en el medio digital. Es frecuente que los alumnos envíen correos al profesor que carecen de cualquier saludo o introducción de la situación. Mensajes de correo electrónico que contienen únicamente una frase del tipo: «¿Qué entra para mañana?» son los más habituales. Debemos enseñarles que las buenas maneras de saludar y despedirse también rigen aquí.
- Cuando se está colaborando en un mismo documento o se tiene acceso a los de otros compañeros del grupo hay que **respetar el trabajo** de todos ellos. Es frecuente ver como, por broma, borran o estropean lo realizado por otros.
- **No copiar y pegar textos o imágenes de Internet** sin citar al autor o la fuente. Hoy en día es muy frecuente esta práctica para realizar los trabajos, muchas veces sin pararse a pensar en lo que se está haciendo. Debemos enseñar a respetar la propiedad intelectual y a actuar en consecuencia.

Estrategias

Estrategias en la escuela

- Dedicar tiempo en clase a trabajar las normas de netiqueta.
- Crear las propias normas de respeto mutuo de la clase.
- Provocar situaciones donde su uso sea crítico. Por ejemplo, se puede compartir el mismo documento con toda la clase para que trabajen de forma simultánea o se pueden crear debates *online* que les motive a la discusión encendida a través de algún tema polémico.
- Ser muy sensibles cuando se rompan las normas para poder rectificar al alumno.

Estrategias en la familia

- Pactar unas horas diarias o semanales de Internet como uso lúdico. Especialmente el tiempo dedicado a navegar sin un destino fijo por las redes sociales y a ver películas o series.
- Evitar que el menor se aísle de la familia en su habitación con el móvil o el ordenador. Buscar un lugar donde esté a la vista de los padres.

Figura 5:
Estrategias en la escuela y la familia para el acceso digital

Nota 5: Elaboración propia

Para saber más

- NETEtiquete[17] (1994) de Virginia Shea. Este libro ha sentado las bases de la netiqueta en Internet. Eduteka ha hecho un resumen titulado «Las 10 reglas básicas de la "netiqueta"».[18]
- «Las buenas maneras en Internet»[19] (2002) de Miguel Zapata.
- «Netiqueta Institucional»[20] (2018) de Diana Rubio. Interesante artículo donde se discute cómo deben comportarse las instituciones en Internet. Aplicable a los centros educativos.

Comunicación digital

La comunicación ha cambiado desde la existencia de los móviles y, especialmente, desde que el acceso a Internet se ha generalizado en casi todos estos dispositivos. Estas nuevas formas de comunicación pueden ser empleadas en un mal sentido si se usan para excluir o acosar a otros. Podemos simplificar los medios de comunicación más usados en los siguientes:

- **Correo electrónico**. Es el sistema de comunicación electrónica más formal. Se utiliza principalmente cuando deseamos que quede constancia de nuestro mensaje o cuando hay que enviar textos largos o adjuntos.
- Mensajes en **foros de discusión**. Son mensajes públicos, aunque restringidos a los miembros de una clase o grupo. Se utilizan para dudas de los alumnos, avisos del profesor, aclaraciones, etc. En general, para cuestiones que interesan a todos los miembros de una clase en particular.
- **Mensajería instantánea**. Puede ser la tradicional (WhatsApp, Telegram o Hangouts, por ejemplo) o los sistemas de mensajes incluidos en algunos de los servicios educativos que, sin ser programas de mensajería, se comportan como si lo fuesen, ya que se reciben notificaciones directamente en el móvil y pueden responderse con este dispositivo. Si se han creado grupos, se pueden utilizar como los foros de discusión. Muchos de los alumnos suelen elegir este sistema para comunicarse en privado con el profesor.
- **Videoconferencia/voz IP**. La videoconferencia y la voz IP —que es el equivalente a una llamada telefónica, pero usando los servicios de Internet—, a través de Skype o WhatsApp, es muy frecuente entre los adolescentes que quedan de este modo para trabajar juntos y hacer deberes sin necesidad de ir a casa de uno de ellos.
- **Mensajes a través de redes sociales**. Especialmente Instagram que es una de las redes más usadas por los jóvenes en la actualidad.

El menor debe saber qué sistema es apropiado en cada ocasión. Para tal finalidad los centros deben trabajar las diferentes facetas de la comunicación y es aconsejable utilizar más de un sistema, según la ocasión. En los alumnos de 16 años pueden incluirse el uso de las redes sociales como parte de la comunicación.

17 http://www.albion.com/netiquette/book/index.html

18 https://eduteka.icesi.edu.co/articulos/Netiqueta

19 https://www.um.es/tonosdigital/znum5/bm/buenas_maneras vers Nov.htm

20 http://revistas.uned.es/index.php/EEII/article/view/22181/pdf

Estrategias

Estrategias en la escuela

- Planificar el uso de los medios más habituales de comunicación en la clase a través de todo el curso escolar mediante el diseño de trabajos que requieran el uso de diferentes medios.
- Fomentar la creación de grupos de trabajo con medios digitales.
- Potenciar el uso de la videoconferencia y la voz IP para el estudio por parejas desde casa.

Estrategias en la familia

- Establecer un diálogo padres-hijos con el fin de que estos últimos les expliquen lo que escriben y publican en Internet, les den a conocer a sus amistades digitales y lo que se envían.

Alfabetización digital

Sin lugar a dudas, este elemento de la ciudadanía digital es uno en los que más pueden aportar los centros porque de ellos depende la decisión de qué deben saber los alumnos en vistas a su integración en la sociedad adulta. Además, la alfabetización digital se lleva a cabo a través de la educación digital en los centros.

Según el artículo «El Derecho a la Educación Digital»,[21] **la educación digital es aquella «que hace uso de las tecnologías digitales y que tiene como objetivo la adquisición de competencias y habilidades para aprender a aprender tanto de profesores como de alumnos, en formación permanente».**

Este artículo también señala estos cuatro aspectos (se cita textualmente):

- La educación digital representa un cambio de paradigmas. De la etapa industrial a la época del conocimiento. De la transferencia de información al propósito de aprender a aprender.
- El rol de profesor como transmisor de conocimientos se transforma en la educación digital y ahora se convierte en guía del proceso de aprendizaje.
- Esta educación digital no tiene restricciones de tiempo ni espacio. Es permanente, está disponible a cualquier hora, en cualquier momento y en cualquier lugar.
- Las tecnologías digitales no son un fin, sino un método para conseguir el desarrollo de competencias y habilidades.

Así, el profesor se ve también inmerso en esta educación digital que se convierte en un aprendizaje y un reciclado permanente. Debido al ritmo de cambio continuo que tiene la tecnología, el **aprender a aprender** no es solamente una expresión de moda, sino un requisito imprescindible para poder utilizarla. Solo de aquellos que sean capaces de amoldarse al momento en el que se está viviendo, podremos decir que están realmente alfabetizados.

Y la alfabetización ya no es aprender una serie de conceptos estáticos, es comprender tecnologías y sistemas que varían su mecanismo y potencial a lo largo del tiempo, pero no su función. Por ejemplo, las nuevas versiones que tienen los programas que usamos a diario hace que un programa de hoy no se parezca casi en nada al mismo de hace unos años. Cambios de diseño y de funciones hace que, aunque la finalidad sea la misma, versiones muy alejadas en el tiempo parezcan en realidad programas diferentes.

21 https://ayudaleyprotecciondatos.es/2018/11/12/derecho-educacion-digital/

Podemos encontrar esta disparidad en la forma de funcionar de los teléfonos móviles, las tabletas o los ordenadores, pero también aparece tecnología nueva, inexistente hace poco, que se incorpora a nuestras vidas (Chromecast, altavoces inteligentes, etc.). Lo único que sabemos es que la tecnología es cambiante, a un ritmo insospechadamente rápido, desde hace tan solo un par de décadas. La finalidad de la alfabetización digital es justamente esta: poder utilizar la tecnología óptima en cada momento y situación.

Estrategias

Estrategias en la escuela

- Fomentar el uso de las nuevas tecnologías entre el profesorado, especialmente de los más reticentes. Por ejemplo, se pueden crear sesiones de trabajo donde los docentes expongan el uso que hacen de la tecnología para intercambiar ideas y ver la idoneidad de cada método.
- Ofrecer/pedir cursos de formación en tecnología del profesorado en el propio centro.
- Fomentar el uso de la tecnología en clase, no como algo diferente que se hace de vez en cuando, sino que se debe integrar de forma natural en el día a día. Por ejemplo:

  - Poner siempre los exámenes con sus respuestas en Internet tras su realización.
  - Cada semana un alumno envía una noticia sobre ciencia al grupo de clase y luego explica qué es lo que ha enviado y por qué en 5 minutos de clase a sus compañeros.
  - Publicar las tareas que tienen que hacer los alumnos en un calendario o grupo de clase.

- El uso de técnicas como Flipped Classroom ya llevan implícito el uso total de la tecnología.

Estrategias en la familia

- Si los padres somos competentes en TIC, tendremos la capacidad de informarnos de los trabajos digitales que hacen nuestros hijos y las herramientas y formatos en el que se los piden, de este modo podremos aconsejarles lo óptimo en cada momento y ayudarles cuando lo necesiten.
- Fomentar el uso de libros electrónicos o tabletas como sustitutos de los libros en papel (no hablamos de libros de texto, sino de los de lectura y otros libros de consulta). Además, los libros electrónicos son más baratos y no consumen papel.

Para saber más

- Se aconseja leer el artículo «10 ventajas de la educación digital».[22]

22 https://entreparentesis.org/10-ventajas-de-la-educacion-digital/

Responsabilidad y derechos

La **responsabilidad,** en este caso, hace referencia a **la que se tiene en el medio digital por nuestras acciones y hechos**, es decir, nuestros **deberes como ciudadanos digitales**. Internet no es ajeno a las leyes que nos rigen en el mundo real, aunque pueda parecer que casi todo está permitido y haya sensación de impunidad porque, por ejemplo, se puede descargar material protegido como películas o canciones.

Esta responsabilidad, que es tanto ética como de carácter legal, debe enseñarse a los niños desde el momento en el que empiezan a usar alguno de los servicios de Internet. Más adelante hablaremos de forma mucho más extensa sobre la propiedad intelectual en Internet y aquello que podemos y no podemos usar de la Red, así como la forma apropiada de hacerlo. También se tratará en otro apartado sobre las conductas de peligro y aquellas que pueden ser claramente delictivas como el acoso o la sextorsión.

Ahora baste recordar que somos responsables de aquello que hacemos en la Red y que debemos tener siempre presente que nuestros actos no son anónimos y no debemos comportarnos de forma diferente a como lo haríamos en la vida diaria.

Del mismo modo que tenemos una serie de **responsabilidades y deberes**, también tenemos los mismos derechos que los demás con aquello que hacemos en el mundo digital. En realidad, la responsabilidad y los derechos son las dos caras de la misma moneda.

Seguridad física y psicológica

La seguridad hace referencia a la salud física y psicológica del ciudadano digital. Más adelante se tratará el tema de la salud psicológica relacionado sobre todo con los peligros de Internet.

En relación a la **salud física,** hay unas cuantas normas de seguridad que podemos seguir para evitar los daños.

Figura 6:
Salud en el ordenador

Nota 6: Tomado del artículo «Salud en la computadora: 10 males frecuentes y cómo evitarlos» de Alonso Martínez, 2012, https://kutt.it/zPQKmX

Pantallas

Los dispositivos móviles de pequeño tamaño deben usarse a una distancia de 35-40 cm si van a utilizarse durante un tiempo prolongado.

La pantalla del ordenador debe estar, al menos, a 50 cm de los ojos.

Si no se lee bien la pantalla (sea cual sea), en lugar de acercarnos a ella, debemos aumentar el tamaño de la letra hasta que lo veamos cómodamente. La mayoría de aplicaciones llevan funciones de *zoom* (en todos los navegadores se amplía la letra con **CONTROL +** y se reduce con **CONTROL -**). En los móviles podemos aumentar el tamaño en la configuración de la pantalla, tanto la letra como el resto de iconos. Además, los sistemas operativos suelen llevar alguna opción para modificar el tamaño general de los objetos en la pantalla. El artículo «Cambiar la resolución y el tamaño del texto en Windows 10»[23] enseña a hacerlo en Windows 10.

Tiempo

Al mirar una pantalla, los ojos parpadean menos, por lo que se resecan y sufren las consecuencias. La recomendación es mirar cada 20 minutos al menos a 6 metros de distancia durante unos 20 segundos. En el caso de los ordenadores, los portátiles resecan menos el ojo que los de sobremesa, ya que al mirar hacia abajo hay menos superficie ocular expuesta al aire.

Postura

Cuando se trabaja con un ordenador, se debe mantener la espalda recta y las manos al mismo nivel que los brazos de forma que la muñeca de la mano con la que cogemos el ratón no esté formando ángulo hacia arriba ni hacia abajo; tampoco debe hacerlo ni hacia la izquierda ni a la derecha.

La silla que se use debe tener la altura regulable para poder situarse a la más apropiada, además de lo dicho anteriormente para las muñecas, las rodillas deben quedar por debajo de las caderas.

Luz

Es preferible que la luz que se use sea natural. También hay que evitar un brillo excesivo de las pantallas. Para la noche se aconsejan los filtros de luz que hay disponibles en Android o iOS (se aconseja el artículo «Usa un filtro de luz azul en tu móvil para proteger tus ojos»)[24] , también en Windows (se puede consultar «Activar modo nocturno en Windows 10»)[25] o en Ubuntu (es muy recomendable «Configurar la temperatura del color de la luz nocturna en Ubuntu 18.04»)[26].

Extensiones como Deluminate[27] permiten invertir los colores en el navegador Chrome con el objetivo de conseguir también un modo nocturno.

Estrategias

Estrategias en la escuela

– Al comienzo de curso, conviene informar a los alumnos sobre la forma correcta de utilizar los dispositivos electrónicos.

23 https://tecnologia.net/cambiar-la-resolucion-y-el-tamano-del-texto-en-windows-10/

24 https://www.movilzona.es/2018/12/25/filtro-luz-azul-movil-android-iphone/

25 https://www.elguruinformatico.com/activar-modo-nocturno-filtro-luz-azul-en-windows-10/

26 http://ubuntinux.blogspot.com/2018/08/configurar-la-temperatura-del-color-de.html

27 https://chrome.google.com/webstore/detail/deluminate/iebboopaeangfpceklajfohhbpkkfiaa

Estrategias en la familia

– El joven debe disponer de un espacio de trabajo correctamente iluminado y con una silla y mesa adecuada para el trabajo continuado. Especialmente en los niños más pequeños hay que evitar que la silla sea demasiado baja para la mesa que usan, ya que a la larga puede conllevar problemas de salud.

Seguridad como autoprotección

A medida que aumenta la incorporación de Internet en la vida del estudiante, este debe aprender a proteger sus datos y su propia persona. Estas medidas van más allá de la seguridad del ordenador o del móvil, ya que incluye actitudes y comportamientos que afectan a la forma en la que se enfrenta al medio digital y cómo reacciona ante los problemas o posibles amenazas que le puedan surgir. Se hace necesaria una actitud activa, coherente, delante del problema de la actividad personal en Internet.

Formación para alumnos

Netiqueta: las normas de mi clase digital

– Tipo de actividad: **Diálogo/debate en la clase.**
– Duración: **1 hora.**
– Niveles implicados: **Cursos de la ESO, aunque puede adelantarse a 6.º de primaria.**
– Objetivos:

  - **Aprender y fomentar el uso de la netiqueta entre los alumnos.**
  - **Toma de conciencia de la importancia del uso de unas normas básicas de convivencia en Internet.**
  - **Elaboración de las normas básicas de convivencia digital que seguirán los alumnos a lo largo del curso.**

Netiqueta: las normas de mi clase digital

En los centros fuertemente digitalizados esta tarea la puede llevar a cabo el tutor. En el caso de que el uso de los medios digitales sea más esporádico, esta función puede ser responsabilidad del profesor de informática o de cualquier otro. Las tareas son:

1. Plantear la pregunta a la clase: **¿Es necesario seguir ciertas normas y reglas en la comunicación con otros a través de Internet?** Establecer un breve diálogo o debate de 10 minutos.
2. Entre todos los alumnos, elaborar una lista de posibles normas a las que ellos se comprometerán a seguir en sus relaciones digitales con el resto de la clase y el profesor.
3. Proyección del vídeo ***Grupo Educare-Netiqueta***: https://www.youtube.com/watch?v=3t3D7IUxPjo
4. Aportar nuevas ideas surgidas tras su visionado.
5. Elaborar la lista definitiva después de eliminar aquellas que no se consideren necesarias y añadir las que falten por parte del profesor.
6. Transcribir la lista a un documento digital y colocar su enlace en algún punto visible para todos (Google Classroom, blog del grupo, tablón de anuncios de la clase, etc.).

Formación para familias

Netiqueta: las normas de la escuela

- Tipo de actividad: **Página web *online*.**
- Niveles implicados: **Todos los niveles.**
- Objetivo: **Informar a los padres sobre el compromiso adquirido por sus hijos en la conducta social digital que mantendrán a lo largo del curso y que ellos deben también conocer y aplicar.**

En los primeros días del curso escolar, se recomienda:

1. Elaborar un documento de síntesis con las normas surgidas en la clase de sus hijos o, en su defecto, un escrito estándar sobre netiqueta básica y colocarlo en la página del centro. Su objetivo es explicar brevemente lo que es la netiqueta y para qué sirve.
2. Difundir esta página entre los padres.

Puede verse un ejemplo de esto en el blog del CEIP San Walabonso.[28]

28 https://informacionparafamilias.blogspot.com/2013/10/netiqueta-la-educacion-en-internet.html

Alfabetización: uso de la plataforma escolar

- Tipo de actividad: **Taller**.
- Duración: **2 horas.**
- Niveles implicados: **Todos los niveles**, pero este tema adquiere más relevancia a partir de 5.º de primaria.
- Objetivos:

  - **Alfabetización de padres y madres.**
  - **Preparación para poder acompañar y ayudar a los hijos en las destrezas digitales.**

Actualmente, la mayoría de centros educativos utiliza alguna plataforma que incluye numerosos servicios tanto para la gestión de la escuela como para información y comunicación con los padres.

Se puede aprovechar la oficialidad de los sistemas de notas a través de plataformas educativas para realizar un taller de 1-2 horas de duración. Mediante el uso de los ordenadores del centro y los teléfonos móviles, se busca formar sobre los siguientes aspectos:

1. El funcionamiento de la plataforma, incluyendo cómo consultar las notas, ausencias y otras informaciones sobre sus hijos.
2. La forma de ponerse en contacto con el profesor o tutor para pedir entrevistas, justificar ausencias, etc.
3. Uso de la aplicación móvil de la misma plataforma del centro.
4. Otros aspectos digitales relacionados con sus hijos, tales como:

   - Programas y sistemas informáticos más importantes que se utilizarán en clase (G Suite, Genially, CmapTools, etc.). De este modo, saben qué es lo que necesitaran los niños durante el curso.
   - Formas de comunicación alumno-profesor (correo, mensajes en foros de clase, plataforma educativa, programa de mensajería, etc.) y normas o aspectos a tener en cuenta relacionados con esta comunicación.

Ética en el mundo digital

En el apartado anterior, dedicado a los elementos de la ciudadanía digital, se ha mencionado de forma implícita la ética en la etiqueta digital o en los deberes y derechos digitales. Pero esto no quiere decir que se circunscriba nada más a estos ámbitos, realmente la ciudadanía digital es una ética de la persona en relación a su presencia activa en Internet.

Del mismo modo que en los últimos años se habla del comercio justo (acción por la que el ciudadano de a pie busca comprar productos que hayan sido obtenidos de una forma éticamente sostenible en lo económico, lo social y lo ambiental, de forma que comprador y vendedor llegan voluntariamente a un acuerdo favorable para ambas partes), en Internet podemos hablar también del mismo concepto en relación a los servicios que utilizamos. Esto nos lleva al concepto de **Internet Justo**.

Ética en lo digital e Internet Justo

El concepto de **Internet Justo** supone que Internet es un **bien común**, entendido como algo de lo que se beneficia el conjunto de los ciudadanos, que debe ser accesible para todos y no debe estar

en manos de particulares o gobiernos que lo dirijan o manipulen para sus propios fines. En el Internet Justo, **todos aquellos que lo usan se benefician,** mediante el establecimiento de **acuerdos voluntarios y mutuamente provechosos** entre sus diferentes partes, **sin que terceros salgan perjudicados**.

Así pues, este concepto de Internet Justo nos lleva a **proteger aquello que lo preserva como bien común** y a rechazar los usos egoístas y que perjudican a parte de sus usuarios. Para poder llevar a cabo este concepto de Internet, hace falta una ética personal. La ética que nos guía en la Red es aquella que nos lleva a preservar su viabilidad en lo económico, lo social y lo personal. No sería ético, por ejemplo, reenviar mensajes falsos sabiendo que lo son, ya que atenta contra otros ciudadanos digitales. Tampoco lo sería descargar un libro de forma gratuita si su autor todavía conserva los derechos sobre él, aunque podamos hacerlo y nadie nos vaya a decir nada.

Busom, en su artículo «Prolegómenos para una ética digital»,[29] nombra cinco deberes de la ética digital, de los que destacamos cuatro de ellos. Son los siguientes:

1. **Deber de transparencia**. La opacidad va en contra de una ética digital. Lo que ocurre en la Red debe ser registrado y se debe luchar contra todo fraude.
2. **Deber de ecuanimidad**. Se busca un equilibrio en la Red que evite los monopolios y el control de las minorías poderosas sobre el uso y acceso de la información.
3. **Deber de participación**. Se promueve la participación activa y se vela por el buen comportamiento en la sociedad digital.
4. **Deber de protección**. La salud, la higiene y la seguridad en la Red corresponden a una responsabilidad colectiva.

Una de las características del mundo digital es que, a diferencia del mundo real, muchos de nuestros actos son totalmente invisibles para los demás y, aunque todo es rastreable, al menos en teoría, la realidad es que para muchas personas Internet no es más que un gran territorio sin ley, donde todo es posible.

Si entramos en un supermercado y nos llevamos sin pagar un litro de leche, lo más normal es que nos paren a la salida y nos pidan explicaciones. Pero, si entramos en Internet y nos descargamos una película sin pagar, lo más normal es que nadie nos diga nada ni nos pidan explicaciones. Esto es lo que hace que aquí, más que en otra parte, sea necesaria una ética de la conducta. La viabilidad de la sociedad digital depende directamente del buen comportamiento de sus ciudadanos.

Para que Internet sea realmente justo y un bien común sostenible, es imprescindible la ética en todo lo que concierne a nuestra relación con la Red.

La falta de ética

Aunque aspectos como las descargas ilícitas, el no respetar los derechos de autor, el acoso, la suplantación de identidad o los fraudes tienen una relación indiscutible con la ética (la personal, sobre todo) y quizás sean las primeras cosas que se nos vienen a la cabeza al hablar de falta de ética, ahora queremos llamar la atención sobre grandes empresas o instituciones cuya ética dudosa nos puede afectar.

Traficantes de datos

A pesar de que no es el único caso, uno de los más famosos es el de Facebook. Esta empresa compartió datos con empresas como Amazon o Netflix, entre otras 150, las cuales podían acceder a información que los usuarios no habían autorizado para ser usada fuera de Facebook. Aunque no se sabe con seguridad, parece que, a cambio, la red social adquiría de esta forma más usuarios. Para más información, se puede consultar el siguiente artículo: «Facebook compartió datos sensibles de sus usuarios con más de 150 grandes empresas».[30]

Además, los datos de todo aquello que se escribe de forma pública en las redes sociales como Twitter, Facebook o Instagram (especialmente la primera, donde casi todas las cuentas son públicas)

29 http://www.digitalresponsability.com/2015/06/prolegomenos-para-una-etica-digital.html

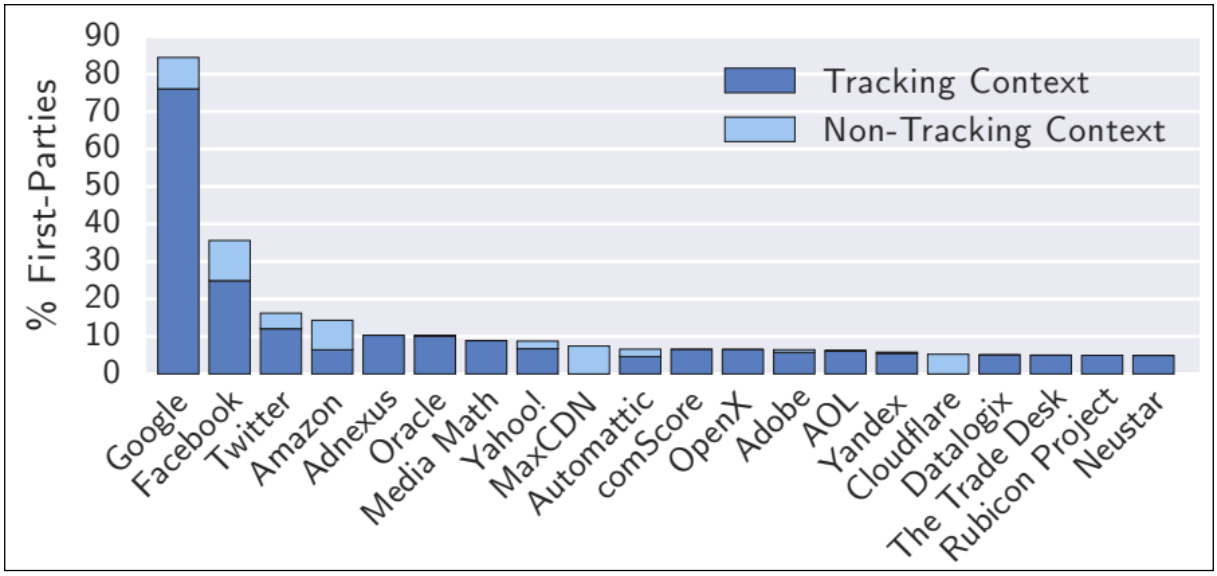
30 https://elpais.com/tecnologia/2018/12/19/actualidad/1545221673_589059.html

pueden ser leídos legalmente por empresas dedicadas a la minería de datos y, aunque suele haber restricciones en el número de datos que se extraen o el alcance de las búsquedas, la realidad es que de este modo se consigue una nutrida cantidad de datos personales.

Rastreo de la actividad

Muchas empresas tienen fragmentos de código en páginas web ajenas a su propio servicio que recopilan información sobre nosotros, de forma que pueden rastrear nuestra actividad a través de Internet. En el artículo «Online Tracking: A 1-million-site Measurement and Analysis»[31] se analiza con detalle, sobre un millón de páginas, las empresas que realizan este rastreo (*tracking*) y, en consecuencia, han elaborado el siguiente gráfico:

Figura 7:
Rastreo a través de Internet



Nota 7. Obtenido de *Online Tracking: A 1-million-site Measurement and Analysis* (p. 8), por Englehardt, S. y Narayanan A., http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

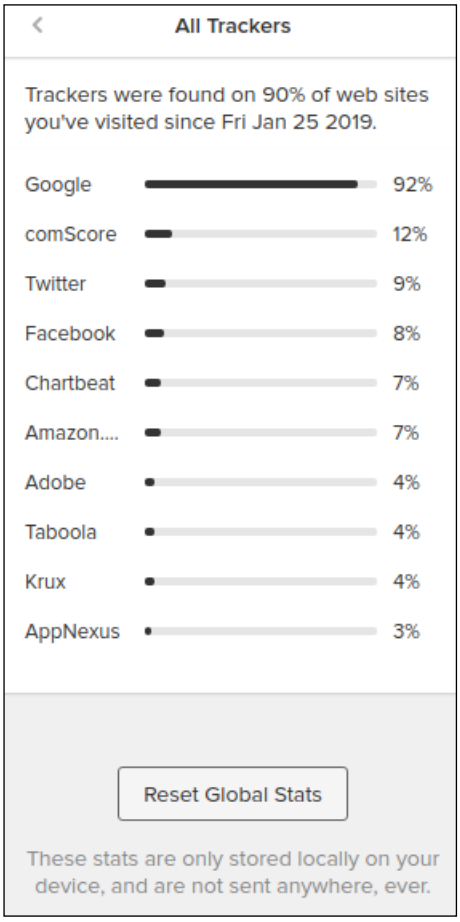
Según se puede comprobar en el gráfico anterior, el rastreo que Google realiza destaca por estar presente en el 75 % de las páginas de todo Internet, seguida a distancia por Facebook, Twitter y Amazon.

También hay extensiones que bloquean el *tracking* y, además, nos informan de las empresas que lo usan a medida que navegamos. Aquí podemos ver el resultado proporcionado por la extensión DuckDuckGo Privacy Essentials:[32]

31 http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

32 https://chrome.google.com/webstore/detail/duckduckgo-privacy-essent/bkdgflcldnnnapblkhphbgpggdiikppg

Figura 8:
Rastreo a través de Internet detectado por la extensión de DuckDuckGo.



Nota 8. Elaboración propia

Puede comprobarse que, aunque estas estadísticas son particulares de un usuario concreto durante algunos días de navegación, no están demasiado alejadas de las citadas por el artículo. Además, la presencia de Google es todavía superior, pues proporciona numerosos servicios para los desarrolladores de páginas web, entre los que se incluyen las estadísticas de visita al sitio con todo tipo de información detallada de sus visitantes (cómo llegaron a una página particular, qué búsqueda hicieron, de qué página venían, en qué página abandonaron el sitio, etc.). Es normal, entonces, que sus servicios sean requeridos por muchos creadores de páginas. Eso sí, a costa de que **toda** nuestra actividad quede reflejada en los servidores de Google.

¿Esta actividad es legal? Sin duda, lo es. Pero ¿es ético? Este es un buen debate para llevar a cabo con nuestros alumnos.

Para conocer el grado de protección de nuestro navegador frente al rastreo, podemos hacer un test en https://coveryourtracks.eff.org/, web que pertenece a la *Electronic Frontier Foundation*, una organización sin ánimo de lucro que trabaja para proteger los derechos de la libertad de expresión en el medio digital. También tiene una extensión, Privacy Badger,[33] que bloquea los rastreadores.

Persecuciones étnicas

En 2017 la mayoría budista persiguió, violó, mató y provocó un éxodo de 700.000 personas de la minoría rohinyá que tuvo que huir de su país natal, Birmania, a Bangladés. En el artículo de *El País,* titulado «El 'mea culpa' de Facebook»[34], podemos leer:

> «Siempre incómodos para la mayoría budista, su pesadilla comenzó el 25 de agosto de 2017, cuando se inició una ofensiva contra ellos en la que tuvo un papel muy destacado, según BSR,

33 https://chrome.google.com/webstore/detail/privacy-badger/pkehgijcmpdhfbdbbnkijodmdjhbjlgp

34 https://elpais.com/elpais/2018/11/07/opinion/1541607377_606778.html

> la división de propaganda del ejército birmano. A través de diferentes cuentas de Facebook, lanzó una campaña de bulos y falsedades sobre los rohinyás que prendió rápidamente y provocó una ola de intimidaciones, agresiones, casas abrasadas y asesinatos que los obligaron a emprender el éxodo hacia Bangladés. Allí permanecen aún 720.000 desplazados, en el mayor campo de refugiados del mundo».

Aunque **Facebook no es el causante** de este genocidio, sin embargo, tiene una responsabilidad directa, ya que, tal como ellos mismos reconocen, su reacción fue lenta y totalmente insuficiente para detener el desastre. Desgraciadamente muchas empresas ponen sus beneficios muy por encima de las personas y su seguridad, solo cuando algunas de sus malas prácticas salen a la luz se produce algún tipo de reacción por su parte.

Redes sociales para cambiar ideas políticas

Se ha constatado en más de una ocasión la existencia de falsos perfiles en las redes sociales formados por *bots* (esto es, programas que imitan a los humanos) que, cuando llega el momento de actuar, reenvían mensajes favorables a la idea que se pretende transmitir —por ejemplo, que determinado candidato electoral es corrupto o noticias falsas denigrantes sobre el mismo— y también generan nuevos bulos. Los usuarios ven cómo estos mensajes aparecen por todas partes, especialmente en Twitter y Facebook, lo que da la falsa impresión de que pertenecen a la opinión pública y a aquellos que rodean al usuario. Además, esto hace que aquellos que están en contra de estas ideas se callan muchas veces por sentirse en minoría. Así, de este modo, se potencian unos mensajes y se silencian otros. En el artículo de *ABC* «Las redes sociales como arma política: mucho más que Trump»[35] puede verse un ejemplo de esta técnica.

No acaba aquí

Pero la lista de actitudes carentes de toda ética no acaba aquí, podríamos seguir con el caso de Apple[36], en el que las baterías hacían ir cada vez más lentos los iPhone. O el espionaje global[37] al que el gobierno de Estados Unidos, así como el de Australia, Canadá y Reino Unido, estaban sometiendo a la población de sus propios países, sin respetar la privacidad ni los derechos de nadie.

¿Qué podemos hacer?

Lógicamente la mayoría de lo que se acaba de exponer está fuera de nuestro círculo de decisión y de influencia, de forma que no podemos modificar su estatus directamente. Sin embargo, será una buena práctica **conocer y usar otros sistemas,** aparte de los que ya utilizamos. No debemos limitarnos un único servicio porque **nos volvemos dependientes** de él.

Podemos tomar decisiones que nos permitan mantener la exigencia de una ética en nuestros actos —especialmente en lo que afecta al **deber de ecuanimidad** del que ya hablamos antes— y esto es lo que nos trae aquí. **Está en nuestras manos decidir qué servicios vamos a usar y cuáles no**, si transigimos con ciertas actitudes o simplemente no las aceptamos, o incluso el derecho de abandonar el servicio que las mantiene.

Para el buscador **Google** existe una buena alternativa, que no guarda la información de lo que buscamos ni rastrea nuestro recorrido por Internet, nos referimos a la aplicación DuckDuckGo[38] ya mencionada, un buscador que **no almacena información privada**. Además, su extensión DuckDuckGo Privacy Essentials[39], **bloquea los rastreadores** y esto la hace especialmente útil. Para el resto de los servicios podemos leer el siguiente artículo: «¿Se puede vivir sin Google? Alternativas con mayor privacidad».[40]

---

35 https://www.abc.es/internacional/abci-redes-sociales-como-arma-politica-mucho-mas-trump-201803250303_noticia.html

36 https://cadenaser.com/ser/2017/12/21/ciencia/1513840177_623732.html

37 https://es.wikipedia.org/wiki/Revelaciones_sobre_la_red_de_vigilancia_mundial_(2013-2015)

38 https://duckduckgo.com/

39 https://chrome.google.com/webstore/detail/duckduckgo-privacy-essent/bkdgflcldnnnapblkhphbgpggdiikppg

40 https://exportic.com/alternativas-google/

Aunque no hemos hablado de **WhatsApp**, es importante señalar que participa de las mismas políticas que Facebook, ya que lo compró en 2016 por 22.000 millones de dólares. Una alternativa que está perfectamente a la altura y que lo supera en más de una funcionalidad es Telegram[41]. Es un programa de mensajería cada vez más usado, ya que presenta ventajas con respecto a WhatsApp. Una de ellas, que además tiene implicaciones educativas, es que **no es necesario ceder el número de teléfono** con las otras personas para utilizar Telegram, basta con tener un nombre de usuario.

Los **sistemas operativos para ordenador** están controlados por Microsoft y Apple, ya que la mayoría de los usuarios utiliza Windows, de Microsoft, o macOS, de Apple. Afortunadamente, existe una alternativa que no deja nada que desear a estos dos sistemas operativos y son las diferentes distribuciones de Linux[42] con docenas de sistemas operativos para escoger y es muy seguro que hay una que se adapta a nuestras necesidades. Ubuntu[43] es probablemente la mejor para empezar. Un acercamiento ético a la informática, conduce siempre a Linux, donde no es necesario piratear o comprar programas para poder usarlos, pues se basan en el concepto de *software* libre, lejos de un uso exclusivamente mercantilista.

Por fortuna, Internet sigue siendo un lugar en el que podemos ejercer nuestra libertad de elección, algo que debemos hacer si no queremos caer de pleno en los brazos de las empresas que negocian con nuestros datos.

Estrategias

Se destacan las siguientes estrategias:

Estrategias en la escuela

- Escoger alguno de los dilemas éticos que se puedan plantear en Internet o de los deberes y organizar un debate o un estudio de profundización.
- Fomentar el concepto de Internet Justo exigiendo a los alumnos el respeto de la propiedad intelectual y los productos que no son gratuitos en Internet.
- Fomentar la enseñanza y el uso de programas alternativos a los más usados.
- Realizar un trabajo en el que los alumnos elaboren listados de alternativas a los programas más usados.

Estrategias en la familia

- Acompañar a los hijos cuando empiezan a utilizar Internet para enseñarles los valores éticos digitales a medida que puedan surgir oportunidades para este fin.
- Realizar alguna compra con ellos por Internet para que vean la necesidad de pagar por los servicios o productos que uno quiera.
- Ser ejemplo para los menores evitando las descargas ilegales.

Para saber más

- BUSOM, R. (2015). «Prolegómenos para una ética digital». *Digital Responsability*. http://www.digitalresponsability.com/2015/06/prolegomenos-para-una-etica-digital.html

41 https://telegram.org/

42 https://es.wikipedia.org/wiki/GNU/Linux

43 https://ubuntu.com/

– BALLADARES, J. (2017). «Una ética digital para las nuevas generaciones digitales». *Revista PUCE*. http://www.revistapuce.edu.ec/index.php/revpuce/article/view/81/174

Formación para alumnos

Debatiendo sobre ética digital

Tipo de actividad: **Debate en clase/cuestionario.**

– Duración: **1 hora o más, según los temas tratados.**
– Niveles implicados: **3.º, 4.º de la ESO y Bachillerato.**
– Objetivos:

- **Ser conscientes de la importancia del buen comportamiento digital y de sus implicaciones.**
- **Adquirir hábitos de uso ético en relación con la Red.**
- **Tomar conciencia de la manipulación que se realiza a través de Internet para estar prevenidos contra ella.**
- **Desarrollar el pensamiento crítico frente al medio digital.**

Existen muchos **temas** posibles de debate en relación con la ética digital. En función de la edad y tipología del alumnado, se puede escoger uno u otro; aquí proporcionaremos solo algunos ejemplos.

Las **cuestiones** pueden trabajarse como un diálogo o como un cuestionario escrito al que se da un tiempo para responder y con la finalidad de comentar después los resultados entre todos.

Manipulación política a través de las redes sociales

Artículo: «Las redes sociales como arma política: mucho más que Trump»[44]

«Facebook ha estado en el punto de mira por su influencia en el resultado electoral: desde la propagación de noticias falsas por parte de plataformas rusas con el objetivo de inclinar la balanza a favor de Trump y desacreditar el sistema democrático estadounidense a la capacidad de la campaña republicana para sobreexponer a su candidato en los anuncios de la red social».

– Cuestiones:

- ¿Somos conscientes de la manipulación de noticias a través de las redes sociales?
- ¿De qué forma se manipulan?

44 https://www.abc.es/internacional/abci-redes-sociales-como-arma-politica-mucho-mas-trump-201803250303_noticia.html

Artículo: «Bannon dirigió la campaña de Trump con datos que sustrajo de Facebook»[45]

> "Nos encontramos con que Facebook y el mundo digital eran los caminos más efectivos para llegar a las grandes audiencias. Por eso fichamos a Cambridge Analytica. Ellos fueron capaces de construir un cúmulo de datos para la campaña que nadie conoció hasta el final" [declaraciones de Kushner a la revista *Forbes*]. El propio Nix, quien se jacta también de la decisiva aportación de esos datos a la campaña de Trump, afirmaba dos semanas antes de la cita con las urnas: "Nuestra compañía es capaz de determinar la personalidad de cada adulto en Estados Unidos".

– Cuestiones:

  - ¿Por qué una empresa como Cambridge Analytica puede determinar la personalidad de la gente?
  - ¿Hay algo que podamos hacer a nivel personal? ¿Qué medidas podemos tomar para evitarlo?

Espionaje de los gobiernos a sus ciudadanos

Artículo: «Revelaciones sobre la red de vigilancia mundial (2013-2015)»[46]

«Los datos acerca de la vigilancia mundial son una serie de revelaciones sacadas a la luz por la prensa internacional entre 2013 y 2015, que demuestran la vigilancia que principalmente las agencias de inteligencia de Estados Unidos, en colaboración con otros países aliados, han estado ejerciendo de manera masiva sobre la población mundial. Las víctimas potenciales de este espionaje podrían cuantificarse en miles de millones de personas alrededor del mundo, además, los periódicos revelaron que cientos de líderes mundiales, incluyendo jefes de Estado e importantes empresarios, fueron o están siendo vigilados».

– Cuestiones:

  - ¿Conocías estos hechos? A nivel ético, ¿qué opinión te merecen?
  - ¿Cuáles deberían ser los límites de los gobiernos en relación a la vigilancia de sus ciudadanos?

45 https://www.abc.es/internacional/abci-bannon-dirigio-campana-trump-datos-sustrajo-facebook-201803220231_noticia.html

46 https://es.wikipedia.org/wiki/Revelaciones_sobre_la_red_de_vigilancia_mundial_(2013-2015)

«Para la vigilancia y recogida masiva de datos las agencias han recurrido a métodos tan diversos como la introducción de software espía en aplicaciones móviles muy populares como ***Angry Birds*** o **Google Maps**, la ruptura de la seguridad de los sistemas operativos **iOS**, **Android**, o la violación de los cifrados de las **BlackBerry**. La NSA también infectó cientos de miles de redes informáticas con ***malware*** a nivel internacional e incluso espía los correos electrónicos **Hotmail**, **Outlook** o **Gmail**. La inteligencia internacional también vigila y almacena miles de millones de **llamadas y registros telefónicos**. Gracias a esto, las agencias capitaneadas por la NSA son capaces de conseguir los contactos, geolocalización, fotografías, aplicaciones o mensajes, **datos que les permiten crear perfiles de prácticamente cualquier individuo**, pues a partir de esto pueden deducir su modo de vida, país de origen, edad, sexo, ingresos, etc. La NSA también intercepta y almacena los datos de millones de transacciones financieras electrónicas, pudiendo tener acceso prácticamente a **cualquier dato bancario**. Según los documentos filtrados, las más importantes empresas de telecomunicaciones, tecnología y de Internet **colaboran con la NSA de manera voluntaria** o a cambio de millones de dólares para la cesión masiva de datos de sus clientes, además del acceso a sus servidores. Entre estas empresas se encuentran: **Microsoft**, **Google**, **Apple**, **Facebook**, **Yahoo**!, **AOL**, **Verizon, Vodafone, Global Crossing o British Telecommunications**, entre otras.»

– Cuestiones:

  - ¿En alguna ocasión hemos utilizado estas aplicaciones en nuestro teléfono móvil u otros de los servicios y empresas que se nombran en el texto? Comenta la opinión que te merecen estas prácticas.
  - Actualmente, esta vigilancia parece que ha finalizado tras el escándalo que surgió en su momento. ¿Crees que, en verdad, se ha detenido? ¿Por qué?
  - En el supuesto de que todavía exista, podemos tomar, sin duda, medidas a nivel personal para minimizar el impacto de esta vigilancia sobre nuestra persona. ¿Qué podemos hacer? Elabora una lista de posibles medidas.

Violencia, derechos humanos

Artículo: «El 'mea culpa' de Facebook»[47]

«Siempre incómodos para la mayoría budista, su pesadilla comenzó el 25 de agosto de 2017, cuando se inició una ofensiva contra ellos [la etnia rohinyá] en la que tuvo un papel muy destacado, según BSR, la división de propaganda del Ejército birmano. **A través de diferentes cuentas de Facebook lanzó una campaña de bulos y falsedades** sobre los rohingyás que prendió rápidamente y provocó una ola de intimidaciones, agresiones, casas abrasadas y asesinatos que los obligaron a emprender el éxodo hacia Bangladés. Allí permanecen aún 720.000 desplazados, en el mayor campo de refugiados del mundo.»

- Esta forma de actuar por parte del ejército birmano, ¿qué similitudes y diferencias guarda con el control político de la población?
- Mira el siguiente vídeo sobre el linchamiento de un supuesto secuestrador de niños en el sur de Bogotá (se advierte que las imágenes pueden herir la sensibilidad de algunas personas): https://youtu.be/yqcqowHe1-0
- El hombre que aparece en este vídeo, desgraciadamente, murió y, según Cablenoticias[48], el ataque obedecía a una **falsa** cadena de mensajes que circulaban por **WhatsApp**. Elabora una lista de, al menos, tres conclusiones que podemos sacar para evitar caer en nuestra vida privada en estos tipos de violencia.
- ¿Qué otros ejemplos, más cercanos, de falsedades semejantes conoces?

Invasión de la intimidad

Artículo: «¿Te afecta el tracking o rastreo?»[49]

> Los sitios web que visitamos, comúnmente, obtienen datos acerca de nosotros con el objetivo de mejorar nuestra experiencia en el sitio. La información que registran les sirve para saber con qué frecuencia visitamos el sitio, para hacernos más fácil la navegación y hasta para recordar qué artículos dejamos en el carrito de compras.

- Cuestiones

  - Las empresas de Internet continuamente están siguiendo tu actividad a medida que visitas páginas y haces clic en un sitio u otro. Es perfectamente legal y das tu consentimiento para ello cuando pulsas el botón «Aceptar *cookies*» que tienen casi todas las webs, pero ¿hasta qué punto es una intromisión en nuestra vida privada? ¿Crees que tiene alguna importancia o repercusión a corto y largo plazo?
  - ¿Ves similitudes con alguno de los puntos que hemos tratado antes?
  - ¿Crees que puede servir para elaborar un perfil tuyo? ¿Qué consecuencias puede tener?

47 https://elpais.com/elpais/2018/11/07/opinion/1541607377_606778.html

48 https://www.cablenoticias.tv/nacionales/turba-lincha-a-supuesto-ladron-de-ninos-en-el-sur-de-bogota/

49 https://ikonno.com.mx/2016/05/18/te-afecta-el-tracking-o-rastreo/

Cinefórum: Snowden

Tipo de actividad: «**Cinefórum: *Snowden***»

– Duración: **3-4 horas.**
– Niveles implicados: **3.º, 4.º de la ESO y Bachillerato.**
– Objetivos:

- **Conocer el espionaje al que podemos estar sometidos, incluso los ciudadanos de a pie, a través de móviles y ordenadores.**
- **Tomar conciencia de la importancia de nuestros datos y el cuidado que debemos poner en ellos.**
- **Desarrollar el pensamiento crítico frente al uso de la tecnología.**

La película Snowden[50] relata los acontecimientos relacionados con la publicación de material clasificado por parte de Edward Snowden, miembro de la NSA estadounidense, donde se ponía de manifiesto el proyecto de vigilancia mundial de políticos, empresarios y población en general, realizado por Estados Unidos y otros países aliados. Su duración es de 134 minutos.

Con esta película se pueden tratar los siguientes temas:

- ¿Hasta dónde puede y debe llegar el control de los gobiernos? ¿Cuáles deberían ser sus límites?
- ¿La seguridad de un país depende de la vigilancia de las comunicaciones entre terroristas, por ejemplo, para evitar atentados como el de 2017 en Barcelona?[51]
- ¿Fue una conducta ética la de Snowden? Tras esta pregunta, discute: ¿Qué es un mal mayor, callarse o hablar?
- Actualmente Snowden sigue en busca y captura por lo que debe esconderse de la justicia estadounidense. ¿Hasta dónde estarías dispuesto a llegar si te vieses en el caso de Snowden?
- ¿Los ciudadanos tenemos alguna forma de evitar este tipo de atropellos? ¿Cuáles?
- En el caso de que esta vigilancia esté todavía activa ¿qué podemos hacer a nivel personal para evitarla?
- Finalmente, investiga: ¿qué ha sucedido con el plan de vigilancia mundial descubierto por Snowden? ¿En otros países se han dado escándalos similares por el mismo motivo?

50 https://www.filmaffinity.com/es/film892502.html

51 https://es.wikipedia.org/wiki/Atentados_de_Catalu%C3%B1a_de_2017

Investigación: alternativas seguras

Tipo de actividad: **Búsqueda e investigación.**

- Duración: **1 hora.**
- Niveles implicados: **Todos.**
- Objetivos:

  - **Concienciarse de la seguridad de las aplicaciones que usamos.**
  - **Adquirir una actitud activa frente a la ética digital, incluso aquella que no depende de nosotros.**

Con esta actividad se pretende buscar alternativas seguras a los programas y servicios web que más utilizamos. De este modo favorecemos que los alumnos conozcan más allá de lo que utilizan cada día.

El profesor comenzará con una introducción sobre el *tracking* y las empresas que lo utilizan, por lo que propondrá buscar alternativas a algunos de los servicios que en estos momentos pueden comportarse casi como un monopolio. Por ejemplo, buscar alternativas seguras para:

- El buscador de Google
- Documentos de Google
- Presentaciones de Google
- Hojas de cálculo de Google
- Google Maps
- Facebook
- Instagram
- WhatsApp

También se buscará *software antitracking* para evitar ser rastreados.

- Esta actividad puede llevarse a cabo en grupos de tres o cuatro alumnos que se distribuirán los servicios a buscar. Al terminar el tiempo dedicado, unos 45 minutos, deben poner en común lo que han encontrado los diferentes grupos y hacer una selección.
- Comprometerse a utilizar durante un mes al menos uno de los servicios seleccionados.
- Pasado este tiempo dedicar un rato a comparar las experiencias de los alumnos en su elección.
- Si procede, tomar una decisión común sobre este aspecto con el fin de que toda la clase la use el resto del curso.

Formación para familias

Escuela de padres y madres, ética digital

Tipo de actividad: **Charla informativa/taller.**

- Duración: **1 hora.**
- Niveles implicados: **Desde primaria hasta 2.º de la ESO.**
- Objetivos:

  - **Concienciar a los padres de la necesidad de un Internet Justo.**
  - **Preparar a los padres para que puedan acompañar a sus hijos en Internet.**

Esta charla informativa puede organizarse también como un taller donde los padres puedan manipular las páginas web y los programas. Los temas que se tratarán son el de la ética en la Red y el concepto de Internet Justo.

Identidad, reputación y huella digital

La mayoría de nosotros llevamos una vida pacífica en Internet, sin problemas en redes sociales o en otros sitios. Eso puede hacernos sentir que no tenemos una reputación definida o que nuestra identidad no es importante.

En este apartado aprenderemos a valorar la identidad digital, a cuidar nuestra reputación y a controlar nuestra huella digital.

Huella e Identidad digital

El concepto de **identidad digital** es todo aquello que nos define en Internet, lo que está relacionado con nosotros. A medida que interactuamos con el medio digital, nuestra actividad va dejando una **huella**. Pero la identidad digital no depende únicamente de nosotros, es posible que una amistad de la vida real o un familiar nos nombre, cite o etiquete en una foto de Facebook o de Instagram o simplemente aparezcamos junto a un grupo de amigos, aunque nadie nos nombre explícitamente. Estas apariciones fortuitas, sin duda alguna, también contribuyen a crearnos una imagen digital, aunque en este caso la huella no haya sido depositada por nosotros, **sino por otros**.

Así pues, la huella digital está constituida por toda esa serie de datos digitales que no tienen, por separado, una relevancia particular, pero que cuando se unen crean una imagen coherente de nuestra persona, es la identidad digital.

Cuando participamos en una red social como Twitter, enviamos textos, imágenes y, quizás, vídeos que son vistos por aquellos que nos siguen. Los que no nos conocen se formarán una imagen de cómo somos uniendo los fragmentos de las diferentes huellas. Esta imagen reconstruida a partir de un número escaso de datos puede ser real o no, pero, a fin de cuentas, es lo que los demás tendrán para crearla.

¿Qué identidad deseamos? Reputación

Si no nos preocupamos por ella, puede pasar que, al no vigilar lo que hacemos, podamos llegar a publicar una amalgama de informaciones sesgadas e inconexas que dan una imagen falsa o no deseada de nosotros mismos. Es necesario ser conscientes de que aquello que publicamos, sea donde sea, configura nuestra identidad digital. Las huellas que dejamos no deben ser aleatorias o fruto del

capricho del momento, sino que debe existir una coherencia por nuestra parte y fijarnos límites tanto en lo que publicamos como en lo que no.

En un grupo familiar de WhatsApp, por ejemplo, puede ser apropiado contar ciertos chistes o hacer determinados comentarios políticos. Pero en otro, como el profesional o el de trabajo no podemos comportarnos de la misma forma que con nuestra familia. Hay que discernir en cada momento dónde estamos y actuar en consecuencia. También hay que ser precavidos para detectar si los grupos son públicos o de tipo profesional. Esta **identidad digital positiva** para la persona es la **reputación digital** o **reputación *online***.

Es más, los **profesores**, los directores o las personas con algún tipo de **responsabilidad social** deben cuidar de forma muy especial lo que publican, ya que tienen a su cargo a otras que difícilmente las respetarán según los contenidos que aparezcan en la Red. Esto nos lleva al concepto de reputación profesional que, lógicamente, es aplicable no solo al mundo de la docencia, sino a cualquiera que dependa de otros para su propio trabajo.

Reputación profesional

Es indiscutible que esta reputación debe merecer una atención especial por nuestra parte. No solo por el hecho de que cada día son despedidos trabajadores por haber realizado un uso poco responsable de las redes sociales, sino también porque estas nos ayudan a ser mejores profesionales.

Aquel que desee tener una buena reputación digital profesional, deberá abstenerse de mezclar su vida privada con su vida laboral. No es raro ver cómo determinadas personas pasan de la foto en el gimnasio, al mensaje institucional de su empresa y vuelta a otro mensaje político. No es que sea malo ir al gimnasio o tener las ideas políticas claras, lo que sí es bastante contrario a la profesionalidad es la no distinción entre ambos perfiles, es decir ambas identidades digitales que no deberían mezclarse nunca. Aquellos que mantienen una relación profesional con nosotros es posible que no comulguen con nuestras ideas políticas o con nuestra forma de vivir la vida (lo que comemos, el deporte que hacemos, etc.), entre otros cientos de detalles personales que pueden afectar a las relaciones personales, sobre todo si hay una dependencia jerárquica laboral o que aquellos que nos sigan sean nuestros alumnos.

Debemos mantener una separación entre vida profesional y personal. Lo más responsable es **tener un perfil profesional público y otro privado personal**. Pero **nunca mezclar indiscriminadamente los dos**, ya que esto no puede traer sino problemas. En el artículo «Despedidos por culpa de las redes sociales»[52] podemos ver el efecto de lo que hemos mencionado. Como muestra, baste uno de los casos extraído de este artículo:

> Uno de los casos más conocidos es el de Justine Sacco, que antes de iniciar un viaje de Nueva York a Sudáfrica escribió en diciembre de 2013: "Me voy a África. Espero no pillar el sida. Es broma. ¡Soy blanca!". El tuit provocó miles de comentarios tachándola de racista y le costó su puesto como directora de comunicación de InterActiveCorp (IAC), una importante compañía que se encarga de gestionar la comunicación de portales como Ask.com[53] o Vimeo.

La mayoría de las empresas no dudan en despedir a aquellos trabajadores cuyos mensajes son contrarios a su política, por ello es importante cuidar la reputación digital.

Consejos para tener una buena reputación digital

Normas generales para los adultos

1. No mezclar nunca lo personal con lo profesional. Mantener un **perfil público para lo profesional** y **privado, visible solo para amigos íntimos y familiares, para lo personal**. No es necesario tener cuentas diferentes, una para cada ámbito, sino que basta con utilizar cada red para una finalidad. Por ejemplo, Twitter para la parte profesional e Instagram para la personal. Lógicamente, cada uno decidirá lo que más le conviene según sus propias necesidades.

52 https://www.lavanguardia.com/tecnologia/redes-sociales/20150508/54430486471/despedidos-culpa-redes-sociales.html

53 https://es.ask.com/

2. Participar de forma pública en redes sociales con mensajes de temática profesional. Pero solo participar.
3. En la cuenta profesional se deben evitar temas que sabemos que son controvertidos y que inducen a la discusión (política, religión, terapias alternativas, etc.).
4. Se puede crear un blog, o algún tipo de publicación *online*, que nos permita expresar más extensamente nuestras ideas y sin la inmediatez del momento que implican las redes sociales. Hay que evitar reproducir artículos creados por otros, como si fuésemos un eco de lo que han dicho los demás, e intentar aportar de vez en cuando algo nuevo o distintivo nuestro.

Este último punto no es apto para todos porque no a todos les gusta escribir o creen que no tienen nada interesante que contar a los demás, aunque los docentes tengan realmente mucho que explicar y compartir acerca de su trabajo.

Normas generales para estudiantes

Los menores de edad no tienen una vida profesional propiamente dicha. Aunque los estudios son «su trabajo», no son muchos los que se deciden a poner en práctica sus conocimientos escolares, ya sea a través de un portafolio digital[54] o mediante la participación en discusiones académicas. Los niños y adolescentes tienen puesta su mente en otros aspectos más propios de su edad, como la autoafirmación frente a los demás o los juegos.

1. En el caso de publicar actividad privada y personal, debemos hacerlo siempre con perfiles cerrados, no públicos. Un conocido refrán moderno dice: *«Lo que se sube a la Red, se queda en la Red»*. Y lo que ahora es simpático para un joven de 15 años puede no serlo en un futuro cuando esté buscando trabajo, pareja, etc. Igualmente, ciertas bromas o poses que se hacen a los 11 años, quizás dejen de hacer gracia a los 14, cuando sus compañeros las vean.
2. Sería recomendable que los jóvenes participasen en discusiones sobre aquello que les gusta: ciencia, historia, literatura, deporte, etc. En este caso, siempre manteniendo la netiqueta cuando sea de forma pública.
3. Si el alumno tiene alguna afición particular destacable, se le debe animar a escribir sobre ello.

Estas normas permitirán la creación de una buena reputación que podrá ser favorable en un futuro inmediato.

Estrategias en la escuela

- Tratar en clase el problema de que cuando se sube algo a Internet, se pierde el control para siempre. Eso condiciona nuestra reputación futura.
- Creación de portafolios digitales donde vayan exponiendo sus trabajos y logros académicos.
- Enseñar las normas de netiqueta para poder interactuar de una forma sana y provechosa en las redes sociales y foros de Internet (véase el apartado «Elementos de la ciudadanía digital»).
- En la asignatura de Informática se puede dedicar tiempo a la creación y a la escritura en blogs o páginas web.

54 https://es.wikipedia.org/wiki/Portfolio_digital

Formación de alumnos

¿Qué subimos a Internet?

Tipo de actividad: **Debate.**

- Duración: **1-2 horas.**
- Niveles implicados: **Todos.**
- Objetivos:

  - **Concienciarse de la pérdida de control de la información personal en Internet.**
  - **Disponer de estrategias para aumentar la seguridad de aquello que se envía a la Red.**

Niños, adolescentes y adultos coinciden muchas veces en que tienen la falsa idea de que controlan aquello que suben a Internet. Por ejemplo, si una foto la comparto con una amiga, ella no va a difundirla nunca. O, si envío una foto que se autodestruye a los dos minutos, la foto quedará efectivamente eliminada; pero nada más lejos de la realidad. Es muy fácil sacar una captura de pantalla en un ordenador o hacer una foto con la tableta, por ejemplo, pero una vez que un texto, una imagen o un vídeo abandona nuestro dispositivo, ya no tenemos ninguna seguridad de cuánto tiempo durará ni quién la podrá ver. Por lo tanto, hay que extremar las precauciones cuando publicamos en la Red.

La actividad consiste en que los alumnos vean las dos primeras historias del siguiente vídeo elaborado por Pantallas Amigas: https://youtu.be/qkDvoSqNkxc.

Tras su visionado, se les puede plantear a los alumnos estas cuestiones:

- En la primera historia una foto, en principio neutra e inofensiva, es causante de un desacuerdo:

  - ¿Crees que se podría producir una situación similar a esta?
  - ¿Conoces algún caso similar?

- En la segunda de las historias, unas fotos que van destinadas a un uso privado acaban en manos de toda la escuela:

  - ¿Crees que es posible esta situación?
  - ¿Te ha pasado o conoces a alguien que le haya pasado algo parecido?

- ¿Qué medidas podemos tomar para que no nos pase algo similar?
- ¿Hasta qué punto podemos controlar lo que publicamos en Internet?

Habilidades y competencias del ciudadano digital

Desarrollo evolutivo y socioemocional en el ámbito digital

Ciertas características de la adolescencia nos ayudan a entender el comportamiento de los preadolescentes y adolescentes en el ámbito digital. En el artículo «La adolescencia y la socialización»[55] se nos dan algunas claves:

- El adolescente tiene la necesidad de abandonar los hábitos de obediencia y dependencia de la niñez y, a la vez, busca **desarrollar los de adulto**, esto es, **decidir y proveer por sí mismo**.
- Con la pubertad se vuelve consciente una relativa necesidad de **soledad.**
- La búsqueda de **intimidad** como algo muy vinculado a la soledad, sobre todo cuando se comprueba que coincide con actividades típica y esencialmente solitarias: diario íntimo, escritura de poesías, etc. Además, dichas conductas casi siempre se muestran asociadas ambivalentemente a la socialización.
- La gran importancia que el adolescente atribuye a las **actitudes y opiniones ajenas**, en particular las de sus iguales.
- Al adolescente le resulta imprescindible **ser aceptado por el grupo** y, a tal fin, es capaz de someterse a todos sus mandatos, aún los menos racionales.
- La **fuerza del grupo** es tranquilizadora y salva la debilidad individual, al tiempo que sirve de campo de entrenamiento para los diversos roles sociales que se van a jugar en la vida: líderes, seguidores, sometidos, huéspedes, enemigos, chivos expiatorios, etc.
- La **tendencia a idealizar** tiene un elevado costo revelado a través del número de desilusiones que sufre el adolescente, sobre todo en las primeras fases de esta etapa.

Estas características, que son propias de la adolescencia, se verán reflejadas en el mundo digital a través del uso que hacen los jóvenes de Internet. Las motivaciones que hacen a un adolescente comportarse de una forma particular en la vida real, también están presentes en la Red.

Para saber más

- «La adolescencia y la socialización». Julio V. Maffei. Artículo donde se explican algunas de las características de la socialización de los adolescentes. https://web.archive.org/web/20070121040550/http://www.eljuegoinfantil.com/psicologia/socializacion.htm
- *Las TIC y su influencia en la socialización de adolescentes*. Estudio realizado por FAD y basado en 1600 entrevistas realizadas a adolescentes. https://www.fad.es/sites/default/files/investigacion_conectados_2018.PDF
- *Dossier de prensa: Las TIC y su influencia en la socialización de adolescentes*. Presentación resumen del trabajo anterior. https://www.fad.es/sites/default/files/dossier_prensa_conectados2018.pdf

Las TIC y los adolescentes

Según el estudio «Las TIC y su influencia en la socialización de adolescentes»[56] el 90 % de los adolescentes españoles tienen de dos a cinco dispositivos digitales:

- El 90 % tiene teléfono móvil inteligente
- El 76 % tiene ordenador portátil
- El 69 % tiene tableta

55 https://web.archive.org/web/20070121040550/http://www.eljuegoinfantil.com/psicologia/socializacion.htm

56 https://www.fad.es/wp-content/uploads/2019/05/investigacion_conectados_2018.pdf

Estas cifras nos dan una clara idea de hasta dónde llega el grado de acceso a Internet y, por tanto, al mundo de lo digital, entre nuestros adolescentes. Un acceso tan generalizado es un indicador de hasta qué punto es importante en su vida y la influencia que adquiere en su desarrollo personal. Además, un 15 % admite estar **pendiente del móvil** cuando está con otras personas y también cuando están **en clase**.

Redes sociales

Aproximadamente el 92 % de los adolescentes entre 14 y 16 años dispone de algún perfil en redes sociales para sentirse integrados en el grupo. El uso que dan a estos medios es el siguiente:

- WhatsApp para la comunicación diaria con amigos y familiares.
- Instagram para publicar y ser vistos por los demás.
- YouTube para consumir contenidos y sentirse fan.
- En menor grado está el uso de Twitter que utilizan para seguir a sus ídolos.
- Y todavía más minoritario el de Facebook que utilizan para jugar y estar en contacto con amistades lejanas.

Cómo usan los dispositivos

- Utilizan el móvil de forma **intensiva** un 83 % en casa y el 56 % cuando están fuera.
- El ordenador propio (portátil o fijo) lo usan de forma **intensiva** un 32 %
- En cuanto al ordenador familiar, de uso común por varios miembros, solo un 16 % lo utiliza de forma **intensiva**.

En la Tabla 1 podemos ver, en concreto, el uso que hacen del móvil:

Tabla 1:
Actitudes ante el móvil

ACTITUDES ANTE EL MÓVIL	MEDIA	DESVIACIÓN TÍPICA	% ALTOS ACUERDOS (7-10)
Miro el móvil constantemente	7,27	2,360	72,4 %
Solo estoy pendiente del móvil cuando espero un mensaje o una llamada	5,69	3,141	46,2 %
Aunque esté con gente (hablando, pasando el rato), sigo pendiente del móvil	3,31	2,798	16,2 %
Incluso en clase estoy pendiente del móvil	2,37	3,085	14,6 %

Nota tabla 1. Encuesta a jóvenes sobre el uso del móvil basada en una escala de 0 («nada de acuerdo») a 10 («totalmente de acuerdo»). Tomado de *Las TIC y su influencia en la socialización de adolescentes* (p. 33) [Documento Digital], por J. C. Ballesteros y L. Picazo, 2018, FAD. https://www.fad.es/sites/default/files/investigacion_conectados_2018.PDF

Para qué los usan

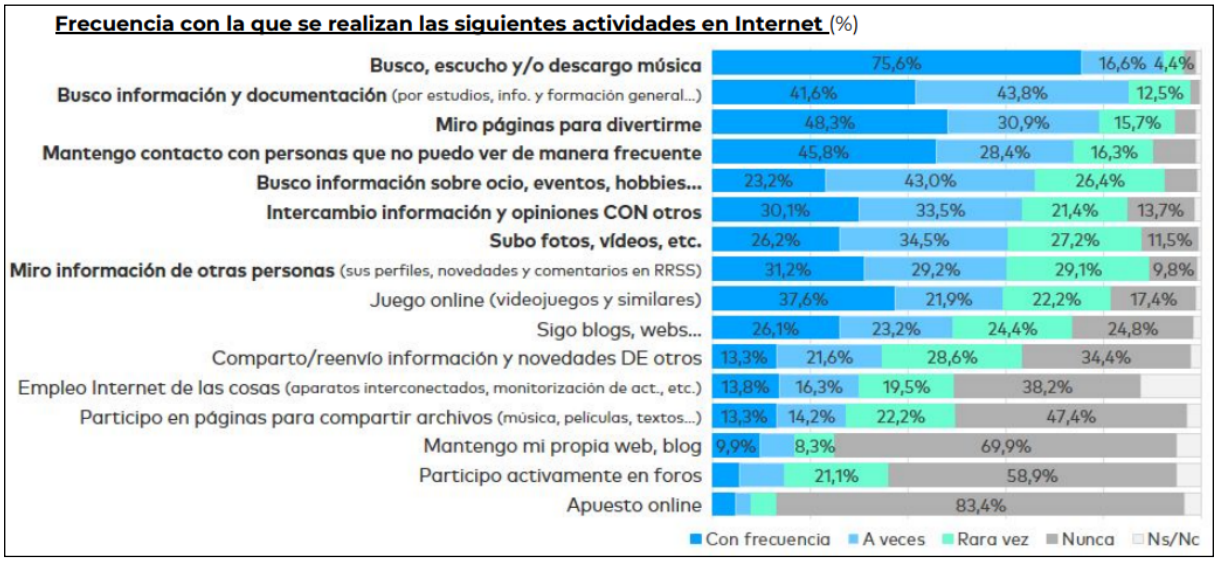
A continuación, indicamos las actividades que los adolescentes declaran realizar en Internet **con frecuencia**:

- El 76 % usan los dispositivos frecuentemente para escuchar música.
- El 48 % para mirar páginas que les divierten.

- El 46 % para mantener contacto con gente que no ven frecuentemente.
- El 42 % para buscar información y documentarse.

En la Figura 9, podemos ver estas y otras actividades.

Figura 9:
Frecuencia con la que se realizan las siguientes actividades en Internet



Nota 9. Tomado de *Las TIC y su influencia en la socialización de adolescentes (p. 6) [Documento Digital], FAD, 2018,* https://www.fad.es/wp-content/uploads/2019/01/dossier_prensa_conectados2018.pdf

La importancia de las redes sociales

El uso diario más frecuente que se hace de la **mensajería instantánea**, sobre todo WhatsApp, es el siguiente:

- El 90,9 % hablar con amigos (simplemente charlar sin un objetivo específico).
- El 82,6 % planificar actividades con amigos.
- El 61,8 % hablar con la familia (simplemente charlar sin un objetivo específico).
- El 47,2 % cuestiones relacionadas con los estudios (citas con los profesores, consultas).
- El 32,6 % planificar actividades familiares (quedar con padres o hermanos, ajustar horarios, organizar tareas de casa…).

En cuanto al uso diario del resto de redes sociales, encontramos las siguientes actividades:

- El 71,6 % mirar información de amigos, familiares o personas cercanas.
- El 70,0 % buscar información de cosas que me gustan o me interesan.
- El 66,4 % hablar con amigos (simplemente charlar sin un objetivo específico).
- El 39,3 % planificar actividades con amigos.
- El 35,1 % mirar información de personas que no conozco mucho o desconocidas.
- El 22,5 % contar mis cosas, mis gustos, mis intereses…

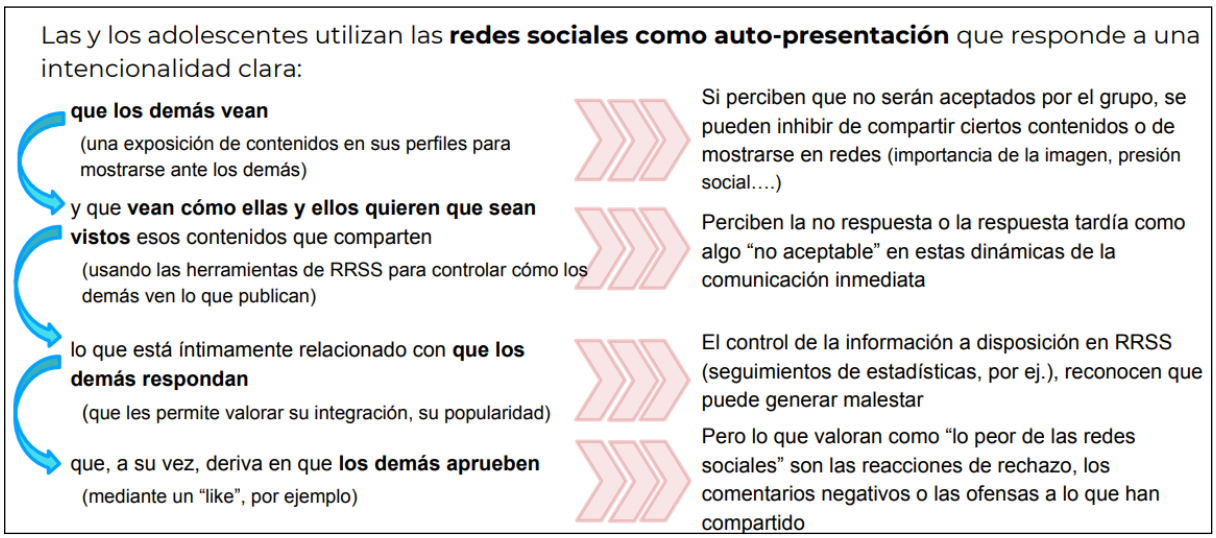
Las redes sociales se configuran como un elemento donde se produce la comunicación con otros y, además, se produce contenido, no solo se consume.

En el dosier de prensa de Las TIC y su influencia en la socialización de los adolescentes[57] encontra-

57 https://www.fad.es/wp-content/uploads/2019/01/dossier_prensa_conectados2018.pdf

mos un gráfico muy interesante donde se muestra la intencionalidad que presentan los adolescentes a través de las redes sociales.

Figura 10:
Intencionalidad en el uso de las TIC por parte de los adolescentes



Nota 10. Tomado de *Las TIC y su influencia en la socialización de adolescentes (p. 12) [Documento Digital], FAD, 2018*
https://www.fad.es/wp-content/uploads/2019/01/dossier_prensa_conectados2018.pdf

Así pues, es en las redes sociales donde se producen la mayoría de las interacciones de los adolescentes con los demás. Y, por eso, adquieren aquí tanta importancia las motivaciones que les impulsan a ser visibles y aceptados por los demás. Además, la existencia de mecanismos explícitos para manifestar la aceptación como los *likes*, algo inexistente en el mundo real, hace que todo vaya mucho más deprisa en Internet. Algo como el ser aceptado por los demás, que en el mundo real requiere tiempo (a través de la actitud, la conversación y la corporalidad, con una aceptación final por parte de otros), en el mundo de las redes sociales se liquida con unos *likes* o, en el peor de los casos, con comentarios desfavorables o ignorando al otro. Así pues, lo que en la vida real puede llevar semanas,

Estrategias

Estrategias en la escuela

- En el período comprendido entre 6.º de primaria hasta los dos primeros cursos de la ESO, debe informarse a los padres sobre el correcto uso de las redes sociales porque sus hijos empezarán a moverse por las redes sociales y deben saber cómo afrontar los posibles peligros que les surjan en este ámbito.
- Además, en estos cursos debería elaborarse un plan de formación para los alumnos, pues es conveniente tratar el tema de Internet y las redes sociales, desde el punto de vista del adolescente, varias veces durante el curso.

Estrategias en la familia

- Cuando los adolescentes y preadolescentes comiencen a usar las redes sociales, es conveniente que sean sus padres los que obtengan la cuenta con ellos y les ayuden a rellenar los datos necesarios e informen sobre su uso en esta fase inicial.
- Los padres deben seguir a sus hijos en las redes sociales y comprobar de vez en cuando lo que hacen en ellas, sin estar continuamente encima. Es importante revisar los comentarios que escriben, las fotos que publican y lo que los demás les escriben a ellos, con la finalidad de detectar cualquier comportamiento inapropiado, ya sea de los hijos o de sus amigos.
- Muchas veces las familias se enteran mucho antes que los centros educativos de comportamientos inapropiados en las redes (fotos en los vestidores del gimnasio del colegio, de los alumnos en clase, acoso a un alumno, etc.). En estos casos deben ponerlo en conocimiento del centro lo antes posible para que se puedan tomar las medidas oportunas.

Formación

Formación para alumnos

Tipo de actividad: **Formación a lo largo del curso**

- Duración: **Varias sesiones por curso, al menos dos.**
- Niveles implicados: **6.º de primaria, 1.º de la ESO.**
- Objetivos:

  - **Iniciarse en el uso las redes sociales.**
  - **Aprender a darse de alta en servicios de Internet dando el menor número posible de datos.**
  - **Aprender las normas de netiqueta básicas.**
  - **Aprender a usar las redes sociales con beneficio.**

  A nivel de centro educativo, conviene plantearse una formación específica para que los preadolescentes sepan gestionar sus emociones y la relación con los demás en las redes sociales.

  Desgraciadamente, en algunos centros solo se informa del lado negativo de las redes sociales. Al ser solo una de sus caras, esta visión es parcial y tendenciosa por lo que muchas veces se produce el efecto contrario o simplemente no se toma demasiado en cuenta por parte del alumnado. Hay que tratar este tema desde un punto de vista positivo, pero neutral. Se debe enseñar lo que son y lo que se puede hacer en las redes sociales.

Para esto conviene tratar con los alumnos los siguientes temas y es aconsejable distribuirlos en dos o más sesiones:

- ¿Tengo edad para registrarme en las redes sociales?
- El registro en servicios de Internet: qué datos proporcionar y cuáles no.
- Normas básicas de comportamiento: netiqueta en las redes sociales.
- Necesidad de autorregularse en todo aquello que publican en la Red.
- Implicaciones negativas de un exceso de información personal en las redes sociales.
- Cómo aprovechar las redes sociales para el estudio académico.

El centro educativo no debe dar de alta a los alumnos en las redes sociales, pero sí debe informarles de cómo hacerlo en condiciones, por este motivo no se debe hacer de forma práctica. Estos temas pueden organizarse con un tiempo para la exposición de las ideas principales y otro para el debate. Además, algunos alumnos tienen mucho que contar sobre estos temas y su testimonio puede ser enriquecedor.

Formación para familias

Tipo de actividad: **Escuela de padres y madres**

- Duración: **1-2 horas**
- Niveles implicados: **6.º de primaria, 2.º de la ESO.**
- Objetivos:

  - **Ser padres informados acerca del buen uso de las redes sociales**
  - **Ser capaces de acompañar a los hijos en las redes**.

Durante los años en que los preadolescentes comienzan a entrar en las redes, es conveniente formar a los padres en el mismo aspecto que a sus hijos. Por lo tanto, los puntos a tratar aquí serían los mismos que se han propuesto en el apartado «Formación para alumnos». Siempre desde un punto de vista positivo, aunque sin olvidar los riesgos y peligros que existen.

Comunicación y colaboración en redes sociales

Formación y colaboración en las redes sociales

Uno de los aspectos fundamentales en los que debemos educar a nuestros alumnos como ciudadanos digitales es en el del **uso efectivo de la Red como mecanismo de crecimiento personal y profesional.**

Internet no debe limitarse a ser un lugar donde acudimos para buscar información, escuchar música, ver vídeos o hablar, sino que tiene que ser mucho más que un simple tomar y usar. A través de Internet debemos **aprender** a colaborar y trabajar junto con otros, a aprender de otros, a resolver problemas de carácter profesional y especializado o a buscar aquello que necesitamos, más allá del buscador de turno.

Sin lugar a dudas, redes sociales como Facebook y Twitter, que tuvieron mucha importancia años atrás, han dejado de ser usadas por los jóvenes en favor de Instagram. Esto ha sido provocado, en parte, por el aumento del uso del móvil, que ha decantado el uso de redes sociales cuyo ecosistema natural es este mismo.

Plataformas sociales

En este apartado solo se mencionarán cuáles son las redes sociales que se explicarán más adelante, junto otros servicios que sirven para poner a las personas en contacto de forma grupal y que, por tanto, actúan a modo de red social.

Un estudio llevado a cabo por HootSuite y We Are Social[58] en 2019, revela cuáles son las redes sociales más usadas a nivel mundial. Las primeras en esta lista son:

1. Facebook
2. YouTube
3. WhatsApp
4. Facebook Messenger
5. Weixin/WeChat
6. Instagram
7. QQ
8. QZone

Las redes sociales Weixin/WeChat, QQ o QZone son de origen chino y son muy utilizadas en su país de origen, sin embargo no son tan relevantes entre la población española. Facebook sigue siendo la más usada a nivel mundial, pero sus principales usuarios son personas adultas, dado que su uso por niños o adolescentes es minoritario.

El estudio «Las TIC y su impacto en la socialización de adolescentes»[59] indica que las redes sociales más utilizadas entre los jóvenes son las siguientes:

1. WhatsApp
2. YouTube
3. Instagram
4. Facebook
5. Twitter

Edad para estar en las redes sociales

Según la actual normativa oficial[60], antes de los 14 años los padres deben dar su consentimiento para la cesión de los datos del menor y, a partir de esta edad, es el mismo menor el que puede dar este consentimiento y, por tanto, registrarse en las redes sociales cuya edad mínima así lo permita.

58 https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

59 https://www.fad.es/sites/default/files/investigacion_conectados_2018.PDF

60 https://boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

WhatsApp

Sin lugar a duda, esta aplicación para móvil, que también puede ser usada vía web, es la reina de las comunicaciones entre los jóvenes. Nació como una aplicación de mensajería instantánea y, posteriormente, se agregó la capacidad de crear grupos. Estos grupos son los que ahora le confieren una mayor versatilidad, ya que es muy popular no solo entre menores, sino también entre sus padres. Se crean grupos de clase, grupos de antiguos alumnos, grupos de padres de clase, etc.

Asimismo, esta aplicación dispone de llamadas de vídeo y voz que permiten la colaboración con los compañeros. Sin embargo, el hecho de tener que proporcionar el número de móvil para poder conversar con otros, lo hace muy poco apropiado para su uso escolar.

La **edad mínima de registro son 16 años**, aunque en los términos del servicio[61] alerta de que, en caso de no tener la edad mínima, serán los padres los que deberán aceptar las condiciones en nombre de su hijo. Por lo que recae en los progenitores la última responsabilidad.

YouTube

Esta herramienta para vídeos de Google es la que domina en este tipo de servicio, casi sin competidores. Los jóvenes y adolescentes consumen una gran cantidad de vídeos de esta red social, principalmente de *youtubers* y de su música preferida. Debido a esto, probablemente es la menos social de todas las redes sociales, ya que la producción personal de los adolescentes y jóvenes es mínima.

La edad de registro[62] en YouTube es de 14 años, aunque en el caso de las cuentas de GSuite para Educación[63] —que es el servicio ofrecido por Google a los centros educativos— será la autorización de los padres la que valide al niño. En el caso de no disponer de GSuite para Educación, Google dispone de una herramienta para que los padres puedan crear una cuenta para sus hijos pequeños llamada Family Link[64].

Instagram

Esta es, sin lugar a duda, la red más usada por nuestros alumnos y jóvenes. Su principal característica es que ha nacido con la clara vocación de difundir imágenes más que palabras. Casi todo lo que se publica en ella es a través de fotos y vídeos de corta duración. Además, apenas tiene soporte para ser usada con ordenador, ya que su filosofía es la de usarse en los **móviles**. Inmortalizar el momento que se está viviendo a través de una foto, ha impulsado la era del *selfie*, donde lo importante es aparecer allí donde otros no pueden. Lo importante no es estar o disfrutar, sino mostrar públicamente que se ha estado y se ha disfrutado.

El asunto de los *selfies* está tan extendido que se han producido muertes por imprudencia a la hora de hacérselos. Incluso existe una investigación médica que estudia la epidemiología de la muerte por selfie como puede leerse en «Selfies: A boon or bane?»[65] que llega a la conclusión de que deben crearse zonas libres de *selfies*, especialmente las turísticas con peligro de accidentes. A propósito de esto también puede leerse el artículo periodístico «Morir por un selfi: 259 personas han fallecido por tener la foto más original».[66]

Otro de los problemas asociados a Instagram es que, al estar basado en la imagen, favorece comportamientos autolesivos[67] y otros como la anorexia y la bulimia[68]. Aunque parece que últimamente ha empezado a limitar este tipo de comportamientos en su red social.

La edad mínima de registro en Instagram viene fijada por la propia red[69] en 13 años.

---

61 https://www.whatsapp.com/legal/?eea=1#terms-of-service

62 https://support.google.com/accounts/answer/1350409?hl=es

63 https://support.google.com/a/answer/139019?hl=es

64 https://support.google.com/families/answer/7101025

65 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6131996/

66 https://www.elperiodico.com/es/extra/20181016/morir-por-un-selfie-259-muertos-por-hacerse-foto-mas-original-7088670

67 https://as.com/betech/2019/02/07/portada/1549578137_439520.html

68 https://www.elespanol.com/social/20180825/cuentas-fomentan-anorexia-instagram-no-hace-evitarlo/332967151_0.html

69 https://help.instagram.com/478745558852511/

Facebook

Esta red es la que más usuarios tiene a nivel mundial, aunque apenas crecen en las franjas inferiores de edad, ya que está formada, sobre todo, por adultos que en su día se apuntaron a ella y en ella siguen. Seguramente en los próximos años podremos ver un declive más o menos pronunciado.

Su creador Mark Zuckerberg[70], además, es el propietario de Instagram y WhatsApp. El flujo de datos entre las tres redes sociales no es ningún secreto. Tanto en los términos del servicio de WhatsApp[71] como en las condiciones de uso de Instagram[72], se avisa sobre este trasvase de datos entre las diferentes redes.

La edad mínima para pertenecer a Facebook es de 13 años, tal como indica en las condiciones del servicio[73].

Twitter

Esta red social intentaba emular a los SMS, que hace años usábamos para enviar mensajes a través del móvil, aunque utilizando el ordenador en lugar de un teléfono. El número de caracteres ha estado limitado desde sus inicios y en estos momentos tiene como límite máximo 280 (en un principio fueron 140). Dado que aquello que se publica en Twitter aparece en la parte superior de la red social como si se tratase de un blog, se le ha llamado *microblogging*.

A diferencia de otras redes, en Twitter las cuentas privadas son absolutamente minoritarias, ya que nuestros comentarios se unen a un flujo de conversación formado por aquellos a los que seguimos y por nuestros seguidores, que en su abrumadora mayoría tienen perfiles abiertos. Además, un perfil cerrado, aunque es posible configurarlo así, probablemente carezca de sentido en esta red. Según los términos del servicio de Twitter,[74] la edad mínima de registro es de 13 años.

Skype

Es uno de los programas de mensajería y videollamadas más antiguo. Actualmente pertenece a Microsoft y su forma de trabajo no ha variado sustancialmente en las últimas décadas, lo cual nos indica que es un programa estable, bien asentado y de éxito.

La edad mínima de registro es la misma que rige para los servicios de Microsoft[75] que exige la mayoría de edad legal en cada país o el consentimiento de los padres. Por lo tanto, en España es necesario tener cumplidos los 18 años para usar Skype por cuenta propia.

Comunicación y colaboración

Sabemos que las redes sociales se utilizan sobre todo para estar en contacto con amigos, sentirse parte de un grupo, buscar la aprobación de aquellos a los que conocemos, explicar lo que hacemos y un largo etcétera que abarca todo lo que es el ocio y otros aspectos de la naturaleza humana.

En este apartado queremos detenernos en aplicaciones que no son únicamente lúdicas, sino de **trabajo, cooperación y colaboración entre personas**. Las posibilidades de las redes sociales como medio de **autoformación, aprendizaje continuo y desarrollo de trabajos conjuntos** son inmejorables y, sin embargo, pocas veces se tratan así frente a los alumnos.

Formación en las redes sociales

Estar al día en un tema o en los conocimientos de una profesión no es algo fácil y, por eso, se recurre muchas veces a los cursos de formación, tanto presenciales como *online*. Su utilidad como un medio

70 https://es.wikipedia.org/wiki/Mark_Zuckerberg

71 https://www.whatsapp.com/legal/?eea=1#terms-of-service

72 https://help.instagram.com/478745558852511/

73 https://www.facebook.com/legal/terms/update

74 https://twitter.com/es/tos

75 https://www.microsoft.com/es-es/servicesagreement/

para descubrir nuevas técnicas y conocimientos es incuestionable, pero no dudaremos tampoco en decir que un buen uso de las redes sociales puede ser tan enriquecedor, o más, que los cursos, ya que nos pueden poner en contacto con personas de primera línea.

De una forma práctica y con una finalidad eminentemente didáctica, hemos dividido las redes sociales en tres tipos, según las implicaciones que tienen para nosotros su uso:

- **Redes sociales tradicionales.** Son aquellas que han seguido el modelo de Facebook. Las primeras redes sociales iniciaron su andadura en la web y, posteriormente, han dado el salto al teléfono móvil. Muchas de estas han desaparecido y, de las que quedan en la actualidad, nos interesan Facebook[76] y LinkedIn.[77] Se basan en **mensajes largos**, aunque su longitud no es importante.
- **Redes sociales basadas en la mensajería instantánea**. Son las que han surgido como evolución de aplicaciones pensadas, en un primer momento, para la comunicación personal a través del teléfono móvil y que, después, han dado el salto a la web. La red más usada es Telegram.[78] Por su naturaleza, lo que se escribe en ellas suelen ser **mensajes cortos**. WhatsApp no puede incluirse en el apartado de formación, ya que los miembros por grupo están limitados a 256, de forma que no es apto para actuar como medio de comunicación cuando los grupos son medianamente extensos.
- ***Microblogging***. Son redes intermedias entre las dos anteriores, pues en ellas se usan **mensajes cortos.** Nacieron para ser utilizadas a través de la web. Solamente hablaremos de Twitter,[79] aunque hay más. El sistema de seguimiento de personas en el *microblogging* es muy diferente al de las otras redes sociales, dado que la **amistad es asimétrica** («x» sigue a «y», pero «y» no tiene que seguir necesariamente a «x»), circunstancia que no se da en las demás redes sociales, en las cuales la amistad es simétrica.

Grupos de profesionales

Sin lugar a duda, un grupo de profesionales en una misma área laboral puede ser una estupenda forma de estar al día en el trabajo de cada uno. Y existen numerosos grupos en los que podemos estar en contacto con colegas de la misma profesión.

Estos grupos pueden ser tremendamente útiles para mantenernos al día en aquello que nos interesa, ya que existen grupos prácticamente de cualquier temática que deseemos tratar. Sin embargo, debemos tener presentes algunos aspectos antes de apuntarnos a ellos:

- Hay que **limitar el número de grupos**. Si los grupos son activos, con varios mensajes diarios, no podremos estar suscritos a más de tres o cuatro. Aunque al principio lo tomemos con muchas ganas, nos podemos ver muy pronto inundados de mensajes que se acumulan tras pocos días de no prestarles atención, con lo que se obtiene un resultado contrario al que se pretendía, debido al exceso de información que no podemos manejar convenientemente, es la infoxicación[80]. Esta sobrecarga informativa requiere un gran esfuerzo para poder ser asumida y, en muchos casos, tiene como efecto el abandono de todos los canales de información que se están siguiendo. Por este motivo, no solo es importante la selección de la red o redes sociales que utilizaremos, sino también la cantidad de grupos y la actividad que tiene cada uno. Por tanto, **conviene saber hacer una selección de unos pocos grupos** que nos interesen para seguirlos y participar en ellos. Evitemos, desde el primer día, la peligrosa tendencia a unirnos a docenas de grupos, por interesante que sea su temática.
- **Elegir cuidadosamente las redes sociales.** Asimismo, es preferible que el número de redes sociales en las que participemos sea limitado y selecto por el mismo motivo que no

76 https://www.facebook.com/

77 https://www.linkedin.com/

78 https://telegram.org/

79 https://twitter.com/

80 https://es.wikipedia.org/wiki/Sobrecarga_informativa

es conveniente pertenecer a numerosos grupos. Si vemos que Twitter cumple con nuestras expectativas, no intentemos también seguir el ritmo de Facebook, Telegram y LinkedIn.
- **Controlar la calidad de los grupos** a los que nos unimos. No hay nada peor que querer informarse de un tema en un grupo que, supuestamente, está dedicado a él y ver cómo de cada dos mensajes, uno no tiene interés. Algunas veces los grupos que no tienen una gran cohesión acaban por variar el tema que les unía y lo cambian por otro como la política, el deporte, las necesidades sociales, etc. Temas que son perfectamente legítimos, pero que no deberían tener cabida en un grupo profesional de temática concreta.

Algunas recomendaciones para no morir por infoxicación:

- Para los adultos que empiezan su andadura en las redes sociales, lo más sensato es iniciar un **período de prueba** en dos o tres de ellas.
- Antes de apuntarse a uno de los grupos, si es posible, conviene **revisar los mensajes que se escriben** en ellos, para ver si realmente son de nuestro interés, la frecuencia de publicación y si ha estado activo en los últimos días, ya que hay grupos que están muertos y abandonados. **Se debe seleccionar aquellos que estén activos y con una frecuencia de unos pocos mensajes diarios**.
- Si el grupo al que nos apuntamos es **hiperactivo**, lo cual es frecuente en algunos grupos de Facebook con miles de usuarios, es aconsejable **desactivar todas las notificaciones** de este, ya sean por correo, alerta en el móvil o ventanas emergentes del navegador. Estos grupos los podremos visitar regularmente cuando nos interese y así marcaremos nosotros mismos el ritmo del tiempo que les dedicamos.
- En las redes sociales tradicionales —las que no están basadas en mensajería instantánea— un buen grupo para poder seguir deberá estará formado desde varios cientos de personas hasta unos pocos miles y la frecuencia de mensajes se situará sobre unos diez o veinte diarios. Más mensajes suelen ser difíciles de seguir cada día y menos no suelen aportar información relevante, ya que suelen ser grupos con una baja motivación.
- Las redes sociales basadas en la mensajería instantánea, como Telegram y WhatsApp, suelen descontrolarse con cierta facilidad en determinados momentos especialmente activos. Además, estas redes, por el hecho de recibir notificaciones en el móvil cada vez que alguien publica algo, son mucho más propensas a la infoxicación y al cansancio. Así pues, los grupos óptimos suelen ser más reducidos, en torno a las 100 o 200 personas. Cuando el grupo se vuelve hiperactivo, siempre existe la posibilidad de **desactivar las notificaciones durante algunas horas**, algo que debemos acostumbrarnos a hacer para evitar ser interrumpidos continuamente.

Lógicamente, podremos encontrar grupos que no se adaptan a estos parámetros y que pueden ser realmente interesantes. La experiencia nos dirá cuáles son y los que merecen la pena.

Figura 11:
Primeros pasos en redes sociales con fines profesionales

Nota 11. Elaboración propia

Estrategias en la escuela

– Debatir en clase el problema del exceso de información y la forma de seleccionar aquello que nos interesa realmente para dejar de lado lo secundario, es decir, seleccionar nuestras fuentes con el objetivo de reducir su número.

Redes sociales tradicionales

Esta categoría está formada por las redes sociales más complejas, las que nacieron con el propósito de conectar todos los aspectos de sus usuarios a través de Internet. Aquí se incluyen redes generalistas como Facebook o Google+[81], la fallida red social de Google que terminó su andadura en

81 https://plus.google.com/

abril de 2019 (pero no sucede lo mismo con las cuentas de G Suite que pueden seguir usándola). Curiosamente, esta última red era bastante utilizada por el mundo educativo que huía del bullicio de Facebook. También incluimos en esta categoría a LinkedIn, la red profesional por excelencia, ya que su modelo es similar a las anteriores.

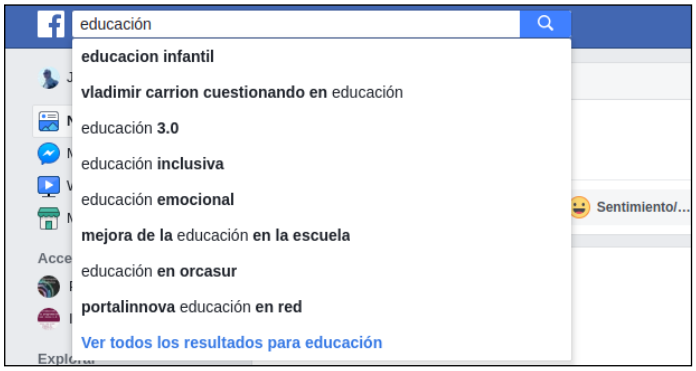
Facebook

Los grupos de Facebook son muy numerosos y, dado el tiempo que tiene esta red, podremos encontrar algunos que han cesado toda actividad y otros que siguen activos y en pleno funcionamiento.

Facebook es un buen lugar para encontrar grupos de tipo profesional, aunque comparte el mismo problema que toda la red social y es la excesiva cantidad de información que circula por ella, mucha inútil como el cambio de imagen de algún contacto o el cumpleaños de otro. Aquellos que abandonan Facebook lo hacen muchas veces por el agobio que produce esta red que es más parecida a un gran mercado, donde todos hablan y gritan a la vez, que a un lugar en el que mantener una conversación.

Los grupos pueden ser totalmente abiertos (basta con pulsar un botón para unirse o tener la aprobación de sus administradores), pero también privados (solo podremos acceder con una invitación expresa).

Figura 12:
Búsqueda de grupos.



Nota 12. Elaboración propia.

Figura 13:
Grupos encontrados. Elaboración propia.

Nota 13. Elaboración propia.

Los temas que podremos encontrar en Facebook son de lo más variado y es muy probable que en esta red haya el mayor número de grupos dedicados a diferentes temáticas.

LinkedIn

LinkedIn, que pertenece a Microsoft desde 2016, es una red que agrupa a profesionales de todo el mundo. Esta red social se basa en la creación de un currículum digital que sirve como punto de encuentro entre empresas y empleados. Dispone de una versión de pago que aumenta las prestaciones ofrecidas a sus usuarios. De todos modos, LinkedIn es perfectamente viable sin necesidad de pagar.

Los grupos de LinkedIn tienen dos modalidades: **ocultos**, a los que solo se puede acceder por invitación y que no aparecen en el buscador; y **estándar,** que aparecen al ser buscados, aunque se necesite autorización para entrar.

La búsqueda es muy similar a la de Facebook. Hay que escribir los términos de búsqueda en el buscador situado en la parte superior, seleccionar los grupos y abrir aquel que nos interese. En todos los grupos se debe pedir la admisión.

Figura 14:
Búsqueda de grupos en Linkedin.

Nota 14. Elaboración propia

Redes sociales de mensajes cortos

Telegram

Esta aplicación de mensajería para móvil, a diferencia de WhatsApp, tiene muy en cuenta la comunicación, no solo entre particulares o pequeños grupos de personas, sino entre una gran cantidad de usuarios (hasta 200.000 por grupo). También se caracteriza por mantener la privacidad de sus miembros, ya que para usar Telegram no es necesario que los demás vean el número de teléfono, tan solo un nombre de usuario.

Además, esta red social tiene dos sistemas de agrupar personas en torno a su aplicación. Por un lado, están los **grupos**, que son utilizados para conversar entre varias personas, y, por otro, los **canales,** que son unidireccionales. En un canal solo los administradores pueden publicar contenido. El canal es la mejor forma de mantener informados a un gran número de personas. Podemos encontrar canales de administraciones públicas, revistas de educación, etc.

Sin embargo, no existe ningún registro completo ni buscador de grupos o canales en Telegram y los usuarios se enteran de su existencia a través de comentarios y de mensajes en redes sociales. Existe el canal, **EduCanales**, en el que se difunden canales educativos; aunque no es exhaustivo, puede ser un buen punto de entrada en el mundo Telegram para los educadores. Además, se puede

utilizar el buscador de Telegram para encontrar **@educanalgrupos** desde la aplicación del móvil o en este enlace https://web.telegram.org/#/im?p=@Educanalgrupos si se utiliza el ordenador.

Hay que tener especial cuidado con los grupos de Telegram, ya que solo con uno o dos especialmente activos podemos tener el móvil dando alertas sin parar. Si un grupo es excesivamente *movido*, deberemos silenciarlo durante algunas horas o de forma permanente. Los canales no tienen este problema, ya que la información es unidireccional y sus miembros no pueden participar de forma directa. No obstante, los grupos suelen ser mucho más enriquecedores que los canales.

Recomendamos estar en algún grupo educativo de Telegram porque es la red social más cercana de todas y la que nos brinda una mayor oportunidad de pertenecer a un grupo de profesionales.

Otra característica muy interesante y que hace de esta red social una aplicación radicalmente distinta a WhatsApp es que no es necesario proporcionar nuestro número de móvil a aquellos con los que hablamos, pues podemos usar un nombre de usuario en lugar del número de teléfono.

Twitter

A diferencia del resto de redes tratadas hasta el momento, el funcionamiento de base de Twitter consiste en seguir y ser seguido, ambos como procesos separados, ya que para seguir no es necesario ser seguido y viceversa. Aunque Facebook añadió está característica más tarde, solo en Twitter forma parte de su filosofía básica.

Esto crea serias diferencias, positivas, con el resto de redes. Si nos interesa seguir a alguien no necesitamos su permiso, podremos leer lo que escribe, aunque jamás llegue a saber que existimos. De esta forma la lista de las personas a las que seguimos forma una línea temporal de mensajes totalmente personalizada. Además, podemos depurar lo que seguimos hasta conseguir ver solo aquello que realmente nos interesa. Este grado de afinamiento es difícil en el resto de redes.

Desde hace algún tiempo, Twitter permite la creación de grupos (conversación grupal en su terminología[82]), aunque de una forma muy básica. Consiste en enviar mensajes directos (privados) a un conjunto de cincuenta personas como máximo. Al enviar un mensaje a más de una persona, se crea automáticamente el grupo al que, incluso, se le puede poner un nombre. Esto lo hace inviable como medio para la formación, aunque sí de comunicación privada a pequeña escala.

Las listas son agrupaciones de personas que hacen los usuarios en Twitter. Podemos hacer una lista con personas que nos interese seguir por un motivo determinado, como la educación en general, por ejemplo. De este modo es posible separar, a través de las listas, las personas según los temas que nos gusten.

Además, Twitter, seguido de Facebook, es la red más utilizada por los docentes en nuestro país. Con la selección apropiada de profesores a seguir, encontraremos una auténtica escuela viva de experiencias. En el artículo «Cuentas de Twitter sobre TIC que debes seguir»[83] tenemos una extensa lista por la que podremos empezar a utilizar esta funcionalidad.

Para saber más

- El artículo «Educanales de Telegram»: http://parapnte.educacion.navarra.es/2017/09/12/educanales-de-telegram/
- El artículo «De Facebook a Telegram, pasando por WhatsApp»: https://jjdeharo.blogspot.com/2016/03/de-facebook-telegram-pasando-por.html

Colaboración en las redes sociales

Creación de grupos

Para colaborar y establecer vínculos a través de las plataformas sociales, serán especialmente útiles Telegram y Twitter.

82 https://help.twitter.com/es/using-twitter/direct-messages

83 https://unaexperiencia20.com/cuentas-twiiter-educacion/

Telegram

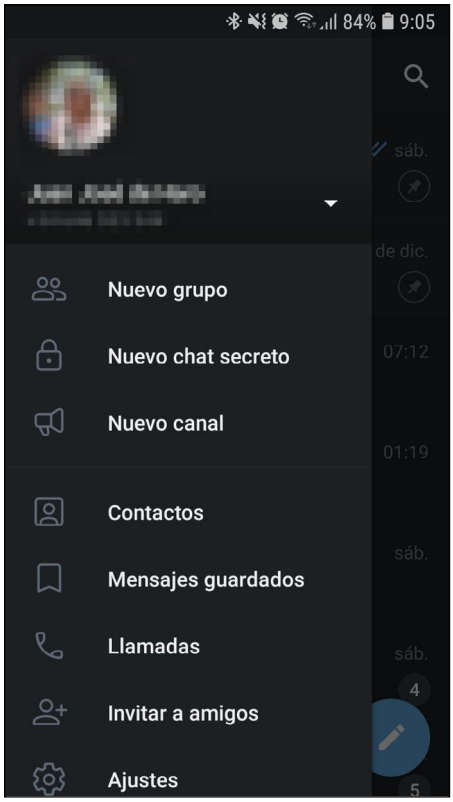
Es la aplicación que permite un mayor control por parte del administrador (o administradores) y dispone de distintas herramientas, por ejemplo, la posibilidad de hacer encuestas en los grupos.

Una vez instalada la aplicación en el móvil y dados de alta, podremos elegir un nombre de usuario en el menú de **Telegram,** solo hay que pulsar **Ajustes > Alias**. Además, nos darán un enlace para iniciar un chat directamente con nosotros (por ejemplo, para poner en un blog).

A continuación se van a mostrar unas capturas de pantalla con el proceso para crear grupos en la aplicación móvil, aunque se sigue un proceso casi idéntico para la versión web de Telegram.

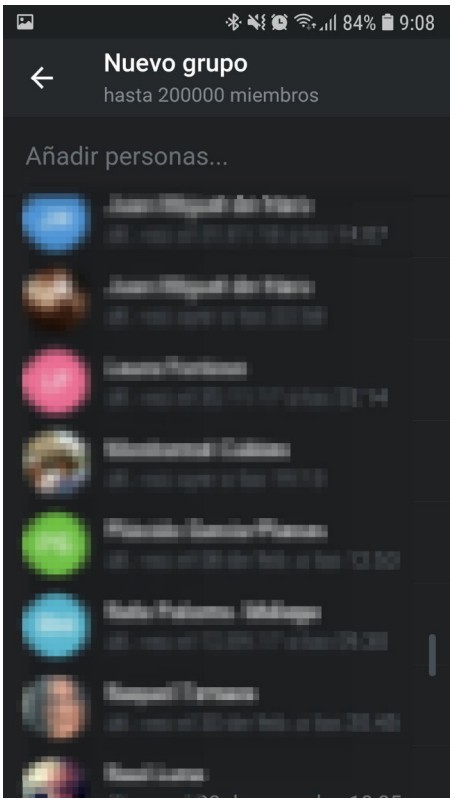
En Android la creación de grupos se puede hacer siguiendo los siguientes pasos:

Figura 15:
Pulsar sobre el menú de Telegram y seleccionar Nuevo grupo.



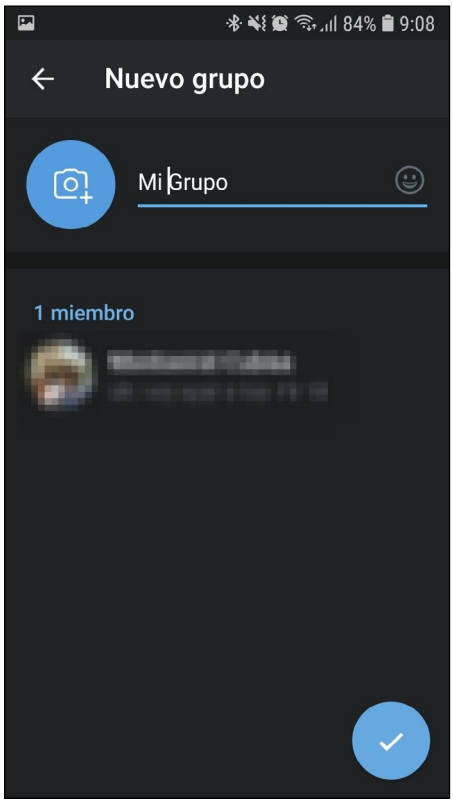
Nota 15. Elaboración propia

Figura 16:
Seleccionar al menos un contacto para poder crear el grupo.



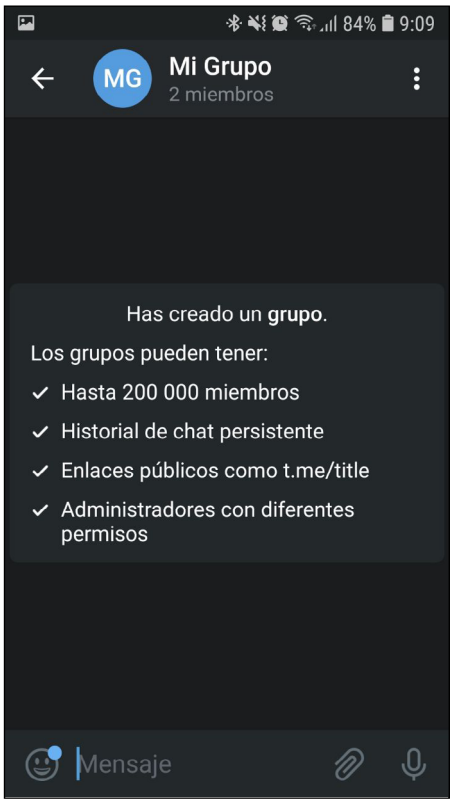
Nota 16. Elaboración propia

Figura 17:
Escribir el nombre del grupo.



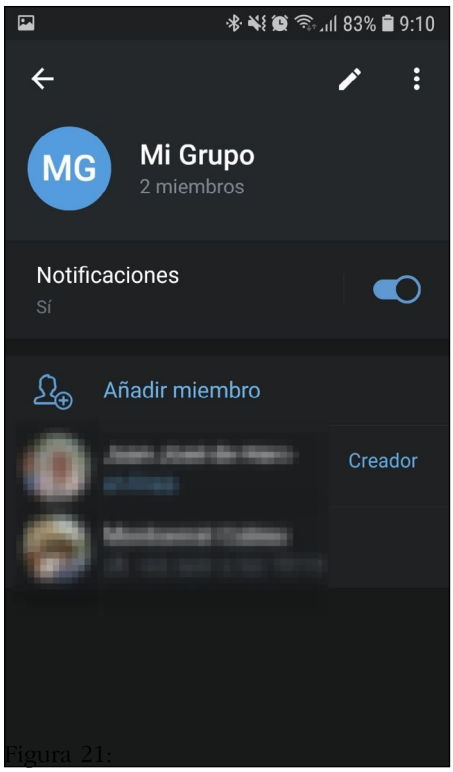
Nota 17. Elaboración propia

Figura 18:
El grupo ya está creado y listo para usarse, pero es privado.



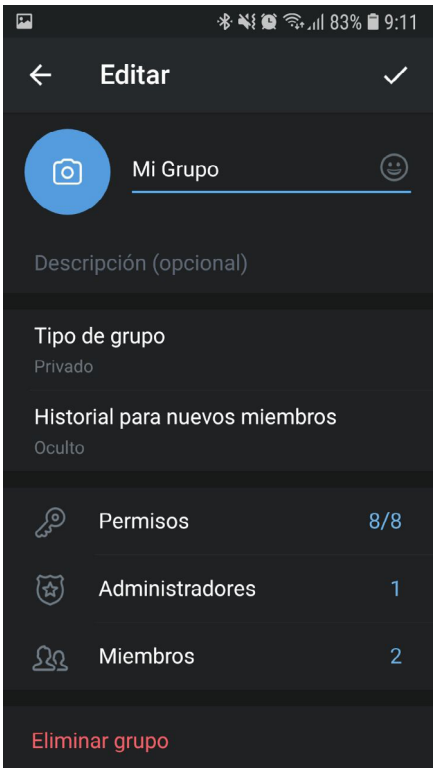
Nota 18. Elaboración propia

Figura 19:
Para hacerlo público hay que pulsar primero sobre el logo circular del grupo y, después, sobre el lápiz.



Nota 19. Elaboración propia

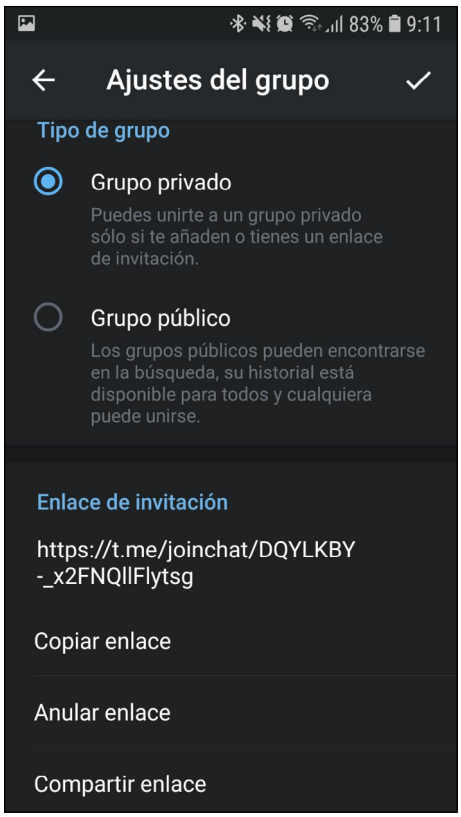
Figura 20:
Seleccionar Tipo de grupo.



Nota 20. Elaboración propia

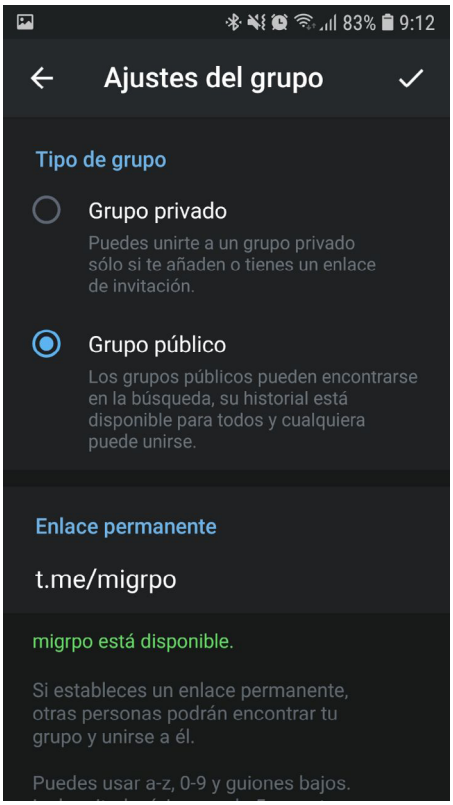
Figura 21:

Figura 21:
Opciones para el grupo privado (recomendado si es para menores).



Nota 21. Elaboración propia

Figura 22:
Opciones para el grupo público.



Nota 22. Elaboración propia

Twitter

Como ya se comentó con anterioridad, para crear un grupo, basta con enviar un mensaje directo a más de una persona y se creará automáticamente.

En la página Información sobre los Mensajes Directos[84] de la ayuda de Twitter, se explica el proceso:

1. Pulsa el icono del **sobre**. Se te dirigirá a tus mensajes.
2. Pulsa el icono de **mensaje** para crear un mensaje nuevo.
3. En el campo de **dirección**, ingresa el nombre o el @usuario de las personas a quienes desees enviar un mensaje. Los mensajes grupales pueden incluir hasta cincuenta personas.
4. Escribe el mensaje.
5. Además del texto, puedes incluir una foto, un vídeo o un GIF, o enviar un *sticker* por Mensaje Directo.

Además, en Administración de los grupos es posible cambiar la imagen del grupo, así como su nombre y otras características:

- Para acceder rápidamente a la lista de participantes de la conversación, pulsa la **foto de perfil** de la conversación grupal en tu bandeja de entrada.
- En la conversación grupal, pulsa el icono de **información** para acceder a la página de configuración.
- Si queremos establecer los detalles de la configuración, los pasos son los siguientes:

84 https://help.twitter.com/es/using-twitter/direct-messages

- Pulsa **Editar** para actualizar la foto de perfil y el nombre de la conversación grupal. Pulsa el icono de la **cámara** para abrir las siguientes opciones para la foto: Ver foto, Cámara, Galería de fotos o Eliminar foto. Pulsa **Guardar** para actualizar.
- Pulsa **Agregar miembros** para agregar personas a la conversación. El creador del grupo es el administrador predeterminado. Si el creador ya no está en el grupo, el primer miembro en unirse al grupo después del administrador se convertirá en administrador. Como administrador, puedes eliminar miembros del grupo.
- Pulsa **Silenciar conversación** para silenciar las notificaciones durante una hora, ocho horas, una semana o para siempre.
- Marca la casilla junto a **Silenciar menciones** para elegir si recibirás notificaciones cuando te mencionan en una conversación grupal. Ten en cuenta que, a menos que actives esta función, recibirás notificaciones cuando te mencionen directamente en una conversación, incluso si activaste la función **Silenciar conversación**. Además, debes ser un participante en una conversación grupal para poder recibir notificaciones de mención de esa conversación.
- Para denunciar la conversación grupal, pulsa **Denunciar la conversación**.
- Para abandonar la conversación grupal, pulsa **Salir de la conversación**.

WhatsApp

Desaconsejamos la creación de grupos de WhatsApp en los que esté implicado un profesor con alumnos, ya que entra en conflicto con el derecho a la privacidad de ambos. De todas formas, será casi imposible impedir la formación de estos grupos por parte del alumnado, ya que casi siempre los crean por iniciativa propia.

Formación

Formación para alumnos

Hablamos de infoxicación

Tipo de actividad: **Debate en clase**

- Duración: **De media a una hora.**
- Niveles implicados: **3.º, 4.º de la ESO y Bachillerato.**
- Objetivos:

  - **Ser conscientes de lo que es la infoxicación.**
  - **Encontrar formas de regular la exposición a lo que se ve en las redes sociales.**
  - **Tomar el control de lo que hacemos en Internet.**
  - **Valorar los medios de comunicación sociales para la formación académica.**

  A partir del siguiente vídeo, se puede establecer un diálogo con los alumnos sobre aquello que vemos por Internet: https://youtu.be/h656PVhJtII

  Los temas que se pueden sacar a colación son muy numerosos, por ejemplo:

- Número de redes sociales o plataformas de las que estamos pendientes a lo largo del día.
- Tiempo dedicado a ver y leer lo que escriben nuestros contactos en las redes sociales.
- ¿Pueden influir los medios sociales sobre el rendimiento escolar?
- ¿Estudiamos con un ojo puesto en WhatsApp y otro en el libro?
- Comparación del tiempo de estudio y el dedicado a YouTube y a otros medios sociales.
- Lluvia de ideas sobre la forma de disminuir la infoxicación.
- Cómo aprovechar las redes para la formación del alumno: se puede preguntar por ideas y proponer las que no salgan.

Calendario cultural

Tipo de actividad: **Elaboración de un calendario de efemérides de la asignatura**

- Duración: **Un curso escolar.**
- Niveles implicados: **Todos los niveles.**
- Objetivos:

  - **Trabajar de forma cooperativa a través de medios sociales.**
  - **Profundizar en los personajes y efemérides relacionados con una materia.**

Dado que la elaboración de un calendario con información relevante tiene muchas posibilidades en cuanto a la forma de elaborarlo y a su temática, daremos aquí únicamente unas líneas generales de cómo se puede llevar a cabo:

- Crear un calendario compartido con toda la clase, donde puedan escribir ellos también. Si usamos Google Classroom, cada clase tiene su propio calendario. Para que los alumnos puedan escribir en él, bastará con ir a la configuración del calendario y, en la sección de compartir, encontraremos tres tipos de usuarios: dos con permisos de escritura (nosotros mismos y los profesores que pertenezcan a esa clase) y otro que solo tiene permiso de lectura. Este último corresponderá al alumnado; bastará con cambiar el permiso con el objetivo de que también puedan añadir eventos.
- Organizar al alumnado para que busque información sobre sucesos temporales relacionados con la materia (fechas históricas, nacimiento de científicos, personajes históricos, descubrimientos, etc.) de forma que vaya completando el calendario con este tipo de efemérides. La información se puede escribir al editar el evento en el calendario de Google, ya que hay un espacio para escribir y adjuntar archivos, imágenes, etc.
- Los días en los que haya un evento recogido en el calendario, el alumno o alumnos responsables lo explicarán al resto de la clase.

Formación para padres: fomentando los medios disponibles

Tipo de actividad: **Fomentar el uso de los medios de comunicación a través de Internet con el centro.**

- Duración: **Sin límite, pero especialmente a principio de curso.**
- Niveles implicados: **Todos los niveles.**
- Objetivos:

  - **Promover el uso de los Internet para la comunicación con el centro.**
  - **Abrir el centro a las nuevas tecnologías.**

Muchos centros educativos disponen de plataformas educativas, pero no aprovechan todas sus funcionalidades, muy especialmente los medios que se ponen a disposición de la comunidad educativa y los padres para comunicarse.

Especialmente a principio de curso, se debe informar a padres y a profesores de los mecanismos que existen a su disposición. Además, se debería fomentar activamente su uso a lo largo del curso.

Engaños en la web

Los engaños, las noticias falsas o las estafas son, sin duda, tan antiguos como el ser humano; muchas veces por diversión, otras por deseo de lucro o por demostrar alguna pretendida superioridad. La verdad es que el fenómeno del engaño no es nada nuevo ni reciente. En la actualidad, la facilidad para pulsar un botón de reenviar; o el copiar y pegar texto en pocos segundos de un mensaje de Facebook a otro de WhatsApp, por ejemplo; o la inmediatez de aquello que enviamos a través de los numerosos medios que tenemos en el móvil, la tableta y el ordenador hace que el fenómeno haya alcanzado un nivel planetario y una falsa noticia nacida en La Patagonia, a los pocos segundos, está en el bolsillo de los habitantes de Madrid o Barcelona.

Hay engaños que son tan simples como el de la noticia sobre la **alineación de Mercurio, Venus y Saturno sobre las pirámides de Giza** en Egipto, lo cual ocurriría cada 2373 años y que fue desmentida por falsa[85].

85 https://www.snopes.com/fact-check/planetary-alignment-over-giza/

Figura 23:
Falsa noticia en Twitter.

Nota 23. Tuit de P. Morillo del 20 de julio de 2018. Twitter https://twitter.com/MPMorilloRocha/status/1020368918442102784

Otros, sin embargo, pueden ser mucho más peligrosos, como la información ofrecida por el artículo «El agua marina purificada cura diversas enfermedades»,[86] que según sus defensores, viene a ser un sanador universal, dado que sirve para:

1. Los problemas de próstata.
2. La psoriasis y otras enfermedades de la piel.
3. Las quemaduras.
4. Las infecciones.
5. La alopecia.
6. La artritis.
7. La osteoporosis.
8. La bronquitis.
9. El asma.
10. La gingivitis.
11. Los problemas gastrointestinales.
12. Los desequilibrios del sistema nervioso central.
13. La hemofilia.
14. La obesidad.
15. La sinusitis.
16. La anorexia y bulimia.
17. La depresión del sistema inmune.
18. La fatiga crónica o aguda.
19. Los desórdenes de huesos.
20. Los dolores del crecimiento en niños.
21. El estrés.
22. También se emplea durante el embarazo y la lactancia, en casos de abortos espontáneos repetidos o para normalizar deficiencias nutricionales.

86 https://www.dsalud.com/reportaje/el-agua-de-mar-purificada-cura-diversas-enfermedades/

Es muy probable que la persona que intente curar su alopecia con el agua de mar no se vea perjudicada, excepto en su bolsillo, pero la que desee curar el asma, las infecciones o la bronquitis puede acabar hospitalizada de urgencia.

Otros engaños pueden afectar directamente a la economía personal como el de aquellos que envían sus datos bancarios a desconocidos que se los piden por Internet. Quizás pensemos que nosotros no lo haríamos, pero el hecho es que el fraude por este medio no hace sino crecer día a día.

Otros bulos intentan directamente hacer daño a personas o a países concretos, por ejemplo, el boicot a los productos provenientes de Marruecos:

Figura 24:

Aviso de una noticia falsa

Nota 24. Tuit de SaludMadrid [@SaludMadrid] del 31 de mayo de 2018. Twitter. https://twitter.com/SaludMadrid/status/1002205083541626881

Podemos dividir los engaños sufridos a través de Internet en tres categorías principales:

1. **Bulos**. Son noticias falsas que, normalmente, tienen la intención de hacer una broma o causar daño a una persona, una empresa, un producto, etc.
2. **Estafas por pagos anticipados**. Se engaña al usuario que adelanta un dinero con la esperanza de obtener más.
3. ***Phishing***. Se utilizan diversas técnicas para conseguir que el usuario entregue datos bancarios, número de la de tarjeta de crédito, etc. para poder robarle.

Figura 25:
Engaños a través de Internet

Nota 25. Elaboración propia

Introducción

Cómo reconocerlos

A nivel general se pueden aplicar unas normas generales en los timos:

- Son ofertas demasiado buenas. Se debe desconfiar de las grandes ganancias casi sin esfuerzo o de los productos exageradamente baratos.
- Hay que revisar su página web y ver los comentarios existentes.
- Los timadores suelen usar correos gratuitos como Outlook o Gmail.
- Se suele evitar el contacto en persona. Por ejemplo, en el caso de las ofertas de trabajo nunca hay entrevistas presenciales, sino que son a través de correo o WhatsApp.

Bulos

Los bulos (también llamados *hoax*) son noticias falsas que se difunden por Internet y que, a veces, duran años; con ligeras variantes que hacen los usuarios que los reenvían. Su temática suele ser muy variada, aunque tienen en común algunas características que **ayudan a reconocerlos**:

- Muchos son anónimos y no citan fuentes concretas para evitar las comprobaciones.
- No están fechados y no llevan referencias temporales para poder alargar su vida.
- Habitualmente son noticias muy llamativas, con algo que enganche al que lo lee: morbo, dinero, miedo, etc.
- Contienen llamamientos a ser reenviados lo máximo posible. A veces, también incluyen amenazas de mala suerte y otras desgracias si no se hace.

A diferencia del fraude, que suele tener como objetivo obtener dinero, el del bulo busca su difusión masiva. Aquí tenemos algunos ejemplos de los ganchos que se utilizan (Wikipedia)[87]:

- WhatsApp va a ser de pago de manera inminente... reenvía este mensaje a X personas antes del día X (gancho de miedo basado en valor monetario).
- Hotmail cerrará sus cuentas. Perdida de contactos y multa de una gran cantidad de dinero (gancho de miedo basado en valor monetario).
- Ya estamos avisados por Google... lo pasaron en la tele... por si las dudas... El uso de Google y Gmail costará dinero (gancho de miedo basado en valor monetario).
- *Actimel* es malo para la salud. Produces L-Casei y dejas de fabricar defensas (gancho de miedo basado en la salud).
- *Redbull* contiene veneno en su composición química (gancho de miedo basado en el daño a la salud).
- Recibes una llamada telefónica y, en lugar de aparecer el número de teléfono de quien te llama, aparece la palabra "INVIABLE!!" o DESCONOCIDO. Si aceptas o rechazas la llamada el extorsionador accede a la SIM de tu teléfono, la duplica y la usa para llamar desde la cárcel (gancho de miedo basado en ser víctima de una estafa).

Qué hacer frente a un bulo:

- Por norma, no reenviar nunca ningún mensaje en el que se diga que debe ser reenviado.
- Si pensamos que es una causa humanitaria o de otro tipo, pero **real**, debemos comprobarlo antes de enviárselo a nadie. Una búsqueda de cinco minutos por Internet bastará para confirmarlo o desmentirlo; pero nunca mandar nada «por si acaso es verdad», porque nunca lo es. Lo muy dramático o excesivamente llamativo suele ser falso. Se debe comprobar siempre si es verdad. Una forma de encontrar rápidamente un bulo es añadir en la búsqueda la palabra bulo (o *hoax*), de este modo veremos con rapidez si ha sido desmentido.

87 https://es.wikipedia.org/wiki/Bulo

Figura 26:
Infografía de la campaña desarrollada por la Federation of Library Associations and Institutions

Nota 26. Obtenido de *How to Spot Fake News [Infografía]*, por IFLA (2017). Wikipedia https://es.wikipedia.org/wiki/Archivo:%C2%BFEsta_noticia_es_falsa%3F_(How_To_Spot_Fake_News).jpg. Creative Commons Atribución Internacional 4.0

Fake news

Un tipo de bulo, que puede llegar a ser más peligroso que los anteriores, son las *fake news* (o noticias falsas) creadas con la intención deliberada de engañar, inducir a error, manipular decisiones personales, desprestigiar o enaltecer a una institución, entidad o persona u obtener ganancias económicas o rédito político (Wikipedia)[88]. Se elaboran como si fuesen noticias periodísticas y, a diferencia de los bulos tradicionales, detrás de ellas hay auténticos expertos del engaño y la manipulación política. La infografía de la figura 26, que pertenece a la campaña desarrollada por la International Federation of Library Associations and Institutions (IFLA)[89] con respecto a este tema, nos propone un ejercicio de reflexión e investigación que debemos acostumbrarnos a realizar cuando estemos ante un bulo.

En la actualidad, las noticias falsas son un auténtico problema, ya que se intenta influir en lo que piensan las personas a base de la difusión de exageraciones, omisiones e incluso auténticas invenciones de lo que está sucediendo en la realidad. El espíritu crítico que debemos tener ha de estar doblemente desarrollado para evitar caer en las redes de aquellos que desean crear su propia imagen de la realidad. Las *fake news* están muy relacionadas con la **posverdad**, de la que se hablará más adelante.

88 https://es.wikipedia.org/wiki/Fake_news

89 https://www.ifla.org/

Estrategias en la escuela

– Los bulos se han convertido en algo cotidiano, por este motivo el profesor deberá tener especial sensibilidad sobre este tema. Es importante traer y discutir en clase aquellos bulos que vayan siendo desenmascarados, especialmente si tienen relación con la materia de alguna asignatura con el objetivo de hacer énfasis en la necesidad de contrastar la información antes de creerla totalmente.

Estafas por pagos anticipados

Estas estafas se producen cuando hay que adelantar dinero para obtener un beneficio, un producto o una ganancia extra. Existen varios tipos de estafas por pagos anticipados, según la forma que adquieran.

Compras online

Se ponen a la venta productos que el comprador paga y jamás llega a recibir. Para evitar este tipo de fraudes lo mejor es comprar *online* únicamente en sitios solventes y reconocidos. Hay que evitar mensajes en redes sociales, correos electrónicos o blogs personales. Servicios de compraventa entre particulares como Wallapop[90] se basan en un sistema de confianza por las compras y ventas realizadas con anterioridad por cada persona. Un estafador podrá estafar, pero seguramente solo una vez, ya que el usuario engañado inmediatamente así lo hará constar en la web.

Debemos actuar con suma precaución en los siguientes casos:

– Al investigar la procedencia de la empresa no hay forma de ubicarla físicamente, ya sea por teléfono, dirección postal, etc.
– Son empresas de las que no hay información. Debe buscarse siempre información sobre la empresa cuando esta no es conocida por nosotros y rechazar, por atractiva que sea la oferta, aquellas que parecen salir de la nada.
– Las ofertas son excesivamente buenas. Móviles a mitad de precio, marcas de ropa cara por un tercio o menos de su valor, etc. suelen ser un indicador de fraude.
– Fijarse si la web utiliza una conexión segura (https). Nunca deberán realizarse transferencias económicas o enviar datos personales si la web donde estamos comprando no dispone, desde el principio, de una conexión segura.
– Comprobar las opiniones de los usuarios sobre esta empresa y su página.
– En las webs y aplicaciones de compraventa es imprescindible leer las opiniones de los usuarios.

Engaños sentimentales

Este tipo de estafas puede producirse a través de webs de contactos y citas donde una persona consigue la confianza de otra hasta que el estafador comienza a pedir dinero a la víctima, siempre por motivos urgentes (pagar una deuda, solucionar un problema familiar, etc.). Hay casos de timadores profesionales que actúan tanto dentro como fuera de la Red y utilizan su empatía para arruinar a sus víctimas. Es el caso del famoso timador de mujeres[91] que utilizaba sus *encantos* para engañar y dejar sin dinero a las que se pensaban que eran sus novias. Estos casos se producen con la misma frecuencia entre los dos sexos.

90 https://es.wallapop.com/

91 https://www.elperiodico.com/es/sociedad/20171217/estafador-mujeres-tambien-enredo-sevilla-internet-6492460

Además, existen engaños organizados donde interviene más de una persona en la estafa. En estos casos se turnan varias personas para estar siempre disponibles cuando el atacado quiere hablar con su relación a través de Internet. Por este motivo, más de una vez no se acuerdan de aquello que han dicho y sus respuestas suelen ser al momento, como si estuviesen siempre pendientes.

Hay señales de que algo de todo esto puede estar sucediendo si:

- El enamoramiento de la otra persona a través de Internet ha sido muy rápido.
- Dicen ser del mismo país que la víctima, pero están en otro muy lejano.
- Piden dinero.
- Van a venir de visita, pero siempre hay algo que se lo impide.
- Están solos y no tienen amigos o familia, la víctima es su única ayuda.

Timos de caridad y sociales

Cada vez que ocurre alguna catástrofe aparecen personas sin escrúpulos que intentan aprovecharse de la desgracia de los demás. Este tipo de engaños suelen producirse con temas como enfermedades incurables o de tratamiento caro, recuérdese el triste caso de la niña Nadia[92] que fue rentabilizada por sus padres a través de las redes sociales.

Siempre que se vaya a hacer una donación monetaria por una causa social, deberemos investigar a quién estamos dando nuestro dinero. Si ha ocurrido cualquier desastre como un terremoto, un huracán, una hambruna, etc., debemos encauzar nuestra ayuda a través de organismos oficiales o de solvencia reconocida.

Deberemos evitar a toda costa:

- Dar dinero a cualquier organización de la que no sepamos nada, hay que comprobar si la organización realmente invierte su dinero en aquello que dice.
- No enviar dinero a cuentas bancarias que circulen por las redes sociales o WhatsApp.
- No deben creerse los mensajes que circulan por las redes sociales, especialmente WhatsApp, cuando hay un desastre. Acudir siempre a fuentes oficiales: policía, bomberos, agencias de noticias o prensa, entre otros.

Falsas ofertas de trabajo

Existen muchas ofertas de trabajo a través de Internet que no son reales. Todas se basan en ofertas excelentes para el trabajador, en muchas de ellas no se requiere experiencia o se trabaja cómodamente desde casa, pero todas tienen en común que piden dinero en algún momento para poder acceder al trabajo o piden que se llame a números telefónicos de facturación muy alta. Tras la llamada, el buscador de empleo es entretenido durante todo el tiempo que son capaces para, al final, no obtener el deseado trabajo.

En estos timos debemos tener cuidado con lo siguiente:

- Son ofertas de trabajo que no se tramitan por webs especializadas, sino a través de mensajes en redes sociales, anuncios en las páginas web o por correo electrónico.
- Las condiciones laborales son excesivamente buenas y casi cualquiera lo puede hacer, ya que intentan llegar al mayor número posible de víctimas.
- Piden un adelanto monetario en forma de tasas de acceso, fotocopias, certificados, compra de material, etc. Nunca debe confiarse en el que pide dinero a cambio de trabajo.

92 https://elpais.com/elpais/2016/12/02/ciencia/1480673352_055858.html

Para saber más

La lectura de los siguientes artículos es muy recomendable:

- «Tiendas *online* fraudulentas»: https://www.osi.es/es/tiendas-online-fraudulentas
- «Estafas de caridad»: https://www.consumidor.ftc.gov/destacado/destacado-s0011-estafas-de-caridad
- «Las 8 falsas ofertas de empleo más utilizadas por ciberdelincuentes en Internet»: https://www.osi.es/es/actualidad/blog/2014/03/04/las-8-falsas-ofertas-de-empleo-mas-utilizadas-por-ciberdelincuentes-en-in

Phishing

El *phishing* es una técnica que consiste en imitar correos electrónicos y páginas web similares a otras reales con la finalidad de engañarnos para obtener nuestros datos y así poder acceder a nuestro dinero a través del banco, la tarjeta bancaria, etc.

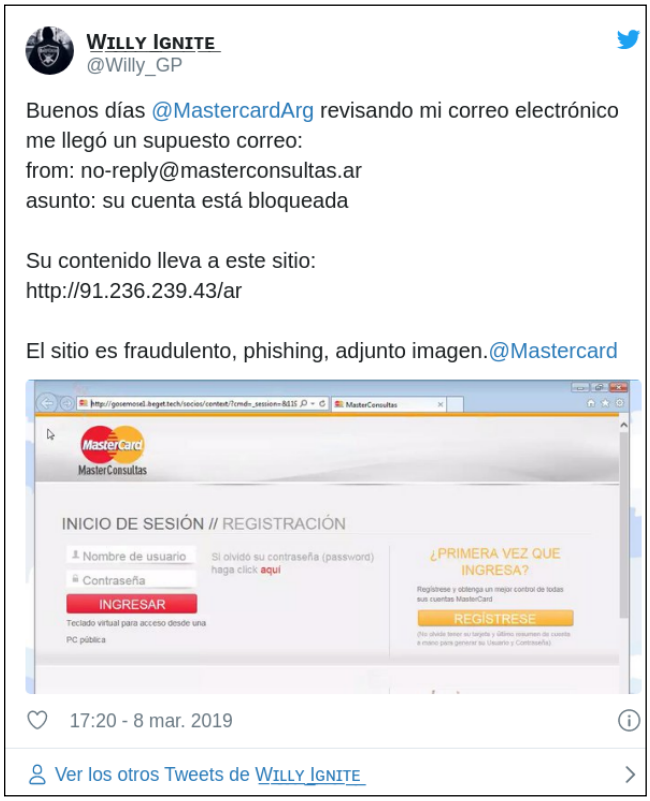
La siguiente imagen es un ejemplo de un mensaje que nos podremos encontrar con facilidad en nuestra carpeta *spam* (o correo basura), en el que se simula que han intentado acceder a nuestra cuenta de correo. Con toda seguridad lo que intentarán será que escribamos nuestro nombre de usuario y contraseña en una web falsa para así hacerse con nuestros datos.

Figura 27:
Mensaje de correo fraudulento

Nota 27. Captura de pantalla de un correo real recibido por el autor. Elaboración propia.

Un usuario de Twitter informa de un correo recibido que le lleva a una web fraudulenta:

Figura 28:
Web Fraudulenta



Nota 28. Obtenido de *Buenos días @MastercardArg revisando mi correo electrónico me llegó un supuesto correo: from: no-reply@masterconsultas.ar asunto: su cuenta está bloqueada Su contenido lleva a este sitio: http://91.236.239.43/ar El sitio es fraudulento, phishing, adjunto imagen.* [Twitt], por WILLY IGNITE [@Willy_GP] (8 de marzo de 2019). Twitter https://twitter.com/Willy_GP/status/1104054234968920064

El objetivo de estos mensajes es asustar al usuario para poder obtener sus datos personales y bancarios. En otros casos simulan sorteos como el del falso anuncio de Correos[93] en el que imitaban su web para anunciar el sorteo de dos móviles de última generación.

Dado que tanto los anuncios como los correos y las webs imitan a las auténticas, debemos tener siempre precaución cuando pensemos que estamos ante algo oficial y comprobar su autenticidad:

- Si es una página web, debemos comprobar que la conexión es segura y la dirección corresponde realmente con la que se supone que debe ser. Por ejemplo, si estamos en una página que debería ser de *Amazon*, pero vemos que su dirección es algo así <http://amazon.marksoon.jp> es que estamos ante un fraude
- En los correos hay que poner atención a la ortografía y a las expresiones utilizadas. Es frecuente que los mensajes de *phishing* tengan faltas ortográficas y estén escritos con expresiones coloquiales.
- Los mensajes son urgentes y suelen requerir una acción inmediata.
- Nos piden datos bancarios o personales a través del correo, algo que nunca hacen las entidades bancarias.
- Se debe comprobar que el remitente de correo se corresponde con quién debe ser. Por ejemplo, un correo que debería ser de Google, pero en su lugar vemos que el remite es <google@googlemaildiv45.com> es que es falso.

Para saber más

- **Se recomienda el artículo** «Conoce a fondo qué es el Phishing»: https://www.osi.es/es/banca-electronica

93 https://www.elidealgallego.com/articulo/espana/estafa-correos-policia-nacional-advierte-timo/20190301110249399005.html

Posverdad

El término *posverdad* se ha venido utilizando desde hace algunos años para describir cómo las *fake news* y los intentos de dominar la realidad pública se han convertido en una tendencia dominante en la política, en los medios que los apoyan y también en otros ámbitos de la sociedad. Los activistas de la posverdad continúan repitiendo sus puntos de vista, aun cuando haya sido demostrado que son erróneos, de este modo se consigue introducir una serie de mensajes en la sociedad que, a fuerza de ser repetidos, acaban calando profundamente.

En la posverdad, apelar a los sentimientos es más importante para convencer a los individuos que la verdad misma o las pruebas que existan en contra de sus postulados. Son numerosos los ejemplos —tanto en política como en otros ámbitos— en los que la creencia supera a la razón y donde la idea que pueda tocar la vena sensible del ser humano tiene prioridad sobre el relato de lo que realmente ha acontecido.

El **conspiracionismo** —la existencia de teorías conspirativas por parte de grupos de poder— es un argumento muy usado en la posverdad, ya que a través de él se puede negar cualquier evidencia científica o histórica, de forma que también se rechaza la propia esencia de la Ciencia (la refutación, que es uno de sus pilares básicos). Tenemos, por ejemplo, los siguientes casos:

- El **terraplanismo** es la creencia de que la Tierra es plana, algo que, aunque sabemos que no es así, es cada vez más aceptado por un elevado número de personas a las que no les falta la educación básica, es decir, no es un problema de incultura, sino de lo que uno decide creer. Es un claro ejemplo de **negación científica** en el que se prefiere la creencia a la prueba, pues las pruebas científicas son tachadas de **conspiracionistas**.
- **Las pseudociencias,** como la **homeopatía,** caso en el que ha sido imposible demostrar científicamente su beneficio (véase, por ejemplo, el artículo «A systematic review of systematic reviews of homeopathy»[94]). Estas siguen estando presentes en nuestra sociedad, incluso forman parte de una temática de las farmacias. El deseo de curación de aquellos que padecen enfermedades, unido a los que no tienen escrúpulos, hace que se sigan comercializando productos formados básicamente por agua como si fuesen auténticos medicamentos. El sentimiento y la emoción juegan aquí un papel muy importante. Relacionados con la salud, hay muchos otros ejemplos de remedios nada ineficaces, que incluso pueden llevar a la muerte, al rechazar la auténtica medicina. Se ha estimado que en España mueren entre 1200 y 1400 personas anualmente[95] debido a las terapias alternativas.
- **Posverdad política**. En la política, las noticias falsas se han usado mucho con la intención de conseguir un rédito político. Se consideran ejemplos de posverdad política las elecciones estadounidenses en las que ganó Trump o las noticias surgidas durante el referéndum para la salida del Reino Unido de la Comunidad Europea.

Para saber más

- «La era de la posverdad: realidad vs. percepción». Monográfico de la revista *UNO* con numerosos artículos sobre el tema. https://www.revista-uno.com/wp-content/uploads/2017/03/UNO_27.pdf

94 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1874503/

95 https://www.efesalud.com/pseudoterapias-muertes-informe-APETP

Estrategias

Estrategias en la escuela

- Organizar debates sobre los temas más problemáticos relacionados con la posverdad: pseudociencias, creencias irracionales, etc. Hay que poner énfasis en la necesidad de utilizar el raciocinio y la ciencia como guía para saber lo que es cierto y lo que no.
- Enseñar a contrastar la información utilizando casos reales de bulos o falsas creencias para que los alumnos investiguen casos concretos y, de esta forma, lleguen al fondo y la verdad de la realidad.

Estrategias en la familia

- Los padres deben fomentar el espíritu crítico de sus hijos haciendo hincapié en aquellas noticias falsas, bulos y engaños que surgen a través de los medios de comunicación u otros medios. Se debe comentar por qué son falsas y la necesidad de contrastar las fuentes ante las informaciones problemáticas.
- Hay que ser conscientes sobre este problema y aprovechar las ocasiones que sean propicias para tratarlo.

Formación de los alumnos

Conceptos falsos

Tipo de actividad: **Investigación y debate**

- Duración: **2 horas**
- Niveles implicados: **ESO y Bachillerato**
- Objetivos:

  - **Aprender a contrastar la información.**
  - **Aprender a determinar lo que es verdad y lo que no lo es.**

  En el artículo «75 frases que debe evitar en Nochebuena si no quiere quedar como un *cuñado*»[95] hay una recopilación de tópicos relacionados con la ciencia, todos falsos. La verdad es que esta selección da mucho juego tanto para ser tratados por separado como en conjunto. Con esta misma fuente, se propone otra actividad más adelante (Encuesta sobre tópicos). Podemos decir que son bulos que, a fuerza de ser repetidos, han quedado fijados como ciertos para muchas personas. Por lo tanto, es un buen tema sobre el que trabajar para desarrollar el espíritu crítico.

- Se forman grupos de cuatro alumnos y se les dan tres de los falsos conceptos a cada uno de ellos, pero sin decirles que son falsos.
- Durante 15 minutos deben decidir cuáles son falsos y cuáles correctos.
- El resto del tiempo lo invierten en buscar pruebas irrefutables que apoyen sus creencias, para ello irán apuntando las pruebas, así como el origen de la información, es decir, las páginas web que los avalan.

96 https://scientiablog.com/2018/12/24/75-frases-que-debe-evitar-en-nochebuena-si-no-quiere-quedar-como-un-cunado/

– Al día siguiente cada grupo expone sus conclusiones y se debate con el resto de la clase. El profesor rectificará aquellas concepciones falsas que todavía persistan. Se debe insistir en la necesidad de tener un espíritu crítico para no caer en la falsedad.

Encuesta sobre tópicos

Tipo de actividad: **Debate**

– Duración: **1 hora**
– Niveles implicados: **ESO y Bachillerato**
– Objetivos:

  • **Aprender a contrastar la información.**
  • **Aprender a determinar lo que es verdad y lo que no lo es.**

– Usando el mismo artículo de la actividad anterior, «75 frases que debe evitar en Nochebuena si no quiere quedar como un *cuñado*»[96], puede crearse un formulario tipo verdadero o falso con varios de estos tópicos.
– Los alumnos lo completan el día anterior a la actividad y el profesor recopila aquellos en los que hay mayor cantidad de errores.
– Al día siguiente, empezando por el que tenga mayor número de verdaderos, se da la palabra a los alumnos para que expliquen sus opiniones tanto a favor como en contra.
– De este modo se van analizando los diferentes casos, mientras se da una explicación racional y científica apropiada para cada caso.

El día más triste del año

Tipo de actividad: **Investigación y debate**

– Duración: **1 hora**
– Niveles implicados: **ESO y Bachillerato**
– Objetivos:

  • **Aprender a contrastar la información.**
  • **Aprender a determinar lo que es verdad y lo que no lo es.**

  Cada tercer lunes del año los medios de comunicación nos informan de que ese día es el más triste del año, el llamado *Blue Monday*. Nada más lejos de la realidad; esta falsa creencia tiene su origen en una campaña publicitaria.[97] Aprovechando estas fechas, podemos elaborar una actividad.

– Se proyecta en clase alguna de las numerosas noticias (escrita o en vídeo) que informa sobre este asunto.
– Se discute en clase durante 15 minutos la posible veracidad del *Blue Monday* y si realmente puede una fórmula explicar la felicidad humana.
– Se dan a los alumnos 15 minutos de tiempo para buscar en Internet el origen de esta fecha.
– Se vuelve a discutir, con los nuevos conocimientos, la autenticidad del *Blue Monday*.

97 https://scientiablog.com/2018/12/24/75-frases-que-debe-evitar-en-nochebuena-si-no-quiere-quedar-como-un-cunado/

98 https://es.wikipedia.org/wiki/Blue_Monday_(fecha)

Derechos de autor y licencias

Los problemas del *copyright*

Una de las constantes con las que se encuentra la persona que produce algún tipo de documento que hace público, de una forma u otra, es **cómo tratar el material ajeno**, aquel que cogemos —habitualmente de Internet— para ilustrar o completar nuestra propia obra. Cualquier obra intelectual tiene **derechos de autor** (***copyright***) que deben ser respetados.

Las obras intelectuales, en principio, están sujetas a la Ley de Propiedad Intelectual, que protege los derechos de autor. He aquí un fragmento:

> Es lícita la inclusión en una obra propia de fragmentos de otras ajenas de naturaleza escrita, sonora o audiovisual, así como la de obras aisladas de carácter plástico o fotográfico figurativo, siempre que se trate de obras ya divulgadas y su inclusión se realice a título de cita o para su análisis, comentario o juicio crítico. Tal utilización solo podrá realizarse con fines docentes o de investigación, en la medida justificada por el fin de esa incorporación e indicando la fuente y el nombre del autor de la obra utilizada. (Real Decreto Legislativo 1/1996, art.32.1[99]).

Así pues, la ley es clara: con fines educativos podemos hacer uso de fragmentos de las obras de otros siempre que citemos la fuente y el nombre del autor. Esto significa que, si deseamos hacer un uso más amplio, o bien pedimos al autor su autorización, o bien debemos abstenernos de usar el recurso.

Por este motivo, existen las licencias Creative Commons que nos permiten usar más ampliamente las obras de otros, sin limitarnos a citar fragmentos. Estas deben ser otorgadas por el autor de la obra y las encontraremos en forma de texto o imagen junto al recurso pertinente. Los artículos de Wikipedia, por ejemplo, tienen una licencia de este tipo. En esta misma categoría entran los Recursos Educativos Abiertos (REA) que utilizan este mismo tipo de licencias para facilitar su uso por todos los docentes.

Algunas licencias especiales —como algunas de las imágenes que ilustran esta publicación digital— no requieren citar a su autor ni el origen que tienen y son utilizables tanto para fines comerciales como de otro tipo (Licencia Pixabay)[100]. No obstante, este tipo de licencias no son las más comunes.

También existen obras de **dominio público**, cuyos logotipos son los que se sitúan a la izquierda de este párrafo. Este tipo de obras no tienen exclusividad en cuanto a su acceso o utilización y, por tanto, lo que pertenece al dominio público puede ser usado libremente. Un autor puede ceder su obra al dominio público, con lo cual renuncia a los derechos que ello comporta. En cuanto a las obras en general, pasado un determinado tiempo, se convierten en obras de dominio público. El número de años varía de un país a otro, en el caso de España este tiempo es de setenta años desde la muerte de su autor. Para una discusión detallada sobre el concepto de dominio público y sus límites, se recomienda consultar Wikipedia[101]

Debemos tener bien claro que no podemos utilizar material de Internet con cualquier propósito. Los recursos que encontremos han llevado, seguramente, muchas horas de trabajo y es de justicia que lo respetemos y les demos el crédito que merecen. En los siguientes apartados se tratará el tema de cómo usar de forma ética los recursos que hay en Internet.

Creative Commons

Entre el *copyright* y el dominio público existe un intermedio llamado *Creative Commons* (CC). Cuando un autor decide poner su obra bajo una licencia de este tipo, permite que otros usuarios puedan

99 https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930&b=50&tn=1&p=20180414#a32

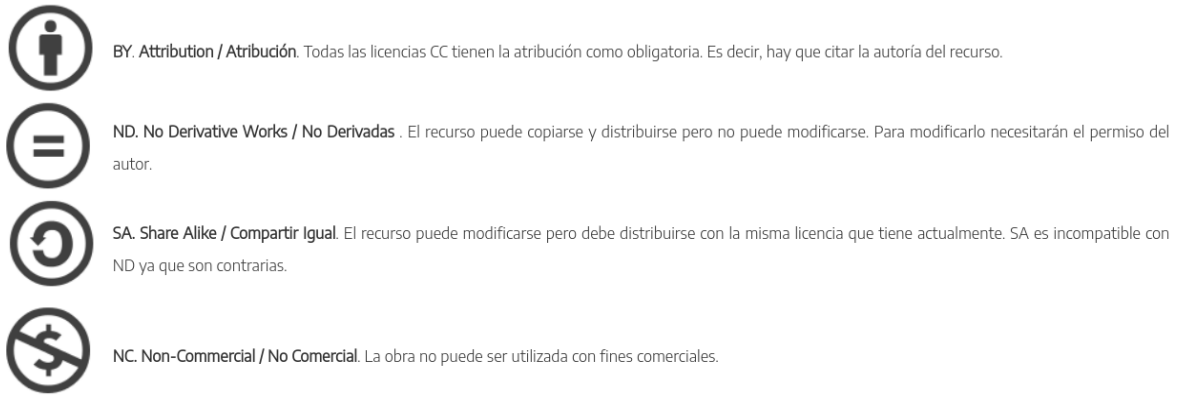
100 https://pixabay.com/es/service/license/

101 https://es.wikipedia.org/wiki/Dominio_público

hacer uso de ella y establece también sus límites. Si deseamos compartir nuestro trabajo con otras personas, Creative Commons es lo que necesitamos.

Licenciar una obra bajo *Creative Commons* es tan sencillo como incluir una imagen para especificar lo que se permite (en este enlace hay una lista de las imágenes posibles)[102] o desde la propia web de *Creative Commons*, tras seleccionar las opciones apropiadas para nuestra obra en un formulario[103] diseñado a tal fin.

Figura 29:
Significado de los diferentes iconos



Nota 29. Tras el icono se indica la abreviatura que se utiliza y el nombre en inglés y castellano. Elaboración propia.

Aunque el recurso no cumpla nuestros propósitos —por ejemplo, si queremos modificarlo, pero se indica que no es posible hacerlo para crear una obra derivada—, siempre podemos acudir al autor para pedirle su permiso porque siempre puede modificar los derechos sobre su propia creación intelectual.

Las licencias CC no solo se usan en los medios digitales, se pueden utilizar igualmente para las obras escritas en papel. Debemos acostumbrarnos a poner una licencia CC en cada obra que coloquemos en Internet (presentaciones, apuntes, etc.), ya que, de este modo, facilitamos a los demás el uso de nuestro propio material y contribuimos activamente a la construcción de la ciudadanía digital. Si no ponemos una licencia CC, en este caso nuestra obra estará protegida por los derechos de autor (*copyright*), de forma que los demás no podrán hacer apenas uso de nuestro material.

Del mismo modo que ponemos a nuestra obra una licencia CC, buscaremos recursos en Internet que tengan también una de ellas y así evitaremos usar aquellas protegidas con *copyright*.

Buscadores de recursos abiertos

Podemos buscar, directamente a través de Google y otros buscadores, recursos abiertos con el fin de utilizarlos para nuestras creaciones, es decir, con licencia Creative Commons o carentes de *copyright*.

Google

Google permite buscar imágenes y textos con licencia CC.

Páginas web con licencia CC

Realizamos una búsqueda normal y seleccionamos **Configuración > Búsqueda avanzada.**

102 https://creativecommons.org/about/downloads

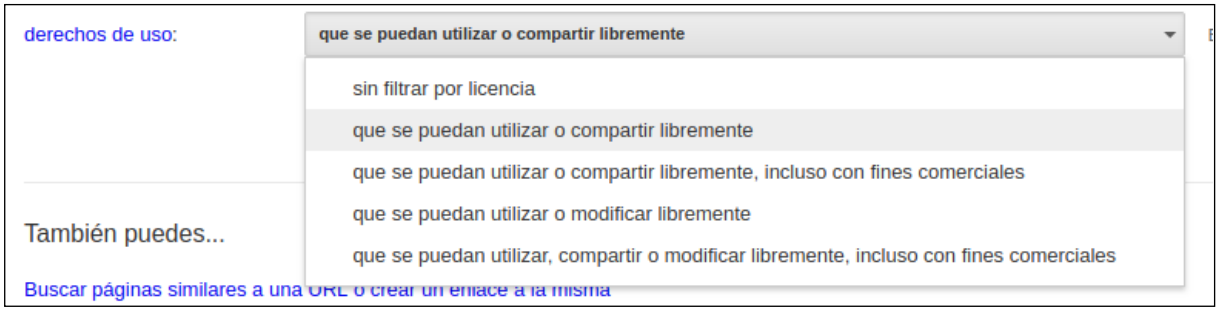
103 https://creativecommons.org/choose/?lang=es_ES

Figura 30:
Búsqueda en Google

Nota 30. Elaboración propia

En Búsqueda avanzada, seleccionamos **Derechos de uso** y después la opción que deseemos, normalmente «que se pueda utilizar o compartir libremente».

Figura 31:
Búsqueda avanzada



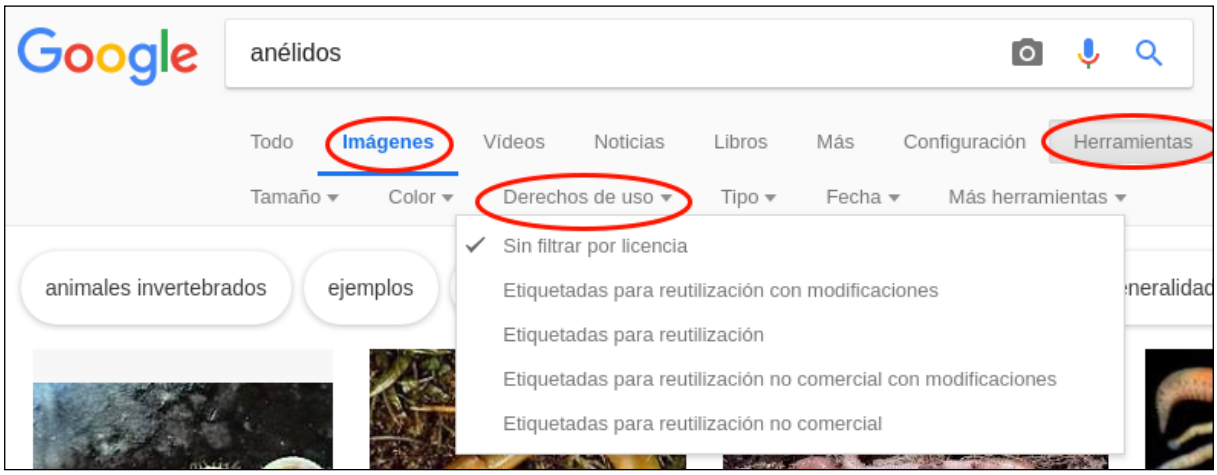
Nota 31. Elaboración propia

Tras pulsar el botón **Búsqueda avanzada**, obtendremos los resultados que podremos usar sin las limitaciones de los derechos de autor.

Imágenes con licencia CC

Lo más habitual es la búsqueda de imágenes. Como en el caso anterior, procederemos a realizar una búsqueda de imágenes normal y después seleccionamos **Herramientas > Derechos de uso** luego la opción que queramos. Si es una imagen para colocar en nuestro texto, elegiremos **Etiquetadas para reutilización**.

Figura 32:
Imágenes con licencia CC



Nota 32. Elaboración propia

Europeana

La Comunidad Europea ha creado Europeana (https://www.europeana.eu) con la finalidad de tener un banco de datos de acceso libre, con contribuciones de instituciones culturales de los 28 estados miembros de la UE. Incluye libros, películas, pinturas, periódicos, archivos sonoros, mapas, manuscritos y otros archivos. Es, por tanto, un excelente lugar al que acudir para buscar material, sobre todo histórico y cultural.

Internet Archive

Internet Archive (https://archive.org/) es una biblioteca digital gestionada por una organización sin ánimo de lucro dedicada a la preservación de archivos, capturas de sitios públicos de la Red, recursos multimedia y también *software*. Esta organización existe con el apoyo de Alexa Internet y de otros colaboradores que han donado materiales y colecciones como la Biblioteca del Congreso y otras muchas bibliotecas públicas y privadas. Alberga una gran cantidad de archivos en diversos formatos: audio, vídeo y texto. Además, la gran mayoría son de dominio público, con licencias tipo Creative Commons u otras licencias que permiten su distribución gratuita (para saber más sobre *Internet Archive se puede consultar este enlace de la* Wikipedia[104]).

Bancos de imágenes abiertas

Hay muchos bancos de imágenes de uso libre, a continuación se van a citar algunos de los más significativos. En la web Herramientas y Servicios TIC Abiertos Para Educación[105] podremos encontrar más. Como se ha indicado, los más importante son:

- **Pixabay** (https://pixabay.com/es/) es un banco de imágenes que tiene una licencia propia y permite usar sus imágenes sin restricciones. Es, sin duda, uno de los mejores.
- **Morguefile** (https://morguefile.com) contiene un gran número de imágenes de uso libre.
- **Creative Commons**. La propia web de Creative Commons tiene un buscador de imágenes que se puede consultar en este enlace: https://ccsearch.creativecommons.org/
- **Banco de imágenes y sonidos del INTEF** (http://recursostic.educacion.es/bancoimagenes/web/). Es una base de datos de imágenes y sonidos que podremos utilizar para nuestros trabajos.

104 https://es.wikipedia.org/wiki/Internet_Archive

105 http://herramientas.bilateria.org/#Bancos de imágenes abiertas

Bancos de música abierta

No existen muchos lugares donde podamos obtener música que pueda ser usada libremente, pero a continuación listamos algunos:

- **Audionautix**: https://audionautix.com/
- **dig.CCMixter**: http://dig.ccmixter.org/
- **Musopen**: https://musopen.org/es/

Bancos de sonidos abiertos

Estos bancos contienen sonidos de diferentes tipos, normalmente de unos pocos segundos. Se pueden citar los siguientes:

- **AudioMicro**: https://www.audiomicro.com/sound-effects
- **Banco de imágenes y sonidos del INTEF**: http://recursostic.educacion.es/bancoimagenes/web/
- **elongSound**: https://www.elongsound.com/sonidos.html

Pueden encontrarse más bancos de sonido en Herramientas y Servicios TIC Abiertos Para Educación[106].

Para saber más

- **Recursos Educativos Abiertos (REA)**. Ofrece más bancos con recursos de la web Herramientas y Servicios TIC Abiertos Para Educación. http://herramientas.bilateria.org/#Recursos Educativos Abiertos (REA)

Estrategias en la escuela

- Se debe enseñar a los alumnos a buscar imágenes que puedan utilizar en sus trabajos.
- También es necesario enseñarles que, siempre que usen un recurso (un texto, un vídeo o una imagen) que no sea suyo, deben asegurarse de que se puede utilizar y que se debe mencionar siempre a su autor e incluir un enlace a la fuente original.

Recursos Educativos Abiertos (REA)

Figura 33:
Logo de la UNESCO para los REA

Nota 33. *Logo REA de la UNESCO,* por Jonathas Mello en Wikipedia. Bajo licencia https://es.wikipedia.org/wiki/Archivo:Logotipo_Global_Recursos_Educacionais_Abiertos_(REA).svg. Creative Commons Atribución 3.0 Unported

106 http://herramientas.bilateria.org/#Bancos de imágenes abiertas

En el apartado anterior hemos visto cómo encontrar **recursos aptos para ser usados sin infringir los derechos de autor**. Esto es algo que **debemos tener profundamente interiorizado**. No podemos usar Internet como un gran bazar de objetos gratuitos, ya que detrás de cada texto y cada imagen hay una persona que ha dedicado su tiempo para ponerlo a nuestra disposición.

Figura 34.
Logo REA en Wikimedia Commons

Nota 34. *Logo en español para los recursos educativos abiertos (REA)* por Juan José de Haro en Wikimedia Commons https://commons.wikimedia.org/wiki/Category:Open_Educational_Resources_-_Logo#/media/File:REA_Logo_sp.png, bajo licencia CC0

Los **Recursos Educativos Abiertos, o REA,** (en inglés, *Open Educational Resources* [OER]) están íntimamente ligados a las licencias CC. Los REA están constituidos por **documentos y material multimedia cuyos fines tienen relación con la educación**, en concreto, con la enseñanza, el aprendizaje, la evaluación y la investigación. Su principal característica es la de estar **plenamente disponibles para ser usados por educadores y estudiantes, sin la necesidad de pagar regalías o derechos de licencia** (modificado de Wikipedia[107]).

Los REA son materiales creados por docentes que se ponen a disposición de otros para que los usen y los puedan modificar también. La Unesco apoya de forma activa los REA a través de numerosas iniciativas. Los objetos de los REA tienen como característica:

- **Reutilizar**. El derecho a reutilizar el contenido en forma inalterada o literal (por ejemplo, hacer una copia de seguridad).
- **Revisar**. El derecho a adaptar, ajustar, modificar o alterar el contenido (por ejemplo, traducirlo a otro idioma).
- **Remezclar**. El derecho a combinar el contenido original o revisado con otro contenido para crear un producto nuevo (por ejemplo, integrar el contenido de fuentes distintas en uno nuevo).
- **Redistribuir**. El derecho a compartir copias del contenido original, de las revisiones o de las remezclas con otras personas (por ejemplo, dar una copia del contenido a un conocido).

En los bancos (llamados *repositorios*) de los REA podremos encontrar unidades didácticas y materiales de diversa índole listos para poder ser utilizados. En la siguiente lista proporcionamos algunos de ellos:

- **Procomún** (https://procomun.educalab.es/) es la red de recursos educativos en abierto del INTEF. Pueden consultarse los REA y también subirse.
- **Proyecto EDIA** (http://cedec.intef.es/proyecto-edia/) ofrece un banco de contenidos educativos para Primaria, Secundaria, Bachillerato y Formación Profesional. Se trata de recursos educativos abiertos, curricularmente referenciados y que ofrecen propuestas ligadas a metodologías activas y al fomento de la competencia digital en el aula.
- **Proyecto CREA** (https://emtic.educarex.es/proyectocrea). El proyecto CREA (Creación de Recursos Educativos Abiertos) es una iniciativa de la Consejería de Educación y Empleo de la Junta de Extremadura que tiene como objetivo proporcionar a la comunidad educativa (y a los diferentes agentes del sector educativo que puedan estar interesados en ellos) un conjunto de recursos educativos abiertos (REA).
- **UNESCO IIEP Learning portal** (https://learningportal.iiep.unesco.org/es/library). Es el banco de recursos de la Unesco.
- **Graasp** (http://graasp.eu/). Pertenece a la Comisión Europea y es un banco de REA, una herramienta de autor para crear REA y un repositorio para subir REA ya creados.

107 https://es.wikipedia.org/w/index.php?title=Recursos_educativos_abiertos&oldid=126507980

– Pueden encontrarse más bancos de REA en esta página: http://herramientas.bilateria.org/#Bancos%20REA

Para saber más

– **Página de la Unesco sobre los REA:** https://es.unesco.org/themes/tic-educacion/rea
– ***Guía básica de recursos educativos abiertos (REA)***. Libro de 150 páginas. Unesco. https://unesdoc.unesco.org/ark:/48223/pf0000232986
– **Open Educational Resources (OER)**. Logos de REA descargables en múltiples idiomas. https://es.unesco.org/node/275488

Estrategias en la escuela

– Desde los centros educativos se debe fomentar la creación de REA por parte del profesorado y su puesta a disposición en Internet, por ejemplo, en Procomún o Graasp.
– Los alumnos también deben acostumbrarse a crear materiales en los formatos propios de Internet y, si es posible, a compartirlos a través de licencias CC.

Formación para alumnos

Normas de los trabajos

– Tipo de actividad: **Normas**
– Duración: **Todo el curso**
– Niveles implicados: **Desde el momento que se les empiezan a pedir trabajos cuya información obtienen de Internet.**
– Objetivos:

  • **Aprender a respetar el trabajo de otros**
  • **Aprender a citar las fuentes consultadas**
  • **Aprender a compartir**

El centro debería dictar unas normas generales aplicables en todos los niveles donde se hacen trabajos consultados a través de Internet para que escriban las referencias que han usado y utilicen una licencia Creative Commons en sus propios trabajos.

– Forma de citar las fuentes:

  • En Primaria puede limitarse al título de la página y la dirección web.
  • En Secundaria se puede añadir el autor, el año de publicación, el título y la dirección web.

– Solo en Secundaria, darles a elegir entre varias licencias Creative Commons para que pongan aquella que mejor se adapte a sus intereses.
– Fomentar el uso de portafolios digitales (por ejemplo, un blog) donde vayan colocando los trabajos que hacen.

La construcción de nuestra identidad digital

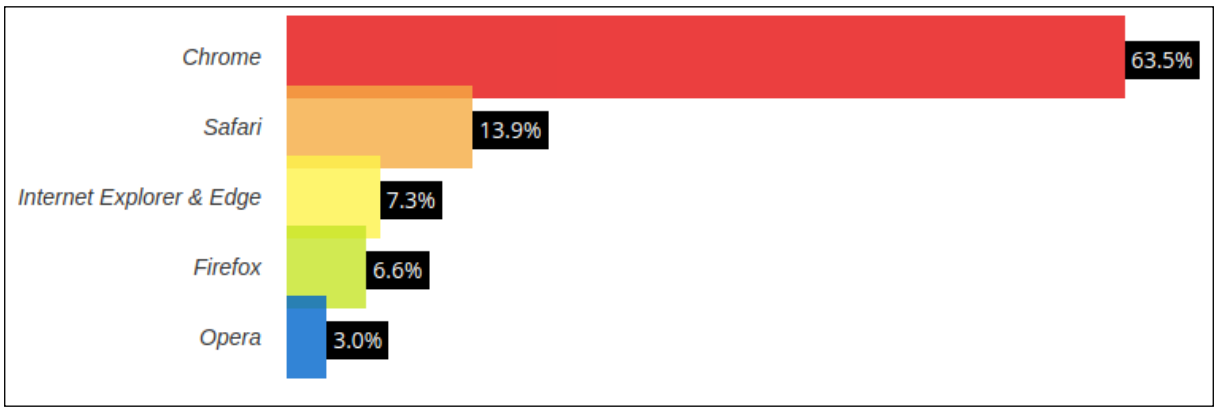
Privacidad y navegación segura

Introducción

Uno de los usos más básicos que se puede hacer de Internet es la navegación a través de la web. Cada vez es más frecuente la existencia de sitios maliciosos que pueden darnos problemas, ya sea por suplantación de otras páginas (en un intento de engañarnos en cuanto a su funcionalidad, pues aparentan ser otras), contener virus que pueden infectar nuestro ordenador o incluir descargas de contenido muy distinto al esperado.

Según la página W3Counter[108] más del 90 % de los usuarios utilizan alguno de los siguientes navegadores: Chrome, Internet Explorer y Firefox. Aunque casi dos tercios de los usuarios utilizan el primero como se puede comprobar en este gráfico:

Figura 35:
Navegadores más utilizados.



Nota 35. *Web Browser Market Share,* por W3Counter, 2019, en https://www.w3counter.com/globalstats.php. Todos los derechos reservados

Dado que Chrome[109] es el navegador más utilizado con diferencia, cuando se expliquen determinadas opciones se hará con este navegador. Además, Chrome está basado en el proyecto de *software* abierto Chromium,[110] cuyo uso es casi idéntico al de Chrome, y, dado que cada vez más navegadores se basan en Chromium, sus opciones de uso también se parecen cada vez más.

En el uso diario de Internet hay ciertos **niveles o anillos de seguridad** que debemos tener en cuenta y ser conscientes de ellos, ya que **mantener una adecuada configuración** en cada uno nos ayuda a **aumentar nuestra protección** en Internet. Los niveles más cercanos, de los cuales podemos tomar fácilmente el control, son:

- Las **herramientas** que el mismo **navegador** nos proporciona es la seguridad más inmediata.
- La posibilidad de utilizar **sesiones (o perfiles) de usuario en el navegador**, lo que nos ayuda a mantener usuarios separados (equivalentes a direcciones de correo) y sin interferencia entre ellos.
- La posibilidad de utilizar **sesiones de usuario en el ordenador** o dispositivo móvil que estemos utilizando. Esto impide que otros usuarios puedan acceder a nuestros datos en el dispositivo que estemos usando.

108 https://www.w3counter.com/globalstats.php

109 https://www.google.com/chrome/

110 https://www.softzone.es/2019/01/09/navegadores-chromium-aumentando/

Por supuesto, existen otros factores que debemos tener en cuenta para realizar una navegación más segura como la presencia de un antivirus en los sistemas de Windows o programas de funcionalidad específica para la seguridad.

Contraseñas

Actualmente, casi toda la seguridad está basada en la elección de una buena contraseña. En la mayoría de servicios se accede escribiendo un nombre de usuario y una contraseña. Si la contraseña es fácil de averiguar, tenemos muchas posibilidades de que en un momento u otro alguien acceda a nuestros datos e incluso se haga pasar por nosotros. En Internet se venden contraseñas robadas de forma que saber elegirlas es una obligación (como se puede comprobar en este artículo: «620 millones de usuarios y contraseñas se venden al mejor postor»[111]). Además, conviene aumentar la seguridad con el inicio de sesión en dos pasos que se explicará en el siguiente apartado.

Una herramienta que nos puede resultar útil es la extensión para Chrome Password Checkup[112] que comprueba si las contraseñas que utilizamos, junto con el nombre de usuario, han sido expuestas en Internet. En caso afirmativo nos avisará para que la cambiemos.

Además, los gestores de contraseñas nos ayudan a realizar un uso correcto de estas tanto a la hora de crear una nueva (nos sugieren contraseñas seguras) como a la hora de recuperarlas, lo que hacen por nosotros cuando nos piden identificación. Chrome lleva incorporado un gestor de contraseñas y, si lo utilizamos frecuentemente, ya nos habrá preguntado en más de una ocasión si deseamos guardarlas. Ciertamente esto plantea un dilema, pues si alguien consigue acceder a nuestra cuenta de Google —o a la que usemos con otro gestor de contraseñas— podrá acceder a nuestras contraseñas. En el caso de Google se encuentran en la dirección https://passwords.google.com/. Se hace evidente que necesitamos contraseñas fuertes, junto al inicio de sesión en dos pasos para poder proteger nuestra cuenta principal.

A continuación se facilitan algunos consejos sobre cómo construir una buena contraseña:

- No debe usarse la misma contraseña en varios sitios distintos. Para la cuenta de Google, que protegerá nuestras cuentas en otros servicios, deberá ser única en el caso de utilizar su gestor de contraseñas.
- No hay que utilizar palabras, sino frases: **«los domingos son días especiales»**.
- Se debe añadir alguna mayúscula y minúscula, por ejemplo, al inicio y al fin de la segunda palabra: **«los DomingoS son días especiales»**.
- Se puede añadir algún número, por ejemplo, en lugar del último espacio: **«los DomingoS son días35especiales»**.
- O bien, añadir algún carácter especial, por ejemplo, en lugar del primer espacio y poner puntos en las oes: **«l.s~D.ming.S s.n días35especiales»**.

Lo mejor es inventarnos nuestras propias reglas, siempre y cuando el resultado final no sea una palabra o una expresión más o menos evidente, o dejar que un gestor de contraseñas lo haga por nosotros. En el artículo «Los mejores gestores de contraseñas»[113] se analizan varios de ellos.

Inicio de sesión en dos pasos

Para aumentar la seguridad y evitar que suplanten nuestra identidad, es conveniente que añadamos una capa extra de protección al inicio de sesión en nuestras cuentas. Especialmente si son servicios sensibles como Google, Dropbox, Facebook, Twitter o Instagram, entre otros.

El inicio de sesión en dos pasos consta de un **nombre de usuario** y una **contraseña**, como es habitual, al que se añade la necesidad de **posesión de un dispositivo** que solo el auténtico propietario posee y que se necesita para acceder al servicio. Por lo general, suele ser un **teléfono móvil** a través del cual se reciben las claves que deberán escribirse, o bien se activa una aplicación

111 https://hipertextual.com/2019/02/hacker-620-millones-passwords-dark-web

112 https://chrome.google.com/webstore/detail/password-checkup/pncabnpcffmalkkjpajodfhijclecjno

113 https://criptomo.com/mejores-gestores-contrasenas/

en la que deberemos responder si somos nosotros realmente los que deseamos entrar en nuestra cuenta. El sistema a seguir dependerá del servicio. Por ejemplo, en Google, después de introducir nuestro nombre de usuario y contraseña, deberemos responder a una pregunta que nos aparece en el móvil; sin embargo, en Dropbox recibiremos un mensaje SMS para que introduzcamos un código.

Hay algunos casos donde el inicio de sesión en dos pasos puede no resultar práctico, ya que interfiere con nuestro trabajo, como puede ser una cuenta en la que tengamos que iniciar sesión con frecuencia en distintos ordenadores. Es el caso, por ejemplo, de una cuenta de centro que tengamos que abrir en diferentes clases. Normalmente, el proceso de ir de una clase a otra y poner en marcha todo lo que necesitemos ya nos lleva un tiempo que, en ocasiones, puede ser excesivo si la tecnología falla. Si a esto le añadimos la necesidad de llevar el móvil y de consultarlo cada vez, puede ser que nuestro trabajo se vea ralentizado en exceso. En estos casos es preferible usar solo una contraseña que vayamos cambiando con cierta frecuencia (por ejemplo, una vez al trimestre). Lógicamente, cada uno decidirá lo que es más conveniente y el balance entre la seguridad y la rapidez de movimientos deberá depender de nuestras propias necesidades.

Para saber cómo activar el método de inicio de sesión en dos pasos, se puede consultar el artículo «Cómo activar la verificación en dos pasos en Google, Facebook, Twitter, Instagram, Microsoft y WhatsApp».[114] También podemos activar el inicio de sesión de este tipo para el ID de Apple; en la página «Autenticación de doble factor para el ID de Apple»[115] se explica cómo hacerlo.

Configuración del navegador

Es importante ser consciente de determinadas características de los navegadores que nos proporcionan la seguridad más inmediata. Hay tres aspectos especialmente importantes: las **actualizaciones** del navegador, la **configuración de privacidad** y el **rastro** que dejamos al navegar.

Actualización del navegador

Es muy importante tener el navegador siempre actualizado con su versión más reciente, ya que continuamente aparecen vulnerabilidades que ponen en peligro al usuario. A medida que estas se van detectando, se van lanzando actualizaciones que solucionan estos problemas. En general, no debemos preocuparnos, pues los navegadores se actualizan de forma automática. El problema surge cuando, por algún motivo, no se llevan a cabo. Esto sucede, por ejemplo, cuando estamos utilizando un sistema operativo anticuado que ya no recibe más soporte, tal y como pasa con Windows XP, Vista o Windows 7, sistemas operativos todavía en uso por muchos particulares y, lo más preocupante, por muchas instituciones educativas que todavía conservan estos sistemas en despachos y salas de profesores. En estos casos se hace necesario el cambio a una versión superior en la que se sigan recibiendo actualizaciones de seguridad.

Así pues, es necesario mantener actualizados los equipos, es decir, el sistema operativo que tienen y sus programas. Si los ordenadores son antiguos y no aceptan sistemas operativos más modernos o no deseamos realizar un gasto en un ordenador que empieza a estar obsoleto, lo mejor es instalar alguna versión de Linux porque este sistema operativo es capaz de funcionar en ordenadores de bajo rendimiento.

Configuración de la privacidad

En todos los navegadores, ya sea en su versión de PC como en la de dispositivo móvil, se permite configurar determinados **parámetros de seguridad** que nos puede interesar revisar, ya que las opciones que traen por defecto suelen ser suficientes para navegar seguros.

En Chrome podremos acceder a esta configuración tras pulsar sobre los tres puntos que hay en la esquina superior derecha. Después hay que seleccionar Configuración y luego **Privacidad y seguridad**. En Elegir la configuración de privacidad[116] podemos ver una descripción de todas las

114 https://www.xataka.com/basics/como-activar-verificacion-dos-pasos-google-facebook-twitter-instagram-microsoft-whatsapp

115 https://support.apple.com/es-es/HT204915

116 https://support.google.com/chrome/answer/114836?visit_id=636820070803313029-2856618290&p=settings_privacy&rd=1

opciones que tenemos disponibles. En la sección **Configuración del contenido** encontramos una información importante sobre la forma de tratar el contenido de las páginas web (puede ampliarse en la página Cambiar los permisos de sitios web[117], tras pulsar en ***Permisos que se pueden modificar***).

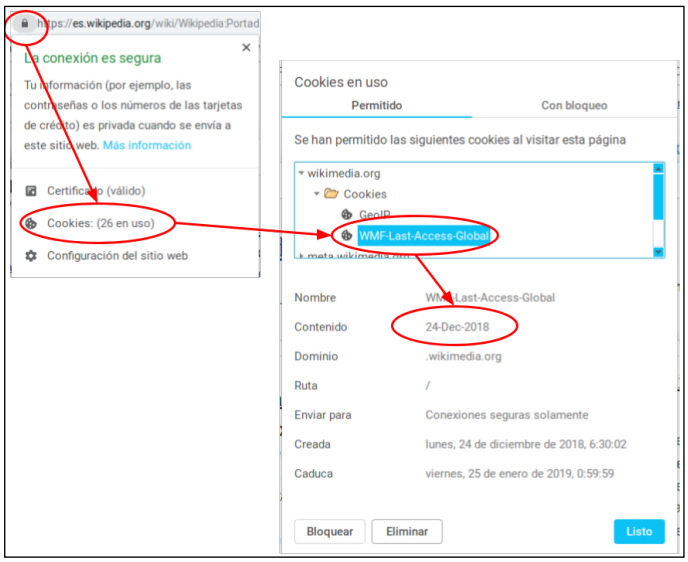
A continuación se van a exponer algunos conceptos configurables relacionados con la seguridad que debemos conocer:

Cookies (galletas)

Son **pequeños archivos** que las páginas web guardan en nuestro ordenador y que, más tarde, pueden leer. Contienen información variada que puede servir para recordar si se ha visitado previamente una página y, por tanto, mostrar o no determinado contenido. No almacena información privada sensible, tampoco escanea el ordenador ni realizan cualquier actividad que nos ponga en peligro, ya que **las *cookies* no tienen capacidad de realizar ninguna acción por sí solas**. A través de la configuración, podemos desactivarlas, pero, en general, debemos mantenerlas activadas porque nuestra navegación será mucho más fluida.

En Chrome podemos ver las *cookies* que utiliza una determinada página tras pulsar sobre el icono del candado que hay delante de la dirección de la página. Después se debe hacer clic sobre la sección **Cookies**. En la siguiente imagen se puede ver el **contenido** de una de ellas. En concreto contiene una fecha de una visita inicial a la página de la Wikipedia.

Figura 36:
Cookies en Chrome



Nota 36. Elaboración propia.

Esto nos permite ver los datos básicos que almacenan las *cookies*. En ocasiones veremos el contenido formado por letras que parecen no tener sentido, dado que la información está encriptada y solo puede ser leída por la página que la puso. Además, en esta ventana también podremos bloquear o eliminar *cookies* individuales. Más adelante, en el apartado «**Rastro de navegación**», veremos cómo se pueden eliminar todas las *cookies* de nuestro navegador de forma simultánea.

Certificados digitales

Los certificados digitales aseguran que determinada información pertenece a una empresa, una institución o un organismo, es decir, entre otros aspectos, certifican que la página que estamos viendo pertenece realmente a la entidad que aparece en ella. Además, estos certificados permiten que el contenido de las páginas webs sean seguras para el usuario, pues cifran el contenido entre el ser-

117 https://support.google.com/chrome/answer/114662?visit_id=636820070803313029-2856618290&p=settings_manage_exceptions&rd=2

vidor y el usuario. En el caso de que el usuario escriba información (por ejemplo, su nombre, su contraseña, el número de la tarjeta bancaria, etc.), la información viajará cifrada hasta el servidor de forma que no podrá ser interceptada por otros.

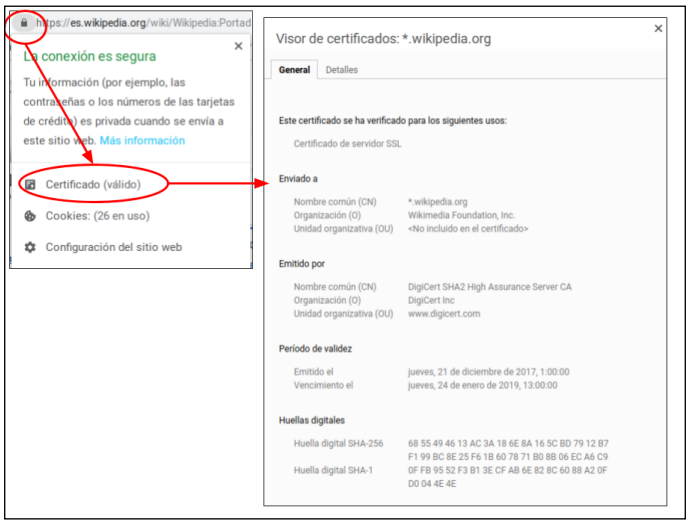
Cuando se navegue por la Red, hay que tener en cuenta lo siguiente:

- Cuando una web dispone de certificado digital válido, aparecerá la imagen de un **candado** y las letras **https** junto a su dirección. En las webs de comercio electrónico deberemos exigir siempre este icono junto al https, lo cual indica que la comunicación es segura. No deberemos hacer ninguna transacción comercial en ausencia del certificado digital.
- Si una página no tiene certificado, aparecerá el texto **«No es seguro»** junto a la dirección. Estas páginas, en principio, no deberían suponer ningún peligro, pero la información no estará cifrada y puede ser vista por una persona que escrutase intencionadamente nuestras conexiones (por ejemplo, en una wifi pública o del trabajo). En este tipo de páginas es mejor no enviar información sensible, ya que, al menos en teoría, puede ser interceptada por no ir cifrada.
- Si el certificado tiene algún problema (está caducado, no coincide con la dirección en la que estamos actualmente, etc.) aparecerá el texto **«No es seguro»** en color rojo, además de un mensaje de error en la página. Esto no quiere decir que la página que visitemos nos vaya a dañar necesariamente, aunque sí deberemos extremar las precauciones porque nos está indicando que el certificado no es válido, por lo que no deberíamos enviar información de ningún tipo a esta página.

Por lo tanto, cuando una página tiene un certificado digital válido (aparece un candado junto a la dirección), podemos tener cierta tranquilidad sobre ella. **Si no tiene el certificado válido, deberemos extremar las precauciones**, especialmente no se deben descargar archivos ni enviar información sensible.

Finalmente, podemos ver el certificado digital de una página tras pulsar sobre el candado y, después, tenemos que hacer clic en **Certificado**. En el diálogo que se abre a continuación se mostrarán los datos referentes al certificado digital, tales como la fecha en la que entró en vigor y en la que caduca, a quién y por quién fue emitido, etc. En esta imagen se puede ver el proceso:

Figura 37:
Certificado digital



Nota 37. Elaboración propia.

Certificado personal

Los certificados no son solo para autenticar páginas, nosotros también podemos disponer y utilizar certificados a nivel personal, normalmente para identificarnos en Internet frente a la administración pública, con una validez legal igual a la del DNI o a nuestra presencia física. Este certificado se obtiene como archivo descargable tras seguir las instrucciones que encontraremos en la web de la Casa de

la Moneda[118] y se instala en el navegador. El proyecto CERES[119] (Certificación Española) liderado por la FNMT-RCM consiste en establecer una Entidad Pública de Certificación que permita autentificar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y administraciones públicas a través de las redes abiertas de comunicación. En el caso de estar interesados en obtener un certificado digital, encontraremos todas las instrucciones y pasos a seguir en los enlaces que se han citado con anterioridad.

Estrategias en la escuela

– Es necesario enseñar a los niños cómo identificar las páginas seguras mediante las que se puede enviar información y aquellas en las que nunca debería hacerse.

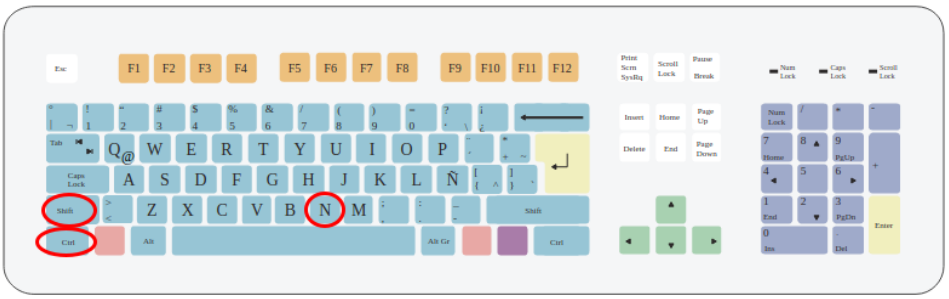
Rastro de navegación y modo incógnito

Cuando utilizamos un navegador, este va guardando información sobre nuestra actividad: el **historial de páginas** que visitamos, ***cookies*** (archivos con información de los lugares que visitamos que pueden ser leídos por las webs a las que accedemos), **archivos descargados**, **copias de las páginas** de Internet, etc. Todo esto va dejando un rastro de toda la actividad que desarrollamos.

Una forma de mantener esta actividad a salvo es la utilización de un **usuario en el navegador** (a veces llamado *perfil*), así como una **sesión** exclusiva para nosotros en el ordenador. De este modo, nuestros datos estarán guardados en el dispositivo, pero a salvo de miradas indiscretas. Después hablaremos con más detalle de estas dos opciones.

En el caso de que no tengamos ni sesión en el ordenador ni usuario en el navegador (por ejemplo, en el ordenador de clase), es aconsejable utilizar una **ventana de incógnito**. Este modo de navegación se puede activar con la combinación de teclas **CONTROL+Mayús+N** (esto es aplicable en la mayoría de los navegadores) o a través del menú de los tres puntos y seleccionando la opción **Nueva ventana de incógnito** en Chrome. De este modo, no dejará rastro de lo que hayamos hecho. **Tampoco guarda contraseñas, datos de formularios, páginas visitadas, etc**. Lo único que permanece en el ordenador o dispositivo móvil, tras cerrar la ventana de incógnito, son los archivos que hayamos podido descargar.

Figura 38:
Activación de una ventana de incógnito a través del teclado

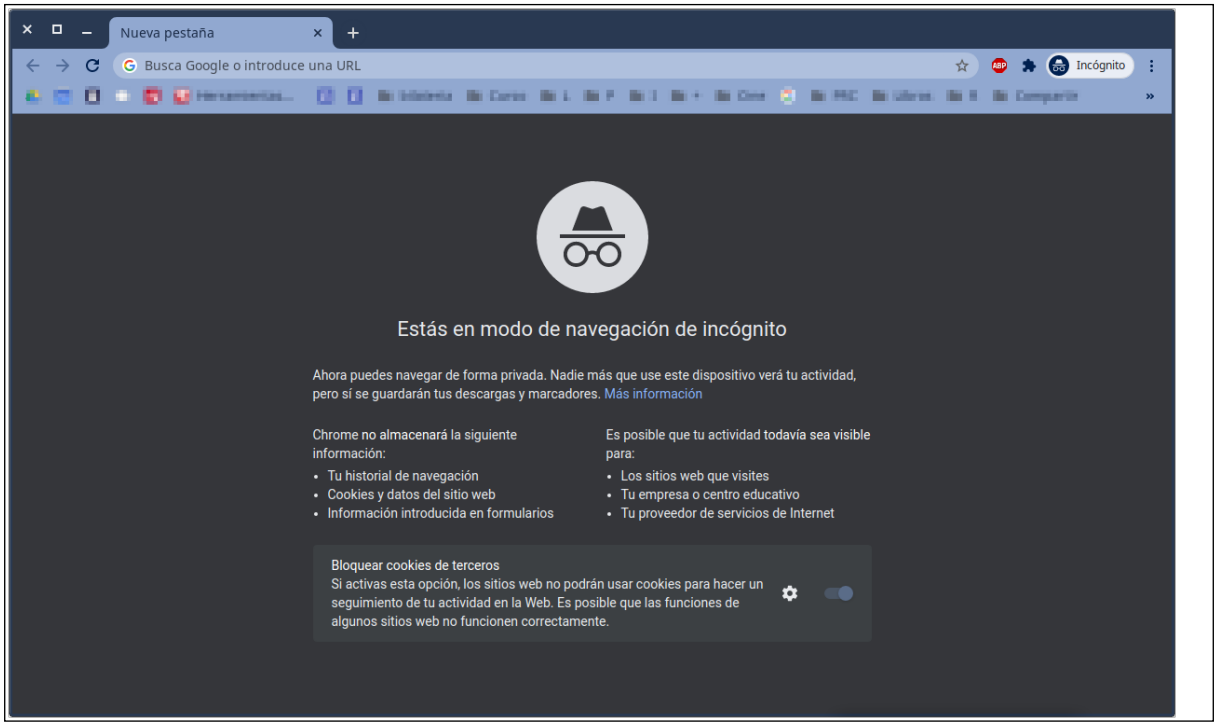


Nota 38. Activación de una ventana de incógnito a través de un teclado de 105 teclas para español. *Modificado de Qwerty* hispanoamérica.svg, *[Imagen]* por Iván Quiñones, 20 de septiembre de 2011, en Wikipedia https://es.m.wikipedia.org/wiki/Archivo:Qwerty_hispanoam%C3%A9rica.svg

118 https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software

119 http://www.cert.fnmt.es/es/

Figura 39:
Ventana de incógnito en Chrome

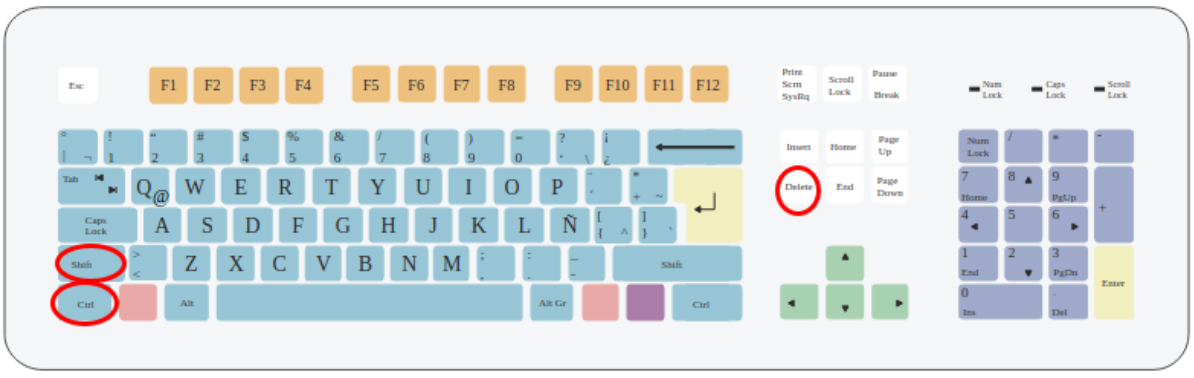


Nota 39. *Elaboración propia*

Con el modo incógnito, como se ha dicho, no se deja rastro de la actividad que hayamos podido desarrollar en la Red. Sin embargo, esta no es la forma más productiva de trabajar, ya que muchas webs utilizan *cookies* para guardar nuestras preferencias de trabajo y la configuración de las páginas y los programas *online* que utilizamos. Al no guardarse en este, determinadas páginas no funcionarán de manera óptima o se nos preguntará una vez tras otra lo mismo.

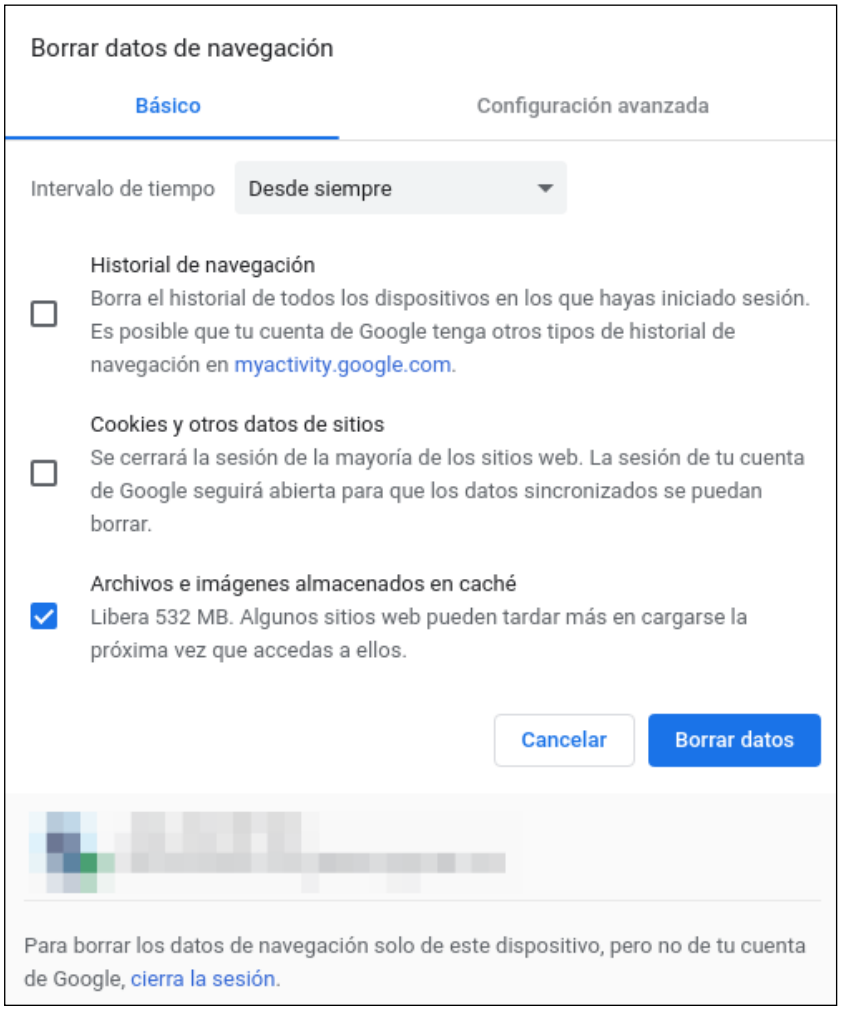
En el caso de que no hayamos utilizado una ventana de incógnito y deseemos **eliminar el historial de navegación, así como otra información almacenada durante este proceso,** podemos borrar los datos de navegación tras pulsar **CONTROL+Mayús+SUPR** (aplicable a la mayoría de los navegadores) o, en Chrome, en el menú de los tres puntos, después hay que pulsar en **Más herramientas**, y, finalmente, en **Borrar los datos de navegación**.

Figura 40:
CONTROL+Mayús+SUPR



Nota 40. *CONTROL+Mayús+SUPR en Teclado de 105 teclas para español distribución Hispanoamérica. Modificado de Qwerty* hispanoamérica.svg, *[Imagen] por* Iván Quiñones, *20 de septiembre de 2011, en Wikipedia* https://es.m.wikipedia.org/wiki/Archivo:Qwerty_hispanoam%C3%A9rica.svg

Figura 41:
Eliminar los datos de navegación



Nota 41. Elaboración propia

A través de esta ventana podremos eliminar las direcciones que hemos visitado, las *cookies* y los datos de acceso a los sitios, así como las imágenes y copias de las páginas realizadas por el programa para acelerar la navegación.

Es muy importante destacar que tanto la navegación de incógnito como el borrado de datos solo afectan de forma local, es decir, que tienen lugar en el dispositivo que está utilizando el usuario o en su cuenta de Google, pero no impide, por ejemplo, que se recopile nuestra **dirección IP** (una dirección numérica única en Internet que identifica nuestra conexión) por parte de las páginas web que visitamos o que nuestro **proveedor de Internet** vea o almacene las direcciones de las páginas que hemos visto.

Estrategias en la familia

– Cada miembro de la familia debe tener su propia cuenta de usuario en los ordenadores, ya sean de uso exclusivo de un miembro o de varios. Aprender a mantener la privacidad implica no mezclar las cuentas de diferentes personas.

Inicio de sesión en el dispositivo

Hay muchas situaciones que, sin darnos cuenta, pueden hacer que la información que pensamos privada pueda extenderse. En ocasiones protegemos nuestras cuentas con contraseñas complejas o utilizamos el inicio de sesión en dos pasos, pero tenemos una tableta en la que se puede acceder a toda nuestra información prácticamente sin esfuerzo. También podemos compartir el ordenador con la familia y mezclar las fotos de las últimas vacaciones con informes privados o notas de nuestros alumnos.

Estamos acostumbrados, o deberíamos estarlo, a tener una cuenta particular en nuestro centro para acceder a los ordenadores y deberíamos extender esta precaución al resto de dispositivos que tengamos tanto en el trabajo como en casa. **Las últimas versiones de Android permiten la creación de usuarios no solo en teléfonos inteligentes, sino también en tabletas**, aunque, dependiendo de la marca que comercialice el dispositivo, nos podemos encontrar que no es posible, al menos en los teléfonos, ya que en las tabletas hay más compañías que permiten la gestión de usuarios. En el artículo «Cómo tener varias cuentas de usuario en un teléfono Android»[120] de la web Androidsis explican cómo crear varios usuarios en el teléfono, siendo el mismo proceso para la tableta.

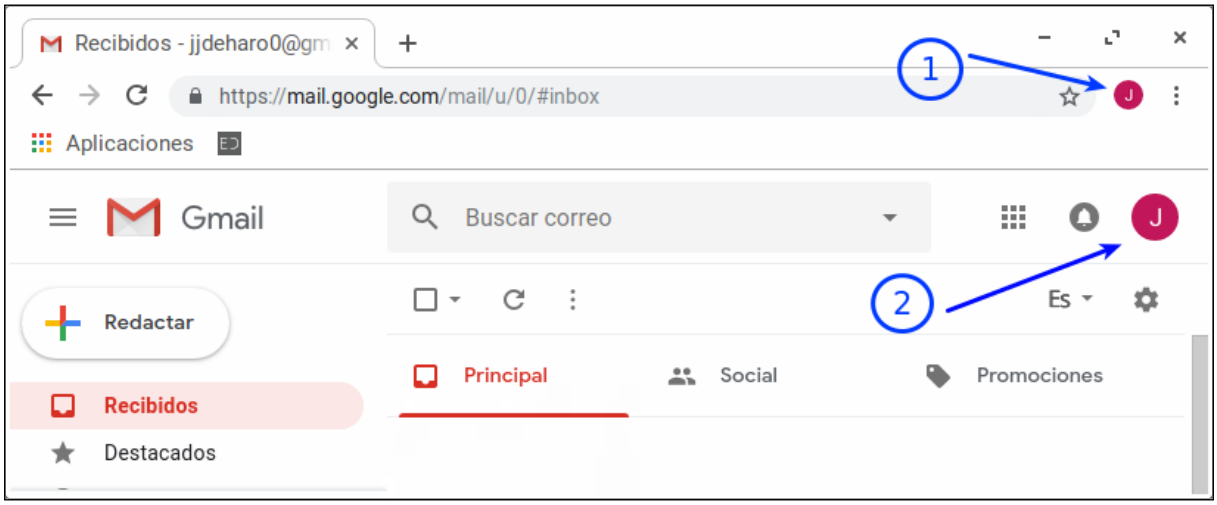
Así pues, **debemos utilizar perfiles o sesiones de usuario individuales,** siempre que el dispositivo lo admita, tanto en casa como en el trabajo. Debemos **evitar los dispositivos compartidos y utilizar la misma sesión** entre varios tanto si es un ordenador como una tableta. La profesionalidad ligada a la necesidad de mantener en secreto cualquier dato sensible de nuestros alumnos, así como el sentido común de la privacidad personal, lo aconsejan.

Sesión de Google en el navegador

Un aspecto importante, y que desconocen muchos usuarios, es que se puede **iniciar sesión en el navegador** con los datos de nuestra cuenta en Google, de forma que podemos tener varias ventanas del navegador con cuentas diferentes, la de nuestra institución y la personal, por ejemplo.

No debemos confundir iniciar sesión a través del navegador con añadir una cuenta a Gmail. En el segundo caso, se nos permite abrir varias cuentas distintas del correo —o de otros servicios de Google— de forma que en diferentes pestañas de la misma ventana podemos tener cuentas distintas. Sin embargo, esta forma de trabajar no debería utilizarse habitualmente, ya que da lugar a la confusión de cuentas y es frecuente pensar que se está usando una cuenta cuando en realidad se está en otra distinta. Esto se produce porque, cuando abrimos una página que usa los servicios de Google, no podemos estar seguros de cuál es la cuenta que se utiliza y es frecuente que la sesión cambie de una a otra según el servicio que utilicemos.

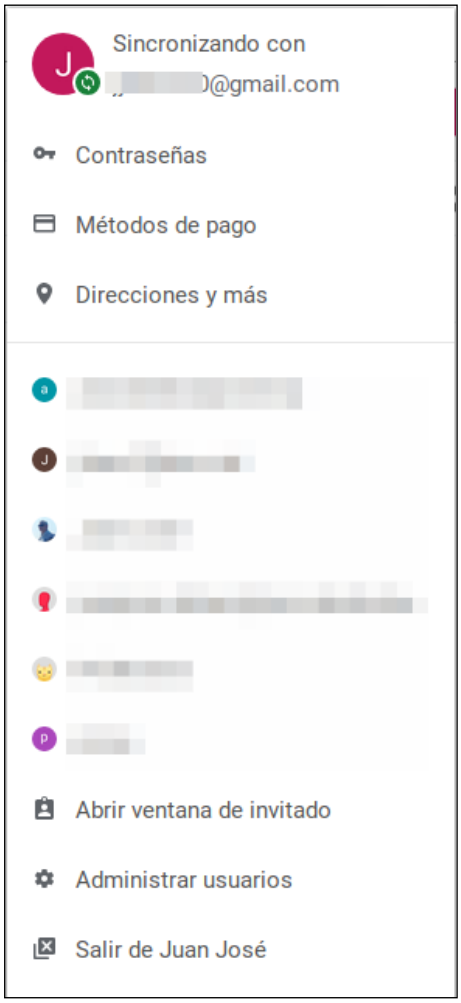
Figura 42.
Inicio de sesión en Chrome



Nota 42. (1) Iniciar sesión en el navegador. (2) Iniciar sesión en otra cuenta de correo de Google. Elaboración propia

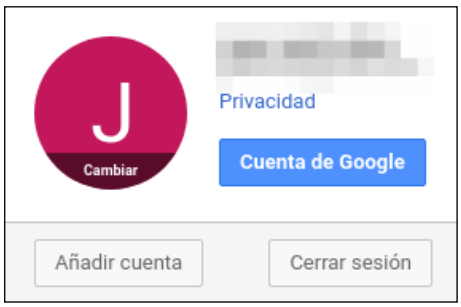
120 https://www.androidsis.com/multiusuario-android/

Figura 43:
Menú de usuario en Chrome



Nota 43. Menú al pulsar sobre el icono 1.- Opciones para controlar las sesiones en el navegador. En el caso de estar usando más de una cuenta en el navegador de Google, esta también aparecerá para poder cambiar a ella fácilmente. Elaboración propia.

Figura 44:
Añadir cuenta en Chrome



Nota 44. Menú al pulsar el icono 2: Opciones para añadir otra sesión de correo en la misma ventana. Elaboración propia.

A través del menú de la izquierda (1), podemos iniciar sesión en una cuenta de Google. Esta cuenta se usará en todas las aplicaciones que utilicemos y las páginas que visitemos a través del navegador. Además, se sincronizarán las contraseñas, los nombres de usuario que tengamos almacenados en los diferentes servicios web, los botones de acceso directo a las páginas que tengamos en el navegador, las extensiones y los complementos de Chrome, así como otros datos que tengamos guardados en el navegador. Esta característica nos permite trabajar en ordenadores (o en dispositivos móviles) distintos, como si estuviésemos en nuestro ordenador principal, con todos nuestros datos y preferencias del navegador.

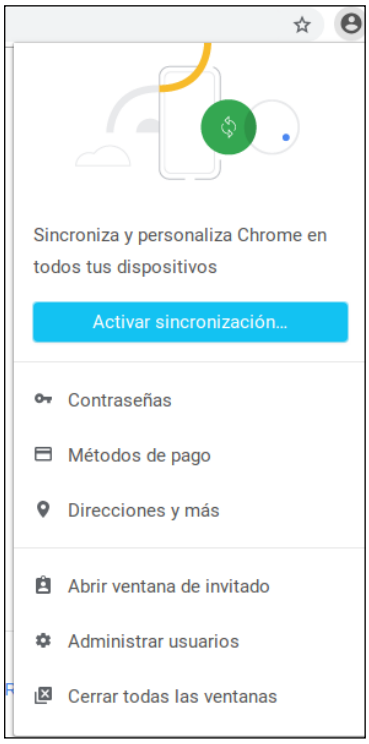
Con el menú (2), podremos utilizar un correo o los documentos de Google de otra cuenta, pero es solo una solución temporal pensada para acceder momentáneamente a esa otra cuenta. No tendremos a nuestra disposición los complementos o extensiones de Chrome instalados con esta segunda cuenta, así como ninguna otra información vinculada a ella.

Iniciar sesión en el navegador Chrome

Al pulsar el icono que está al lado de los tres puntos, obtendremos un menú para iniciar sesión en Chrome o, si ya lo hemos hecho con anterioridad, el menú mostrado antes, con todas las cuentas disponibles con la posibilidad de añadir nuevas.

Si todavía no hemos iniciado sesión, obtendremos algo parecido a lo siguiente:

Figura 45:
Iniciar sesión



Nota 45. Elaboración propia

Pulsando el botón azul **Activar sincronización**, podremos introducir un nombre de usuario y una cuenta de Google que será sincronizada.

Figura 46:
Sincronización de una nueva cuenta

Nota 46. Elaboración propia

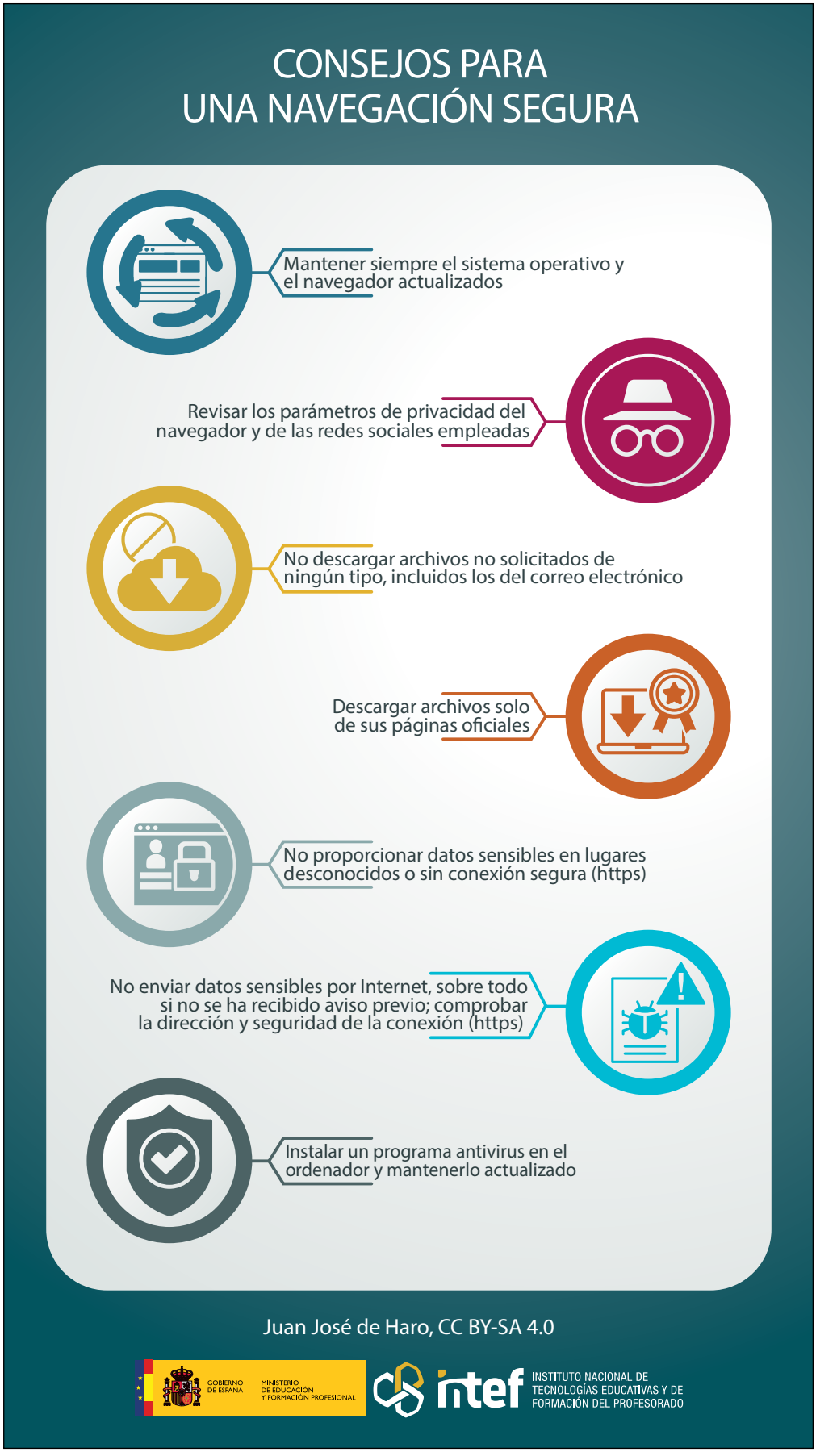
Siguiendo los pasos indicados en el gráfico superior, podremos tener todas las cuentas que deseemos y trabajar con ellas de forma totalmente independiente sin que se mezclen, pues cada una se abre en una ventana diferente.

Consejos para la navegación segura

Terminamos este apartado con una serie de consejos que debemos tener siempre en cuenta a la hora de navegar por Internet. Son los siguientes:

- Mantener siempre el sistema operativo y el navegador **actualizados**.
- Repasar los **parámetros de privacidad** del navegador, así como los de las redes sociales que utilicemos.
- No aceptar la **descarga de archivos** no solicitados; tampoco la de los archivos adjuntos no solicitados por correo.
- **Descargar archivos solo de las páginas oficiales**, para lo que debemos fijarnos que la dirección de descarga coincida con la de aquello que queramos descargar.
- No proporcionar **datos sensibles** (como nuestra dirección o el número de la tarjeta bancaria) en lugares que no conozcamos, mucho menos si no tienen una conexión segura (marcada con las letras https).
- Tampoco deben darse datos sensibles en los enlaces de correos electrónicos recibidos, a no ser que, previamente, nos hayan avisado por algún medio que nos los pedirán. Ninguna organización seria pide contraseñas o datos directamente por correo sin aviso previo. En caso de que debamos hacerlo, se debe comprobar siempre que la dirección donde introducimos los datos corresponden con la de aquellos que nos la piden y utilizan una conexión segura (con https).
- Tener un programa **antivirus** instalado y actualizado, especialmente en equipos con Windows, ya que son los más vulnerables.

Figura 47:
Consejos para una navegación segura.



Nota 47.
Elaboración propia

Formación para alumnos

El ataque hacker

Tipo de actividad: **Juego**
- Duración: **1 hora**
- Niveles implicados: **Todos**
- Objetivos:

  - **Aprender la importancia de una buena contraseña**
  - **Aprender a crear una buena contraseña**

- En fichas de papel se apuntan motivos que normalmente se usan en las contraseñas:

  - Año de nacimiento
  - Fecha de nacimiento
  - Segundo apellido de la madre
  - Nombre de la mascota
  - Ciudad de nacimiento
  - Número del DNI
  - Otros que se crean convenientes

- A varios alumnos se les dan estas fichas en las que apuntarán la contraseña que corresponda con su caso particular. Es decir, si a Luisa le ha tocado el segundo apellido de su madre y este resulta ser Gómez, su contraseña será Gómez.
- Un alumno con su contraseña responderá las preguntas del resto que no tiene contraseña. Le hacen solo una pregunta por alumno en cada turno.
- Hay dos tipos de preguntas. Las que se responden con sí o no (por ejemplo, «¿es el nombre de un familiar tuyo?») y las que directamente le preguntan: «¿Cuál es el segundo apellido de tu madre?». Si ha acertado el alumno que ha hecho la pregunta gana; si no, queda eliminado de la ronda de preguntas.

  Lo que se ha explicado se puede hacer con unas pocas contraseñas, ya que adivinarlas puede requerir algún tiempo. Esta es la técnica de la ingeniería social que consiste en averiguar todos los datos personales posibles de una persona para averiguar su contraseña. Posteriormente, se indicará cómo hacer una contraseña segura y que no sea apta para este tipo de investigación sobre las personas.

Riesgos de Internet

A medida que se hace un uso cada vez más extensivo de Internet, empiezan a aparecer problemas que antes no existían y otros, que ya son antiguos, se potencian gracias a la velocidad y omnipresencia de las redes.

La Red se ha convertido en el medio ideal para el acosador, el embaucador y, en general, para la expresión de seres egoístas y antisociales, es decir, de la maldad que encierran determinadas personas. Hay tres características que lo hacen especialmente idóneo para esto:

1. La relativa facilidad para falsificar la autenticidad de las personas. Podemos crearnos una vida imaginaria y contarla y documentarla con relatos e imágenes falsas como si fuera real.
2. La posibilidad de contactar al momento con cualquiera, independientemente del lugar donde se encuentre.
3. La universalización de los dispositivos móviles conectados a Internet, no solo entre los adultos, sino también, y muy especialmente, entre los menores de edad.

Esto, unido a que la ciberdelincuencia puede ser ejercida sin salir de casa, hace que personas que en la vida real serían incapaces de delinquir o de realizar determinadas acciones contra otros, sean capaces de hacerlo a través de Internet. En la web AseguraTIC[121] encontraremos abundante información que nos ayudará a conocer y prevenir los riesgos de Internet para los menores.

Estos riesgos, de los que hablaremos a continuación, se pueden esquematizar del siguiente modo:

- *Ciberbullying* (o ciberacoso). Es un término general para cualquier acoso realizado a través de los medios digitales (redes sociales, programas de mensajería, correos electrónicos, etc.), tales como los siguientes:
    - *Grooming* (o engaño pederasta). Un adulto acosa a un menor con intenciones de tipo sexual.
    - *Ciberbullying* entre iguales. Es el que se realiza entre los mismos menores.
- *Sexting*. Es el envío voluntario de material erótico, sexual o pornográfico a través de los teléfonos móviles.
- Sextorsión. Es el chantaje derivado de la posesión por parte de un extraño de material de carácter sexual sobre un menor.

El Canal Joven[122] de la Agencia Española de Protección de Datos (AEPD) cuenta con un servicio de ayuda dirigido tanto a menores como a familias y a docentes donde se podrán plantear cuestiones relacionadas con protección de datos personales en el ámbito de los menores. Estas consultas podrán realizarse o por correo electrónico (canaljoven@aepd.es), por teléfono (901 23 31 44) o WhatsApp (616 172 204).

Grooming

El ***grooming***, también conocido como **engaño pederasta**, es, en pocas palabras, el acoso sexual al que pueden verse sometidos los menores por parte de un adulto.

Dado que el objetivo es siempre sexual, el adulto tiene una serie de estrategias cuya finalidad es la de **irse ganando la confianza** del niño poco a poco. Para ello simula tener su misma edad o, al menos, ser mucho más joven de lo que en realidad es. Las conversaciones, en un principio, son inocentes y las propias de un niño o adolescente, pero con el tiempo y el aumento de la confianza, se empiezan a producir el **intercambio de fotos** (falsas por parte del adulto) que terminan siendo de carácter sexual. En el momento en que el acosador tiene algún material de este tipo, se destapa y comienza a **chantajear** al menor, de forma que, si no hace lo que él quiere, amenaza con enviar las fotos y las conversaciones a sus amigos más cercanos o familiares. Lo que puede empezar en Instagram o en alguna otra red por Internet, puede acabar por WhatsApp o Telegram, donde la sensación de cercanía y acoso es mayor que en otras redes sociales.

El acosador utilizará este control para obtener imágenes explícitamente sexuales del menor, grabaciones de vídeo del mismo tipo y, en algunos casos, incluso encuentros reales donde puede abusar del menor.

En el artículo «Grooming, acoso a menores en la Red»,[123] se citan algunos factores que actúan a modo de catalizador:

121 https://intef.es/aseguratic/

122 https://www.tudecideseninternet.es/aepd/jovenes/si-tienes-problemas.html

123 https://www.pantallasamigas.net/grooming-acoso-a-menores-en-la-red/

- La cámara web o la del móvil permiten la grabación y recepción al momento de las imágenes.
- El pedófilo anterior a la era Internet se veía solo y aislado, con lo que su actividad estaba reprimida. Actualmente, los pedófilos pueden ver la experiencia de otros, contar con foros y no sentirse unos *bichos raros*, así pues, ya no hay razón para sentirse mal con uno mismo y lo único que evitan es ser pillados.
- La exposición continuada a la pornografía podría inducir a la permisividad con la pornografía infantil e incluso fomentar su consumo.

Cómo detectarlo

En el artículo «Características comunes de las víctimas de grooming»,[124] la psicóloga Maribí Pereira cita los cambios de conducta más habituales entre aquellos que sufren *grooming*:

- **Retraimiento social**. Se observan cambios en la manera de relacionarse, es decir, o hay una falta de defensa o una exagerada reacción ante supuestas bromas o acciones públicas.
- **Reserva excesiva** para comunicarse con otros.
- **Modificación en su lenguaje corporal** ante adultos, observándose en ocasiones la cabeza baja, la falta de contacto ocular, rechazo a estar con adultos.
- **Alteraciones en el rendimiento escolar**.
- **Cambios de humor**: tristeza, apatía y desmotivación general.
- **Explosiones de ira**.
- Procuran **ocultarse o apartarse** cuando emplean el móvil.
- Pueden presentar **miedo a salir de casa**.
- **Síntomas psicosomáticos** como dolores de cabeza, náuseas, mareos, ataques de ansiedad, lesiones físicas sin justificar o diarreas frecuentes.

Cómo prevenirlo

Los pederastas conocen a sus víctimas a través de Internet, especialmente a través de las redes sociales, por lo tanto, hay unas normas básicas que pueden seguirse siempre en el caso de los menores de edad:

- **No usar perfiles públicos en las redes**. De otro modo cualquiera puede conocer la vida e incluso llegar a deducir el lugar en el que vive el menor, aun cuando no lo haya publicado nunca explícitamente. Es muy fácil localizar el barrio o los lugares en los que se desenvuelve una persona cuando está bien documentado fotográficamente. **Los perfiles deben estar limitados a los conocidos** de forma personal.
- **No admitir desconocidos como amigos** o seguidores, ya que, dada la facilidad para falsear el perfil de una persona, llega un momento en que se tiene un conjunto de seguidores total y absolutamente desconocido, aunque se hable habitualmente con ellos.
- **No responder mensajes de desconocidos**. Lo mejor es no hablarles y, mucho menos, acceder a cualquier petición de fotos, webcam o chat.
- En los **perfiles, poner fotos de personajes ficticios** para evitar que aquellos que localizan a los menores, mediante la utilización del buscador de perfiles de las redes sociales, puedan saber quién y cómo es.

Aquellos niños que son víctimas del acoso de un adulto suelen tener una gran vergüenza ante sus padres y, por lo tanto, tienden a retraerse sobre sí mismos, por lo que el diálogo con ellos y la atención a lo que hacen es fundamental. En concreto, los padres pueden:

- **Explicar las normas básicas de seguridad** que deben mantener en Internet.
- **Mantener un diálogo fluido** sobre lo que sus hijos hacen en Internet, para que, en el caso de que aparezca un elemento disruptor, puedan localizarlo fácilmente. Si nunca hablan con sus hijos, difícilmente se darán cuenta a tiempo.

124 https://www.isep.es/actualidad/caracteristicas-comunes-de-las-victimas-de-grooming/

- **Observar los hábitos de uso de Internet**. Si el menor se conecta de forma regular, a la misma hora, cuando todos duermen o está solo, es posible que esté en contacto con alguien que no quiere que se enteren sus padres.

Qué hacer

La web Derecho de la Red[125] da una guía para el caso de estar sufriendo *grooming*:

Primeras medidas

- No borres ningún contenido del teléfono o el ordenador.
- Puede parecer doloroso, pero las conversaciones, imágenes y los vídeos que el acosador y la víctima se hayan enviado deben ser guardados para usarlos como prueba. Como añadido, puedes realizar una impresión de estas para evitar su pérdida.
- No denuncies el perfil al servicio web desde el que se produce el acoso, únicamente bloquéalo, así evitas que los administradores del sitio tomen medidas contra el usuario, que se pondría en alerta pudiendo desaparecer y borrar la información. Además, de esta forma, el acosador se podría hacer otro perfil para seguir acosando a otros niños.

Denúncialo

- Una vez detectado, hay que denunciar de forma inmediata un caso de *grooming*.
- La denuncia deben cursarla los tutores del menor, que pueden acudir a tres instancias: cuerpos policiales (policía, guardia civil, policías autonómicas), juzgado de guardia y fiscalía de menores.
- Sin embargo, hay casos en los que la vergüenza que pueda sentir el menor agredido lleva a realizar denuncias anónimas a través de las webs de los cuerpos de seguridad. Existe una tercera vía que es acudir a ONG especializadas en ciberacoso, pero las autoridades recuerdan que este método no tiene repercusiones legales sobre el agresor.

Apóyale

- No le recrimines. Puede que tu primera reacción sea recriminar a tu hijo al haberse puesto en contacto con desconocidos por Internet y haber compartido información íntima. Pero recuerda, tu hijo es una víctima y el abusador, en cambio, es un especialista en conseguir lo que busca.
- No le culpes. El acosador, muchas veces recurre a la extorsión de mostrar los contenidos íntimos del menor si no cumple con los nuevos pedidos. Por ello, cuando te enteres, evita hacerle sentir vergüenza o culpa, ya que de esa forma únicamente aumentarás el poder que tiene el acosador sobre tu hijo.
- Habla con tu hijo porque se siente responsable, tiene miedo y siente mucha vergüenza de lo que le ha sucedido. Tienes que acompañarle, hablar con él y orientarle para conseguir que se sobreponga a esta situación tan angustiante.

Este vídeo, https://youtu.be/XjydCCCFAzE, nos puede servir para plantear el tema en clase e iniciar un diálogo donde los alumnos puedan expresar sus ideas y experiencias.

125 https://derechodelared.com/que-hacer-ante-un-caso-de-grooming/

Estrategias

Estrategias en la familia

- Los padres deben estar pendientes de los cambios de comportamiento de sus hijos para poder detectar si están pasando por problemas como el *grooming*, así como del resto de cambios conductuales indicados anteriormente. La detección temprana del *grooming* es importante para evitar que el niño caiga en una espiral autodestructiva en manos de sus acosadores.
- Como en todos estos casos lo más importante es mantener una relación fluida con los hijos que les permita denunciar ante sus padres cualquier tipo de acoso.

Estrategias en la escuela

- La educación en los diferentes riesgos que tiene Internet debe formar parte del plan de formación de los colegios e institutos, especialmente a partir de 6.º de primaria hasta 3.º de la ESO, ya que es en estas edades cuando son más susceptibles de caer en manos de desaprensivos. Solo por el hecho de saber que existe el *grooming*, ya puede hacer que más de un niño no caiga en sus redes.

Ciberbullying escolar

Algunas veces se utiliza el término *ciberbullying* como un término exclusivo para indicar acoso entre escolares y se reserva la palabra ciberacoso, es decir, su traducción al español, para el que se produce entre adultos. Dado que usar el mismo término para indicar dos procesos distintos, según el idioma que se utilice, es muy confuso, hemos utilizado los términos, ampliamente aceptados, *ciberbullying* y ciberacoso como sinónimos del acoso producido a través de medios electrónicos en general y, para indicar el acoso entre los menores de edad, hablamos de *ciberbullying* **(o ciberacoso escolar**, a veces también se llama *ciberacoso académico*).

El ciberacoso escolar es, probablemente, uno de los problemas a los que se enfrenta un mayor número de menores. La búsqueda de la pertenencia al grupo, en contraposición a los demás, hace que, en algunas ocasiones, se tome a los niños como un objetivo al que atacar por cualquier diferencia o suceso que sirva como excusa para el acoso. Igual que sucede con el *grooming*, es un problema viejo que ha adquirido una nueva dimensión debido a la irrupción de Internet en la vida de los niños.

La Guía legal sobre Ciberbullying y Grooming[126] del Instituto Nacional de Tecnologías de la Comunicación (INTECO) lo define como:

> «el uso y difusión de información lesiva o difamatoria en formato electrónico a través de los medios de comunicación como el correo electrónico, la mensajería instantánea, las redes sociales, la mensajería de texto a través de dispositivos móviles o la publicación de vídeos o fotografías en plataformas electrónicas de difusión de contenidos». (INTECO, s.f., p.3)

El vídeo que podemos encontrar en este enlace, https://youtu.be/SEC_dOWFN5M, de Pantallas Amigas[127] nos puede ayudar a visualizar y comprender el tema.

126 https://www.is4k.es/sites/default/files/contenidos/herramientas/guia_legal_ciberbullying_grooming.pdf

127 https://www.pantallasamigas.net/

Características del ciberacoso:

- **Acusaciones y publicaciones falsas**. Los acosadores intentan dañar la reputación del acosado difundiendo falsedades e intentando poner a otras personas en su contra, normalmente a través de las redes sociales o grupos de programas de mensajería como WhatsApp.
- **Se busca asustar y aterrorizar a la víctima**. Esto es habitual a través de mensajes privados difundidos por WhatsApp, correo electrónico, redes sociales, etc.
- **Recopilación de información sobre la víctima.** Los ciberacosadores pueden espiar a los amigos de la víctima, su familia y compañeros de trabajo para obtener información personal.
- **Manipulación del entorno de la víctima.** Pueden enviar regularmente correos difamatorios al entorno de la víctima para poder manipularlos.
- **Pérdida de la privacidad**. El acosador que traslada a Internet sus insultos y amenazas puede hacer pública la identidad del acosado, incluso facilitando en algunos casos su teléfono y otros datos personales para que terceras personas se unan al acoso.
- **No existe un propósito legítimo,** o sea, que el acoso no tiene un propósito válido, aunque algunos acosadores están persuadidos de que tienen una causa justa para acosarlo, normalmente creen que ha cometido un error y que debe pagar por él.
- **Repetición.** El ciberacoso se caracteriza por no ser un hecho aislado, sino que los ataques a la persona se producen de forma reiterativa.

Figura 48: Formas de ciberacoso

Nota 48. Elaboración propia

La Fundación ANAR[128] (Ayuda a Niños y Adolescentes en Riesgo) elabora cada año, desde 2016, un informe exhaustivo sobre los casos atendidos por ellos. Resumimos a continuación algunos datos importantes hechos públicos en 2018 a través del «III Estudio sobre el acoso escolar y *ciberbullying* según los afectados».[129]

Perfil del acosado

- La edad media a la que se inicia el ciberacoso es de 12.2 años, siendo los casos de menos de 10 años inferiores al 15 %. La edad media de los acosados es de unos 13 años.
- Casi dos tercios son niñas (65.6 %) y un tercio niños (34.4 %).
- El rendimiento escolar no parece especialmente relevante, aunque hay predominancia de rendimiento alto (30.6 %) y medio (41.6 %) frente al bajo (27.8 %).

Perfil del acosador

- Actúan como acosadores solo niños el 46.7 % de las veces, solo niñas el 23.3 % y de ambos sexos el 30 %.
- El 70 % son mayores de 12 años y su edad media es de unos 14 años.
- En el 94.4 % de los casos son de la misma clase que el acosado.
- En cuanto al número de acosadores es de uno, en el 25.9 % de los casos, de dos a cinco en el 55.5 % y más de cinco en el 18.6 %.
- En el 49 % de los casos, alguno de los acosadores había sido amigo de la víctima.

Figura 49:
Ciberacoso: perfil del acosado y del acosador

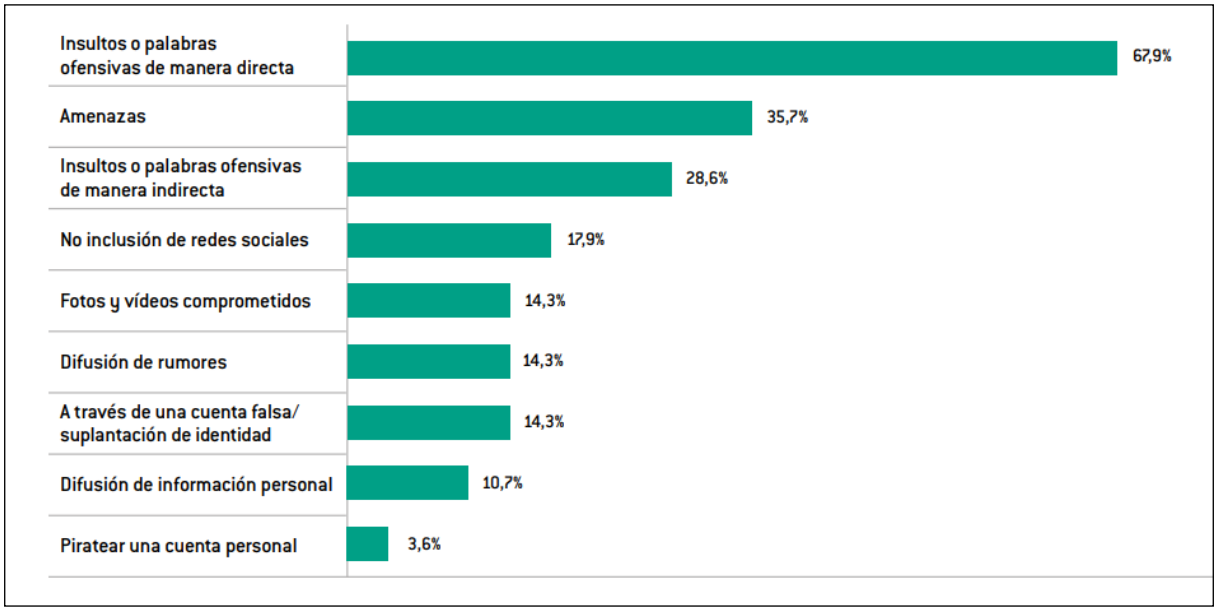
Nota 49. Elaboración propia

128 https://www.anar.org/

129 https://www.anar.org/wp-content/uploads/2018/09/III-Estudio-sobre-acoso-escolar-y-ciberbullying-según-los-afectados.pdf

Tipos de ciberacoso

Figura 50:
Ciberacoso, Tipos y cuantía



Nota 50. Obtenido del «*III Estudio sobre el acoso escolar y ciberbullying según los afectados*», (p. 85) por ANAR (2018) en https://www.anar.org/wp-content/uploads/2018/09/III-Estudio-sobre-acoso-escolar-y-ciberbullying-seg%C3%BAn-los-afectados.pdf

En cuando al medio utilizado, el teléfono móvil supone el 93 % de los dispositivos usados y la tableta u ordenador el resto. El medio preferido a través del móvil es por WhatsApp (76 % de las veces) seguido de otras redes sociales.

Todos estos datos nos permiten hacer una idea bastante exacta de cómo se produce el ciberacoso que empieza en los últimos cursos de primaria, pero es máximo en 2.º y 3.º de la ESO, teniendo lugar principalmente en chicas, aunque también chicos, a través del móvil y por compañeros de su clase. A diferencia del *grooming*, donde el acosador conoce al menor por el rastro que deja en Internet, con el *ciberbullying* no sucede lo mismo, ya que este se suele dar a partir de sus propios compañeros de clase, con los que, seguramente, tendrá contacto a través de redes sociales, algo que está totalmente dentro de la normalidad. Al no poder permanecer al margen de sus acosadores, da igual si la víctima se conecta o no, ya que la cercanía de los acosadores le hará sentir a través de los amigos sus efectos, es un problema más difícil de controlar por el menor, aunque, si se siguen los cauces apropiados, se conseguirá una pronta solución sin secuelas, al menos no de importancia.

Prevención del acoso

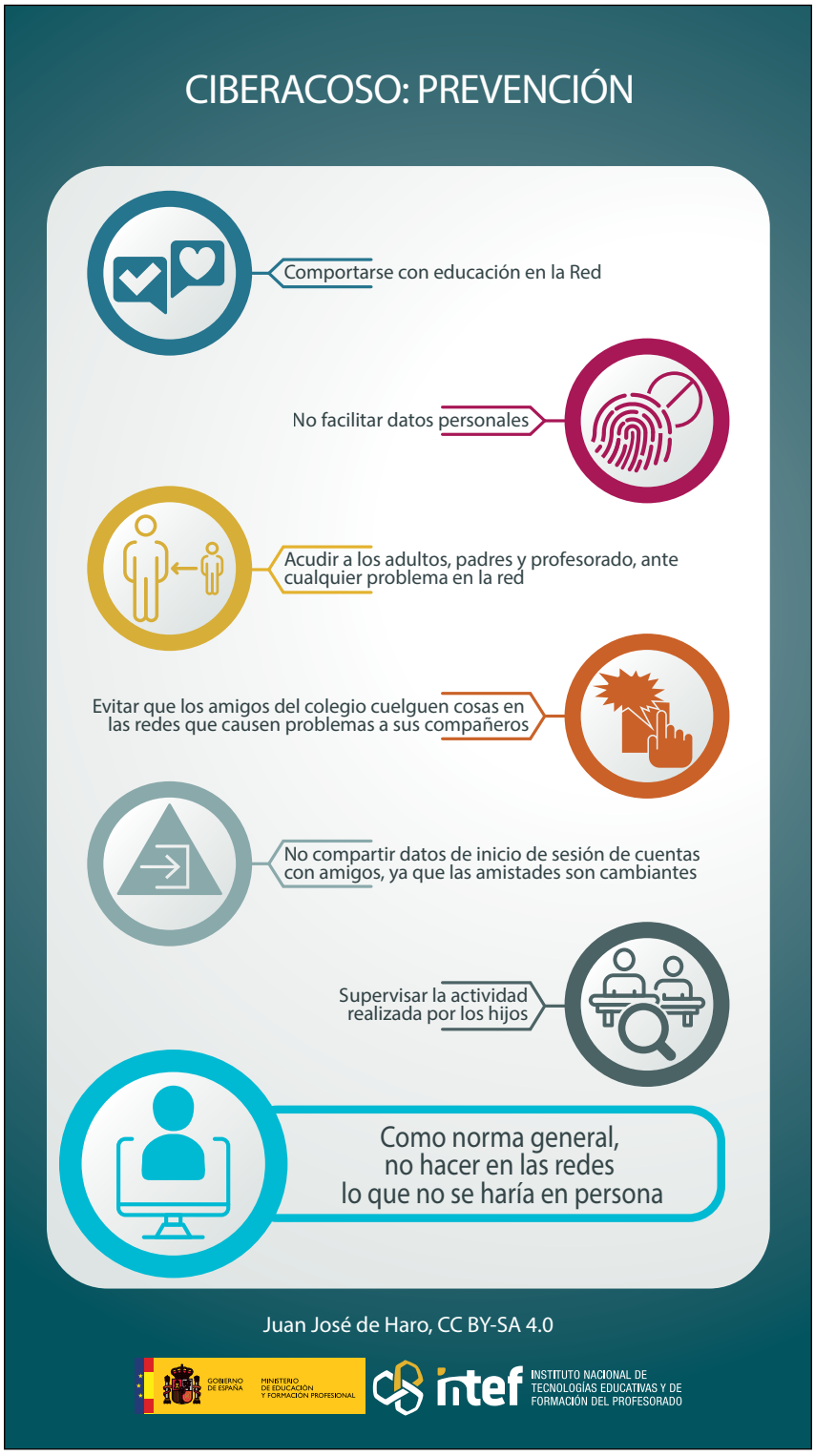
Como en el *grooming*, es muy importante el diálogo con los hijos y la información también desde la escuela. Es fundamental que conozcan y pongan en práctica las siguientes pautas de actuación:

- **Comportarse con educación** en la Red.
- **No facilitar datos personales**.
- Que ante cualquier problema puedan **acudir a los adultos**, ya sean padres o profesores, para exponerles lo que les está sucediendo a través de la Red.
- Aun cuando tengan sus perfiles restringidos a sus amigos de la vida real, normalmente los amigos del colegio **no deben publicar fotos o comentarios que sean susceptibles de causar problemas** por parte de otros no muy bien intencionados. Hay que ser prudentes y no publicar nada que no expondríamos en el tablón de anuncios de la clase.
- En ocasiones, se comparten nombres de usuario y contraseñas con amigos, es algo que NUNCA debe hacerse. **Los datos de inicio de sesión de las cuentas personales** deben ser

conocidas únicamente por sus dueños. Lo que ahora es amistad puede cambiar rápidamente con un malentendido y un enfado, y convertirse en una suplantación de personalidad que toma posesión de una cuenta de la víctima para hacerle daño.

- Como norma general, **no hacer en las redes lo que no se haría en persona**.
- Por parte de los padres, es aconsejable s**upervisar la actividad realizada por sus hijos** de forma que se sientan acompañados. Esta supervisión ayudará a detectar conductas de riesgo, así como a localizar posibles acosadores.

Figura 51:
Ciberacoso: prevención



Nota 51. Elaboración propia

Si se produce el ciberbullying

- No contestar a las provocaciones, ignorarlas.
- Advertir a los acosadores de que lo que hacen es un delito.
- Guardar **capturas de pantalla** de cualquier evidencia de acoso.
- Ante cualquier problema, el menor debe avisar a sus padres o profesores.
- El siguiente paso, una vez avisado el centro escolar y si no se ha conseguido solucionar, deberá ser la denuncia ante la policía.

Para saber más

- **CiberBullying**: https://www.ciberbullying.com/
- ***Guía legal sobre ciberbullying y grooming***: https://www.is4k.es/sites/default/files/contenidos/herramientas/guia_legal_ciberbullying_grooming.pdf
- **«Cómo detectar el acoso escolar en las aulas»**: https://www.psicomemorias.com/acoso-escolar-bullying/
- Canal Prioritario[130] de la Agencia Española de Protección de datos (AEPD). Canal para evitar el acceso de los menores a contenidos inapropiados y solicitar la retirada de los mismos de la Red.
- Línea de ayuda 017[131] del Instituto Nacional de Ciberseguridad (INCIBE). Servicio público, gratuito y confidencial, disponible todos los días del año de 9 a 21 horas, que proporciona asesoramiento técnico en ciberseguridad a empresas, ciudadanos, menores y su entorno. Además, de forma específica, presta asistencia psicosocial sobre mejores usos, conflictos o situaciones de riesgo que experimentan los menores en el uso de Internet y la tecnología.

Estrategias

Estrategias en la familia

- Estar atentos a los cambios de comportamiento de nuestros hijos con la finalidad de poder detectar problemas como el *ciberbullying*. Siempre que se produce acoso escolar se producen cambios de conducta, especialmente en relación con la escuela y los amigos.
- Mantener un diálogo constante con los hijos y estar enterados de sus preocupaciones. La confianza es el mejor preventivo para que los padres puedan estar al tanto.

Estrategias en la escuela

- Desde la escuela, debe haber una especial sensibilidad en relación con el acoso, ya que esta suele ser su lugar de origen. Observar el comportamiento en la hora del recreo y en los cambios de clase puede ayudar a detectar posibles casos. También existen programas informáticos, técnicas para realizar en clase y encuestas que permiten detectarlo (se aconseja ver el apartado «Para saber más»).
- Hay que supervisar aquello que hacen los alumnos cuando están trabajando con los ordenadores, no dejarlos a su aire. Véase por ejemplo el artículo «Google Docs, el último juguete para ejercer ciberbullying sin que lo parezca».

130 https://www.aepd.es/canalprioritario/

131 https://www.incibe.es/linea-de-ayuda-en-ciberseguridad

Sexting y sextorsión

Sexting y sextorsión son conceptos relacionados, pero no son exactamente lo mismo. El primero es el envío voluntario de material de carácter sexual (normalmente fotos y vídeos). Suele ser algo consentido y que no es delictivo, sin embargo, sí es extremadamente peligroso, ya que se pierde totalmente el control de unas imágenes que son íntimas. Aunque la persona a la que se envía sea de completa confianza, con el tiempo las relaciones cambian y es muy frecuente que esas fotos o vídeos puedan ser usadas en contra de las personas que se las hicieron. El segundo concepto, la sextorsión, deriva muchas veces del primero, ya que, cuando cae en manos de personas poco escrupulosas, las imágenes podrán ser usadas para el chantaje.

Patricia Alonso ha realizado su tesis doctoral[132] en 2017 sobre el *sexting* y ha realizado entrevistas a 1.286 estudiantes de la ESO y Bachillerato con una media de 15,6 años. Ha encontrado que los resultados muestran que los adolescentes tienen actitudes positivas, considerando el *sexting* una práctica divertida con la que establecer relaciones; siendo los chicos y los estudiantes de ámbito urbano los que más positivo ven las prácticas de *sexting*. Aproximadamente el 46 % de las chicas habían enviado algún *sexting* alguna vez y el 60 % de los chicos. Desgraciadamente es una conducta que parece estar bastante normalizada entre los adolescentes, a pesar de que ellos mismos lo reconocen como una actividad de riesgo.

Figura 52:
Sextorsión

Nota 52. Nota: Adaptado de ¿Qué es la sextorsión? de Pantallas amigas (s.f.). https://www.sextorsion.es

132 http://www.investigo.biblioteca.uvigo.es/xmlui/bitstream/handle/11093/786/Evaluación_del_fenómeno_del_sexting.pdf?sequence=1

Tipos de sextorsión según www.sextorsion.es:

- A menores de edad o a adultos.
- Por medio de imágenes obtenidas mediante *webcam*, *e-mail*, mensajería instantánea, teléfonos u otros dispositivos móviles, es decir, por todos los medios que sirven para realizar *sexting*.
- Por medio de imágenes obtenidas en el contexto de una relación sentimental.
- Con objeto de un abuso sexual, una explotación pornográfica para uso privado, para redes pedófilas o comercial, una extorsión económica o cualquier otro tipo de coacción.
- Puntual o continuada.
- Realizada por conocidos, examantes o personas desconocidas.

El vídeo https://youtu.be/sVqeJXhF6OA es una buena introducción para tratar este tema con padres y alumnos.

Consejos

Desde la web Sexting,[133] que pertenece a Pantalla Amigas, se recomiendan una serie de consejos[134] que, por su importancia, recomendamos leer detenidamente.

Razones para no realizar sexting

La web Pensar antes de sextear[135] proporciona diez razones —acompañadas de un vídeo cada una y un póster— para no realizar *sexting*. El póster-resumen recoge los diez motivos en un único archivo PDF y puede ser muy útil para plantear el tema ante padres y alumnos:

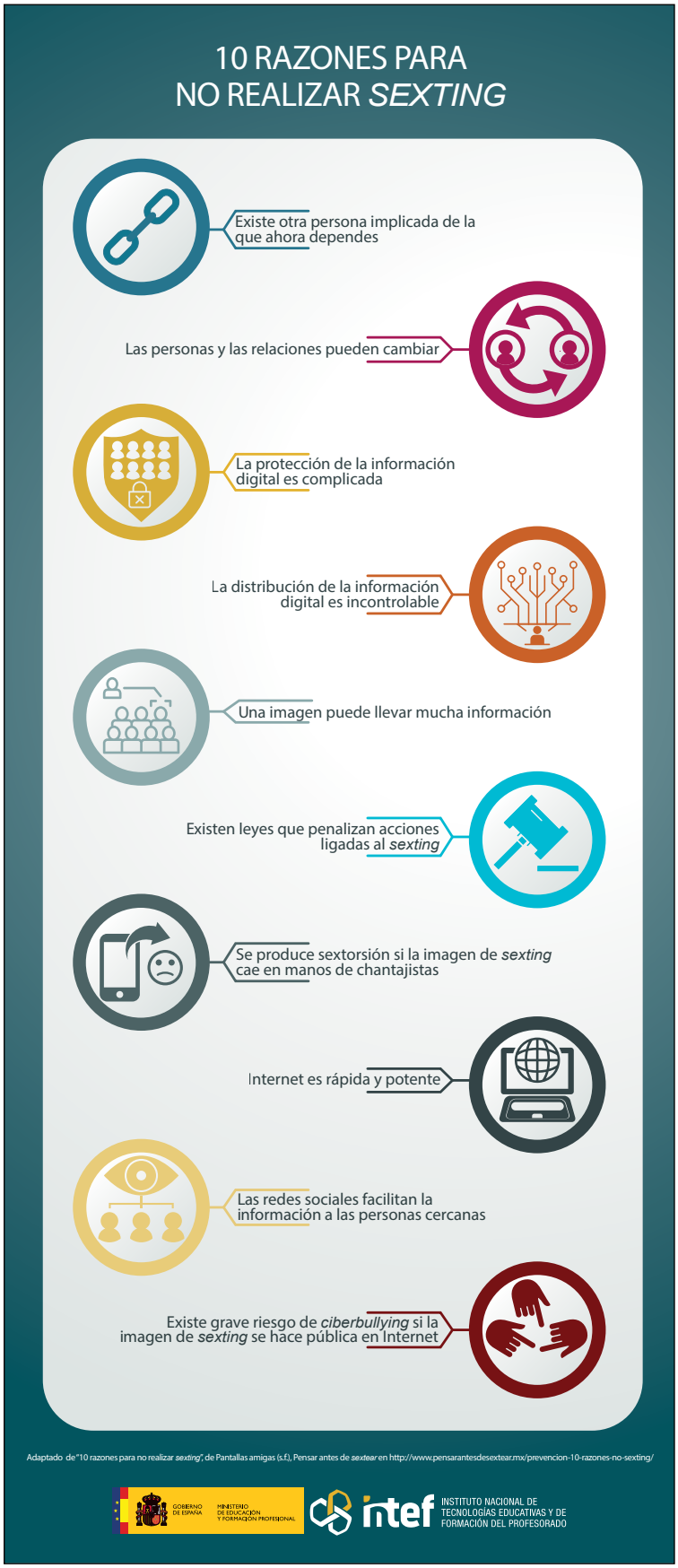
1. Al hacer *sexting* se pasa a depender de otra persona y no sabemos lo que hará.
2. Las relaciones cambian. Aunque ahora estemos seguros del otro, más adelante puede cambiar.
3. No es posible garantizar la seguridad que tendrán otros con las fotos. Hay personas descuidadas que, por ignorancia o descuido, pueden contribuir a difundir las fotos.
4. La información de la distribución digital no puede controlarse. Una vez sale de nuestro poder, desconocemos la difusión que podrá llegar a tener.
5. Aunque la cara de la persona que hace *sexting* no se vea en realidad hay muchas formas de saber quién es: *piercings*, tatuajes, marcas, lugar de la foto, etc.
6. Las leyes protegen a los menores. Si participamos en el reenvío de este tipo de imágenes, seremos responsables ante la ley.
7. Si la imagen cae en malas manos, se puede producir la sextorsión.
8. Aunque las imágenes se transfieran por medios privados, pueden acabar llegando a Internet, el medio de difusión más potente que ha existido jamás.
9. A través de las redes sociales, las personas más cercanas pueden ver aquello que no iba destinado a ellos.
10. Si la imagen llega a distribuirse por Internet, es muy posible que se desencadene el *ciberbullying*; hay gente que disfruta viendo a otros sufrir.

133 https://www.sexting.es/

134 https://www.sexting.es/consejos

135 http://www.pensarantesdesextear.mx/prevencion-10-razones-no-sexting/

Figura 53:
10 razones para no realizar sexting



Nota 53. Adaptado de «*10 razones para no realizar sexting*», de Pantallas amigas (s.f.), Pensar antes de sextear en http://www.pensarantesdesextear.mx/prevencion-10-razones-no-sexting/

Para saber más

– **Pensar antes de sextear**: http://www.pensarantesdesextear.mx/prevencion-10-razones-no-sexting/

Estrategias

Estrategias en la familia

– Llegada la edad de la preadoslescencia, cuando los hijos empiezan a comunicarse regularmente a través de las aplicaciones de móvil con sus amigos, deben tratar el tema del *sexting*, los motivos para no hacerlo y los peligros que conllevan.

Estrategias en la escuela

– El póster 10 razones para no sextear[123], junto con los vídeos cortos presentes en la página Pensar antes de sextear[124], pueden servir para tratar este tema, buscando el debate y la implicación de los alumnos.

Sextorsión

La sextorsión es la extorsión derivada de la amenaza de revelar fotos o vídeos de carácter sexual de la víctima. A diferencia del grooming, que se realiza por pederastas, en la sextorsión lo que se busca principalmente es el dinero. El sexting acaba en numerosas ocasiones como sextorsión y se acaba pidiendo dinero u otro tipo de favores para mantener los vídeos y fotos en secreto. Es algo que no solo afecta a los adolescentes, sino de lo que también son víctimas los adultos. Existen mafias organizadas dedicadas a crear perfiles falsos, sobre todo femeninos, donde intentan iniciar una relación de tipo sexual con la víctima para chantajearlo posteriormente. En estos casos, tanto para adultos como para menores, los pasos a seguir son:

– No acceder al chantaje.
– Cortar toda relación con esta persona.
– Guardar todas las pruebas que se tengan: conversaciones, mensajes de voz de vídeo, etc. Si se ha producido ya la difusión de imágenes en redes sociales, realizar capturas de pantalla.
– Informar a las autoridades y denunciar el caso ante la policía.

En el caso de los menores se puede producir un ocultamiento de lo que sucede debido a la lógica vergüenza y miedo que se está pasando. Se necesita mucha comprensión y, posiblemente, la ayuda de un especialista en psicología para afrontarlo. Debe evitarse el reñir y atormentar a los niños que lo estén padeciendo, con lo que les pasa ya tienen más que suficiente.

Para prevenir estas situaciones, además de la formación directa y de tratar estos temas, lo más importante es hablar, hablar y hablar. Hacer que el menor tenga la confianza suficiente para acudir a sus padres y profesores en caso de producirse algo así. Es muy importante que, desde el primer momento, los adultos puedan intervenir para parar la sextorsión y evitar que el niño se vea involucrado en un infierno, que puede durar meses antes de que se decida a decirlo.

136 https://www.pantallasamigas.net/wp-content/uploads/2016/07/P%C3%B3ster-Pensar-antes-de-Sextear-Resumen-10-Razones-No-Sexting-PantallasAmigas.jpg

137 https://www.pantallasamigas.net/pensar-antes-de-sextear-10-razones-para-no-realizar-sexting-campana-prevencion-y-concientizacion/

Juegos peligrosos

Desde hace unos años han surgido una serie de juegos o retos carentes de todo sentido y cuya aparente finalidad está exclusivamente en demostrar que uno es capaz de hacer algo fuera de lo habitual. Desgraciadamente, estos juegos son perjudiciales no solo para quien los practica, sino que también lo pueden ser para otras personas que se vean involucradas en ellos y que puedan acabar, como de hecho ha pasado en múltiples ocasiones, con la vida de alguien, ya sea por la peligrosidad implícita que tengan, como porque la prueba final es el suicidio. Muchas veces son retos virales que aparecen, causan sensación durante un corto tiempo y luego desaparecen.

El vídeo que se enlaza a continuación describe algunos de estos juegos como el de la ballena azul, el ahorcado, surfear en el tren o beber por los ojos, entre otros. **Contiene imágenes que pueden resultar molestas para determinadas personas especialmente sensibles:** https://youtu.be/8uPzMebPKxk

Veamos la descripción de algunos de ellos:

Ballena azul

Este juego nació en Rusia en 2016 y una de las últimas víctimas ha muerto en 2019, por lo que el juego parece que sigue activo. En él los participantes reciben un mensaje a través de las redes sociales indicando si quieren jugar a un juego. Los administradores ponen diversas «pruebas» consistentes en hacerse cortes, subirse a edificios con peligro para sus vidas, hacer daño a otros, ver imágenes psicológicamente perturbadoras a altas horas de la mañana, etc. Estas pruebas terminan con la instrucción final de suicidarse. Puede leerse uno de los casos en el artículo «Muere adolescente por el juego de la ballena azul»[138] podemos leer uno de los casos.

Momo Challenge

Este juego apareció en 2018 y es semejante al de la ballena azul, aunque ha circulado principalmente por WhatsApp. Se incita a la realización de retos como los explicados anteriormente y, si el menor se niega, sufre amenazas de diverso tipo. Momo está más relacionado con situaciones de terror psicológico que la ballena azul. En el artículo «Joven francés habría muerto por juego de internet»[139] puede verse el efecto en un adolescente francés.

Balconing

Consiste en tirarse desde un balcón o terraza a una piscina con el consiguiente peligro para la integridad física. El objetivo es tener una foto que certifique que se ha hecho.

Surfear en el tren

Esta modalidad de reto consiste en viajar en el exterior de un tren o camión, en su techo, agarrado a una puerta, etc. para filmarse haciéndolo.

Selfies arriesgados

Hay toda una gama de actividades arriesgadas por hacerse el *selfie* más original que acaban en tragedia. El reto de los *selfies* peligrosos no es algo que debamos obviar, ya que es una auténtica moda entre jóvenes y adultos.

Precauciones ante estos juegos y retos virales:

- Hay que tener mucho cuidado con las personas nuevas que se contactan a través de la Red.

138 https://elclarinweb.com/noticias/sucesos/muere-adolescente-por-el-juego-de-la-ballena-azul

139 https://www.eltiempo.com/tecnosfera/novedades-tecnologia/joven-en-francia-habria-muerto-por-el-momo-challenge-283730

- Ante cualquier problema acudir a un adulto.
- No compartir nunca el teléfono en Internet, así como cualquier dato personal.
- Informar a los niños de los distintos bulos, juegos o desafíos que se pueden encontrar en Internet e insistir en la importancia de no compartir y no participar en ellos.

Algunos retos son positivos

No obstante, algunos retos como el llamado *trashtag* o *basurachallenge*, pueden ser, incluso, una fuente de inspiración y de contrapeso. Este reto consiste en elegir una zona degradada por la basura y, a continuación, hacer una foto antes y después de limpiarlo. Puede verse en https://twitter.com/search?q=%23trashtag algunos mensajes de Twitter con este *hashtag*.

Estrategias en la familia

- Los padres deben estar informados de las actividades que realizan sus hijos y vigilar sus cambios de comportamiento relacionados especialmente con lo que puede suceder a través del móvil.

Para saber más

- **CiberBullying**: https://www.ciberbullying.com/
- ***Guía legal sobre ciberbullying y grooming***: https://www.is4k.es/sites/default/files/contenidos/herramientas/guia_legal_ciberbullying_grooming.pdf

Formación

Formación de familias

Grooming* y *sexting

- Tipo de actividad: **Sesión informativa**
- Duración: **1-2 horas**
- Niveles implicados: **Todos**
- Objetivos:
  - **Estar informados sobre los peligros de Internet**
  - **Conseguir herramientas para detectar los peligros e intentar ponerles solución**

Grooming

Empezar con la proyección del vídeo que está en este enlace: https://youtu.be/XjydCCCFAzE

Explicar lo que es

El ***grooming***, también conocido como **engaño pederasta**, es el acoso sexual al que pueden verse sometidos los menores por parte de un adulto (normalmente del sexo femenino).

Explicar la forma de detectarlo

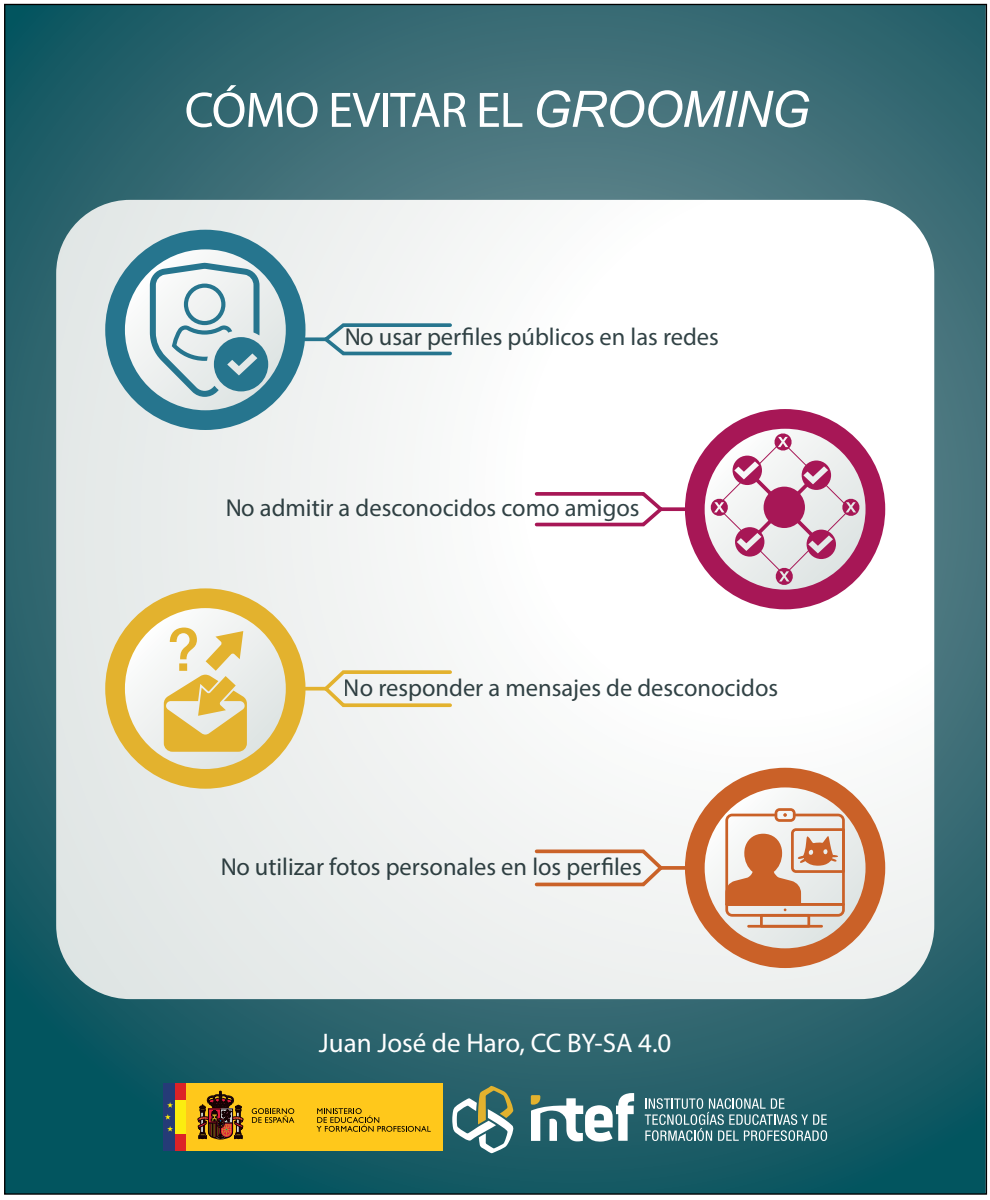
- **Retraimiento social**: se observan cambios en la manera de relacionarse, es decir, o hay una falta de defensa o una exagerada reacción ante supuestas bromas o acciones públicas.
- **Reserva excesiva** para comunicarse con otros.
- **Modificación en su lenguaje corporal** ante adultos, observándose en ocasiones la cabeza baja, la falta de contacto ocular, rechazo a estar con adultos.
- **Alteraciones en el rendimiento escolar**.
- **Cambios de humor**: tristeza, apatía y desmotivación general.
- **Explosiones de ira**.
- Procuran **ocultarse o apartarse** cuando emplean el móvil.
- Pueden presentar **miedo a salir de casa**.
- **Síntomas psicosomáticos** como dolores de cabeza, náuseas, mareos, ataques de ansiedad, lesiones físicas sin justificar o diarreas frecuentes.

Cómo evitarlo

Los pederastas conocen a sus víctimas a través de Internet, especialmente a través de las redes sociales, por lo tanto, hay unas normas básicas que pueden seguirse siempre en el caso de los menores de edad:

- **No usar perfiles públicos en las redes**, de otro modo cualquiera puede conocer la vida e incluso llegar a deducir el lugar en el que vive el menor, aun cuando no lo haya publicado nunca explícitamente. Es muy fácil localizar el barrio o los lugares en los que se desenvuelve una persona cuando está bien documentado fotográficamente. **Los perfiles deben estar limitados a los conocidos** de forma personal.
- **No admitir desconocidos como amigos** o seguidores, ya que, dada la facilidad para falsear el perfil de una persona, llega un momento en que se tiene un conjunto de seguidores total y absolutamente desconocido, aunque se hable habitualmente con ellos.
- **No responder mensajes de desconocidos**, lo mejor es no hablarles y mucho menos acceder a cualquier petición de fotos, webcam o chat.
- En los **perfiles poner fotos de personajes ficticios** para evitar que aquellos que localizan a los menores mediante el buscador de perfiles de las redes sociales y puedan saber quién y cómo es.

Figura 54:
¿Cómo evitar el grooming?



Nota 54. Elaboración propia

Aquellos niños que son víctimas del acoso de un adulto suelen tener una gran vergüenza ante sus padres y, por lo tanto, tienden a retraerse sobre sí mismos, por lo que el diálogo con ellos y la atención a lo que hacen es fundamental. En concreto los padres pueden:

- **Explicar las normas básicas de seguridad** que deben mantener en Internet.
- **Mantener un diálogo fluido** sobre lo que sus hijos hacen en Internet, para que, en el caso de que aparezca un elemento disruptor, puedan localizarlo fácilmente. Si nunca hablan con sus hijos difícilmente se darán cuenta a tiempo.
- **Observar los hábitos de uso de Internet**. Si el menor se conecta de forma regular, a la misma hora, cuando todos duermen o está solo es posible que esté en contacto con alguien que no quiere que se enteren sus padres.

Sexting

Mostrar el vídeo siguiente para introducir el tema: https://youtu.be/sVqeJXhF6OA

Razones para no hacer *sexting*

Explicar el concepto y, haciendo uso del póster 10 razones para no sextear[139], comentar los peligros que puede llegar a tener. Para que se sientan más interpelados, se puede proporcionar impreso en DIN A4 a los asistentes. A continuación se dan algunos consejos:

1. Al hacer *sexting* se pasa a depender de otra persona. No sabemos lo que hará.
2. Las relaciones cambian. Aunque ahora estemos seguros del otro, más adelante puede cambiar.
3. No es posible garantizar la seguridad que tendrán otros con las fotos. Hay personas descuidadas que, por ignorancia o descuido, pueden contribuir a difundir las fotos.
4. La información de la distribución digital no puede controlarse. Una vez sale de nuestro poder, desconocemos la difusión que podrá llegar a tener.
5. Aunque la cara de la persona que hace *sexting* no se vea en realidad hay muchas formas de saber quién es: *piercings*, tatuajes, marcas, lugar de la foto, etc.
6. Las leyes protegen a los menores. Si participamos en el reenvío de este tipo de imágenes, seremos responsables ante la ley.
7. Si la imagen cae en malas manos, se puede producir la sextorsión.
8. Aunque las imágenes se transfieran por medios privados, pueden acabar llegando a Internet, el medio de difusión más potente que ha existido jamás.
9. A través de las redes sociales, las personas más cercanas pueden ver aquello que no iba destinado a ellos.
10. Si la imagen llega a distribuirse por Internet es muy posible que se desencadene el *ciberbullying*, hay gente que disfruta viendo a otros sufrir.

Qué hacer si se produce el sexting *o el grooming*

Las medidas a tomar son muy similares, ya que en ambos casos es el acoso a un menor, en el que únicamente varía la intencionalidad.

Primeras medidas

- No borrar ningún contenido del teléfono o el ordenador.
- Las conversaciones, imágenes y los vídeos que el acosador y la víctima se hayan enviado deben ser guardados para usarlos como prueba. Como añadido, se puede realizar una impresión de estas para evitar su perdida.
- No denuncies el perfil al servicio web desde el que se produce el acoso, únicamente bloquéalo para evitar que pueda ponerse en contacto contigo. De lo contrario, los administradores del sitio podrían tomar medidas contra el usuario que se pondría en alerta pudiendo desaparecer. De esta forma el acosador se podría hacer otro perfil para seguir acosando a otros niños.

140 http://www.pensarantesdesextear.mx/prevencion-10-razones-no-sexting/pdf/10-razones-para-no-realizar-sexting.pdf

Denunciarlo

- Una vez detectado hay que denunciar de forma inmediata un caso de *grooming*.
- La denuncia deben cursarla los tutores del menor, que pueden acudir a tres instancias: cuerpos policiales (policía, guardia civil, policías autonómicas), juzgado de guardia y fiscalía de menores.
- Sin embargo, hay casos en los que la vergüenza que pueda sentir el menor agredido lleva a realizar denuncias anónimas a través de las webs de los cuerpos de seguridad. Existe una tercera vía que es acudir a ONG especializadas en ciberacoso, pero las autoridades recuerdan que este método no tiene repercusiones legales sobre el agresor.

Apoyarle

- No hay que recriminar al menor. Puede que la primera reacción sea recriminarle al haberse puesto en contacto con desconocidos por Internet y haber compartido información íntima. El hijo es una víctima y el abusador, en cambio, es un especialista en conseguir lo que busca.
- No hay que culparle. El acosador, muchas veces recurre a la extorsión de mostrar los contenidos íntimos del menor si no cumple con los nuevos pedidos. Hay que evitar hacerle sentir vergüenza o culpa, ya que de esa forma únicamente aumentará el poder que tiene el acosador sobre tu hijo.
- Habla con tu hijo porque se siente responsable, tiene miedo y siente mucha vergüenza por lo que le ha sucedido. Hay que acompañarle, hablar con él y orientarle para conseguir que se sobreponga a esta situación tan angustiante.

Ciberbullying

- Tipo de actividad: **Sesión informativa**
- Duración: **1-2 horas**
- Niveles implicados: **Todos**
- Objetivos:

  - **Estar informados sobre el *ciberbullying*.**
  - **Tener herramientas para detectar el *ciberbullying* e intentar ponerle solución.**

Además de tratar el *ciberbullying* de forma general, es conveniente conocer el protocolo de actuación en estos casos de cada comunidad autónoma. En la página Protocolos de actuación del Ministerio de Educación y Formación Profesional se proporcionan enlaces a todos ellos, aunque habría que comprobar que los documentos están actualizados.

Empezar con este par de vídeos, el primero (https://youtu.be/SEC_dOWFN5M) introduce el tema y el segundo (https://youtu.be/gXvG53ccyJY) da una serie de consejos para la convivencia en Internet.

Características del ciberacoso

Explicar las características del ciberacoso:

- **Acusaciones y publicaciones falsas**. Los acosadores intentan dañar la reputación del acosado difundiendo falsedades e intentando poner a otras personas en su contra. Normalmente se hace a través de las redes sociales o grupos de programas de mensajería como WhatsApp.
- **Se busca asustar y aterrorizar a la víctima**. Es habitual a través de mensajes privados de WhatsApp, correo electrónico, redes sociales, etc.
- **Recopilación de información sobre la víctima.** Los ciberacosadores pueden espiar a los amigos de la víctima, su familia y compañeros de trabajo para obtener información personal.
- **Manipulación del entorno de la víctima.** Pueden enviar regularmente correos difamatorios al entorno de la víctima para poder manipularlos.
- **Pérdida de la privacidad**. El acosador que traslada a Internet sus insultos y amenazas puede hacer pública la identidad del acosado, incluso facilitando en algunos casos su teléfono y otros datos personales para que terceras personas se unan al acoso.
- **No existe un propósito legítimo**, o sea, que el acoso no tiene un propósito válido, aunque algunos acosadores están persuadidos de que tienen una causa justa para acosarlo, normalmente creen que ha cometido un error y que debe pagar por él.
- **Repetición.** El ciberacoso se caracteriza por no ser un hecho aislado, sino que los ataques a la persona se producen de forma reiterativa.

Prevención del acoso

Como en el *grooming*, es fundamental el diálogo con los hijos y la información también desde la escuela. Es importante que conozcan:

- **Comportarse con educación** en la Red.
- **No facilitar datos personales**.
- Que ante cualquier problema pueden **acudir a los adultos**, ya sean padres o profesores, para exponerles lo que les está sucediendo a través de la Red.
- Aun cuando tengan sus perfiles restringidos a sus amigos de la vida real, normalmente los amigos del colegio, **no deben publicar fotos o comentarios que sean susceptibles de causar problemas** por parte de otros no muy bien intencionados. Hay que ser prudentes y no publicar nada que no expondríamos también en el tablón de anuncios de la clase.
- En ocasiones se comparten nombres de usuario y contraseñas con amigos es algo que NUNCA debe hacerse. **Los datos de inicio de sesión de las cuentas personales** deben ser conocidos únicamente por sus dueños. Lo que ahora es amistad puede cambiar rápidamente con un malentendido y un enfado y convertirse en una suplantación de personalidad que toma posesión de una cuenta de la víctima para hacerle daño.
- Como norma general, **no hacer en las redes lo que no se haría en persona**.
- Por parte de los padres, es aconsejable **supervisar la actividad realizada por sus hijos** de forma que se sientan acompañados. Esta supervisión ayudará a detectar conductas de riesgo, así como a localizar posibles acosadores.

Netiqueta: Normas de conducta

La netiqueta ayuda a minimizar el riesgo de cometer determinados errores que pueden acabar en *ciberbullying*:

- Nunca debemos olvidar que **al otro lado hay un ser humano**, hay que tratar de no herir sus sentimientos, ponerse en el lugar de la otra persona y preguntarse si desearíamos que nos traten como lo hacemos con esa persona. Los alumnos deben tener muy claro que el hecho de no ver en ese momento a aquel a quien escriben, no significa que lo que digan va a causar menos impacto en él.
- La **honradez y la responsabilidad** han de ser nuestra forma de conducta tanto dentro como fuera de la Red.
- Hay que cuidar el **estilo con el que escribimos**, muchas veces es lo único que los otros percibirán de nosotros:

    - Vigilar la **ortografía**, especialmente en los mensajes enviados con el móvil, la tendencia es a acortar los mensajes con abreviaturas y prescindir de los acentos.
    - Evitar escribir con **mayúsculas**. LAS MAYÚSCULAS SE UTILIZAN PARA GRITAR.

- Hay que ayudar a mantener los **debates sanos y en un tono educativo**. Debemos evitar las provocaciones y participar activamente para que no se produzcan entre otros.
- Los mensajes de **correo** que enviemos deben ir precedidos de un **saludo** y una **despedida** al final de este.
- **No reenviar mensajes** a no ser que sea necesario. Vivimos en la época del reenvío de mensajes porque nos parecen graciosos, simpáticos o *por si acaso* lo que dicen es verdad. La realidad es que uno de los motivos de cansancio en la comunicación electrónica es la afluencia masiva y continua de mensajes intrascendentes, falsos y que no aportan nada. Si reenviamos algo, que sea porque es necesario que la persona que lo reciba lea ese mensaje. Evitemos los mensajes de tipo cadena y, sobre todo, aquellos que dicen que hay que reenviarlos al mayor número de personas.
- Antes de enviar un mensaje en una red social o grupo de mensajería, **debemos pensarlo dos veces**, llegará inmediatamente a sus destinatarios y, aunque podemos borrarlos si nos arrepentimos, casi con seguridad, ya habrá sido leído por más de uno. Lo mismo sucede con los vídeos e imágenes. Procuremos no enviar **material gráfico** que pueda ofender o del que nos podamos arrepentir más adelante. Una buena guía es pensar si colocaría esas imágenes en el tablón de anuncios de clase o de la escuela. Debemos recordar que **lo que se coloca en la Red, se queda en la Red**. Una vez un texto o imagen abandona nuestro ordenador, tableta o teléfono móvil ya no tenemos más control sobre él, aunque nos parezca lo contrario.
- En los grupos y redes sociales debemos tener mucho cuidado con el **sentido del humor**, lo que nos parece gracioso o normal, a otros les puede parecer ofensivo o ridículo. Este es uno de los mayores motivos de desencuentro y enfrentamiento *online*: los malentendidos derivados de un uso diferente del lenguaje y su interpretación.
- En situaciones informales, al escribir en redes sociales, podemos utilizar los **emoticonos** para reforzar los sentimientos que queremos transmitir. Como ya se ha indicado, uno de los problemas de la comunicación textual es la interpretación del tono con el que se está hablando.
- Nunca debemos crear perfiles falsos o que den una idea contraria de lo que somos.

Si se produce el *ciberbullying*:

- No contestar a las provocaciones, ignorarlas.
- Advertir a los acosadores de que lo que hacen es un delito.
- Guardar **capturas de pantalla** de cualquier evidencia de acoso.
- Ante cualquier problema el menor debe avisar a sus padres o profesores.
- El siguiente paso, una vez avisado el centro escolar y si no se ha conseguido solucionar, deberá ser denunciado ante la policía.

Formación de alumnos

Amanda Todd

- Tipo de actividad: **Actividad y debate**
- Duración: **1-2 horas**
- Niveles implicados: **ESO y Bachillerato**
- Objetivos:

  - **Reflexionar sobre los riesgos de enviar fotografías comprometedoras a través de Internet**
  - **Establecer mecanismos de protección ante el *sexting***

Amanda Todd fue una chica que fue víctima del *grooming*, en primer lugar, y después de *ciberbullying*. Ante la insistencia de un conocido por Internet, Amanda acabó enviándole una foto de carácter sexual. El conocido le dijo que o bailaba para ella o enviaría la foto a todos sus amigos de la escuela. Ella se negó y sus amigos la recibieron. A partir de ese momento, pasó por un auténtico calvario donde sus compañeros la insultaban, le ponían motes y se burlaban de ella por Internet y en persona. Acabó suicidándose en 2012, a la edad de 15 años, después de publicar un vídeo donde explicaba lo que le había sucedido. El vídeo ha permanecido en YouTube por voluntad de su madre que ha querido que sirva como ejemplo.

Comenzar explicando brevemente qué es el *grooming* y el *ciberbullying*.

A continuación, ver el vídeo de Amanda Todd: https://youtu.be/6yIhGau0qXg

Hacer grupos de cuatro o cinco alumnos para que hablen y debatan, y después plantearles las siguientes preguntas:

- ¿Qué parte de *grooming* y cuál de acoso entre iguales sufrió Amanda?
- ¿Qué errores pudo cometer en todo el proceso?
- ¿Qué debería haber hecho?
- ¿Cómo podemos prevenir este tipo de actos?
- ¿Conoces algún caso similar?

Estos mismos grupos elaborarán cinco fichas de papel, al estilo del vídeo, donde expondrán sus conclusiones a lo que han respondido.

Cada grupo pasa sus fichas a los demás y se inicia un debate sobre la temática del *grooming*, el *ciberbullying* y la actitud de los que miran estos sucesos desde fuera y su responsabilidad.

Privacidad y seguridad

- Tipo de actividad: **Actividad semanal**
- Duración: **15 minutos por sesión**
- Niveles implicados: **6.º de primaria, ESO**
- Objetivos:

  - **Aprender los conceptos básicos de seguridad y privacidad en Internet.**
  - **Interiorizar normas básicas de conducta en relación con la seguridad y la privacidad.**
  - **Reflexionar sobre por qué a veces no se siguen las recomendaciones para corregirlas.**

La Agencia Española de Protección de Datos (AEPD) ha publicado una serie de 18 fichas que tratan de forma general el tema de la seguridad. Existen varias formas de trabajar estos contenidos, pero recomendamos hacerlo con una ficha cada 1-2 semanas, de manera que la formación se alarga durante gran parte del curso.

Cada semana, o el período deseado, se imprime una ficha, se debate y se cuelga en la clase. Cuando llega el momento de comentar la siguiente ficha, se hace una recapitulación de la ficha de semanas pasadas preguntando a los alumnos si han puesto en práctica lo aprendido, o no, y por qué. Es importante detectar los errores cometidos, aun sabiendo ellos mismos que los cometen para poder prevenirlos y ponerles solución.

Durante la primera sesión se puede rellenar el cuestionario[140] de ocho preguntas de verdadero y falso creado por la Oficina de Seguridad del Internauta para comentar los resultados y servir como introducción.

Las fichas pueden ser descargadas desde la siguiente página: Privacidad y Seguridad en Internet.[141]

141 https://www.osi.es/es/test-evaluacion/mitos-sobre-seguridad-en-internet-verdaderos-o-falsos

142 https://www.aepd.es/sites/default/files/2019-09/guia-privacidad-y-seguridad-en-internet.pdf

No te enredes

- Tipo de actividad: **Actividad en clase**
- Duración: **1 hora**
- Niveles implicados: **6.º de primaria, ESO**
- Objetivos:

  - **Reflexionar sobre los hábitos de los alumnos en Internet**
  - **Aprender buenas prácticas en relación con la privacidad y seguridad**

Esta serie de actividades consisten en presentar un vídeo para después realizar la rutina de pensamiento Antes pensaba... Ahora pienso, donde el alumno reflexiona sobre lo que ha aprendido escribiendo lo que pensaba antes y después de recibir la información.

- Pasar el vídeo.
- Realizar la rutina de pensamiento.
- Leer y comentar los resultados, haciendo hincapié en las ideas erróneas que se tenían previamente y en la falta de reflexión de muchas de las que hacemos.

Proponemos diversos vídeos con diferentes temáticas:

- *Grooming*

  - https://youtu.be/-x1-hdcF2TU
  - https://youtu.be/KzahZqZPwLc

- *Ciberbullying*

  - https://youtu.be/D57vDI7w_mA

- *Sexting*

  - https://youtu.be/qKs7qnHvY2U

Pautas para la protección de datos en centros educativos

Introducción

En los centros educativos hay dos ámbitos principales en los que debemos tener presente la protección de datos. El primero es el uso de la tecnología en el aula, con el uso de servicios web, aplicaciones para móvil o programas de carácter educativo. El otro es el tratamiento de los datos de los alumnos, el uso y custodia que se hace de los mismos.

Aplicaciones usadas en clase

La Agencia Española de Protección de Datos, en su «Informe sobre la utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas»,[143] cita una serie de aspectos que deben ser tenidos en cuenta a la hora de hacer uso de las mismas.

Adecuación a la normativa

Los centros deben velar por que las aplicaciones cumplan la normativa sobre la protección de datos, teniendo en cuenta que algunas de estas aplicaciones no proporcionan información suficiente sobre el uso que se hace de ellos. Por ejemplo, en materia de seguridad, sobre la ubicación de los datos, el período de retención de estos, ni los responsables de los tratamientos. En ocasiones no incluyen información ni tan siquiera sobre las finalidades de los tratamientos, detectándose falta de transparencia y la posibilidad de prácticas de retención de datos opacas.

Se podría llegar al extremo de que las aplicaciones elaborasen un perfil sobre los hábitos de los menores, el uso que hacen de la información y sus preferencias. Por estos motivos las aplicaciones deben indicar claramente el tratamiento que se hace de los datos.

Autorización de las aplicaciones

Las aplicaciones que se usan en un centro deben constar en su política de seguridad, de forma que se haga una evaluación sobre su idoneidad. Deben establecerse procedimientos que obliguen a solicitar la autorización del centro para el uso de estas aplicaciones. Una solicitud de autorización conllevará la evaluación de la aplicación desde el punto de vista de la seguridad de la información y la consiguiente autorización o denegación por parte del centro.

Información a los padres

Los padres o tutores legales de los alumnos deben ser informados del uso de estas aplicaciones, especialmente de aquellas que almacenen datos en la nube.

Control

Los profesores y padres deben poder controlar los contenidos que se han subido en las aplicaciones, como vídeos, fotos, grabaciones de voz, etc.

Datos de terceros

Debe guardarse especial cuidado con los tratamientos de datos personales que sean facilitados por terceros sin mediación del titular de los datos y, en concreto, con la publicación de fotografías o vídeos de alumnos facilitados por otros alumnos o profesores.

Protección de datos personales

Debe formarse a profesores y alumnos sobre la forma de proteger los datos personales y sobre la importancia de utilizar correctamente las aplicaciones. En concreto:

- Hay que tener especial cuidado al subir imágenes de terceros para no exponer su intimidad.
- Debe leerse la política de privacidad y términos de uso de la aplicación que vaya a ser usada y no tener ningún reparo en dejar de usar la aplicación si la información no va a estar correctamente custodiada. Nuestros datos pueden pasar a otras empresas o el material que generamos deja de ser nuestro para pasar a ser de la empresa que proporciona el servicio.

143 https://www.aepd.es/media/guias/guia-orientaciones-apps-datos-alumnos.pdf

- Cuando se usen redes sociales, configurar la privacidad para poder interactuar solo con un grupo previamente establecido de personas.
- Evitar proporcionar datos excesivos o abusivos sobre los menores como el lugar de residencia y otros datos privados que no deberían ser necesarios.
- Las contraseñas deben ser robustas para evitar ser descubiertas con facilidad por otros. Del mismo modo, debe evitarse que los menores den su contraseña a otras personas, algo que sucede más de lo que debería y que suele ser una fuente de problemas.

Datos sensibles

Para los casos de tratamientos especiales de datos personales que puedan suponer un mayor riesgo, tal como el reconocimiento facial de menores de edad, que implica el tratamiento de datos biométricos, el responsable debe obtener el consentimiento expreso de los alumnos (si son mayores de 14 años) o de los padres o tutores (si son menores de 14 años) para aplicar dicho tratamiento a las imágenes con fines de identificación y asegurarse que esta tecnología se utiliza únicamente para fines concretos especificados y legítimos.

Evaluación de aplicaciones

Desde el punto de vista de la seguridad de datos se aconseja evaluar las siguientes características:

- El responsable de la aplicación debe informar de lo siguiente:
    - la identidad y dirección del responsable,
    - las finalidades para las que serán utilizados los datos,
    - las posibles comunicaciones de datos a terceros y su identidad, así como la finalidad por la que se ceden,
    - los derechos que asisten a los titulares de los datos,
    - la ubicación de los datos y sus períodos de conservación,
    - las medidas de seguridad facilitadas por la aplicación,
    - los posibles accesos que realiza la aplicación a los datos personales almacenados en el dispositivo o a sus sensores.

- Los datos deben ser analizados en un país del Espacio Económico Europeo o en alguno de los países con niveles de seguridad equivalentes.[144] También pueden estar en Estados Unidos si se ha adherido al Escudo de Privacidad, puede consultarse la lista de empresas en Internet[145].
- Es conveniente probar la aplicación previamente sin usar datos reales de menores. El resultado de esta evaluación es conveniente que quede documentado en el centro.

Temas de interés para el profesorado

Sobre el uso de WhatsApp

Se desaconseja totalmente el uso de la mensajería instantánea, tanto para comunicación profesor-alumno como profesor-padres y madres. Si es necesario, se pueden establecer canales específicos de comunicación. Deberían emplearse los medios y herramientas establecidas por el centro educativo y puestas a disposición de alumnos y profesores (por ejemplo, áreas específicas en la intranet del centro o uso de plataformas que cumplan los requisitos que se verán más adelante) o por medio del correo electrónico.

144 https://www.aepd.es/reglamento/cumplimiento/transferencias-internacionales.html#paises

145 https://www.privacyshield.gov/list

Expediente académico

La publicidad de esta comunicación, a diferencia de la educación universitaria, no está regulada, por lo que hay dudas sobre cómo proceder con las notas de los alumnos. **Las calificaciones de los alumnos se han de facilitar únicamente a los propios alumnos y a sus padres**. En el caso de comunicar las calificaciones a través de plataformas educativas, estas solo deberán estar accesibles para los propios alumnos, sus padres o tutores, sin que puedan tener acceso a las mismas personas distintas. No obstante, sí sería posible comunicar la situación del alumno en el entorno de su clase, por ejemplo, mostrando su calificación frente a la media de sus compañeros. En el caso de que se digan oralmente al resto de la clase es mejor no hacerlo, pero se podría hacer evitando comentarios personales que pudiesen afectar al alumno, tal como se indica en la página 29 de la *Guía para centros educativos* de la Agencia Española de Protección de Datos[146].

El profesor podrá tener acceso al expediente académico de sus alumnos, no está justificado el acceso a aquellos a los que no imparte la docencia.

Datos de salud

Los profesores han de conocer y, por tanto, acceder únicamente a la información de salud de sus alumnos que sea necesaria para la impartición de la docencia o para garantizar el adecuado cuidado del alumno, por ejemplo, respecto a discapacidades auditivas, físicas o psíquicas, trastornos de atención, TDAH o enfermedades crónicas.

Información a familiares diferentes de los padres

Es relativamente frecuente que a las reuniones con el tutor de un alumno acudan hermanos, tíos, etc. A no ser que exista una autorización expresa, solo se podrá dar información sobre un alumno a sus padres o tutores legales.

Tratamiento de las imágenes

Se pueden realizar imágenes de los alumnos sin necesitar su consentimiento siempre que la finalidad sea estrictamente educativa, por ejemplo, para trabajos escolares o de carácter evaluativo. Solo deberán estar accesibles para los alumnos involucrados en dicha actividad, sus padres o tutores y el profesor correspondiente.

Cuando su fin sea acontecimientos o eventos que se graban habitualmente con fines de difusión en la revista escolar o en la web del centro, es necesario recabar el permiso y, además, informar claramente si el acceso será indiscriminado o limitado al propio centro.

En los eventos del centro los padres pueden grabar o tomar imágenes de los alumnos siempre que su uso sea particular y familiar y que, por lo tanto, no será subido a las redes. Si hacen público el material necesitan el consentimiento de aquellos que salgan en las imágenes, cosa que difícilmente podrán conseguir. Por este motivo, conviene avisar a los padres de la responsabilidad que tienen a la hora de tomar las imágenes y divulgarlas en espacios abiertos.

Se pueden publicar imágenes de los alumnos en la web del centro siempre que se disponga del consentimiento de los alumnos o de sus padres o tutores. También podría llevarse a cabo de manera que no se pudiera identificar a los alumnos, por ejemplo, pixelando las imágenes. En ocasiones, sería posible su publicación cuando responda a determinados eventos desarrollados en el entorno escolar con la única finalidad de que los padres pudieran tener acceso a ella. Este acceso debería llevarse a cabo siempre en un entorno seguro que exigiera la previa identificación y autenticación de los alumnos, padres o tutores (por ejemplo, en un área restringida de la intranet del centro), limitándose a la información correspondiente a eventos en los que el alumno concreto hubiera participado. En todo caso, sería preciso recordar a quienes acceden a la información que no pueden, a su vez, proceder a su divulgación de forma abierta.

146 Informe de la Agencia Española de Protección de Datos: Guía para Centros Educativos. Guías Sectoriales AEPD. Madrid. 2017. http://tudecideseninternet.es/aepd/images/guias/GuiaCentros/GuiaCentrosEducativos.pdf

Publicar otras informaciones de los alumnos

En general, salvo que se tenga autorización, no deben publicarse datos en sistemas abiertos como blogs o redes sociales de forma que pueda reconocerse al alumno. En estos casos lo que se puede hacer es utilizar pseudónimos o cualquier otro sistema que ayude a mantener en el anonimato al alumno.

Protección de datos del centro

En la *Guía para Centros Educativos*[147], la AEPD proporciona un extenso documento, adecuado a la última normativa de diciembre de 2018 y del cual extraemos algunas consideraciones importantes:

- Los equipos directivos, profesores, personal administrativo y auxiliar de los centros educativos en el ejercicio de sus funciones y tareas necesitan tratar datos de carácter personal de los alumnos y de sus familiares, lo que deberán realizar con la debida **diligencia y respeto a su privacidad e intimidad,** teniendo presente el interés y la protección de los menores.
- Por regla general, **los centros educativos no necesitan el consentimiento de los titulares de los datos para su tratamiento**, que estará justificado en el ejercicio de la función educativa y en la relación ocasionada con las matrículas de los alumnos. No obstante, se les debe informar de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo, que se puede realizar en el mismo impreso en el que se recojan los datos de:

    - la **finalidad** para la que se recaban los datos y su licitud, por ejemplo, para el ejercicio de la función educativa, o para difundir y dar a conocer las actividades del centro,
    - la **obligatoriedad o no** de facilitar los datos y las consecuencias de la negativa a facilitarlos,
    - los **destinatarios** de los datos,
    - los **derechos** de los interesados y dónde ejercitarlos,
    - la **identidad** del responsable del tratamiento: la administración educativa o el centro.

- Cuando sea preciso obtener el consentimiento de los alumnos o de sus padres o tutores para la utilización de sus datos personales por tratarse de finalidades distintas a la función educativa, se debe informar con claridad de cada una de ellas, permitiendo a los interesados oponerse a aquellas que así lo consideren.
- Las TIC son herramientas fundamentales para la gestión y el aprendizaje de los alumnos. **Las administraciones educativas y los centros deben conocer las aplicaciones que se vayan a utilizar, su política de privacidad y sus condiciones de uso de estas antes de utilizarlas**, debiendo rechazarse las que no ofrezcan información sobre el tratamiento de los datos personales que realicen.
- Las administraciones educativas y los centros deben disponer de **protocolos, instrucciones, guías, directrices o recomendaciones para el uso de las TIC** por los profesores, que deberán utilizar las que la administración educativa o el centro hayan dispuesto. Su enseñanza y uso deberán adaptarse al grado de desarrollo del alumnado.
- Las comunicaciones entre profesores y padres de alumnos deben llevarse a cabo, preferentemente, **a través de los medios puestos a disposición de ambos por el centro educativo** (plataformas educativas, correo electrónico del centro).
- El uso de aplicaciones de mensajería instantánea (como WhatsApp) entre profesores y padres o entre profesores y alumnos no se recomienda. No obstante, en aquellos casos en los que el interés superior del menor estuviera comprometido, como en caso de accidente o indisposición en una excursión escolar, y con la finalidad de informar y tranquilizar a los padres, titulares de la patria potestad, se podrían captar imágenes y enviárselas.
- Los profesores deben tener cuidado con los contenidos del trabajo de clase que suben a Internet. Deben enseñar a valorar la privacidad de uno mismo y la de los demás, así como

147 http://www.tudecideseninternet.es/agpd1/images/guias/GuiaCentros/GuiaCentrosEducativos.pdf

enseñar a los alumnos que **no pueden sacar fotos ni vídeos de otros alumnos ni del personal del centro escolar sin su consentimiento** y hacerlos circular por las redes sociales, para evitar cualquier forma de violencia (ciberacoso, *grooming*, *sexting* o de violencia de género).

– Cuando los centros educativos organicen y celebren eventos (fiestas de Navidad, fin de curso, eventos deportivos) a los que asistan los familiares de los alumnos, constituye una buena práctica **informarles, por ejemplo, al solicitarles la autorización para participar** o mediante avisos o carteles, de la posibilidad de grabar imágenes exclusivamente para su uso personal y doméstico (actividades privadas, familiares, etc.).

Existe una nueva responsabilidad que ha aparecido en siglo XXI, la de saber ser un buen ciudadano digital. En la actualidad, la Red se ha difuminado en una serie de servicios, herramientas y utilidades de las que no siempre somos conscientes del todo. La interconexión entre las personas se ha visto incrementada a medida que el tiempo pasa. Nuestra actividad digital no ha cesado de aumentar y el flujo de información se pierde muchas veces por caminos que no podemos controlar. Además, la edad en la que los más jóvenes empiezan a disponer de un teléfono con conexión a Internet va disminuyendo con el tiempo. Estos son algunos de los motivos por los que es tan importante la educación, ya que, desde muy pequeños, los niños están teniendo acceso a Internet y deben saber desenvolverse.

Este libro va dirigido a educadores y padres conscientes de la importancia que las comunicaciones globales a través de Internet han adquirido hoy en día y que desean aprender cuáles son sus derechos y deberes en la Red, así como la forma de proteger a jóvenes y adultos de los peligros que puede llegar a tener. Además, se proporcionan numerosas actividades prácticas para ser llevadas a cabo tanto en la familia como en la escuela.

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL