GOBIERNO DE ARAGON

Manual del taller

"INTERNET EN EL ENTORNO FAMILIAR: FORMANDO NAVEGANTES"

Presentación. Taller de “Internet en el entorno familiar: formando navegantes”

Desde el Departamento de Hacienda, Interior y Administración Pública, se promueve la realización de este taller, con el objetivo de acercar a padres y madres, tutores y cualquier otra persona que interviene en la formación de menores, la utilización de forma segura de las nuevas tecnologías (Internet, redes sociales, etc.,) por parte de los más pequeños, así como la seguridad y protección básica de dichos equipos informáticos.

Este manual forma parte de los materiales de la formación presencial que se lleva a cabo en centros públicos o de uso público de diversas localidades de la Comunidad Autónoma de Aragón.

Última actualización de este manual: noviembre 2024.

Talleres TIC [1]

Talleres TIC. Manuales; 2

[1] https://www.aragon.es/-/talleres-tic

Índice de contenidos

Este taller está dirigido a padres, madres, tutores y todas aquellas personas que conviven con menores y no tienen los conocimientos suficientes para ayudar y tutelar a sus hijos cuando están navegando por la red, y que desconocen los riesgos que asumen cuando lo hacen.

El control o la supervisión absoluta de lo que hacen o de los contenidos que ven en Internet nuestros menores es complejo y hay que conseguir que la navegación por Internet sea sensata y prudente, a la vez que permita aprovechar al máximo las posibilidades que ofrece la red.

Este taller les ayudará en el aprendizaje y conocimiento de distintas herramientas web, así como de las redes sociales, y de sus características más importantes. Les ayudará a conocer asimismo las denominadas herramientas de control parental y los aspectos vinculados a la seguridad.

Trata la protección de los niños y cómo hacer un uso seguro de internet en aquellas aplicaciones más utilizadas y de más fácil acceso de los menores: mensajería, correo electrónico, juegos de azar, compras on-line, comunicaciones virtuales por Skype, etc., y otros tipos de contenidos que pueden interferir negativamente en la vida de los niños.

Una segunda parte de este manual está centrado en la seguridad informática; tipos de antivirus y cómo hacer uso de ellos, qué son los cortafuegos y su instalación, y la configuración de la seguridad, entre otras cuestiones que pueden ayudar a usuarios de todos los niveles a gestionar la seguridad de sus equipos informáticos en general.

01. Seguridad en internet: protección para tus hijos.

1.1. Introducción

Internet es un medio con enormes **posibilidades** para encontrar información, aprender, expresar opiniones y comunicarse, así como un canal de ocio. Pero Internet también puede ser un lugar donde existen ciertos **riesgos y peligros** que se acentúan en los menores, al ser estos mucho más vulnerables que los adultos. Por tanto, hay que conocer los riesgos y peligros y poner los medios necesarios para proteger de ellos a los menores.

¿A qué riesgos se pueden enfrentar los menores?

Los posibles riesgos que un menor puede encontrar en Internet se resumen en tres tipos:

- **Contenidos inapropiados**. Al navegar por Internet pueden encontrarse con contenidos no adecuados para su edad, como por ejemplo páginas con un lenguaje inadecuado, con contenidos para adultos o contenidos violentos, etc.
- **Privacidad**. Todo el mundo debe tener cuidado a la hora de facilitar datos privados en Internet. Este riesgo se ve incrementado en el caso de los menores ante su mayor ingenuidad. Deben de tener claro que no deben facilitar información personal que pueda poner en riesgo a sus familiares, compañeros y a ellos mismos.
- **Discriminación, abusos y acosos**. Esto sucede, sobre todo, a través de programas de mensajería, chats, foros, etc.

1.2. Educación

Todos debemos mentalizarnos de que la Red tiene peligros de los que hay que proteger a los hijos, pero también que, con un buen uso de ella, tiene **extraordinarias posibilidades**.

Las ventajas superan con mucho sus inconvenientes. **Educar a los menores en el uso de Internet** tal vez sea la mejor propuesta para protegerlos de los posibles peligros que se pueden encontrar en Internet.

El número de escolares que tienen acceso a Internet en sus centros docentes es cada día mayor, pero el hogar familiar es el lugar privilegiado de acceso a Internet.

Es por ello que la colaboración y participación activa de las familias es un elemento clave para el uso educativo, relevante, divertido y seguro de las posibilidades que Internet nos brinda.

La manera más directa de evitar los riesgos es la prevención, teniendo en cuenta que:

- Las familias deben confiar en los centros y en los docentes e informar a los tutores de las incidencias que les parezcan sospechosas.
- Los padres y madres han de confiar también en sus hijos e hijas, propiciando un ambiente familiar de comunicación directa y libertad, utilizando conjuntamente Internet, hablando de ello, no culpabilizando a los menores o convirtiendo Internet en una niñera con la que tener a nuestros hijos e hijas ocupados.

Los riesgos son una parte mínima de todo lo que Internet ofrece, y no se debe adoptar una actitud alarmista, pero sí es recomendable educar en ciertas prácticas que pueden ayudar en dicha prevención, tales como:

- Compartir la experiencia. Siempre que sea posible, navega por Internet con tus hijos.

- Dialogar con los hijos. Háblales con sinceridad y naturalidad sobre los contenidos inadecuados que se pueden encontrar.
- Hacer partícipes a tus hijos. Intenta conseguir que confíen en ti cuando encuentren un contenido inapropiado o que te informen cuando en una conversación o foro se puedan sentir atemorizados.
- Normalizar el tema. Explica sin ambages tus preocupaciones acerca de cuándo ellos hacen uso de Internet.
- Inculcar el respeto a la privacidad de las personas. Enséñales a no dar datos personales suyos, de su familia, ni de un tercero.
- Confianza. Aun teniendo presente todo lo anterior, dar a los hijos la dosis de confianza que merecen.

1.3. Supervisión

El control o la supervisión absoluta de lo que hacen o los contenidos que ven en Internet nuestros hijos es complejo y en ocasiones materialmente **imposible** y podría no ser educativamente lo más recomendable.

Los padres deben conocer la **tecnología** que manejan sus hijos, ya que sin unos mínimos conocimientos no es fácil ayudarles en la adopción de medidas de seguridad ni comprenderles cuando tienen problemas en la red.

Algunas buenas prácticas para su supervisión pueden ser:

- Dar reglas concretas sobre la forma de uso de Internet para su seguridad, y el tipo de información a la que se puede acceder.
- Establecer límites de tiempo, tanto en el uso de los dispositivos como en el uso de Internet. Ten en cuenta que tus hijos pueden acceder a Internet desde otros sitios (escuelas, telecentros, casas de amigos, ciber centros, etc.).
- Situar el ordenador o dispositivo móvil en una sala común de la casa, no en sus habitaciones personales.

- Conocer cuáles son sus hábitos. Pregunta a tus hijos por sus contactos, quiénes son, cómo los ha conocido, qué relaciones tiene con ellos.
- Regular los accesos a Internet desde cualquier dispositivo móvil u ordenador que utilicen: tablet, smartphone, ordenador, etc.
- Y, estar atentos a cualquier cambio de conducta de los niños y adolescentes.

Otras pautas de navegación responsable

- Indicarles que no deben intercambiar información personal, contraseñas o datos de la familia a desconocidos, o subirlos o publicarlos en sitios públicos.
- Deben respetar en la misma medida la privacidad de los amigos y conocidos no subiendo fotos o vídeos; y no etiquetándolos con sus nombres sin contar con su permiso.
- Solicitar en la misma medida respeto por su propia privacidad cuando identifiquen una foto o vídeo en el que aparecen y les genera incomodidad o se les falta el respeto; pidiendo en ese caso su inmediata eliminación.
- No revelar las contraseñas y ser cuidadoso y no guardarlas nunca en equipos compartidos. Ante la pregunta, **"¿Desea guardar la contraseña?**", deben responder que **no**.
- Recordarles que deben ser respetuosos en sus conversaciones o chats. No digan cosas que tampoco dirían abiertamente o personalmente.
- Deben tener cuidado con las fotografías, imágenes y vídeos que guardan en sus móviles porque pueden acceder a ellos personas ajenas y que podrían difundirlas.

1.4. Filtros de contenidos

Los filtros de contenido son herramientas para impedir el acceso a diferentes tipos de contenido en la Red como: sitios clasificados como de contenidos para adultos (pornografía,…); webs de ideología extrema, intolerante o xenófoba; sitios vinculados al uso de drogas; y webs que usen un lenguaje inadecuado para los menores.

Estas herramientas pueden estar incluidas en los ajustes de los propios navegadores (por ejemplo, el “Asesor de contenidos” del navegador web [Internet Explorer, Mozilla…]), pueden ser plugin (pequeñas aplicaciones que se instalan en los navegadores, como por ejemplo “FoxFilter” para Firefox), softwares específicos para el control de contenidos (“Optenet”, “Cyberpatrol”, “Net Nanny”, etc.); programas antivirus; etc.

Los filtros de contenidos actúan básicamente de dos formas:

- **Por palabras clave**: Se restringe el acceso a todas las páginas que contengan las palabras que hayamos seleccionado.

  Este sistema tiene el inconveniente de que puede llegar a bloquear contenidos interesantes para los niños o que búsquedas, en teoría inocuas, hagan llegar al menor a un contenido inapropiado.

- **Por listas “negras" o "blancas”**: Las “listas negras” son una recopilación de webs de contenido inadecuado que son bloqueadas. No son eficaces, ya que cada día surgen nuevas o cambian las antiguas y es por lo tanto imposible que estén totalmente actualizadas. El concepto de “listas blancas”, por su parte, se refiere a un conjunto de sitios web por los que es seguro navegar.

  Es posible configurar el navegador web para que este permita visitar solo los sitios incluidos en esta lista blanca. Es más eficaz que las listas negras, pero hay que reflexionar sobre si es o no necesario censurar el resto de todos los contenidos que ofrece Internet.

Existen sistemas de búsqueda en Internet especialmente orientados a menores.

Asesor de contenido (para versiones inferiores de Internet Explorer)

IMPORTANTE: Esta sección no aplica al sistema operativo Windows 10 o superiores.

El **Asesor de contenido** nos permite autocensurar aquellos contenidos que consideremos inadecuados en función de diferentes categorías. Veamos cómo funciona:

Hacemos clic en el botón de “Inicio”, “Panel de control” y luego seleccionamos “Centro de seguridad”. Pinchamos sobre “Opciones de Internet” y abrimos la pestaña “Contenido” haciendo clic sobre la misma. Para habilitar el Asesor de Contenidos hacemos clic en el botón “Habilitar”:

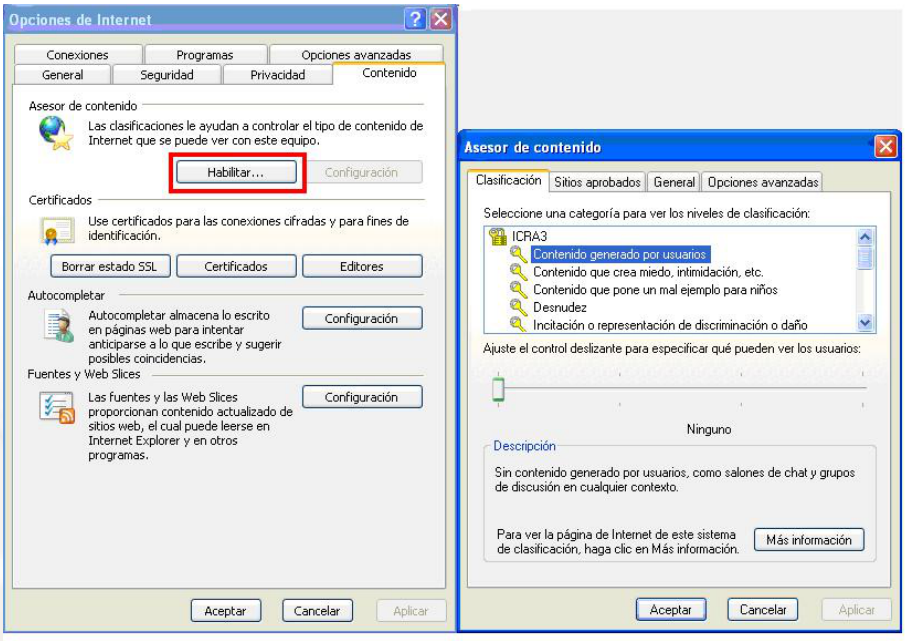

Imagen 1. Opciones de Internet, Asesor de contenidos.

Se abre el Asesor de Contenidos. En la pestaña “Clasificación” podemos establecer para cada una de las categorías su **nivel de restricción**.

Vamos a aplicar una restricción para los contenidos en el lenguaje, por ejemplo. Restringiremos todas aquellas páginas que contengan cualquier tipo de **lenguaje vulgar y malsonante** con gestos obscenos.

Para ello hacemos clic en “Lenguaje soez” y desplazamos la barra deslizante para establecer los límites que deseamos, en este caso, hasta el nivel “limitado”:

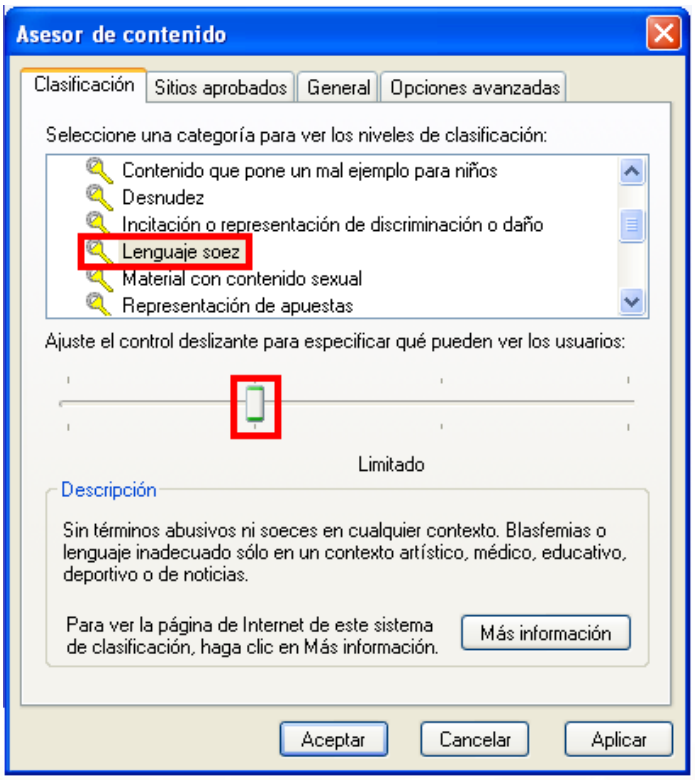

Imagen 2. Clasificación del asesor de contenido.

Además, si sabes de algún sitio web que quieres permitir siempre, puedes **añadirlo** en “Sitios Aprobados.” Para ello hacemos clic en la pestaña “Sitios aprobados” y luego escribimos la dirección del sitio en el campo destinado para tal efecto, y pulsamos el botón “Siempre”.

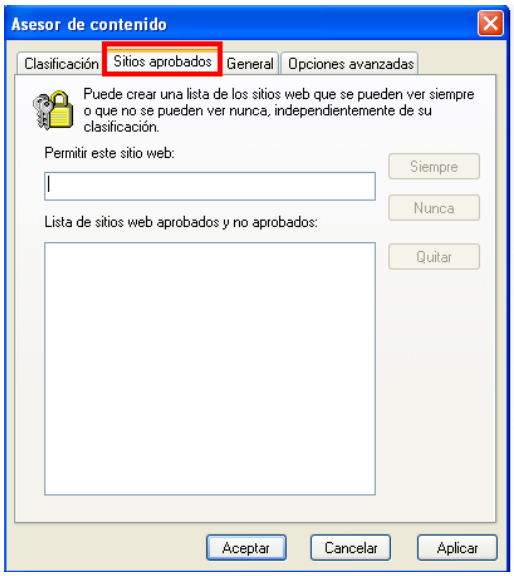

Imagen 3. Sitios aprobados en el asesor de contenido.

Puedes establecer una **contraseña** de supervisor para poder acceder al Asesor de Contenidos y modificar su configuración. Para ello hacemos clic en la pestaña “General”. Después pulsamos el botón “Crear Contraseña”. Se abre una ventana donde debemos introducir la contraseña y una pista que, en caso de olvido de la contraseña, nos sirva para recordarla. Y por último pulsamos “Aceptar”.

Se abre una ventana que nos indica que la contraseña se creó correctamente. Hacemos clic en "Aceptar". De esta forma **nadie podrá modificar** nuestra configuración en el Asesor de Contenido, sin introducir previamente la contraseña. Por último, hacemos clic en el botón “Aceptar” para guardar esta configuración.

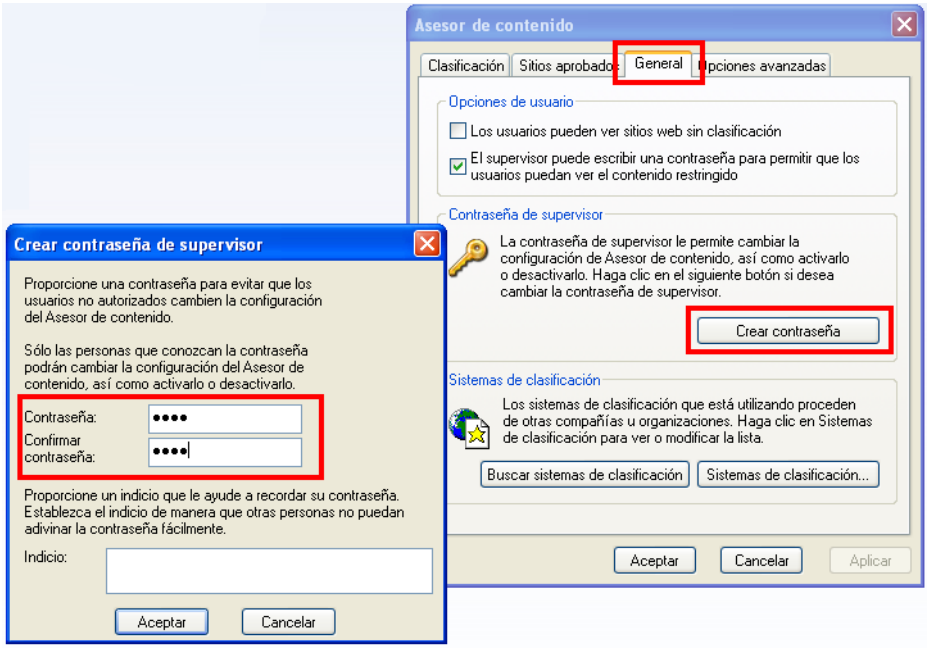

Imagen 4. Crear contraseña de supervisor.

Aunque la incorporación de filtros de contenidos es la opción "fácil", dejar que un ordenador haga *nuestro trabajo* de vigilancia y control de los contenidos a los que tienen acceso nuestros hijos, **no es ni mucho menos la más fiable** (no son capaces de bloquear correctamente muchos contenidos) ni la más confiable (nuestros hijos también pueden llegar a acceder a Internet en otros lugares fuera de nuestra supervisión y de la acción del filtro).

1.5. Dónde encontrar recursos seguros

Buscar información en Internet de forma segura

No siempre que se realizan búsquedas en Internet obtenemos el resultado esperado. Es más, en ocasiones, el resultado puede contener información no adecuada e incluso **ofensiva**.

Es por ello que los motores de búsqueda disponen de algunas medidas de seguridad que facilitan la posibilidad de **filtrar** los resultados. Google, por ejemplo, incluye una herramienta denominada *SafeSearch* (búsqueda segura). Para activarla y configurar sus opciones, lo primero que debemos hacer es acceder a la dirección web de Google, hacemos clic en “Configuración” en la parte inferior derecha de la pantalla y clicar en la opción “Búsqueda avanzada”:

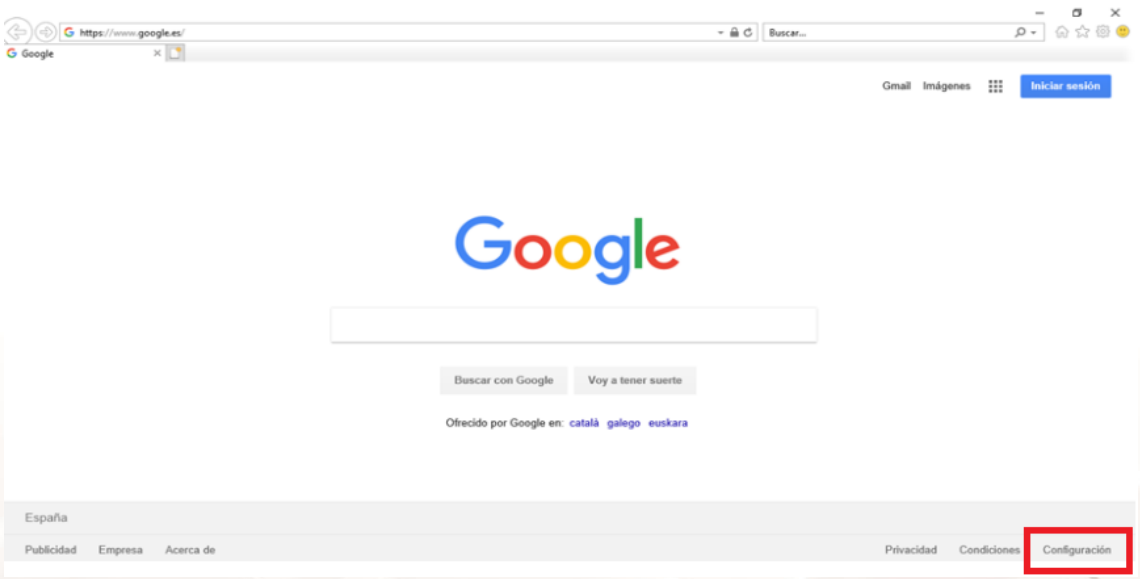

Imagen 5. Configuración de la Web de Google.

Accederemos a las opciones de búsqueda avanzada. En el apartado “A continuación limitar los resultados por…” buscar el desplegable de “Búsqueda segura” Este, por defecto, está configurado para “Mostrar los resultados explícitos” pero podemos cambiar dicha opción por la de “ocultar resultados explícitos” de la barra:

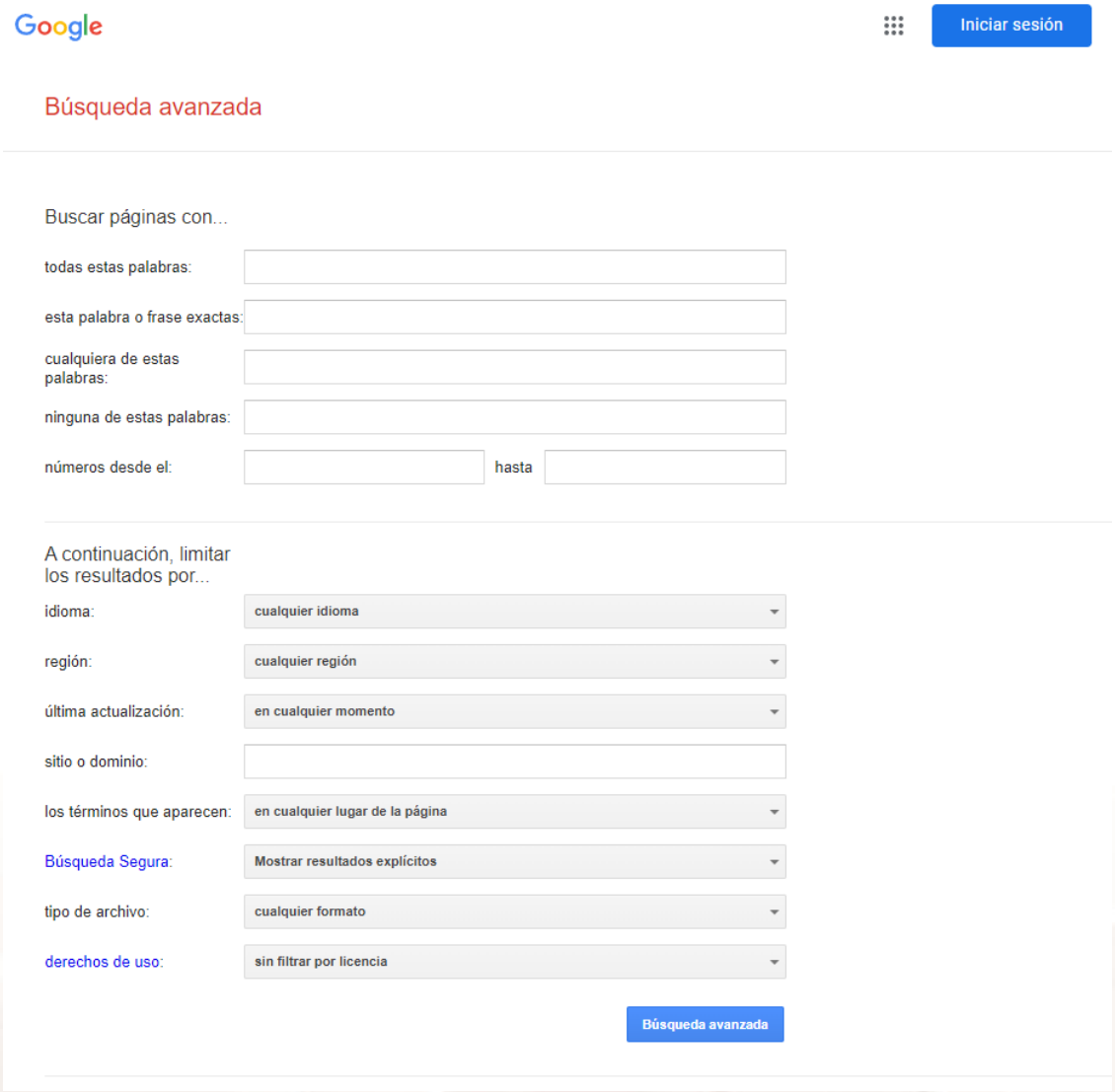

Imagen 6. Búsqueda avanzada de Google.

Es posible conocer más información acerca de este filtro haciendo clic en el enlace SafeSearch[2], y desde allí acceder a “ordenador” y hacer los pertinentes “ajustes” para tus búsquedas.

[2] https://support.google.com/websearch/answer/510?hl=es&p=adv_safesearch

Recursos didácticos y consejos

Una opción más eficiente que realizar búsquedas generales en motores de búsqueda es acudir directamente a sitios web especializados en ofrecer, tanto recursos didácticos para los niños, como buenas prácticas y consejos para que los padres aprendan a sacar partido de las TIC en la educación de sus hijos.

Estas son algunas webs de interés:

A) Recursos didácticos y ocio para menores:

1. Vikidia[3]: Es una "Wikipedia para niños" con secciones temáticas (Ciencias naturales, Matemáticas, Lengua y Literatura, etc.).

2. Banco de imágenes y sonidos del INTEF[4] El Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), dependiente del Ministerio de Educación y Formación Profesional ofrece un banco de imágenes y sonidos para que los alumnos y profesores los utilicen libremente en sus trabajos educativos.

3. Khan Academy[5]: Se trata de una plataforma educativa sin ánimo de lucro para promocionar la educación gratuita a nivel mundial y que cuenta ya con más de 4.300 vídeos educativos.

4. Pequenet[6]: Se trata de un portal de ocio y entretenimiento para menores donde pueden encontrar juegos, adivinanzas, chistes, etc.

5. Aplicaciones para dispositivos móviles y formatos electrónicos**.** Hoy en día, existen dispositivos electrónicos que son herramientas de complemento perfectas para la educación de nuestros hijos. Es el caso, por ejemplo, de las tabletas digitales. Estos aparatos, unidos a los formatos electrónicos (PDF webs, podcasts, vídeos, etc.), pueden sernos de gran ayuda. Algunos ejemplos son:

[3] https://es.vikidia.org/wiki/Vikidia:Portada
[4] https://procomun.intef.es/
[5] https://es.khanacademy.org/
[6] http://www.pequenet.com/

- iTunes Educación[7]: Se trata de una aplicación para el iPad dedicada a recopilar documentos, archivos de audio, vídeos y demás material educativo que pueda ser usado para crear cursos a medida.
- Podcasts para niños y familias:[8] La plataforma de música online Spotify, ofrece una recopilación de podcasts (piezas de audio) que están dirigidas a niños y público familiar.

B) Sitios web con información y buenas prácticas dirigidas a los padres:

1. Pantallas amigas[9]: Este portal nace en el año 2004 con la misión de la promoción del uso seguro y saludable de Internet y otras TIC, así como el fomento de la ciudadanía digital responsable en la infancia y la adolescencia y contiene multitud de recursos apropiados para la mediación parental.

2. Día de Internet segura[10]: Es un evento que tiene lugar cada año en el mes de febrero, con el objetivo de promover en todo el mundo un uso responsable y seguro de las nuevas tecnologías, especialmente entre menores y jóvenes.

3. Educación 3.0[11]: Es una revista digital dedicada a fomentar el uso de las TIC en el entorno educativo. La información y recursos que ofrece va dirigida, tanto a docentes, como a padres y alumnos.

[7] https://www.apple.com/es/education/k12/
[8] https://open.spotify.com/genre/0JQ5DAqbMKFB2zqQiMq8qz
[9] https://www.pantallasamigas.net/
[10] https://www.is4k.es/programas/dia-de-internet-segura/
[11] https://www.educaciontrespuntocero.com/

Imagen 7. Página web Educación 3.0.

C) Programas de supervisión y control parental

Existen programas que permiten supervisar las actividades que realiza el menor mientras navega en Internet. Permiten bloquear sitios inadecuados, supervisar el tiempo que el menor está en la red y monitorizar desde otro ordenador el ordenador del menor.

Aunque se debe respetar la privacidad de los menores ante todo; esto sería necesario en el caso de que sospecháramos algún problema del menor en la red.

A modo de ejemplo citamos algunos de ellos:

Aula 365[12]

Aula 365 es un portal de aprendizaje dirigido a niños y adolescentes. Es una solución de aprendizaje innovadora con miles de recursos interactivos para aprender jugando y creando dentro de una comunidad que promueve la inteligencia colaborativa y el pensamiento crítico en los niños que además cuenta con muchas actividades todas ellas dirigidas a fomentar los conocimientos del curso escolar. Desarrolla muchas materias agrupadas en diferentes áreas: Matemáticas, Ciencias, Lengua y Literatura, inglés, Nuevas Tecnologías… También enseña técnicas de estudio. Aunque su servicio ha pasado a ser premium, en su canal de YouTube hay una gran variedad de videos y actualmente tienen más de 1’4 millones de suscriptores.

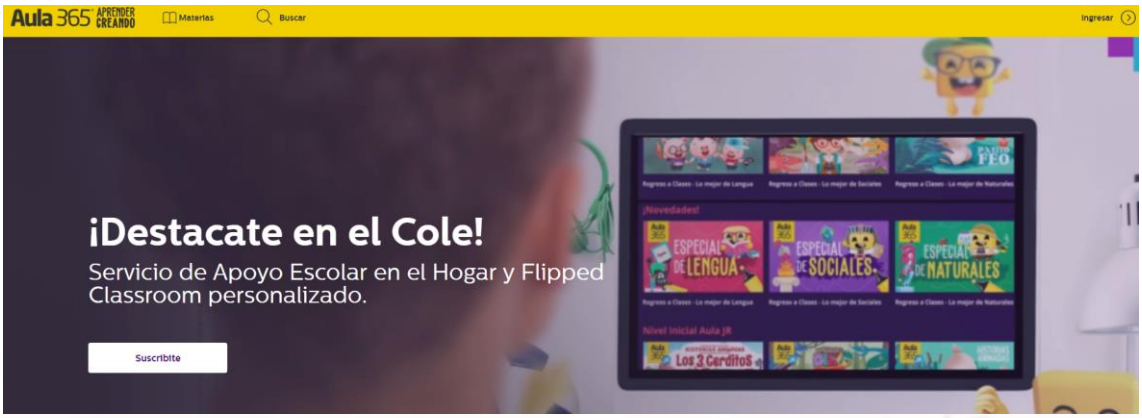

Imagen 8. Página web de Aula 365

Qustodio[13]

Establece límites en el uso de Internet para los niños y jóvenes, informándoles de las actividades que realiza el menor en internet, qué busca, qué redes sociales usa y las aplicaciones. Una de las ventajas es que funciona en ordenadores de mesa, portátiles, dispositivos móviles y tabletas.

[12] https://sitios.educatina.com/Aula365/

[13] https://www.qustodio.com/es/

Por otro lado, también protege a los menores manteniéndolos fuera de contenido problemático, deteniendo las páginas peligrosas de una web –no solo la página inicial– y les filtra el contenido inapropiado de búsquedas.

Muestra si se usa el ordenador para hacer tareas importantes o entretenimiento, bloquea dispositivos cuando se superan los límites, y supervisa redes sociales como Facebook o X (antes Twitter).

También muestra las amistades online de sus hijos y el contenido que comparten, así como monitoriza llamadas y SMS y permite configurar los contactos permitidos o bloqueados.

Qustodio está disponible para Windows, Mac, Android, Kindle y dispositivos iOS.

Existen dos tipos de versiones. La gratuita que protege un único dispositivo e incluye funciones básicas de protección. Y las versiones Premium que pueden proteger múltiples dispositivos, y dan acceso a funciones Premium como Seguimiento de Ubicación, Control de Mensajes de Texto y Llamadas, y Control de Aplicaciones. La lista completa se encuentra en su sitio web.

Para su instalación basta con registrarse dando ciertos datos y una dirección de correo.

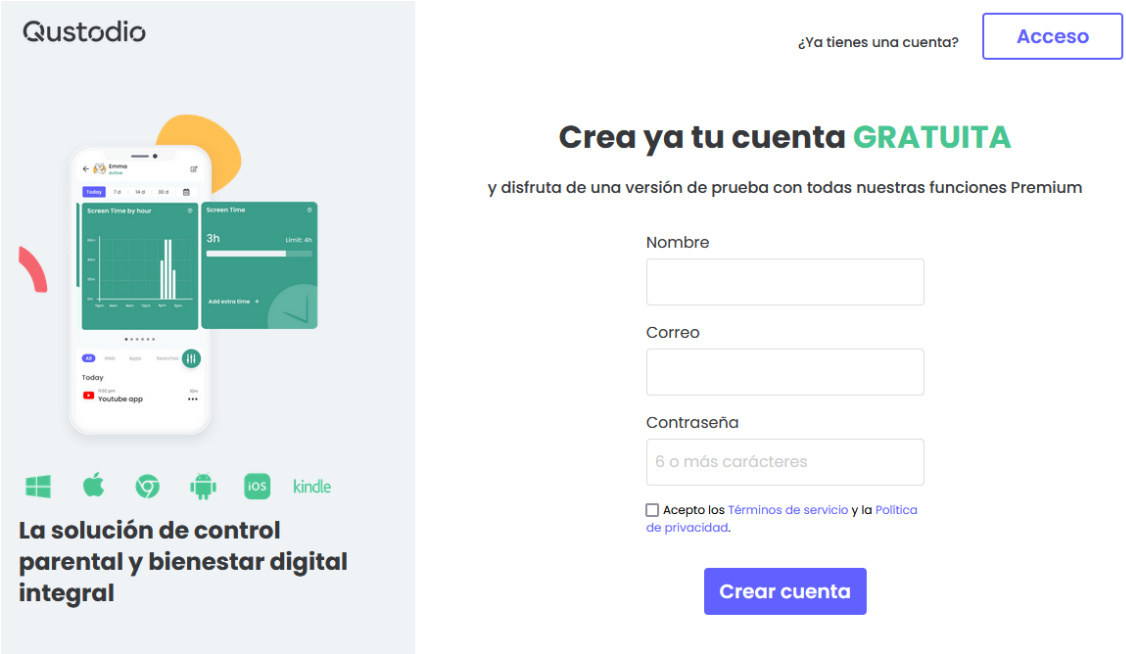

Imagen 9. Crear cuenta en Qustodio.

Al configurar la cuenta, te permite dar de alta a cada uno de los menores que quieres proteger con su año de nacimiento:

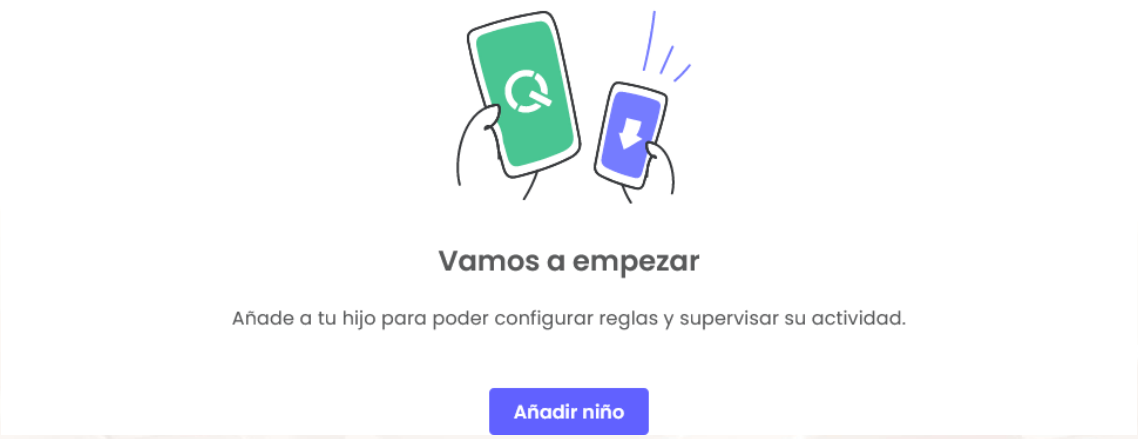

Imagen 10. Bienvenido a Qustodio.

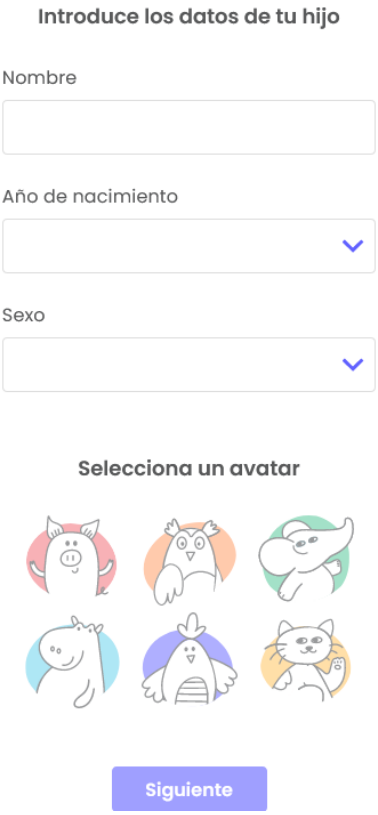

Imagen 11. Añadir datos del niño

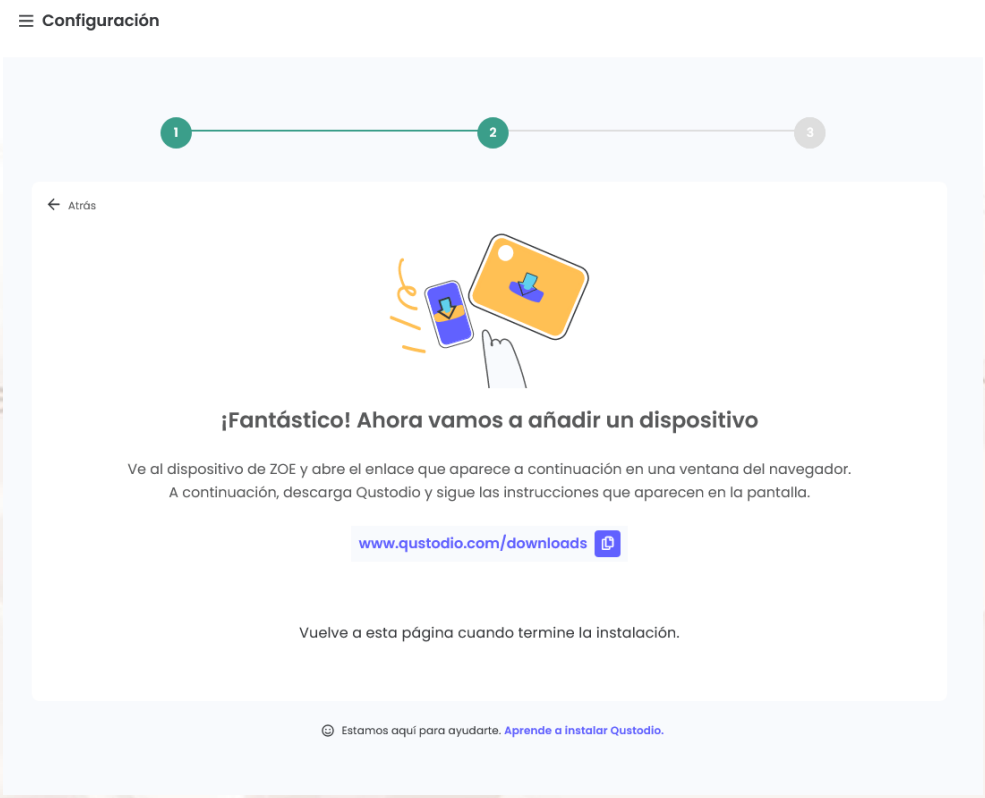

Imagen 12. Pantalla con el link de descarga.

Cuando hayamos dado de alta a un menor, nos aparecerá el link de descarga del programa, que deberemos instalar en los dispositivos que usa el menor. En cada dispositivo deberás instalar este software de manera independiente.

Imagen 13. Enlaces de descarga para cada tipo de dispositivo.

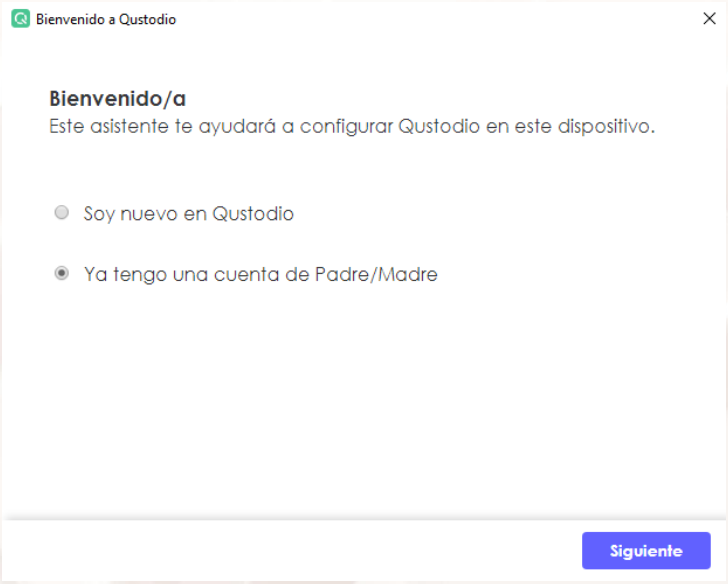

Imagen 14. Pantalla de bienvenida a la aplicación Qustodio instalada en PC

En el proceso de alta e instalación en cada equipo, te permite identificar el nombre del dispositivo y además mantener oculto a los otros “usuarios o menores” que dicho dispositivo está siendo supervisado; opción muy útil para menores con cierto conocimiento digital.

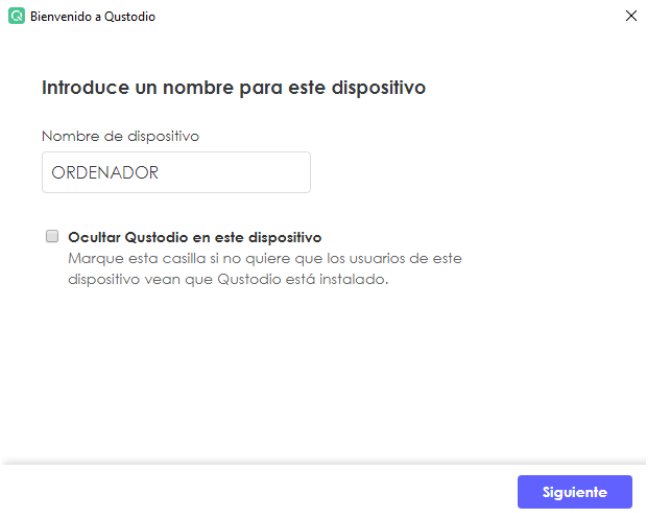

Imagen 15. Ventana para identificar el dispositivo.

Una vez instalado en el dispositivo te pedirá el nombre o usuario con el cual entrará ese menor al mismo. En caso de no disponer de ningún nombre específico, Qustodio te asignará uno.

Una vez configurado cada menor en cada dispositivo, se puede acceder al portal Familiar Qustodio para ver el acceso de cada uno a las redes sociales, a qué portales, el tiempo que destinan en cada uno de ellos y a la configuración especial de la cuenta, para que te lleguen resúmenes diarios de los informes.

Imagen 16. Ventana “Mi familia” en Qustodio.

Acceso desde cualquier ordenador al informe de cada menor y sus accesorios.

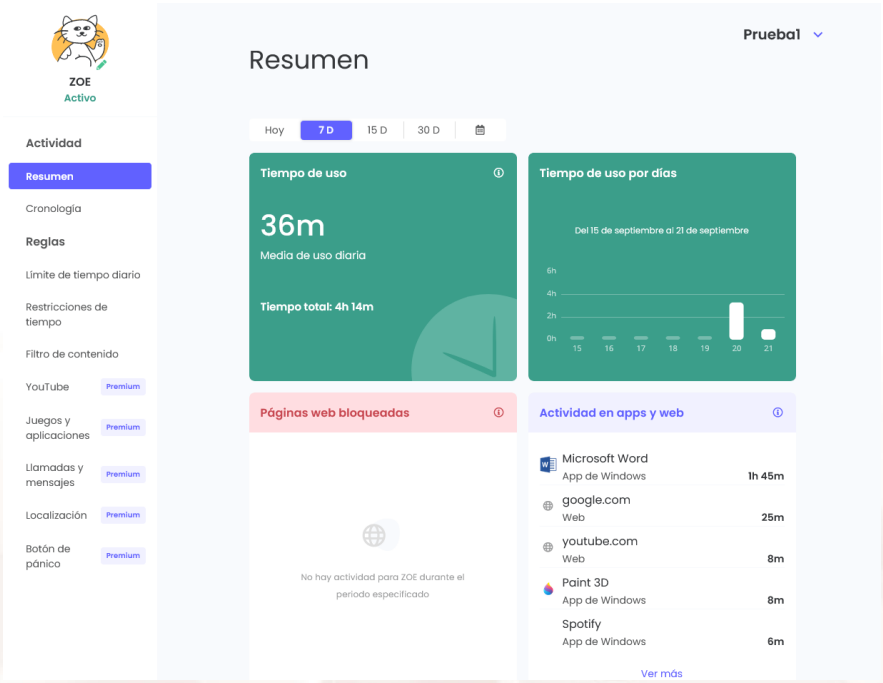

Imagen 17. Información acceso diario de Qustodio.

Configuración para el envío de mails diarios con el informe de cada menor.

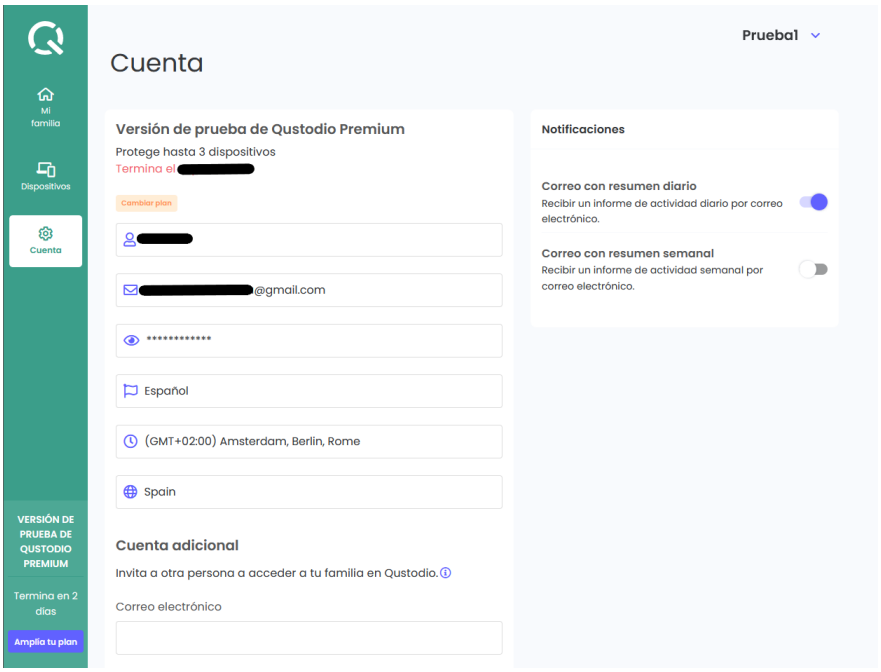

Imagen 18. Página de configuración

Cada report enviado por mail nos ofrece información de la actividad de cada menor:

Imagen 19. Resumen de la actividad en Qustodio.

También nos llega información en otra pestaña de la cronología de actividad en cada página web y desde qué dispositivo:

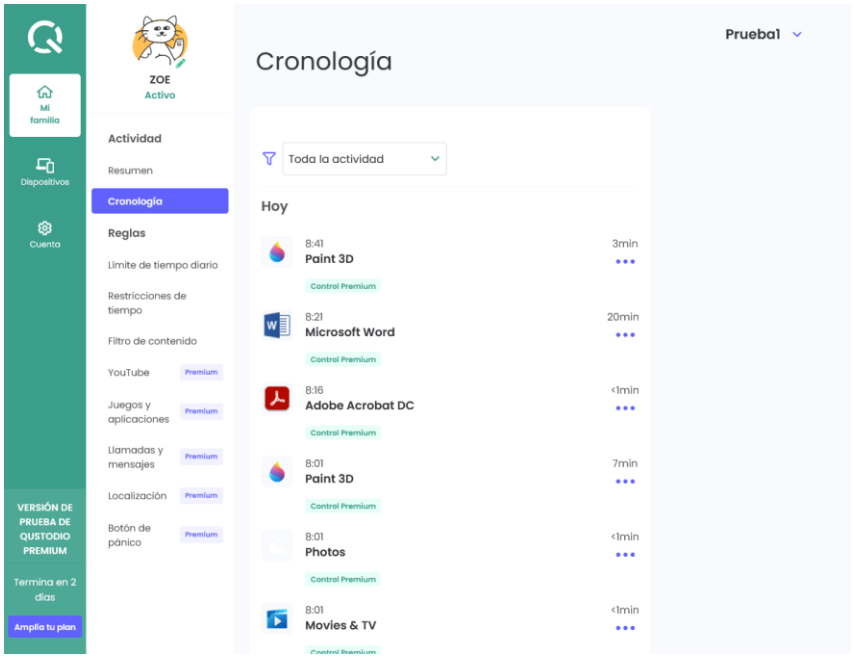

Imagen 20. Cronología de actividad detallada.

Y siempre con la posibilidad de dotar de diferentes permisos y reglas para cada usuario, ya sea limitando el acceso a ciertas páginas o a cierto tipo de contenidos: juegos, redes sociales, apuestas, etc.

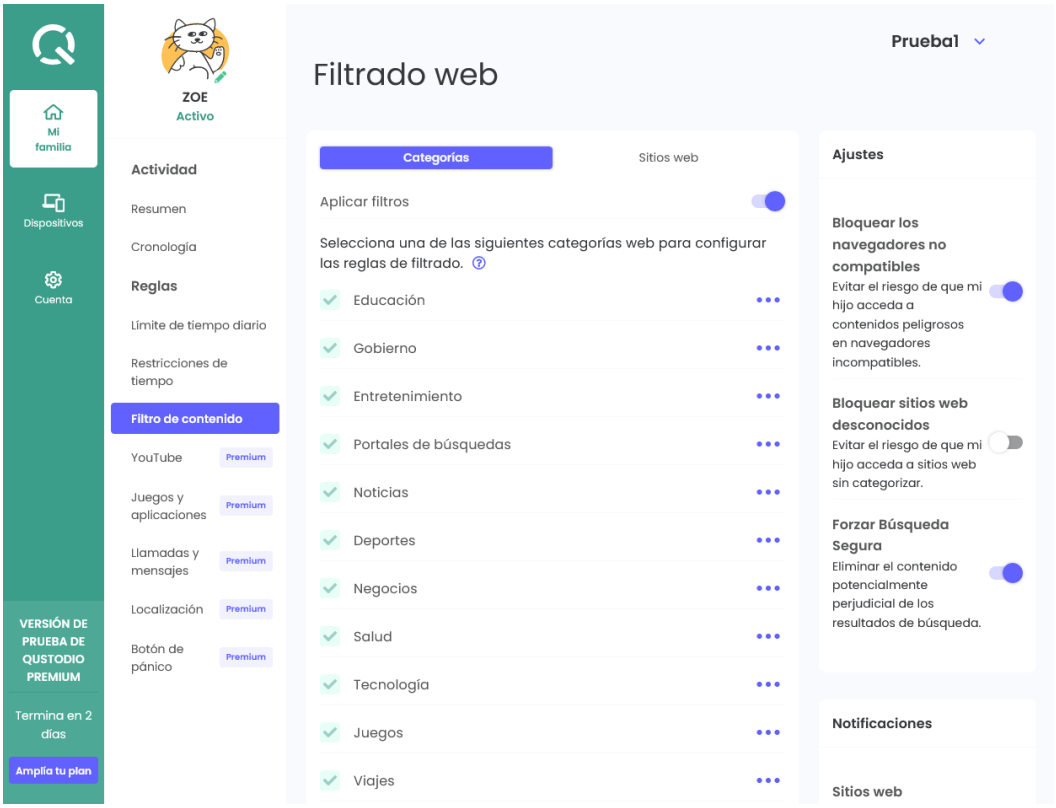

Imagen 21. Reglas y ajustes en Qustodio.

Página que contiene los ajustes que permiten limitar o controlar el tipo de sitios web a los que el/la menor puede acceder, así como los resultados que recibirá de los buscadores.

Una opción muy interesante de Qustodio es la limitación del tiempo de uso de Internet, por franjas, por días y por horarios:

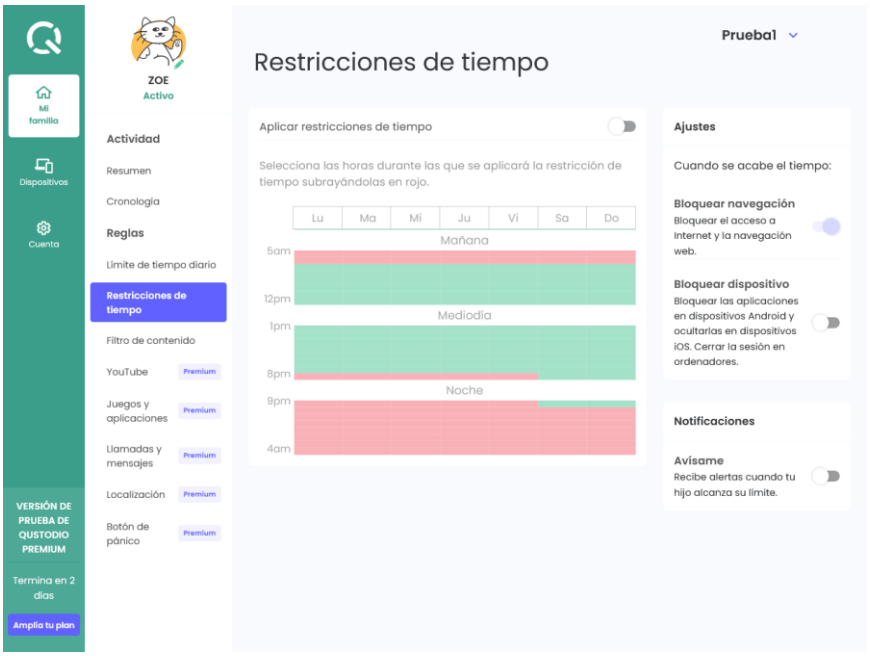

Imagen 22. Limitación tiempo de uso en Qustodio.

1.6. Portales y sitios web dedicados a la protección del menor

Existen iniciativas y asociaciones sin ánimo de lucro dedicadas a la protección del menor en Internet. Esta labor la llevan a cabo mediante la denuncia de sitios web que contengan contenido inapropiado para ellos y la realización de campañas de difusión y sensibilización.

Algunos ejemplos son los siguientes:

1. Menores is4k (Internet Segura For Kids)[14]: Iniciativa de la Oficina de Seguridad del Internauta (OSI) dedicada al fomento de la seguridad en Internet entre los más pequeños.

[14] https://www.is4k.es/

Imagen 23. Página Web de Internet Segura For Kids

2. aseguraTIC[15]: Web destinada a educadores, familias, alumnos, centros educativos y administraciones con el objetivo de proteger a los menores en su interacción con Internet y facilitar a los adultos de su entorno próximo herramientas para ello. En esta web se incluye una amplia colección de materiales en formato digital: contenidos didácticos, guías, unidades didácticas, presentaciones, webs, tareas, juegos, cursos de formación…

3. Safer Internet [16]: El Programa de la Comisión Europea Safer Internet pretende fomentar un uso seguro de la red, así como concienciar sobre diversas cuestiones, como es la distribución de contenidos ilegales y los contenidos no deseados e incluso dañinos

[15] https://intef.es/aseguratic/
[16] https://ec.europa.eu/digital-single-market/en/policies/better-internet-kids

Imagen 24. Página Web de la Comisión Europea.

Discriminación y denuncias

Conviene tratar con los niños y adolescentes el tema de los abusos, el acoso y la "discriminación ", e indicarles qué deben hacer en caso de que conozcan la existencia de alguna amistad víctima de ellos, o cuando a él mismo le suceda.

Deben tener en cuenta que la discriminación es cualquier acto que pretenda excluir o denigrar a una persona o grupo por sus características físicas, sexo, religión, condiciones económicas, orientación sexual, etnia, etc. Estos actos pueden tener lugar en forma de insultos en chats, redes sociales, mensajes en cadena de grupos contra alguien, llamadas acosadoras donde se le exija algo o será reprendido o cualquier otra amenaza que atemorice o minusvalore a la persona.

Los niños y adolescentes deben reflexionar acerca de que tras cada perfil de usuario hay una persona, por lo que cada insulto, amenaza, burla o discriminación tiene consecuencias en la persona receptora de los mismos.

Esos actos están prohibidos por las propias redes, la Constitución Española y las Leyes Nacionales e Internacionales.

Conviene que sepan que deben hacerlo saber a sus padres y/o tutores para ayudarles en la denuncia a las propias redes, plataforma o página web donde esté alojado el contenido, así como a las autoridades pertinentes según sea el caso.

1.7. Tipos de amenaza a la seguridad de los niños en la red

Citamos a continuación una lista de posibles amenazas a la seguridad de los niños y jóvenes en Internet. Se incluyen posibles soluciones para cada amenaza y la forma de evitarlas por parte de padres, tutores o adultos. En algunos casos, estas amenazas pueden afectar a adultos que no vigilen su privacidad lo suficiente.

Este listado está extraído del Instituto Nacional de Ciberseguridad[17], y del Manual “Internet en familia”.

Imagen 25. Página web INCIBE (Instituto Nacional de Ciberseguridad).

[17] https://www.incibe.es/

Cyberbullying

El **cyberbullying** es un tipo de acoso en el que se utilizan los medios digitales para hacer daño a la víctima, conscientemente y de forma repetida en el tiempo.

Solución posible

Trata de evitar alimentar cualquier tipo de respuesta con el *bullie.* Si ignorando la situación no resulta o es inapropiado, informa del problema a las autoridades competentes, como pueden ser la policía local.

Forma de evitarla por parte de los padres/tutores

Los padres pueden ayudar a proteger a sus hijos manteniendo las líneas de comunicación abiertas, así los chicos se sienten cómodos contando los problemas inmediatamente. Enséñeles buenos hábitos para reducir el riesgo de los bullies. Como con otros temas de familia, la clave es mantenerse involucrado.

Pérdida de privacidad

Esto se produce cuando se da, a través de Internet, información sobre la vida personal para poder entrar en determinados espacios comunes o para la utilización “gratuita” de servicios. Los niños y adolescentes desconocen a veces los límites de la información que se debe dar.

Solución posible

- No usar siempre el mismo nombre de usuario y contraseña en todos los servicios que utilice.
- No proporcionar, por principio, datos personales como nombre, dirección, número de DNI, número de teléfono o fotografías suyas o de su familia, a no ser que sea un sitio que garantice la privacidad.

Forma de evitarla por parte de los padres/tutores

Diálogo con sus hijos y hacer saber los límites de la privacidad.

Compras por internet

Internet es, igual que sucede con otros medios de comunicación, un sitio dominado por la publicidad y propaganda comercial igual que la TV. De esta forma, muchas páginas que parecen orientadas a la “educación o el entretenimiento” contienen gran cantidad de anuncios de productos o servicios que no siempre son necesarios ni beneficiosos, e incluso que no son gratuitos. Por otra parte, es cierto que la compra “on-line” en algunas empresas es muy segura, pero comprar en Internet no es siempre seguro.

Solución posible

Cuando vayas a comprar asegúrate que la empresa utiliza un “protocolo seguro” (comprueba que la dirección de Internet comienza con “https://” y que en la parte baja de la página web aparece un candado cerrado). No facilites tus datos personales y bancarios si no estás seguro de la “fiabilidad” de la empresa en la que compras.

Forma de evitarla por parte de los padres/tutores

Haz saber a los niños y jóvenes que no están autorizados a comprar por Internet, sin el permiso y consentimiento de un adulto.

Imagen 26. Protocolo de páginas de compra segura y de acceso a sitios protegidos.

Acoso online

Este tipo de abuso se produce cuando se acosa a un niño/a a través de Internet, a través de programas de mensajería instantánea o por correo electrónico.

Suele ser una continuación del acoso escolar, pero utilizando otros medios y no se deben subestimar los problemas que el acoso causa.

Solución posible

Se debe observar cómo chatea el pequeño, las caras que pone, las reacciones tras entrar en sus dispositivo móvil o PC, si se siente intimidado, se vuelve agresivo, huidizo, etc. Es mejor posicionar el ordenador en una zona común; aunque con los móviles esta solución es más complicada. Debe haber una gran comunicación padres-hijos-tutores.

Forma de evitarla por parte de los padres/tutores

No permitas que los niños o niñas envíen mensajes o e-mails de acoso a otros niños o niñas; han de comprender que el acoso provoca muy serios perjuicios. Si son sus hijos el objeto del acoso de compañeros y compañeras de la escuela, habla con el tutor o tutora.

Contacto a través de internet: pedofilia y pornografía infantil

Existe el riesgo de que personas con intereses ocultos puedan establecer alguna vía de contacto con sus niños y niñas, generalmente por mediación de algún sistema chat, sin que el menor sea consciente de ello.

Solución posible

- No enviar archivos adjuntos de fotos.
- Asegurarse de con quién se está hablando.
- No dar datos físicos ni direcciones.
- No informar de los horarios que tiene.

Forma de evitarla por parte de los padres/tutores

Inscríbase y participe en los mismos chats que los niños para conocer qué se dice y de qué tratan. Debería hacerles entender y aceptar a los menores que no pueden proporcionar información personal (fotografías, nombre, número de teléfono, dirección, etc.) a nadie en un chat o en internet, sin su previo conocimiento. Nunca un menor puede encontrarse en persona con alguien que sólo conoce online, sin su conocimiento o presencia.

Los propios contenidos de la red

Se trata de un riesgo que no suele ser tan conocido como los anteriores. Podemos encontrar páginas desde las que se incita a la anorexia y a la bulimia, otras que nos ofrecen contenidos racistas, xenófobos, pornográficos o aquellas otras en las que determinadas sectas pretenden reclutar a nuevos miembros.

Solución posible y forma de evitarla por parte de los padres

- Elabora un código de uso de Internet para toda la familia, con el tiempo de uso permitido y tipo de información a la que se puede acceder.
- Instala en el ordenador algún sistema de filtro que limite el acceso a páginas con información pornográfica o de otros tipos no aptas para menores.
- Utiliza sistemas de búsqueda en Internet especialmente orientados a menores.
- Si se accede a alguna página pornográfica, habla sobre la misma con el menor en lugar de ocultarla o culpabilizarle.
- Comprueba el historial del navegador de los niños y habla con ellos si encuentras páginas de estos tipos.
- Solicita información sobre sitios de Internet con contenidos interesantes para la formación y educación de tus hijos e hijas y visítalos con ellos.
- Si alguna vez encuentras sitios con contenidos como los mencionados, conviértelos en motivo de reflexión, discusión y debate con tus descendientes.

Imagen 27. Decálogo de buenas prácticas con el uso de las tecnologías digitales.

02. Mensajería instantánea

La mensajería instantánea (conocida también en inglés como IM) es una forma de comunicación en tiempo real entre dos o más personas basada en texto e iconos, con la posibilidad de incorporar fotografías, enlaces y emoticonos. Estos mensajes son enviados a través de dispositivos conectados a una red como Internet, y se pueden realizar desde el ordenador o PC, Smartphone o cualquier otro dispositivo móvil.

En general, casi todas las aplicaciones de mensajería instantánea tienen su versión para ordenador y para dispositivos móviles; pudiendo intercambiar mensajes desde distintos dispositivos simultáneamente entre varios interlocutores: Ordenador-Smartphone; Smartphone-Tablet; Tablet – Ordenador, y así sucesivamente...

La mensajería instantánea requiere el uso de un cliente (programa que se instala en el equipo o una aplicación en dispositivos móviles) de mensajería instantánea que realiza el servicio y se diferencia del correo electrónico en que las conversaciones se realizan en tiempo real y de manera instantánea. Muchas de ellas permiten el envío de ficheros, fotografías, emoticonos, etc., e incluso algunas como WhatsApp o Skype llamadas a través de videoconferencias.

La mayoría de los servicios ofrecen el "aviso de presencia", indicando cuando el cliente de una persona en la lista de contactos se conecta o en qué estado se encuentra, si está disponible o no para tener una conversación, si está conectado pero ausente, etc.

Los clientes de mensajería instantánea más utilizados son Skype[18], WhatsApp[19] , Line[20] y Telegram[21]; disponiendo todos de versión móvil y de escritorio.

[18] https://www.skype.com/es/
[19] https://web.whatsapp.com/
[20] https://line.me/es/
[21] https://web.telegram.org

El chat (término proveniente del inglés que en español equivale a **charla**), también conocido como cibercharla, designa una comunicación escrita realizada de manera instantánea a través de Internet entre dos o más personas.

Es un hábito muy extendido entre nuestros adolescentes y jóvenes en la actualidad, estableciéndose como una forma de ocio muy popular. Lo habitual es que estén conectados entre sí y con muchas personas formando **redes** muy amplias de contactos estableciendo relaciones mediadas por el ordenador y basadas en pequeños textos o comentarios.

Actualmente, gran cantidad de las conversaciones de las que se producen entre adolescentes es mediante teléfonos inteligentes (*Smartphone*), tabletas y demás **dispositivos móviles**. La posibilidad de conectar estos aparatos a Internet, ya sea mediante una red wifi o a través de tarifas de datos, propicia que se puedan enviar y recibir mensajes en cualquier momento y lugar. Este hecho hace que muchas veces sea complicado para los padres conocer con qué personas se comunican sus hijos y qué tipo de contenido recibe o envía. Es por ello que es importante extremar la precaución a la hora de permitir a nuestros hijos usar estos aparatos.

2.1. Recomendaciones y buenas prácticas

El Chat puede ofrecer a los adolescentes la posibilidad de mantener un contacto permanente con sus amistades, pero también con los padres y familiares. Con la pantalla encendida de forma constante a través del chat se crean un lugar de pertenencia y un espacio de referencia que brinda nuevas formas de acceso a una identidad común. Participar o no de estos encuentros virtuales puede ser la clave de estar dentro o fuera de cierta realidad juvenil condicionada por la tecnología.

Al chatear, interactúan como si hablaran entre ellos y no como si se estuvieran escribiendo mensajes; la sintaxis y el estilo, son muy cercanos a una charla común, una conversación telefónica o cara a cara, pero dentro de un nuevo espacio psicosocial, que es básicamente de encuentro. En este entorno, la

palabra (escrita) está retomando un valor que parecía haber perdido desde el surgimiento de la televisión. La modalidad de escritura en el ciberespacio se dice que es una modalidad más bien irreverente, desprejuiciada, libre de ataduras y estilos; el Chat es señalado como uno de los responsables de los malos hábitos de escritura de los jóvenes y la desvalorización del lenguaje escrito. El tono utilizado en la comunicación tecleada suele ser informal, y sus contenidos tienden a estar atravesados por lo casual y el juego.

Aunque se recurra al alfabeto para la comunicación, tiene características que lo separan claramente del tradicional género escrito. Esta escritura está afectada por modos de comunicar propios de la Red: abreviaciones, simbologías, emoticonos, etc.

Por ejemplo:

Imagen 28. Emoticonos.

La serie sigue hasta juntar varias docenas y, seguramente, seguirán apareciendo, popularizándose y desapareciendo al ritmo frenético que impone la red.

Se ha conformado un nuevo lenguaje que deja a una generación de padres "**iletrada**" en el uso de estas tecnologías. Hay poco cuidado en la escritura de las frases, ausencia de corrección, rapidez en las líneas y saltos temáticos, en lugar de mantener el orden consecutivo y lineal.

2.2. Riesgos de la mensajería instantánea

Se ha instalado en la sociedad un debate respecto de si el lenguaje del chat "empobrece" la capacidad de los jóvenes para **expresarse y trasmitir ideas**. Es obvio que resulta complicado controlar la manera de expresarse que tienen los jóvenes, pero quizás una buena manera de paliar este déficit es promoviendo la costumbre de la lectura “convencional” entre ellos.

Han venido surgiendo grupos sociales en torno a las nuevas tecnologías en los que se observan comportamientos que pueden verse total o parcialmente en nuestros jóvenes. En Japón ha surgido un grupo de jóvenes que viven en un mundo virtual, los llamados *hikikomoris.* Se trata de adolescentes que se sienten incapaces de cumplir los roles que se esperan de ellos, reaccionando con aislamiento; la única forma de interacción social que tienen es gracias a su computadora; rehúsan abandonar la casa de sus padres y se pueden llegar a **encerrar** en una habitación durante meses.

Se estima que podría haber un millón de *hikikomoris* en Japón (uno de cada diez jóvenes), la mayoría de ellos varones. Llegan a tener dependencia de los ordenadores y estos se convierten en instrumentos para crear dependencias antisociales.

Se pueden alterar los niveles de **confianza y honestidad**; hay cierto nivel de problemas con los estudios y con la familia; les encanta chatear hasta la madrugada y no acatar las reglas del hogar.

Los que están más expuestos son los **niños**; los mayores pueden cerrar y salir de la sesión, pero ellos tienen curiosidad. Muchas personas pueden aprovecharse de la tecnología para actuar mal. La relación, la convivencia interpersonal y hablar cara a cara, pueden estar en riesgo o perdiéndose. Chatear con personas que están lejos, te acerca, pero con los de cerca, te aleja. Los padres no están junto al niño y éste experimenta por sí mismo.

Este es un ejemplo de riesgos de la mensajería instantánea, al que como adultos se debe estar atento, para tratar de evitarlo y/o corregirlo.

Otro riesgo importante que conlleva la mensajería instantánea es que personas con intereses ocultos, desconocidos, o adultos haciéndose pasar por menores puedan establecer contacto con los niños/as, por mediación del chat, sin que el menor sea consciente de sus intenciones.

Para este caso es muy importante saber bloquear en todas las aplicaciones (como veremos más adelante) cualquier posibilidad de que un usuario que no sea un contacto previamente aceptado pueda intercambiar mensajes con el niño.

Otra opción es inscribirse en los chats que mantiene el niño para conocer qué se dice y de qué tratan; aunque es una opción difícil en algunos casos cuando la mensajería no es grupal.

2.3. Ventajas de la mensajería instantánea

Algunas de las ventajas que ofrece la mensajería instantánea son:

- El chat amplía las posibilidades, te permite estar más cerca de mucha gente, puedes mantener una conversación a distancia con amigos o desconocidos, sin importar el espacio.
- Sirve para hacer trabajos en equipo: cada quien en su casa y todos en un mismo canal; no hay pérdida de tiempo en la reunión. Pueden hacer más de una cosa a la vez, es cuestión de simultaneidad y se reduce el tiempo. Es muy importante la interactividad constante con la gente y las posibilidades de nuevos encuentros.
- Un ejemplo claro son los grupos de WhatsApp, que en los últimos años han proliferado mucho para la conversación síncrona y asíncrona entre grupos de profesionales, amigos, familiares, padres de un grupo de alumnos. E incluso otros de ellos que se crean temporales para organizar una fiesta, evento o acordar un regalo.
- Te permite ser tú mismo, sin la necesidad de exponerte públicamente. Puedes decir cosas que normalmente no te atreves a decir cara a cara,

jugar momentáneamente a ser otra persona, sin sentir que se corre peligro.

Las salas de chat públicas vienen siendo desde hace años una nueva vía donde gente desconocida interacciona, como algo propio de la tecnología y hace que las nuevas generaciones interrelacionen de una forma abierta y sin tapujos. Si uno no tiene chat, parece que se aísla; es como una necesidad, pero no una adicción; es solo una nueva forma de comunicación.

No es que pierdan el tiempo, es como una sala llena de amigos. Debes tener respeto por tu propia **intimidad**.

La gente piensa que el Chat crea adicción y que no tienes privacidad, porque no sabes con quién hablas, pero ellos no lo perciben como un verdadero problema. Otros piensan que la tecnología hace indiferente a la juventud, pero ellos no lo creen así. La tecnología puede usarse para **fines positivos**, todo depende de tus valores; influye mucho la educación en casa o en la escuela.

Para los jóvenes el aislamiento no existe, la vida social continúa y este medio se utiliza como una forma de entretenimiento, es una herramienta que facilita la transferencia de información. Es solo una nueva tecnología a la que **el joven se adapta**, sin deformar realmente sus actividades; la ha convertido en una forma de vida, con el objetivo de facilitar y agilizar la comunicación.

Es también un **entretenimiento**. A pesar de que existe el riesgo, al no conocer a la persona que está del otro lado, esto no parece ser un inconveniente, desarrollan su conversación como si tuviesen la certeza de quién está del otro lado. Con el chat la gente no siente que está siendo invadida o manipulada por este medio. El problema se da solo en aquellos que son poco sociables y que naturalmente se encierran.

La sociedad debería buscar que las nuevas generaciones sean plenamente conscientes de su integridad, dignidad e intimidad. El adolescente debe vivir otras actividades, saber que no solo existe el mundo virtual, que también existe el **mundo físico** y el de los valores.

2.4. WhatsApp

Imagen 29. Logotipo de la aplicación de WhatsApp.

WhatsApp[22] es una aplicación de mensajería para teléfonos inteligentes, que envía y recibe mensajes mediante Internet, complementando servicios de mensajería instantánea, servicio de mensajes cortos o sistema de mensajería multimedia. Además de utilizar la mensajería en modo texto, los usuarios de la libreta de contacto pueden crear grupos y enviarse mutuamente imágenes, vídeos y grabaciones de audio.

El Servicio de mensajería instantánea WhatsApp anunció el 12 de febrero del 2020 que cuenta con 2.000 millones de usuarios activos en el mundo. Solo en España tiene 25 millones de usuarios.

Aunque esta no se considera una red social, es un canal de comunicación muy importante.

Funciones de WhatsApp

Mensajes

Envía mensajes gratis a tus amigos y familiares. WhatsApp usa la conexión a internet de tu teléfono móvil para enviar mensajes y así evitar cargos de SMS.

Chat de grupo

Mantiene en contacto con el grupo de personas que más te importan, como familia o compañeros de trabajo. Con los chats de grupo se pueden compartir mensajes, fotos, y videos con hasta 512 personas a la vez. También se puede dar un nombre a tu grupo, silenciarlo, personalizar las notificaciones, y mucho más.

[22] https://www.whatsapp.com/

WhatsApp para el ordenador

Con WhatsApp para web y escritorio se pueden sincronizar todos tus chats con tu ordenador para que puedas enviar mensajes usando el dispositivo de tu preferencia.

Llamadas y videollamadas de WhatsApp

Con las llamadas, se puede hablar con amigos y familiares gratis, incluso si están en otro país. Y con las videollamadas gratis, se pueden tener conversaciones cara a cara cuando la voz o un texto no es suficiente. Las llamadas y videollamadas de WhatsApp utilizan la conexión a Internet de tu teléfono, en vez de los minutos de voz de tu plan de telefonía móvil, así que no hay que preocuparse por cargos de llamadas costosos.

Comparte fotos, videos y documentos de manera instantánea.

Política de WhatsApp

Durante el mes de noviembre del año 2019 WhatsApp comenzó a bloquear a los grupos que violen normas de comportamiento. Igualmente está eliminando la cuenta de aquellas personas que tengan chats grupales con nombres sospechosos. WhatsApp quiere acabar con cuentas que tengan nombres inoportunos o vejatorios, por ejemplo, si contienen términos relacionados con la pornografía infantil, terrorismo o racismo. También comienzan a ser expulsados determinados usuarios.

Videollamadas

Las videollamadas o videoconferencias son una actividad que permite una comunicación simultánea bidireccional de audio y vídeo en tiempo real. Existen servicios y aplicaciones gratuitas que permiten realizar estas videollamadas con nuestros contactos y chatear a la vez con ellos.

Los servicios que permiten estas comunicaciones incorporan las opciones de intercambiar archivos, mensajes escritos, intercambiar la imagen de la pantalla y de llevarlas a cabo con grupos de varias personas, desde dispositivos móviles u ordenadores de sobremesa.

La pandemia y la consiguiente implantación rápida del teletrabajo, puso en el punto de mira este tipo de servicios que experimentaron un crecimiento exponencial.

Una aplicación muy extendida por su facilidad de uso y su gratuidad es Skype. A ella dedicaremos el siguiente epígrafe. Por su potencia, usabilidad y gran presencia destacamos además los siguientes servicios de videoconferencia:

- Zoom[23]. Es un programa de software de videoconferencia con servicio de chat que, en su versión gratuita, permite hasta 100 participantes al mismo tiempo, con una restricción de tiempo de 40 minutos. Es compatible con los principales sistemas operativos tanto de ordenadores como de móviles y además de para reuniones, también se utiliza para albergar eventos tales como congresos o webinars. En 2020 en fue la quinta app más descargada con 477 millones de descargas.

- Meet[24]. Es la herramienta de videoconferencia online de Google. Se trata de un desarrollo del anterior servicio llamado Hangouts que ha incluido en los últimos dos años muchas mejoras y utilidades para competir en el mercado. Como todos los servicios de Google

[23] https://zoom.us/

[24] https://meet.google.com/

Workspace, las versiones de pago ofrecen más prestaciones que las gratuitas.

- Teams[25]. La versión del paquete ofimático y de trabajo colaborativo de Microsoft. Permite hacer llamadas o videoconferencias con personas de la misma institución o de fuera de la misma, mantener conversaciones privadas con una persona en particular y reuniones con hasta 1000 personas a la vez. Al igual que Zoom o Meet (en la versión de pago), las reuniones pueden ser grabadas y los asistentes pueden comunicarse a través del chat y compartir su pantalla con el resto de asistentes.

3.1. Skype

Skype es un programa gratuito que utiliza la última tecnología P2P (punto a punto) para poner al alcance de todas las personas del mundo conversaciones de voz económica y de alta calidad. Skype permite hablar o chatear **gratuitamente** con otros usuarios de Skype de cualquier parte del mundo.

Instalación de Skype

Skype se puede descargar gratuitamente en la actualidad, en la siguiente dirección [26].

25 https://www.microsoft.com/es-es/microsoft-teams/group-chat-software?ms.url=microsoftcomteams&rtc=1
26 https://www.skype.com/es/get-skype/

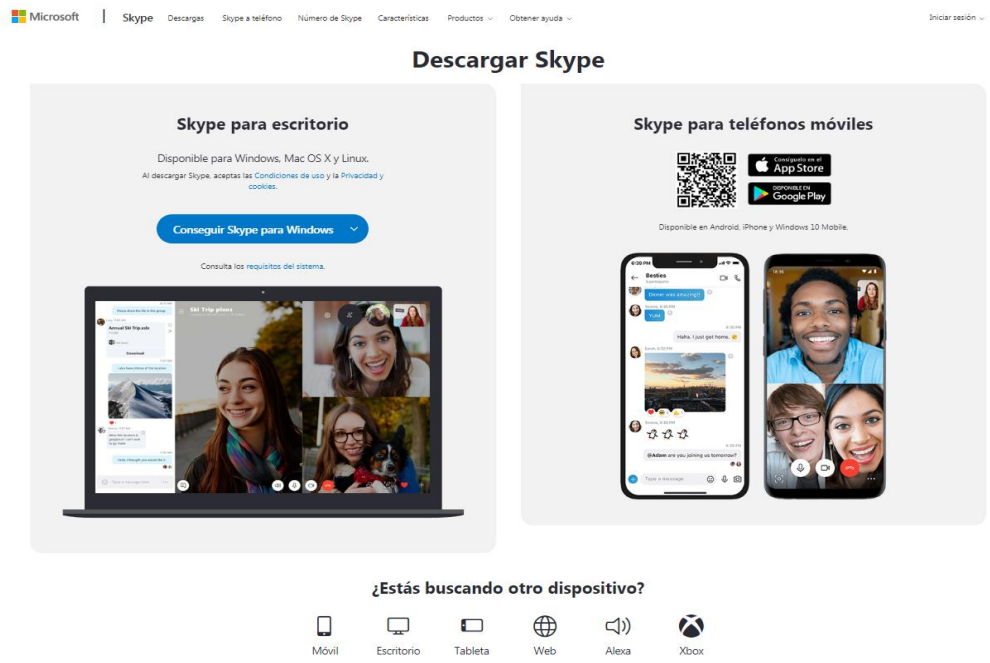

Imagen 30. Comenzar a usar Skype, iniciamos la descarga de Skype.

Para descargarlo en su equipo, simplemente hay que clicar en el vínculo de descarga. Guarda el archivo de instalación en tu equipo en algún lugar **fácil de recordar**, como, por ejemplo, el escritorio. Una vez que el archivo se haya descargado completamente debes **ejecutarlo** para iniciar la instalación de Skype en tu equipo. Estos son los datos que debes indicar en el proceso:

- Escoge el **idioma** que deseas utilizar en la instalación y después elige la opción “Acepto los términos del acuerdo”. Después clica Siguiente.
- Selecciona la **carpeta destino** donde se instalará Skype. Se recomienda el que sale como predeterminado, después clica en Siguiente.
- Selecciona si desea instalar la **barra de Google** en Internet Explorer, después clica en Siguiente.
- Ya está instalado Skype en tu ordenador, pulsa en “Inicia Skype” para continuar.

Inicio de Skype por primera vez

Puedes usar Skype identificándose con su cuenta de Microsoft o de Skype. En el caso de que no dispongas todavía de una cuenta de usuario de Skype, deberás pulsar en el botón "**Crear una cuenta**". Al hacerlo, el navegador nos abrirá una nueva ventana con el siguiente formulario:

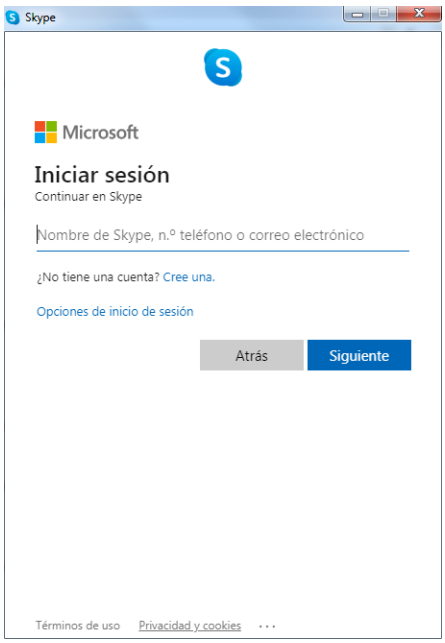

Imagen 31. Inicio de sesión en Skype.

En caso de que tengas que crearte una nueva cuenta de Skype, la información de los campos "Nombre de usuario" y "Contraseña" es obligatoria para usar el *software.* Puedes escoger cualquier nombre, pero debe tener un mínimo de 6 caracteres. Si otro usuario ya ha escogido ese nombre, deberás elegir otro. Has de aceptar el acuerdo de licencia de usuario.

Configuración de Skype

Tras la instalación, el programa suele estar ya configurado para empezar a realizar llamadas, tanto de voz, como de vídeo. No obstante, en el menú **Configuración** que se muestra en la parte izquierda disponemos de varios ajustes con los que podremos configurar Skype **a nuestro gusto**.

Además, Skype nos ofrece la opción de probar el audio, seleccionando la "**Audio y vídeo**", así podemos comprobar que el altavoz y la cámara web funcionan correctamente.

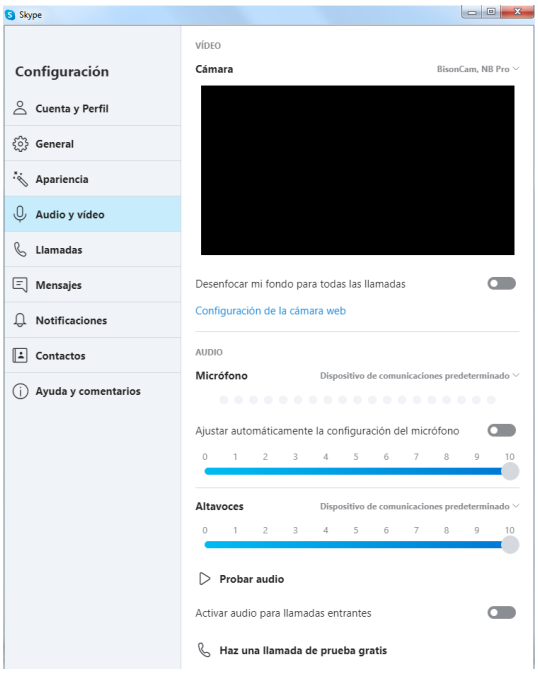

Imagen 32. Hacer audio de prueba.

Para hacer esta prueba pulsamos **Probar audio**. Se iniciará una llamada en la que primero oiremos una locución grabada (con esto comprobamos que los altavoces o auriculares de nuestro equipo funcionan bien). En caso de fallar esta prueba es recomendable **revisar los ajustes de audio** mencionados anteriormente.

Cómo buscar y agregar un nuevo contacto

En cuanto a la sección de contactos, podemos agregar amigos automáticamente mediante dos opciones: usando tu libreta de direcciones, en la que Skype añadirá automáticamente gente que conoces a tu lista de contactos; o, sin usar dicha libreta de direcciones, por lo que tendrás que encontrar contactos nuevos y agregarlos manualmente. Además, desde esta sección se permite administrar los contactos bloqueados.

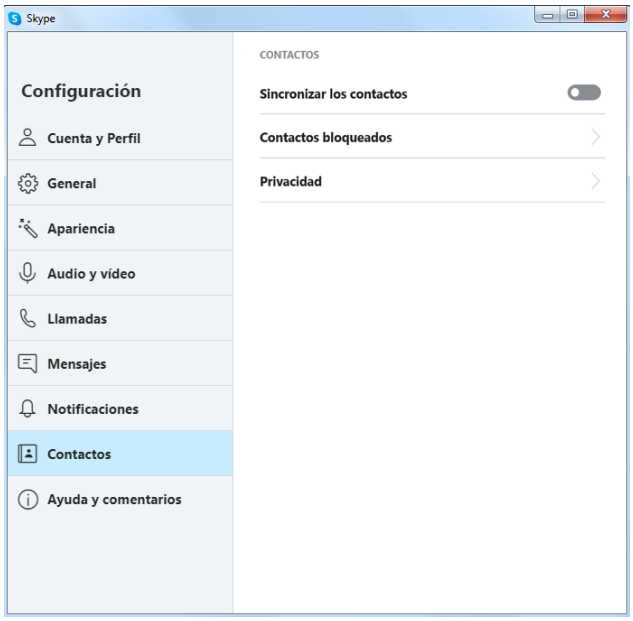

Imagen 33. Registro y contactos.

Cómo usar Skype Chat

Skype Chat permite chatear con diferentes contactos **a la vez**. Si seleccionamos un usuario en la lista de contactos y clicamos el botón Chat. A continuación, se abrirá una ventana a partir de la cual puede comenzar a chatear.

Cómo realizar una llamada

Con Skype las llamadas se pueden realizar de dos maneras, solo **con voz** o **con voz y vídeo** (si nosotros y la persona a quien llamamos dispone de webcam). En cualquier caso, la llamada se realiza de la misma manera: seleccionamos al contacto y pulsamos el botón del teléfono verde.

En el caso de una videoconferencia, veremos una ventana grande con el vídeo de nuestro contacto y debajo otra más pequeña con nuestro vídeo.

Si la ventana de nuestro vídeo no aparece ir al menú “**Configuración”**.

Cómo realizar una conferencia

Skype nos permite llamar y hablar con **varias personas a la vez**; a esto se le llama conferencia. Para iniciarla clica en el botón “Videollamada”. Luego,

selecciona los contactos que deseas agregar a la nueva conferencia y pulsa el botón “Inicio” para iniciar la conferencia.

Para **terminar** cualquier llamada, ya sea de voz o vídeo, simplemente clica en el botón rojo donde aparece el símbolo del teléfono colgado.

Cargar dinero en nuestra cuenta Skype (opciones de pago)

Si queremos tener algunos servicios añadidos (envío de SMS a móviles, llamadas a teléfonos fijos y móviles), tenemos que tener crédito en nuestra cuenta Skype.

Para cargar nuestra cuenta Skype con saldo, tenemos que clicar en la opción “**Cuenta y Perfil**” dentro de la ventana de “**Configuración**” eligiendo en la sección “**Administrar**” la opción “**Tu cuenta**” donde puedes gestionar tu crédito de Skype.

Nos da opción de comprar 5€, 10€ o 25€ euros, y diferentes **posibilidades de pago**: tarjeta de crédito, Moneybookers, transferencia bancaria, PayPal, etc.

Para **cambiar** la forma de pago pinchamos sobre la opción "Cambiar forma de pago".

Las más importantes de las diferentes **formas de pago** que existen:

- PayPal.
- Tarjeta de crédito.
- Paysafecard.
- Google Pay.
- Transferencia.

Una vez hemos elegido nuestra forma de pago y le damos a “Siguiente”, deberemos seguir los pasos de dicha forma de pago para terminar de cargar nuestra cuenta. Cuando se haya cargado, nos llegará un mensaje por correo electrónico avisándonos de la carga y del importe que tenemos.

Configuración de la seguridad de Skype

Es muy importante dedicar un tiempo para revisar las opciones de seguridad y privacidad que nos permite configurar dicha aplicación.

Puede ir a dicha configuración desde la Opción de **"Configuración**" haciendo clic en la opción "**Contactos**" o desde el menú de inicio: "Skype _ Privacidad".

Se abre un menú general que permite configurar:

- **General**: la configuración de sonido, vídeo, alertas.
- **Privacidad**.

Donde se puede modificar la "Configuración de privacidad" y el listado de "Personas Bloqueadas".

Entre las opciones de "privacidad" se debe señalar que se permitan llamadas, vídeos, pantallas compartidas y mensajes instantáneos de: "solo personas en mi Lista de Contactos".

Así se impide que cualquier persona no autorizada o desconocida pueda llamar, enviarnos mensajes o videollamadas y se evita posibles acosos o cualquier forma de publicidad o spam de personas ajenas a nuestra lista de contactos. De esta manera, nos aseguramos que cualquier contacto debe enviarnos una solicitud o autorización previa para autorizarla a formar parte de nuestra lista de contactos y aceptar de esa manera sus llamadas, chat o videoconferencias.

Existe una opción dentro de este menú que puede resultarnos interesante activar como mentores, padres o tutores de un menor que utiliza Skype para chatear o llamar a sus amigos.

Esta opción es la que permite "Guardar historial "de los mensajes /conversaciones que haya mantenido el usuario o menor con cualquier persona o grupo de su lista de contactos. Así se puede en cualquier momento revisar conversaciones que se hayan establecido por un periodo de tiempo e incluso "indefinidamente".

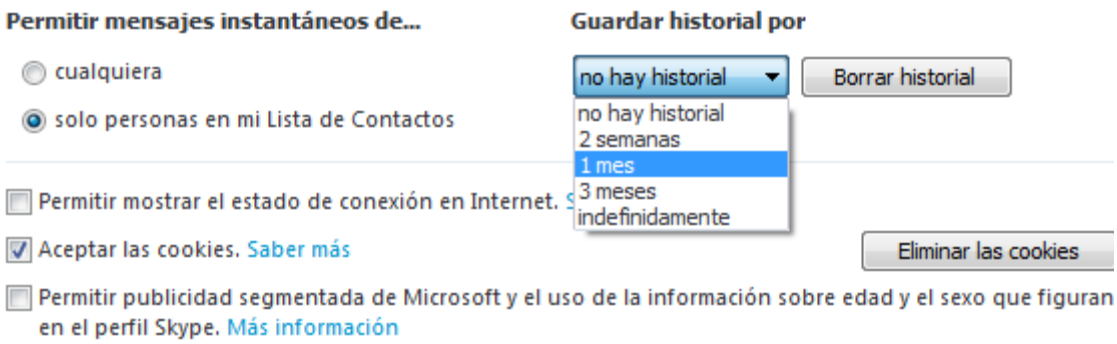

Imagen 34. Opciones de historial Skype.

Si se accede a la opción de “personas bloqueadas” se puede ver el listado de personas que hemos bloqueado, y te permite incluir nuevos usuarios a los que bloquear, y, por tanto, no permitirle verte conectado en Skype, ni entablar conversación o solicitarte autorización para ello.

Skype ofrece un apartado en su web destinado exclusivamente a ofrecer información de cómo proteger tu seguridad y privacidad en Skype y en internet[27].

[27] https://support.skype.com/es/faq/FA34649/como-proteger-tu-seguridad-y-privacidad-en-internet

04. ¿Qué es el correo electrónico?

4.1. Conceptos básicos

El correo electrónico, o e-mail en inglés (electrónica mail), es un servicio de red que permite a los usuarios enviar y recibir mensajes rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos. Estos mensajes pueden llevar ficheros adjuntos tales como imágenes, hojas de texto, hojas de cálculo, etc.

Principalmente se usa este nombre para denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías. Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales. Su eficiencia, conveniencia y bajo coste (con frecuencia nulo) están logrando que el correo electrónico desplace al correo ordinario para muchos de los usos habituales.

Dirección de correo

Una dirección de correo electrónico es un conjunto de palabras que identifican a una persona que puede enviar y recibir correo. Cada dirección es única y pertenece siempre a la misma persona.

Un ejemplo es persona@servicio.com (se leería persona arroba servicio punto com). El signo @ (llamado arroba) está presente en todas las direcciones de correo y divide a esa en dos partes: el nombre de usuario, a la izquierda de la arroba (en este caso persona) y el dominio a la derecha de la arroba (en este caso, servicio.com). La arroba también se puede leer "en", ya que persona@servicio.com identifica al usuario persona que está en el servidor servicio.com (indica una relación de pertenencia).

Una dirección de correo se reconoce fácilmente porque siempre tiene la @; en cambio, una dirección de página web no. Por ejemplo, mientras que http://www.servicio.com/ puede ser una página web en donde hay información (como en un libro), persona@servicio.com es la dirección de un correo; es decir, un buzón a donde se puede mandar correos.

Lo que hay a la derecha de la arroba es precisamente el nombre del proveedor que da el servicio de correo y, por tanto, es algo que el usuario no puede cambiar. Por otro lado, lo que hay a la izquierda depende normalmente de la elección del usuario y es un identificador cualquiera, que puede tener letras, números, y algunos signos.

Es aconsejable elegir en lo posible una dirección fácil de memorizar para así facilitar la transmisión correcta de esta a quien desee escribir un correo al propietario, puesto que es necesario transmitirla de forma exacta, letra por letra. Un solo error hará que no lleguen los mensajes al destino.

Correo web

Casi todos los proveedores de correo dan el servicio de correo web (*webmail*): permiten enviar y recibir correos mediante un sitio web diseñado para ello, y por tanto usando solo un **navegador web**. La alternativa es usar un programa de correo especializado (*cliente de correo*).

El correo web es **cómodo** para mucha gente, porque permite ver y almacenar los mensajes desde cualquier sitio (en un servidor remoto, accesible por el sitio web) en vez de en un ordenador personal concreto.

Cliente de correo

Los clientes de correo electrónico son programas informáticos que se instalan en el ordenador y sirven para **gestionar** todo lo relativo a la recepción y envío de correos electrónicos.

Suelen incorporar **herramientas** destinadas a facilitar las tareas más importantes de la gestión del correo: agenda, creación de grupos (varios contactos agrupados), clasificación de correos mediante reglas, filtros antispam, etc.

Estos clientes de correo necesitan que el **proveedor** ofrezca este servicio, ya que no todos permiten usar un programa especializado (algunos solo dan correo web). En caso de que sí lo apruebe, el proveedor tiene que explicar detalladamente cómo hay que configurar el programa de correo. Esta información siempre está en su página web, ya que es imprescindible para poder hacer funcionar el programa, y es distinta en cada proveedor. Entre los datos necesarios están: tipo de conexión (POP o IMAP), dirección del servidor de correo, nombre de usuario y contraseña. Con estos datos, el programa ya es capaz de obtener y descargar nuestro correo.

El funcionamiento de un programa de correo es muy diferente al de un correo web, ya que un programa de correo **descarga** a nuestro ordenador todos los mensajes que tenemos disponibles, y luego pueden ser leídos sin estar conectados a Internet. En cambio, en una página web se leen de uno en uno, y hay que estar conectado a la red todo el tiempo.

Algunos ejemplos de programas que realizan las funciones de cliente de correo electrónico son Outlook[28], Mozilla Thunderbird[29] o Gmail[30].

4.2. Algunas características del correo electrónico

Se puede enviar y recibir un email en cualquier momento del día y cualquier día de la semana, no hay horarios establecidos. Es un servicio de **24 horas los 365 días del año**.

- En general, un email tarda apenas unos segundos en llegar a su destino. **El concepto de distancia desaparece**. Se puede enviar una carta o unos archivos a donde se quiera.

[28] https://www.microsoft.com/es-es/outlook-com/
[29] https://www.thunderbird.net/es-ES/
[30] https://www.gmail.com/

- Es **económico y práctico**, en especial para comunicación de larga distancia.
- Se pueden **adjuntar ficheros multimedia** como imágenes, sonidos, vídeos, archivos de ofimática, etc.
- Utilizando el email, podrás acceder a **grupos de discusión** sobre temas que te interesen para intercambiar mensajes con personas de todo el mundo.
- Permiten **recibir RSS** (*Really Simple Syndication*) con lo cual, una persona recibe información en su propio buzón sobre los temas que le interesa sin tener que buscarlos él.
- **Ayuda al medio ambiente** al evitar el uso de papel, en caso de que no sea impreso.

4.3. Problemas del correo electrónico

El principal problema actual es el spam, que se refiere a la recepción de correos no solicitados, normalmente de publicidad engañosa. Estos correos intentan convencernos de comprar productos que no hemos pedido, de calidad sospechosa y en sitios web de dudosa procedencia.

Usualmente los mensajes indican como remitente del correo una dirección falsa. Por esta razón, es más difícil localizar a los verdaderos remitentes, y no sirve de nada contestar a los mensajes de correo no deseado: las respuestas serán recibidas por usuarios que nada tienen que ver con ellos.

Los clientes de correo electrónico, por sí mismos, no son capaces de identificar los mensajes spam de manera infalible. Es necesario que nosotros hagamos un análisis personal de los mismos antes de abrirlos. De todos modos, estos clientes incorporan herramientas antispam que cada día son más eficaces y que basan su clasificación de spam en lo que nosotros le vamos indicando; es decir, el sistema aprende gracias a nosotros a identificar qué es spam y qué no lo es.

Además del spam, existen otros problemas que afectan a la seguridad y veracidad de este medio de comunicación:

- Los virus informáticos: si recibimos un correo electrónico de dudosa procedencia y que además contiene un fichero adjunto, es preferible que no lo abra; puede tratarse de un virus. Es necesario tener especial precaución si la extensión de ese fichero corresponde a ficheros ejecutables (.exe, .bat, .com, etc.). Veremos más adelante qué son exactamente estos virus o también denominados «gusanos y troyanos» y los problemas que pueden causar a nuestro ordenador.

- La suplantación de identidad (*phising*): el *phising* es uno de los problemas más peligrosos que se derivan del uso de correo electrónico. Tenemos que verificar siempre que el remitente es quien dice ser. En especial, si recibimos un correo de una entidad bancaria. No debemos introducir datos personales o de acceso a cuentas bancarias si no estamos seguros de la procedencia del correo.

- Engaños (*fakes*): con frecuencia recibimos correos falsos que alertan de malas noticias o inventadas y nos piden que las difundamos a nuestros contactos. Son especialmente peligrosas las que informan de personas enfermas o necesitadas de dinero y nos piden que hagamos un donativo o ayuda económica. Debemos desconfiar y cerciorarnos de la veracidad de la información recibida.

- Las cadenas de correo electrónico: consisten en reenviar un mensaje a mucha gente; aunque parece inofensivo, la publicación de listas de direcciones de correo contribuye a la propagación a gran escala del “Correo no deseado” y de mensajes con virus, suplantadores de identidad y engaños.

- El correo masivo consiste en la recepción de una gran cantidad de correo electrónico no solicitado, que invade y puede incluso bloquear las cuentas que utilizamos.

4.4. Precauciones recomendables

Cuando recibamos un mensaje de correo electrónico que hable de algo que desconocemos (aunque nos lo haya mandado un contacto conocido) conviene hacer ciertas verificaciones. Podemos documentarnos a partir de buscadores de la web, tratando de consultar en el sitio web de la supuesta fuente de la información o en webs fiables y especializadas en el tipo de información.

Solo si estamos seguros de que lo que dice el mensaje es cierto e importante, lo reenviaremos, teniendo cuidado de poner las direcciones de correo electrónico de los destinatarios en la casilla CCO (copia oculta) y borrando del cuerpo del mensaje y encabezados previos para que no aparezcan direcciones de correo electrónico de otras personas. Así evitaremos la propagación del correo no deseado, spam, suplantaciones de identidad o engaños. Conviene que hagamos saber esto a nuestros contactos en cuanto nos reenvían mensajes con contenido falso, sin utilizar la casilla CCO o sin borrar encabezados previos con direcciones de correo electrónico.

Cuando el mensaje recibido lleve uno o varios ficheros adjuntos tendremos cuidado. Hay peligro de que los archivos contengan virus (u otro tipo de malware). Solo los abriremos si estamos seguros de su procedencia e inocuidad. Si, tras esto, comprobamos que los ficheros son inofensivos e interesantes para nuestros contactos podremos reenviarlo siguiendo las precauciones del párrafo anterior (en este caso, para que lleguen los ficheros adjuntos es más rápido pinchar en reenviar que crear un mensaje nuevo y volverlos a adjuntar aunque tendremos cuidado de borrar todo el texto que repite previos reenvíos; quizá pegando después el cuerpo principal del mensaje recibido si tiene información de interés o relacionada con los archivos adjuntos).

Cuando un mensaje sospechoso nos ofrece la posibilidad de darnos de baja o cancelar la supuesta suscripción a ellos, es preferible no clicar en ningún enlace del correo y utilizar las herramientas antispam de nuestro proveedor de correo. Todos los clientes de correo tienen un botón con el texto "Es spam", "Correo no deseado", "Marcar como spam" o similar.

05. Redes sociales

5.1. Introducción

Un servicio de red social se centra en la construcción y la verificación de **comunidades online de personas** que comparten intereses y actividades.

La mayoría de los servicios están principalmente basados en la **web** y ofrecen una colección de diversas vías para que los usuarios puedan interactuar, como el chat, mensajería, correo electrónico, videoconferencia, chat de voz, el uso compartido de archivos, blogs, grupos de discusión, etc.

En la actualidad, Facebook[31] es la red social más extendida, llegando recientemente a **superar los 2.740 millones de usuarios activos en un mes**. Si Facebook fuera un país, sería el más grande del mundo superando incluso a China y La India.

Pero no es Facebook la única red social, ni mucho menos. Algunas de las más conocidas y usadas por todo el mundo son: YouTube[32], Instagram[33], X (antes Twitter)[34], Pinterest[35], TikTok[36], etc. Veamos a continuación los tipos de redes sociales que existen y cómo están clasificadas.

Antes de decidirse a entrar en una red social o permitir que un menor acceda a ella, se deben conocer sus términos y condiciones; además teniendo en cuenta que estos cambian frecuentemente.

La mayoría de redes sociales tienen una edad mínima de admisión. Por ejemplo, **Facebook** y **X** (antes Twitter) no admiten usuarios menores de 14 y 13 años, respectivamente. Y, algunas exigen ser mayor de edad, como **Taringa.**

[31] https://www.facebook.com/
[32] https://www.youtube.com/
[33] https://www.instagram.com/
[34] https://x.com/?lang=es
[35] https://pinterest.com/
[36] https://www.tiktok.com/

La mayoría de las redes sociales coincide en algunas cuestiones importantes, como:

- No permitir la difusión de contenidos sexuales o material pornográfico, especialmente de menores.
- No admitir el lenguaje violento o que invite al odio o la violencia, o expresiones que ofendan a un grupo, persona o comunidad.
- No permitir ninguna forma de discriminación.
- Prohíben la creación de perfiles que no representen a una persona real o que suplantan la identidad de otra persona.

La mayoría de las redes cuentan con herramientas para denunciar este tipo de contenidos. Utilízalo cuando se encuentren publicaciones que violan estas normas para que sean eliminadas.

Cabe citar que hay algunas redes o comunidades virtuales especialmente diseñadas para niños, como Mundo Gaturro[37] que incluyen filtros y controles de contenidos además de moderadores automáticos y humanos en sus foros y salas de chat.

5.2. Amistad virtual

Las herramientas tecnológicas permiten que los niños y jóvenes establezcan contactos con otros usuarios y niños conocidos y/o desconocidos de otras ciudades y partes del mundo.

Estos nuevos contactos no requieren un conocimiento previo cara a cara, y pueden surgir vínculos virtuales que los menores pueden iniciar por un amigo en común, por un chat, por aceptar una solicitud como contacto viendo simplemente una fotografía, o por curiosidad.

[37] http://www.mundogaturro.com/

Es importante que sepan distinguir la amistad y los amigos reales, de los contactos o “amistades virtuales”. La información que deben saber de nosotros estos contactos o amistades virtuales no debe ser la misma que ofrecemos a nuestros amigos verdaderos; y deben evitar que les envíen información personal: datos personales, dirección, fotografías, etc.

Los padres principalmente al igual que deben hacer por conocer las amistades de los menores, deben tratar de conocer a los conocidos en línea, así como su lista de contactos.

La comunicación virtual no reemplaza el encuentro presencial, pero tampoco los conocidos o amigos virtuales pueden tener la misma consideración ni confidencialidad que los auténticos amigos con los que comparten su día a día.

Las redes sociales a veces “engañan” a niños y adolescentes cuando ven en una gran lista de contactos un gran grupo de amigos.

El gran atractivo que ofrecen las redes sociales debe ser para ellos conectar con antiguos amigos, reencontrarse con otros amigos que no ven con frecuencia o incluso recuperar a algunos perdidos, así como facilitar los encuentros virtuales con otros que ya se tienen.

5.3. La privacidad y acceso a contenidos

El concepto de privacidad ha cambiado mucho en estos años, y lo que hace unos años era exclusivamente conocido por nuestros familiares y más allegados, actualmente se comparte sin ningún pudor. Muchos niños y adolescentes comparten sin reserva información vinculada a su aspecto físico, sus pensamientos, rutina personal y un sinfín de opiniones que pertenecen a su esfera íntima y personal, sin olvidar las fotografías, y vídeos de su día a día.

Pero todo eso no quita que debemos de prevenir a los adolescentes de que todo lo que uno da a conocer en las redes sociales deja de ser privado y deja de pertenecer al usuario. Igualmente, aunque sea publicado en nuestro perfil o muro exclusivamente para nuestros contactos o amigos, podría llegar a personas extrañas y alejadas de nuestra red.

En todas las redes sociales de las cuales formen parte, deben tener un especial cuidado con lo que comparten, dicen y el material audiovisual que cuelguen, para que nunca pueda llegar a ser utilizado en su contra. Por eso en dichas redes, el sistema permite aumentar la información de nuestro perfil y configurar la privacidad del mismo.

Esta configuración de los parámetros de privacidad a veces no es fácil o sencilla por lo que los padres y tutores deben conversar con ellos y orientarles sobre los criterios de privacidad de lo que van a subir a internet; procurando asesorarles que siempre es preferible que lo que publiquen sea compartido exclusivamente entre sus contactos y no sea público.

Igualmente es importante que solo amigos o contactos previamente aceptados puedan acceder a su perfil de usuario.

Conseguir la confianza con los adolescentes es de vital importancia y se logra abriendo el diálogo y la empatía a sus preocupaciones e inquietudes. Se puede hacer que se cuestionen si dirían a la gente de su barrio lo que comen, o enseñarían fotos suyas por todo el vecindario. Es decir, preguntas que les ayuden a reflexionar si compartirían toda la información de manera pública; y que así vean lo difícil de controlar que puede resultar cuando se da a conocer a los demás.

5.4. Facebook

Facebook es una red social que **conecta amigos** de todo el mundo. Como se ha comentado anteriormente, a mediados de 2019 se llegó a los 2.449 millones de usuarios activos en un mes.

Según la descripción que Facebook hace en su propia web:

> La misión de Facebook es dar a las personas el poder de compartir y hacer el mundo más abierto y más conectado. Miles de millones de personas usan Facebook cada día para mantener el contacto con sus amigos, subir un número ilimitado de fotos, compartir links y vídeos y obtener más información acerca de las personas que van conociendo.

Para **registrarse**, tan solo es necesario disponer de una cuenta de correo electrónico y rellenar un pequeño formulario. Vamos a ver a continuación el proceso.

5.5. Crear cuenta en Facebook

Es imprescindible estar registrado en Facebook para poder acceder a todos sus servicios. Así que vamos a ver cómo se realiza este proceso. Abre una ventana de tu navegador y accede a la dirección web de Facebook[38]:

Como puedes observar, los usuarios **registrados** pueden acceder a su perfil rellenando los campos "Correo electrónico o teléfono" y "Contraseña" situados en la zona superior de la pantalla.

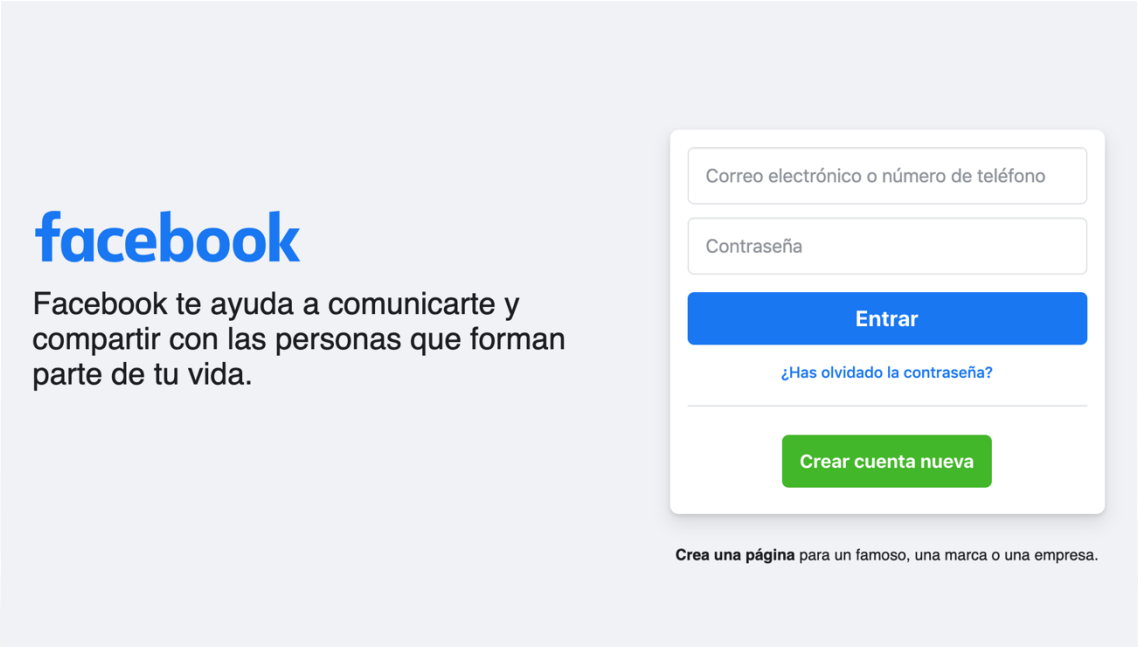

Imagen 35. Acceso a Facebook para usuarios registrados.

Por su parte, los **nuevos** usuarios deben cumplimentar el formulario situado en la zona derecha de la pantalla. Este formulario se compone de los siguientes campos:

[38] https://www.facebook.com

Imagen 36. Registrarse en Facebook.

1. "**Nombre**": Indica tu nombre.

2. "**Apellidos**": Indica tus apellidos.

3. "**Tu correo electrónico o móvil**": Es importante que indiques un correo electrónico que uses de manera habitual o tu número de móvil, ya que Facebook te enviará allí todos los avisos, notificaciones, mensajes, etc.

4. "**Contraseña nueva**" Para acceder a Facebook, deberás escribir el correo electrónico indicado en el campo anterior y la contraseña que establezcas en este campo.

5. "**Fecha de nacimiento**" Es importante indicar tu edad real, ya que Facebook permitirá el acceso a ciertos contenidos teniendo en cuenta tu edad y su "Política de uso de datos". Este aspecto es aún más importante en los casos de usuarios menores de edad.

6. "**Sexo**": Indica tu sexo.

Una vez que hayas rellenado todos los campos del formulario, pulsa en el botón “**Registrarte**” para enviar los datos:

Una vez ingresados los datos anteriores, se recibe un correo electrónico para verificar que dicha dirección de correo pertenece a la persona que se está registrando. Para ello se pide ingresar un código de cinco dígitos enviado a ese correo electrónico.

Imagen 37. Ingreso del código recibido en la cuenta de correo.

Confirmada correctamente la cuenta de correo electrónico la aplicación te ofrece empezar a buscar amigos y editar tus datos personales ampliando la información introducida anteriormente.

La búsqueda de amigos se puede realizar de varias formas (que se presentan todas en la misma pantalla):

- Mediante tu dirección de correo electrónico.
- Introduciendo directamente el nombre de la persona que estás buscando.
- A través de tus contactos de mensajería instantánea.

En Facebook, tras registrarte, cada usuario tiene un perfil. Este permite la posibilidad de introducir bastante **información personal**. No es obligatorio rellenar toda la información para pertenecer a la red, pero cuánta más aportes, más sabrán tus amigos de ti (recuerda que el perfil es privado, es decir, no es accesible a todo el mundo, solo a los amigos que tú aceptes como tal).

A diferencia de otras redes sociales, en Facebook los usuarios solo pueden hacer públicos sus perfiles a otros usuarios de Facebook.

Inicio

La primera vez que entres a Inicio, como aún **no tendrás amigos**, Facebook te dará la opción de que los busques a través de las opciones señaladas anteriormente.

Una vez que tu comunidad de amigos vaya creciendo, en este menú, podrás tener una **visión general de tu comunidad de amigos** y ver la actividad de la misma: comentarios entre amigos, fotos que hayan subido, etc.

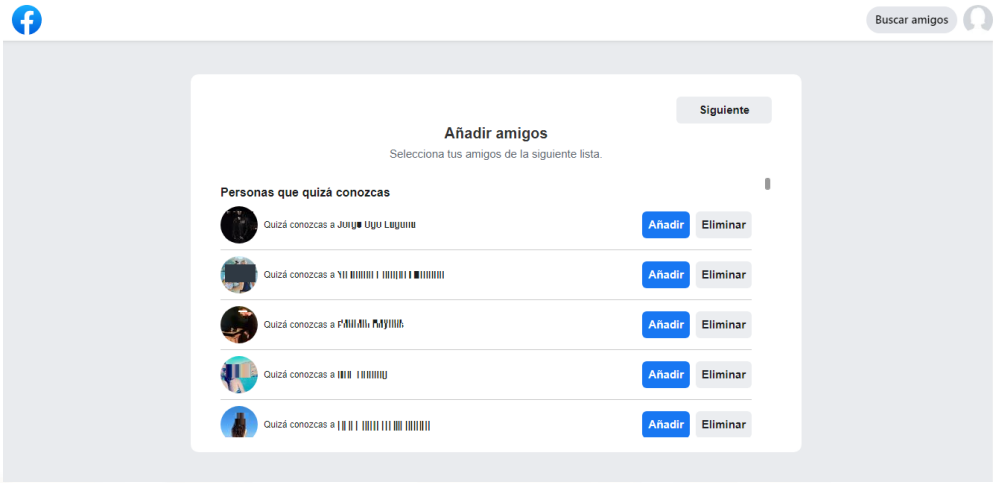

Imagen 38. Añadir nuevos amigos a Facebook.

Información de perfil

- Información básica: sexo, fecha de nacimiento, ciudad natal, barrio, familiares, situación sentimental, interés (tendencia sexual, qué buscas), ideología política y creencias religiosas.
- Información personal: actividades, intereses, música favorita, programas favoritos de televisión, películas favoritas, libros favoritos, citas favoritas y acerca de mí.
- Información de contacto: dirección de correo electrónico, nombres en pantalla de mensajería instantánea, teléfono móvil, teléfono fijo, dirección, ciudad/población, vecindario, código postal y página web.

- Formación y empleo: universidad, carrera, segunda especialidad, tercera especialidad, titulación, instituto, empresa, puesto, descripción, cuidad/población y periodo de tiempo.

Si dudas sobre la conveniencia o no de publicar información personal en Internet, Facebook te hace la siguiente **recomendación**:

> Gracias a los controles de privacidad de Facebook, puedes controlar quién ve las diferentes secciones de tu información. Millones de usuarios de Facebook comparten hasta su número de teléfono móvil, porque saben que tienen control absoluto de la lista de personas que puede verlo. Puedes decidir la configuración de privacidad de toda tu información, así como del contenido que publicas en Facebook.

Biografía

La biografía (anteriormente conocida como Muro) es donde expresarte desde tu perfil. Mediante el editor, que aparece en la parte superior, podrás poner comentarios, agregar elementos como fotos, vídeos o notas.

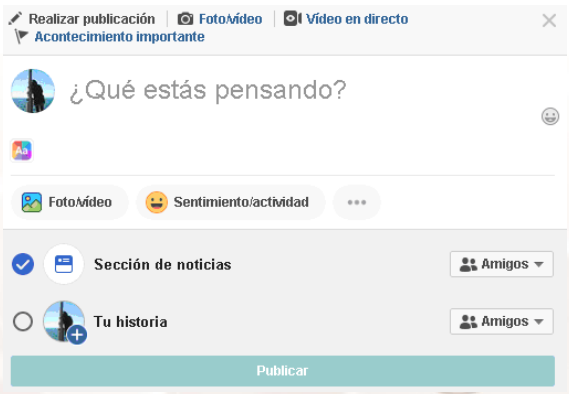

Imagen 39. Añadir un estado en Facebook.

En el editor clica sobre el icono “Foto/Vídeo”. Seleccionamos la foto (desde el equipo) y la compartimos en la biografía.

También podemos especificar **qué personas queremos que vean** cada una de las publicaciones que hagamos:

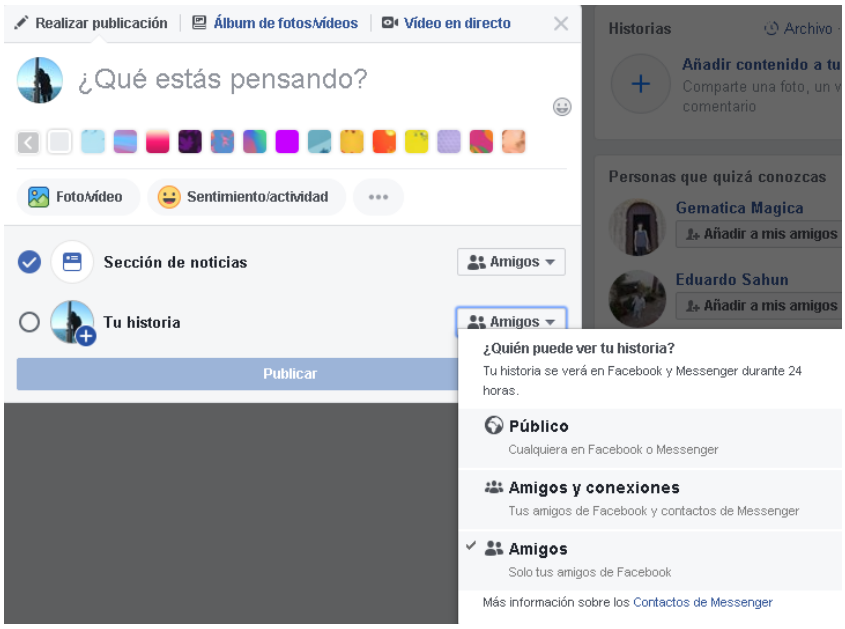

Imagen 40. Audiencia de las publicaciones y etiquetado.

Buscar amigos

Es una forma de **localizar amigos** del pasado con quienes se perdió el contacto o agregar otros nuevos con quienes intercambiar fotos o mensajes; el servicio de Facebook te ayuda a buscarlos y además te sugiere posibles futuros amigos.

En la caja de búsqueda que aparece en la parte superior izquierda de la página se puede realizar la búsqueda de amigos de las siguientes formas:

- Mediante tu **agenda de correo electrónico**: Facebook ofrece la posibilidad de buscar en la red social a tus contactos de correo electrónico, mediante las direcciones de correo. Para ello basta con seleccionar la opción “Importar contactos de tu correo electrónico” y seguir los pasos que ahí se indican. Facebook te advierte de lo siguiente al usar esta opción:

> “No almacenaremos tu contraseña después de haber importado la información de tus amigos. Es posible que usemos las direcciones de correo electrónico que importes para ayudarte a conectar con amigos, como por ejemplo para generar sugerencias para ti y tus contactos de Facebook”.

- La otra opción es **enviar una invitación** directamente a un amigo tuyo. Introduciendo directamente el nombre de la persona que estás buscando y haciendo clic en el botón **Añadir** que aparece a la derecha de la persona buscada o mediante facilidades que te da Facebook, tipo:
- “Buscar antiguos compañeros del colegio o instituto”.
- “Buscar compañeros antiguos o actuales de la universidad”.

Mensajes

Este menú es como una versión simplificada de cualquier aplicación para **gestión de correo electrónico**.

Nos permite “Ver Bandeja de entrada de mensajes” y realizar operaciones sobre los mensajes existentes: suprimir, marcar como no leído, etc.

La otra opción que podemos realizar desde este menú es la de “Redactar nuevo mensaje”. En el campo “Para” podemos incluir amigos de nuestra comunidad (Lista de Amigos):

Imagen 41. Enviar mensaje a amigos de Facebook.

Al mensaje se le pueden **adjuntar** imágenes, vídeos y *links.*

Configuración de la cuenta

Hacemos clic en la fecha que aparece en la parte superior derecha de la pantalla. Al desplegarse se selecciona la opción **Configuración** y desde aquí podemos configurar todo lo que se refiere a la cuenta.

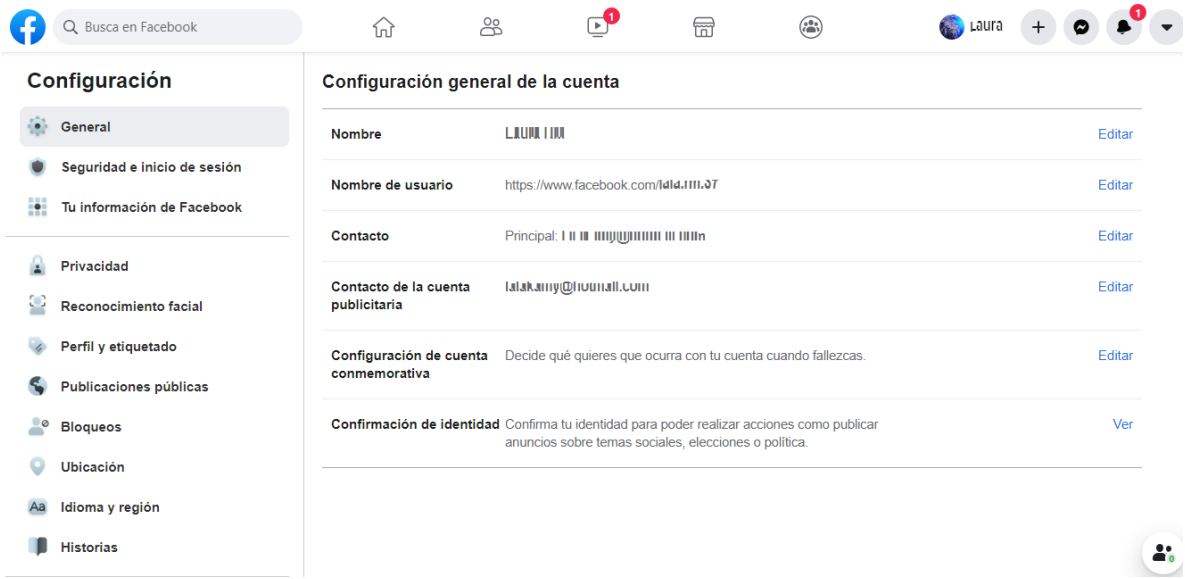

Imagen 42. Configuración general de la cuenta de Facebook.

Nombre (tu nombre real), Nombre de usuario, Correo electrónico (dirección de contacto), Contraseña (para iniciar la sesión), Cuentas vinculadas (utiliza otras cuentas para iniciar sesión), pregunta de seguridad (te identifica como propietario de la cuenta), Privacidad (Controla que información compartes) y Desactivar la cuenta.

Redes

Configuras en qué red estás dentro de Facebook. En nuestro caso: Spain, aunque podría ser cualquier otra.

Notificaciones

Facebook te avisa cuando se realizan acciones que tienen que ver contigo en la red social. Cada aplicación de Facebook tiene asociada su propia configuración de notificaciones. Para acceder a las notificaciones debes hacer clic en el icono con forma de campana que aparece en la parte superior derecha de la página.

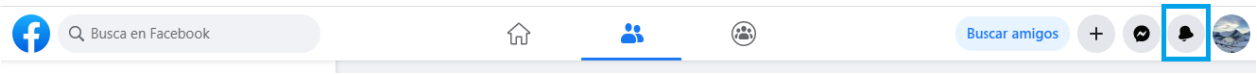

Imagen 44. Sección de notificaciones de Facebook.

Así se puede configurar que te llegue una notificación a tu correo electrónico de contacto con las funcionalidades típicas de la aplicación de Facebook: mensajes que te envíe un amigo por la red, alguien que te añada como amigo, etc.

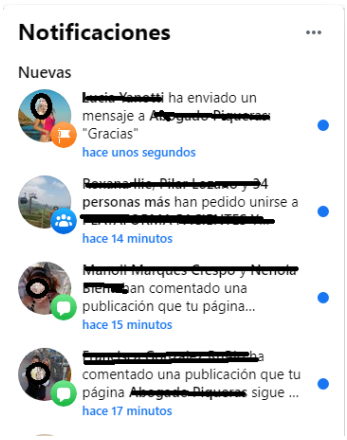

Imagen 43. Notificaciones de Facebook.

O con otras aplicaciones asociadas como Fotos (que te llegue un mensaje cuando alguien te etiquete en una foto, que comenten una foto tuya, etc.), Grupos (cuando te inviten a unirte a un grupo), Eventos (que te llegue el mensaje cuando te inviten a un evento), etc.

Móvil

En el menú de la parte izquierda aparece la opción "**Móvil"**. Si configuras este servicio conseguirás que Facebook te envíe mensajes de texto a tu **terminal móvil**. Se pueden recibir mensajes de solicitud de nuevos amigos, mensajes, comentarios en la biografía y actualización del status de tus amigos.

Una vez configurado, desde tu móvil podrás actualizar tu estado, buscar números de teléfono, cargar fotos y vídeos.

Idioma

También en el menú de la parte izquierda aparece la opción “**Idioma y región”**. Haciendo clic en esta opción puedes configurar el idioma que quieras que utilice Facebook para tu perfil. En nuestro caso el español.

Facebook pagos

En el menú de la parte izquierda aparece la opción “**Facebook Pagos”**. Haciendo clic en esa opción Facebook te permite introducir los datos de tu tarjeta de crédito para realizar compras de regalos, anuncios, etc. También se puede configurar la moneda a usar (euro, dólares, etc.).

Configuración de privacidad

Otra opción más que figura en ese menú de la parte izquierda es “**Privacidad”**. Desde aquí se controla quién puede ver la información de cada una de las secciones de tu perfil. Es decir, de manera independiente puedes decidir qué información compartes con el resto de la red: solo información básica, personal, amigos, etc.

Las opciones a la hora de aumentar o disminuir la privacidad son: Todos, Mis redes y amigos, Amigos de amigos, Solo amigos, personalizar…

Imagen 44. Quién puede ver las publicaciones que haces en Facebook.

Desde la opción de configuración de seguridad de Facebook podemos configurar no solo la visibilidad de lo que publico, sino también si permitimos o no que nos etiqueten en las fotos, o que puedan acceder o no a nuestro perfil de manera pública.

Si accedemos a la **opción de privacidad**:

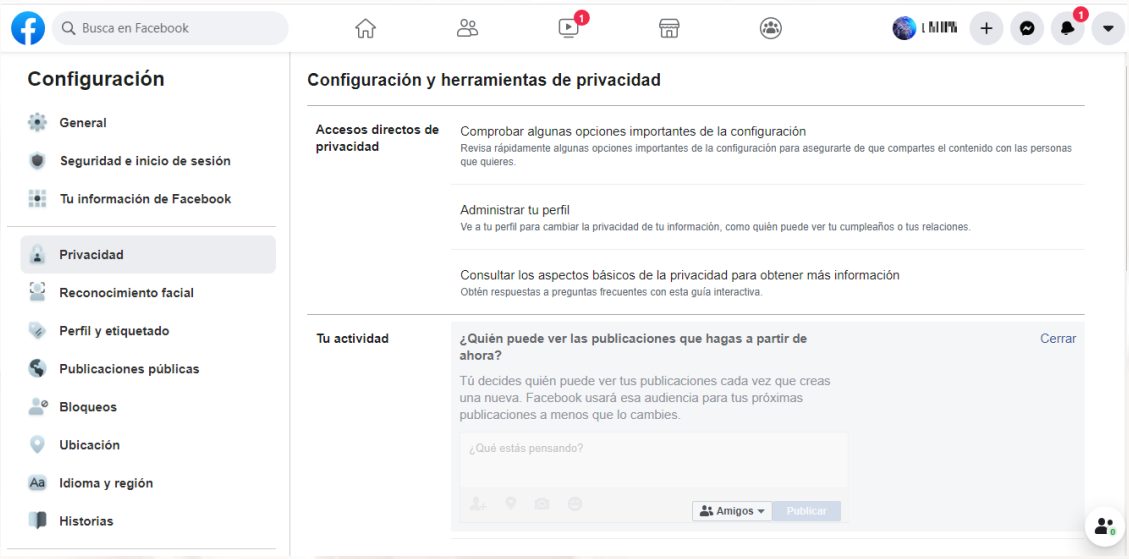

Imagen 45. Pestaña de privacidad en Facebook.

Tenemos la opción de **“¿quién puede ver mis cosas**?”. Aquí es donde se debe señalar que solo puedan verla los amigos/contactos; y bloquear a que contactos que no sean “amigos de amigos” soliciten amistad. La otra opción permite que cualquiera pueda pedir al usuario solicitudes de amistad.

Otra opción del menú es la exclusión de aquellos que no son amigos en el buscador por el correo electrónico y/o el teléfono.

Imagen 46. Configuración de perfil y etiquetado.

En el menú, de la izquierda, el apartado de “**Perfil y etiquetado**”, nos permite configurar quién puede agregar contenido en mi perfil. Es aconsejable no permitir que nadie publique en el perfil personal de uno o que etiquete fotografías del niño o joven.

Información básica del directorio

Determinada información está visible a todos porque es **esencial** para ayudar a otros a que te encuentren y conecten contigo en Facebook. Esta información es la siguiente:

- El nombre y foto de perfil están visibles para todos, así amigos reales pueden reconocerte. Además, se mostrarán cuando escribas en el muro de alguien.

- El sexo es público para que podamos mostrar el género gramatical correctamente (por ejemplo, "Añadirla como amiga").
- Las redes son visibles a todos para que puedas ver quién más forma parte de tu red (y tendrá acceso a tu información) antes de elegir "Amigos y redes" en cualquiera de las opciones de privacidad.

Otra información de esta sección, incluida tu **ciudad de origen** y los **intereses**, está visible de forma predeterminada para ayudar a tus amigos y a otras personas con quienes tienes cosas en común a conectar contigo.

Compartir en Facebook

En esta sección se controla **quién puede ver** todo el contenido que publicas diariamente (como actualizaciones de estado, fotos y vídeos). También se incluye parte de lo que compartes sobre ti (fecha de nacimiento e información de contacto), así como el contenido que otros comparten sobre ti (comentarios en tus publicaciones y las fotos y los vídeos en los que estás etiquetado). Configura estas opciones con un clic y tu configuración se aplicará a todo el contenido diario que publiques en el futuro. "Personalizar la configuración" muestra una lista completa para que puedas controlar el nivel de privacidad para cada configuración.

Aplicaciones y sitios web

En el menú de la izquierda, en esta sección de “**Aplicaciones y sitios web**” se controla **la información que se comparte con los sitios web y las aplicaciones**, incluidos los motores de búsqueda (las aplicaciones y los sitios web que tú y tus amigos usáis ya tienen acceso a tu nombre, foto del perfil, sexo, redes, lista de amigos, ID de usuario y otra información que compartes con todos). Puedes ver tus aplicaciones, eliminar las que no desees usar o desactivar la plataforma por completo. Si la desactivas, no podrás usar las aplicaciones y los sitios web de la plataforma y no compartiremos tu información con ellos.

Listas de bloqueados

También en el menú de la izquierda en la sección “**Bloqueos**” puedes **bloquear a las personas para que no interactúen** contigo o vean tu información en Facebook. También puedes especificar los amigos de los que deseas que se ignoren las invitaciones de aplicación, así como ver una lista de aplicaciones específicas a las que has bloqueado para que no accedan a tu información ni se pongan en contacto contigo.

Fotos

Haciendo clic sobre su perfil Facebook permite que tus fotos sean **compartidas con amigos** de la red. Para ello o tienes que crear tus propios álbumes de fotos o etiquetarte en fotos que estén en la red social en las que aparezcas.

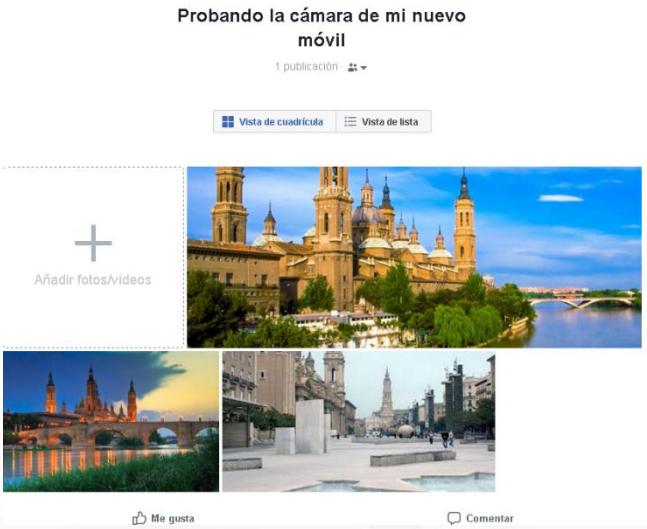

Imagen 47. Sección de fotos en Facebook.

Los **comentarios** y el **etiquetado** de fotos te permiten compartir fotos con tus amigos y tu familia. Sin importar dónde se encuentren. Puedes compartir una foto de Facebook con cualquiera de tus amigos de Facebook haciendo clic en el enlace "Compartir" situado debajo de la foto o el álbum de fotos.

¿Cuántas fotos puedo cargar? Carga las fotos que desees, incluso toda tu **colección** de fotos de animales. Puedes subir hasta 1000 fotos a un álbum, pero puedes cargar todos los álbumes que desees.

El almacenamiento es ilimitado, los usuarios de Facebook han subido más de 5 mil millones de fotos que comparten con amigos de todo el mundo.

Vídeo

Igualmente, haciendo clic sobre tu perfil puedes cargar vídeos. Para ello el vídeo debe cumplir los siguientes **requisitos**:

- No superar los 1024MB y durar menos de 20 minutos.
- Fue grabado por ti o tus amigos.
- En el vídeo aparecéis tú o alguno de tus amigos.

Sigue estos **pasos**:

- Ve a tu perfil.
- Haz clic en "Añadir fotos o video".
- Selecciona el tipo de vídeo que deseas colgar desde tu ordenador, smartphone o Tablet.
- Sigue las instrucciones de la pantalla para tu tipo particular de carga.
- Cuando acabes, haz clic en "Publicar" para generar una historia sobre tu vídeo y almacenar el vídeo permanentemente en Mis vídeos.

¿Qué necesito para ver un vídeo de mis amigos?

Podrás ver un vídeo desde cualquier equipo siempre que tengas instalada la versión más reciente del reproductor VLC media player[39]. VLC es un reproductor ejecutable en todas las plataformas y reproduce la mayoría de los archivos multimedia. Comprueba que tienes instalado el reproductor VLC, si no instálatelo, es de libre distribución.

[39] https://www.videolan.org/vlc/index.es.html

Busca en Facebook sobre la **normativa de vídeos**. Si tienes algún vídeo que cumpla la norma súbelo. Si no pide a algún compañero que te pase un trozo de vídeo para practicar.

Grupos

Situado en tu perfil, la opción más incluye entre otras muchas "**Grupos**" donde puedes unirte y crear hasta 200 grupos de Facebook. Pueden estar basados en **intereses comunes**, actividades o cualquier cosa que quieras. La aplicación de "Grupos" muestra tus grupos actualizados recientemente, así como los grupos a los que tus amigos se han unido últimamente.

Es una de las utilidades de mayor desarrollo reciente. Se trata de reunir personas con intereses comunes. En los grupos se pueden añadir fotos, vídeos, mensajes...

En cuanto a las páginas, estas también se crean con fines específicos, solo que en estas no hay foros de discusión y están encaminadas hacia **marcas o personajes** específicos, más que a convocatorias.

Además, los grupos también tienen su **normativa**, entre la cual se incluye la prohibición de grupos con temáticas discriminatorias o que inciten al odio y falten al respeto y la honra de las personas. Como esto no se cumple en muchas ocasiones, existe la opción de denunciar a los grupos que vayan contra esta regla, por lo cual Facebook incluye un link en cada grupo para poder realizar reclamaciones y quejas.

Eventos

Con Eventos de Facebook, puedes organizar reuniones y fiestas con tus amigos, así como permitir que la gente de tu comunidad conozca eventos próximos.

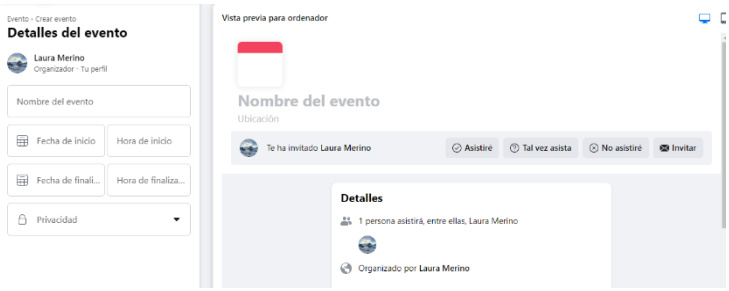

Imagen 48. Crear nuevo evento en Facebook.

La página de la aplicación "**Eventos**" muestra tus próximos eventos, cualquier invitación que haya pendiente y enlaces a tus propios eventos.

5.6. Recomendaciones y buenas prácticas de Facebook

En primer lugar, hay que tener claro que Facebook es un balcón abierto a todo el mundo y que tu perfil se indexa en Google, al igual que los millones de páginas públicas de Internet. Algo que no sucede, por ejemplo, con otras redes sociales en las que solo se ofrece información de la comunidad dentro de su propio espacio. Es por eso que, si utilizas Facebook, conviene ser cauto y seguir estos consejos al pie de la letra:

No publiques fotos que pueda ver todo el mundo

Recuerda que toda tu red de contactos puede echar un vistazo a tus álbumes y ver el viaje loco que te pegaste durante el fin de semana o el careto de cada uno de tus amigos en una fiesta privada.

Cuidado con tus datos personales

Si tu intención es la de hacer amigos a través de Facebook, empieza por entender que una red social es un espacio lúdico. Evita rellenar tu perfil con datos personales como el teléfono, tu dirección y cualquier otra información que

pueda ser útil para cometer un delito de suplantación. O simplemente, caer en manos de las empresas que tienen por oficio bombardear con publicidad no deseada.

Di NO a encuestas y aplicaciones

Algunas encuestas y aplicaciones que se ofrecen en Facebook suelen tener gancho, por eso la gente se apunta fácilmente. Recuerda que cada una de estas 280.000 aplicaciones ya existentes, están hechas por terceras personas o empresas. Y, aunque Facebook afirma supervisar su uso, puede colarse algún indeseado. Así que, la próxima vez que te llegue una invitación a ver un vídeo o un regalo virtual en forma de tarta, piénsatelo dos veces antes de aceptar que una nueva aplicación acceda a tu perfil de Facebook.

No aceptes amigos “fantasma”

Y no nos referimos a aquella persona que no te cae bien, sino a aquel que ni siquiera conoces y que está intentando convertirse en tu amigo. Si no abres los correos SPAM, tampoco aceptes la amistad de cualquiera, dispuesto a robarte los datos o ver tus vídeos y fotografías más personales.

Controla tu privacidad

Por último y lo más importante, en Facebook dispones de un apartado para hacerte dueño de tu propia privacidad. Lo encontrarás en la parte superior de la página, pulsando en “**Configuración**” y después en “Privacidad “, en el menú de la izquierda. En este espacio dispones de tres apartados:

- **Accesos directos de privacidad.**: Desde este menú podrás decidir quién puede ver lo que compartes, como proteger tu cuenta, como pueden encontrarte las personas, configurar los datos de Facebook y modificar tus preferencias de anuncios de Facebook. Además de una sección para administrar tu perfil y un apartado para obtener más información. Por defecto, estos datos solo son observables por tu red de amigos.

- **Tu actividad.** Como bien sabes, cualquier usuario de tu red de contactos puede ver los mensajes que escribes en las biografías de los demás, tus comentarios sobre una foto, un vídeo o incluso la información que has eliminado de tu perfil. En este espacio podrás determinar qué es lo que te interesa que vean o no tus contactos. También tiene la opción de revisar todas tus publicaciones y contenidos.

Cómo pueden encontrarte y ponerse en contacto contigo las personas: Decide qué es lo que puede ver sobre ti cualquier persona que te busque a través de Facebook. Aunque tus amigos siempre podrán encontrarte, tienes la opción de seleccionar el nivel de personas que no quieres que te encuentren. Asimismo, podrás seleccionar si quieres que se vea tu foto, el listado de tus contactos o eliminar la posibilidad de que te agreguen como amigo. En este apartado también podrás configurar si quieres que otras aplicaciones de búsqueda fuera de Facebook enlacen a tu perfil: este es otro de los peligros de Facebook ya que esas aplicaciones son creadas por particulares o empresas. Es ese sistema de alertas de los cumpleaños, el listado de ciudades del mundo que has conocido o las canciones que puedes dedicar a tus amigos. Cuando aceptas utilizar cualquiera de estas 280.000 aplicaciones, la empresa responsable de la aplicación puede ver todos los datos privados que compartes con tu red de contactos. En este caso es recomendable seleccionar la opción “No compartir ninguna información mía a través de API de Facebook” y deshacerse de topos que buscan nuestros datos más personales. Nunca hay que informar cuándo uno está de vacaciones o de viaje ni por cuánto tiempo ni a dónde, puesto que esta información puede utilizarse por terceras personas con fines no positivos.

En el caso de fotos y vídeos, por ejemplo, es menester asegurarse de que no estamos poniendo en evidencia nuestra dirección postal, los horarios familiares, la escuela a la que van nuestros hijos, la existencia de un patrimonio que pudiera tentar a sujetos malintencionados. Conviene evitar, dentro de lo posible, publicar fotos de chicos menores de edad. Nunca, por ningún motivo, hay que subir fotos de los hijos de nuestros conocidos, familiares o amigos.

Debemos tener siempre presente que esa potestad es exclusiva de sus respectivos padres.

5.7. YouTube

YouTube

Imagen 49. Logotipo de YouTube.

YouTube tiene más de 2.00 millones de usuarios activos en un mes. Aunque YouTube tiene excelentes funcionalidades sociales, las marcas lo usan como un repositorio de video ya que los videos que se hacen virales no lo hacen con las opciones sociales de la red social, sino a través de las otras redes sociales. El servicio que nos brinda Google a través de su plataforma **YouTube** es muy amplio en el ámbito multimedia. Es verdad que la mayoría de gente piensa que YouTube es un espacio de Internet donde visualizar todo tipo de vídeos e incluso poder compartir nuestras propias producciones audiovisuales, no obstante, **YouTube** también nos brinda la posibilidad de registrarse como usuario y crear un canal. El canal es una página que ven los demás usuarios registrados y que contiene la información del perfil del usuario, sus vídeos, sus favoritos…Puedes cambiar tu perfil, modificarlo con imágenes y colores a tu gusto, donde te pueden dejar comentarios, etc. Enviar una invitación o un mensaje personal a un “amigo” o a otro usuario registrado… También puedes suscribirte los vídeos de un canal para estar informado sobre lo que publica sin tener que visitarlo constantemente.

Por otra parte, dentro de los vídeos tenemos la posibilidad de escribir un comentario sobre el vídeo, responder al comentario de otro usuario (y votar a favor, votar en contra de los comentarios), indicar: ‘me gusta’ o ‘no me gusta’… O compartir el vídeo enviando a tus amigos la URL del vídeo acortándola automáticamente a través del correo electrónico, la mensajería instantánea, o redes sociales: Facebook, Twitter, Whatsapp, hi5,…

Acceso a YouTube

Tecleamos en el navegador de Internet la dirección de YouTube [40]

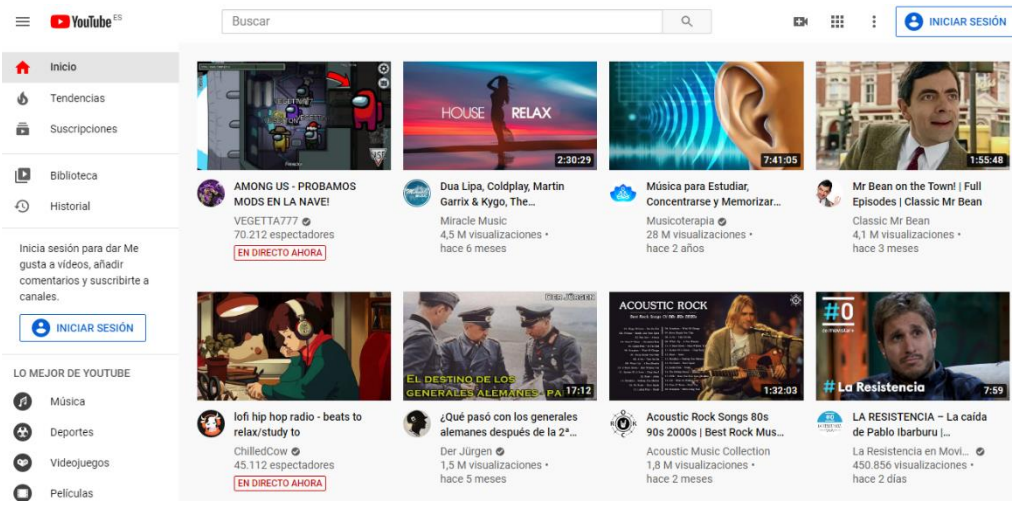

Imagen 50. Acceso a YouTube.

Inmediatamente accederemos a la página principal de YouTube, como puedes comprobar.

¿Cómo funciona YouTube?

El funcionamiento de YouTube es muy sencillo.

Imagen 53. Barra de herramientas de YouTube.

YouTube es un servicio que te permite crear una cuenta con tu canal de YouTube. Para crear la cuenta hacemos clic en la opción "**Iniciar sesión**" que aparece en la parte superior derecha.

Una vez creado tu canal, puedes subir tus vídeos en prácticamente cualquier formato moderno. Para crear una cuenta hay que iniciar sesión en la barra de herramientas de la página principal.

[40] https://www.youtube.com/

Imagen 51. Cómo iniciar sesión en YouTube.

Una vez iniciada la sesión, en la página puedes ver tu perfil, editarlo y seleccionar tu canal, subir videos, etc.

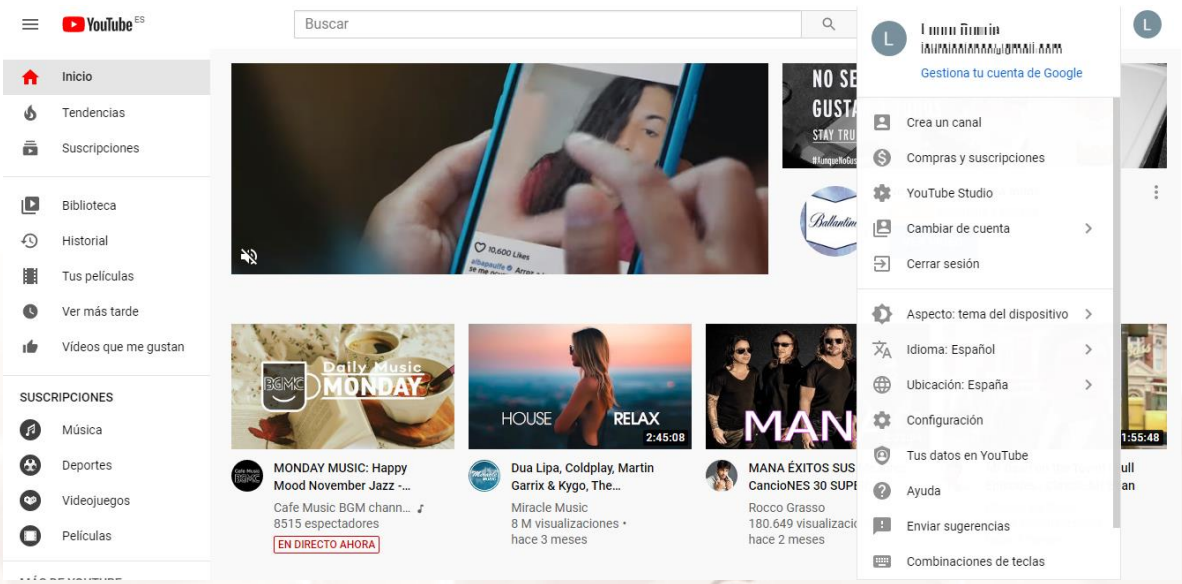

Imagen 52. Opciones tras haber iniciado sesión en YouTube.

¿Cómo añadir un video a YouTube?

Para añadir un video, en la barra de herramientas de la página inicial, aparece el siguiente icono.

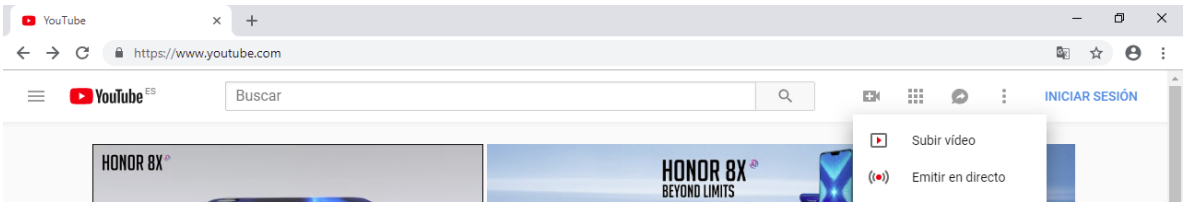

Imagen 53. Opción subir video en YouTube.

Tus vídeos pueden ser públicos o privados, puedes agruparlos por secciones (serían algo así como por etiquetas) y listas de reproducción. Ten en cuenta las opciones y recomendaciones de privacidad.

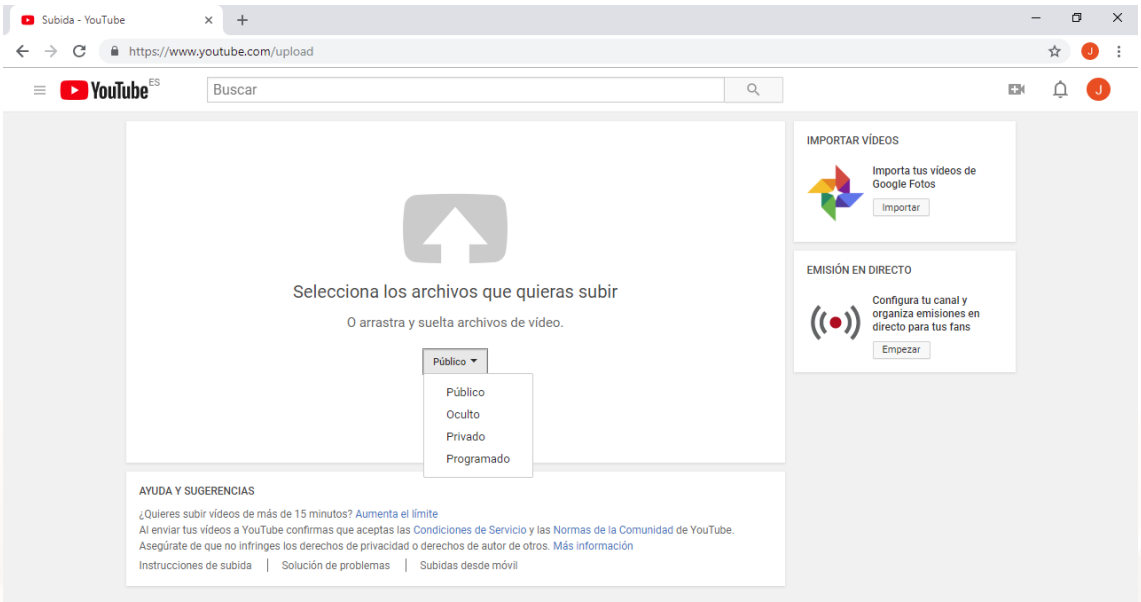

Imagen 54. Pantalla de subir video en YouTube.

5.8. Redes sociales de imagen

En el mundo online, el contenido visual es el que resulta más atractivo, divertido y entretenido al utilizar fotografías y vídeos para expresarnos. En el ámbito profesional, es una de las maneras más efectivas para llamar la atención de nuestro público objetivo, transmitir un mensaje determinado y promocionar una marca o producto.

Consecuentemente, las imágenes y vídeos han ganado terreno para convertirse en un imprescindible del "kit de supervivencia" en redes sociales, ampliando oportunidades de éxito entre las orientadas al ámbito social de las imágenes.

Las tres más utilizadas, Flickr[41], Instagram[42] y Pinterest[43], se fuerzan a buscar puntos diferenciadores entre ellas, para satisfacer al usuario y ganar posicionamiento en la mente del consumidor.

Flickr

Imagen 55. Logotipo de Flickr.

Orientada a la organización de imágenes, es la red social más antigua de las tres, aunque también la más estancada. Originalmente, se pensó para PC, pero después del auge de su lanzamiento no avanzó mucho más. Estas son sus principales ventajas y desventajas:

Ventajas:

- Versión básica gratuita.
- Almacenamiento y clasificación de vídeos e imágenes.
- Opción de compartir archivos con quien quieras, cuando quieras.
- Posibilidad de editar imágenes con filtros y efectos de máxima resolución.

Desventajas:

- La versión gratuita es de baja calidad y limitada resolución de imagen.
- Existe una versión Premium (de pago), que cuenta con funcionalidades adicionales de almacenaje y resolución.

[41] https://www.flickr.com/
[42] https://www.instagram.com/
[43] https://www.pinterest.es/

- Servicio lento y algo pesado de subida y descarga de imágenes.
- Bastante obsoleto a nivel social, ya que los botones para compartir en otras redes están poco visibles.

La popularidad de Flickr se debe fundamentalmente a su capacidad para **administrar imágenes** mediante herramientas que permiten al autor etiquetar sus fotografías y explorar y comentar las imágenes de otros usuarios.

Esta característica fundamental de Flickr es la que hace que no sea un mero sitio donde almacenar tus fotos, si no que consigue darle una dimensión más social al abrir la posibilidad de etiquetar, comentar, etc.

Instagram

Imagen 56. Logotipo de Instagram.

Es el alma de la imagen social debido a que fue pensada, desde un principio, para dispositivos móviles inteligentes. Instagram es la red social más utilizada entre usuarios jóvenes. Se diferencia del resto mediante el concepto de "compartir momentos puntuales".

Por ello, Instagram representa la herramienta ideal para promocionar una marca o concepto específico, transmitir información sobre la cultura empresarial o compartir imágenes asociadas con un único tema.

Instagram tiene más de 1.000 millones de usuarios activos en un mes y más de 600 millones de ellos usan la plataforma diariamente.

Esta es la red social con mayor crecimiento, llegando duplicar el número de usuarios en solo dos años.

Ventajas:

- Gratuita.
- Puramente social, con mucha facilidad a la hora de compartir imágenes de forma interna, con seguidores, o externa, a través de otras redes sociales.
- Opción de editar imágenes con filtros, efectos y marcos.
- Ideal para transmitir valores o mensajes determinados
- Potenciado con el uso de etiquetas (*hashtags)* y *emojis*.
- Dispositivo móvil como canal principal.

Desventajas:

- Imposibilidad de organizar imágenes por categorías, sino que se almacenan en un solo lugar, por orden de publicación. Por lo que, para buscar una imagen específica, habría que recorrer el perfil de arriba abajo hasta encontrarla.

Descarga y registro

Instagram es una aplicación totalmente gratuita. Está disponible para iPhone, iPad y iPod touch en la App Store[44] de Apple y en Google Play Store[45] si tienes un smartphone o tablet Android.

Al abrir la app en tu dispositivo móvil, tendrás las opciones de registrarte o iniciar sesión. El proceso de registro es bastante amigable y sencillo. Debes elegir un nombre de usuario y tu contraseña, para eso te damos un consejo: si tienes X (antes Twitter), utiliza el mismo nombre que utilizas en esa red social para evitar identificarte de distintas formas en diferentes plataformas. Será más fácil para tus seguidores.

[44] https://itunes.apple.com/es/app/instagram/id389801252?mt=8/
[45] https://play.google.com/store/apps/details?id=com.instagram.android&hl=es

En la pantalla de registro verás una opción para utilizar tu información de Facebook. Si eliges esto, tendrás tu misma foto de perfil en ambas redes sociales y utilizarás el mismo correo electrónico con el que creaste tu perfil de Facebook.

Para la foto de perfil también tienes la opción de utilizar la misma que utilizas actualmente en X (antes Twitter), tomar una tú mismo directamente con la cámara o elegir una que ya tengas en la galería.

Finalmente pones tu nombre completo, dices qué correo electrónico quieres utilizar y estás listo para usar Instagram.

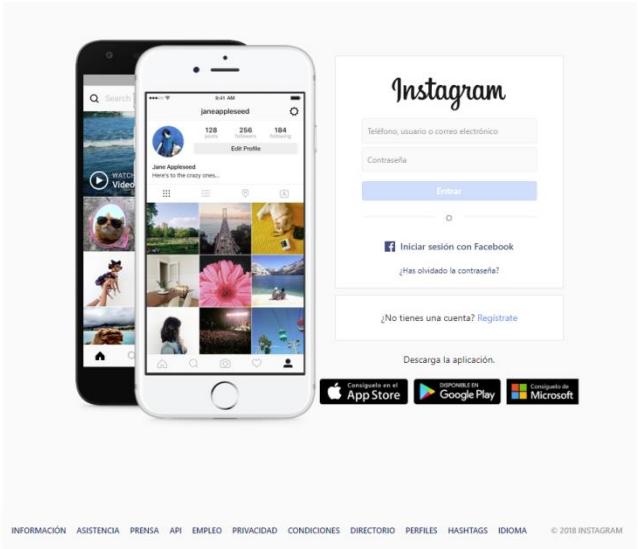

Imagen 57. Página principal de Instagram.

Navegación

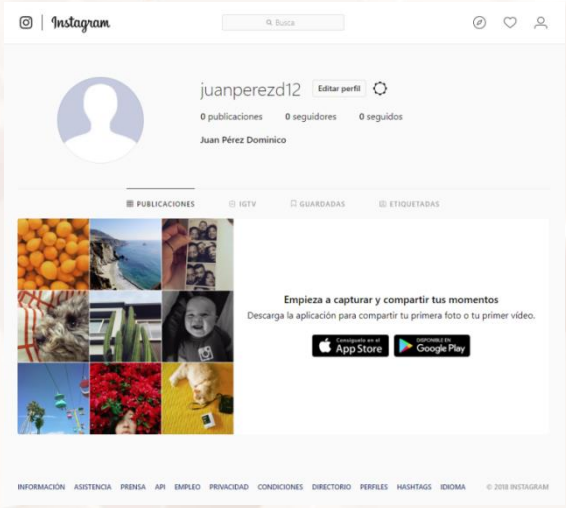

Imagen 58. Página que aparece tras el registro en el ordenador.

Tras la descarga de la aplicación al móvil, te encuentras con 5 opciones principales en el menú de la parte inferior:

Imagen 59. Menú principal de la aplicación.

Inicio

Es el botón principal por defecto que se identifica con un ícono de una casa. Muestra las fotos que son publicadas por los usuarios que sigues, dando la oportunidad de dar “like” para indicar que te gusta, escribir comentarios o enviar a otro usuario de manera privada. Anteriormente se mostraban por orden cronológico como Twitter, pero recientemente se estableció un algoritmo que ordena las publicaciones según tus gustos. A medida que utilices la app, esto se irá estructurando automáticamente.

Explorar

Tiene un ícono de una lupa. Es la segunda opción principal disponible de derecha a izquierda en el menú inferior. Te permitirá mostrar las fotos más populares, que tienen más likes por tu red de seguidores y te permite buscar otros usuarios para seguir, además de hashtags y lugares a través de un sistema de geolocalización. Con esto, podrás hacer crecer tu cuenta y encontrar nuevos intereses.

Reels

Tiene un icono de claqueta con un triángulo dentro. Los reels son uno de los tipos de publicación que se pueden hacer en Instagram y consisten en vídeos cortos que no desaparecen tras 24 horas como las stories. Puedes darles like, comentarlos y compartirlos, tanto por mensaje directo como en tus stories. Los botones para hacerlo se encuentran en el lado derecho inferior de la pantalla.

Para pasar de un reel al siguiente, hay que desplazarlo hacia arriba. Mientras se reproducen, no se pueden pausar pero se pueden silenciar dando un toque

sobre el centro de la pantalla. Los reels que te aparecen varían en función de tus gustos y de aquellas cosas que ves con más frecuencia así que puede que los que te aparecen sean completamente distintos a los de otras personas de tu entorno.

Tienda

Instagram también funciona como un escaparate para aquellos usuarios que tienen productos que ofertar. En esta sección puedes encontrar productos de la gente que sigues como si fuera una tienda online conjunta. Las publicaciones aparecen en un muro igual que el del perfil de una persona. Pulsando sobre cualquiera de las fotos aparece más información sobre el producto y el precio que tiene.

También se puede buscar por nombre en la barra de búsqueda superior y guardar algún producto para verlo más tarde. En la parte superior derecha hay un icono con tres rayas horizontales que permite ver más información, como la actividad de compra de tu cuenta y las tiendas que tienen las personas que sigues. También encontrarás vídeos y tiendas sugeridas por Instagram en función de tus gustos, aunque no sean de gente que sigues.

Perfil

Pulsando aquí entrarás en tu perfil tal y como lo ven otros usuarios. Podrás ver las fotos que has publicado, los reels y las publicaciones en las que te han etiquetado. También encontrarás un botón para Editar el Perfil.

Editar perfil: cambiar tu información disponible en tu perfil para los demás usuarios.

En la parte superior derecha hay un botón con tres rayas horizontales que te permite ver más opciones relacionadas con el perfil. Desde aquí puedes acceder a más opciones sobre la aplicación y tu cuenta. Las opciones que te aparecen son las siguientes:

- Configuración: Configura tu cuenta y la aplicación. Puedes invitar a amigos, ajustar las notificaciones, la privacidad de tu cuenta…

- Archivo: Aquí puedes ver todas las stories que has subido a Instagram.
- Obtener Insights: Aquí puedes configurar tu cuenta como una cuenta de creador para obtener más información (Insights) de tus publicaciones, su alcance, las interacciones que tienen…
- Tu actividad: Puedes consultar más información sobre tu uso de Instagram, cuánto tiempo pasas en la app, ver el contenido que has compartido, tus interacciones, tus likes…
- Código QR: Genera un código QR para ver tu perfil de Instagram. También te permite escanear otros códigos.
- Guardado: Aquí puedes ver todas las publicaciones que hayas guardado para ver más tarde.
- Pedidos y pagos: Aquí puedes ver información sobre las compras que hayas hecho.
- Mejores amigos: Lista de personas que hayas guardado en mejores amigos.
- Favoritos: Puedes consultar la lista de favoritos, que saldrán de manera preferente en las stories que se muestran al entrar en la aplicación.
- Descubrir personas: Aquí puedes buscar amigos utilizando tus contactos guardados. Tendrás que darle acceso a Instagram a tu lista de contactos para poder hacerlo.
- Centro de información sobre COVID-19: Instagram tiene un centro de información en el que consultar datos verificados sobre la pandemia.

Pinterest

Imagen 60. Logotipo de Pinterest.

Pinterest es la red social más benjamina de las tres, y probablemente la más versátil, ya que nació para ser utilizada tanto en PC como en móvil.

Ventajas

- Máxima interacción social, a través de otras redes, con opción de seguir a terceros y compartir imágenes dentro y fuera de la plataforma.
- Posibilidad de seleccionar las fotografías que más te gusten (con un pin), que se agrupan automáticamente en un mismo grupo, creando un grupo de “favoritos”.
- Opción de catalogación de imágenes.
- Viralización a través de etiquetas, hashtags y repins.
- Diseño atractivo y dinámico.
- Rapidez en la subida de fotos.

Desventajas

- La subida de imágenes ha de hacerse de manera individual. Por ello, si quisiéramos subir una colección, tardaríamos bastante.
- Foco en países anglosajones, por lo que hay poca presencia en España.

5.9. Otras redes sociales

MySpace

MySpace[46] es una red social que provee de: redes de amigos, grupos**, blogs, fotos, vídeos y música**, además de una red interna de mensajería que permite comunicarse a unos usuarios con otros y un buscador interno.

Imagen 61. Logotipo de MySpace.

LinkedIn

LinkedIn[47] es una red social orientada a profesionales y negocios. Es un gran recurso para generar más tráfico hacia tu *website* y ganar más visibilidad para tu persona y tu negocio.

LinkedIn cuenta con 663 millones de usuarios activos en un mes En España hay unos 12 millones de usuarios de LinkedIn.

Esta red social, orientada a grupos profesionales, también ha tenido un importante crecimiento en el último tiempo y ha evolucionado en los últimos años pasando de ser un canal de social media de reclutamiento a uno donde se comparte información de valor agregado de las diferentes profesiones.

LinkedIn es otro canal de social media necesario para todas las empresas que quieran utilizar las redes sociales como un canal de comunicación y marketing.

Imagen 62. Logotipo de LinkedIn.

[46] https://myspace.com/
[47] https://es.linkedin.com/

TikTok

TikTok[48] es una red social para compartir vídeos muy cortos: de tres segundos a un minuto. En dicha red se pueden encontrar vídeos de diferentes temáticas, principalmente danza y comedia. Es propiedad de la empresa china ByteDance.4 país donde recibe el nombre de Douyin. TikTok ha tenido un crecimiento exponencial y en estos momentos cuenta con 800 millones de usuarios activos al mes en todo el mundo. Aglutina a un público muy joven: el 41% de los usuarios de TikTok tienen entre 16 y 24 años.

Imagen 63. Logotipo de TikTok.

X (antes Twitter)

X (antes Twitter[49]) es una red social, que permite a sus usuarios estar en contacto mediante pequeños **mensajes de texto** (menos de 280 caracteres) que son denominados “tweets”.

X cuenta con más 350 millones de usuarios activos en un mes. Es una red social que es mayoritariamente pública lo que permite a las marcas realizar escucha social a través de ella. El envío de estos mensajes puede ser tanto desde el sitio web X como desde un teléfono móvil, un servicio de mensajería instantánea o desde otra red social como Facebook.

Imagen 64. Logotipo de X

[48] https://www.tiktok.com/

[49] https://x.com/?lang=es

06. Seguridad informática

La seguridad de nuestros equipos informáticos es muy importante, y debemos tener especial cuidado sobre todo cuando nos conectamos en red y accedemos a páginas web o archivos que pueden amenazar nuestros equipos y acceder incluso a información personal y privada, e incluso a datos confidenciales como cuentas bancarias, y otra documentación sensible.

Esta seguridad tiene que existir para todos los usuarios de Internet, es decir, todas aquellas personas que tengan conectado un ordenador a la red o cualquier otro dispositivo móvil a una red wifi, tienen que asegurarse de trabajar con las mejores condiciones posibles.

6.1. Tipos de amenazas a la seguridad informática en la red

En la red hay posibles peligros que puedan encontrarse entre lo que se conoce como ingeniería social: (spoofing, phishing, pharming…).

Spoofing

Hace referencia a todas las posibilidades de suplantación de identidad.

Solución posible

La configuración de cortafuegos en los router puede prevenir estos ataques.

Forma de evitarla por parte de los padres

Asegurarse de una correcta configuración de los router que permita filtrar la información que pueda llegar a los equipos.

Phishing

Consiste en el robo de contraseñas para su posterior mal uso.

Solución posible

Los antivirus más modernos suelen contar con aplicaciones para combatirlo.

Forma de evitarla por parte de los padres

Verificar que las webs que visitan son las auténticas a través de los certificados digitales, instalar programas de seguridad.

Además, también hay otros riesgos posibles relacionados con los equipos. Pueden existir las siguientes amenazas: Virus, Troyanos, Spyware, Exploits, Keylogger, etc.

Esta información extraída del Blog en familia recoge de manera muy clara los peligros de la red, una solución posible y cómo los padres/tutores podemos protegernos:

Citamos a continuación una lista de posibles amenazas a la seguridad informática de nuestros equipos y dispositivos móviles. Se incluyen posibles soluciones para cada amenaza y la forma de evitarlas por parte de padres, tutores o adultos. En algunos casos, estas amenazas pueden afectar a adultos que no vigilen la seguridad de sus equipos.

Virus

Un virus es un programa informático que infecta al ordenador. El modo en que afecta al sistema depende del tipo de virus, ya que hay algunos del tipo gracioso que lo único que hacen es sacar un mensajito, hasta los más poderosos que se propagan y destruyen datos, y podrían anular información valiosa.

Es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario, y habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este.

Solución posible y forma de evitarla por parte de los padres

- Evitar descargar archivos de fuentes no fiables.
- Instalar un software para la eliminación de virus (antivirus).

Gusano

Es un virus informático que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

Solución posible y forma de evitarla por parte de los padres

Los programas antivirus y antispyware son de ayuda, pero se deben mantener actualizados periódicamente con los patrones de los nuevos gusanos que puedan ir apareciendo con nuevos patrones de archivos periódicamente.

Spyware

Son programas maliciosos que recopilan información del ordenador del usuario para usarlo de forma no autorizada, normalmente transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

Solución posible y forma de evitarla por parte de los padres

Las soluciones más adecuadas son:

- Borrar el historial del navegador cada vez que se termine la sesión; y, sobre todo, las cookies.
- Instalar software para la eliminación de spyware.

Malware

Al igual que el spyware son programas maliciosos que tienen por objetivo dañar el equipo.

Solución posible y forma de evitarla por parte de los padres

Tener unas buenas herramientas de eliminación de software malicioso, así como un antivirus o un cortafuegos.

Keylogger

Es un tipo de spyware cuya acción consiste en capturar nuestro teclado y las pantallas si es screenlogger.

Solución posible y forma de evitarla por parte de los padres

Las soluciones más adecuadas son borrar todo el rastro de navegación e instalar software para eliminar spyware.

Rootkits

Un rootkit es un programa que permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones. Los rootkits tratan de borrar las huellas de los atacantes de los equipos. Fuente: Wikipedia[50].

Forma de evitarla por parte de los padres

- Instalación de antivirus y antispyware, así como programas que eliminen programas malintencionados.
- Evitar descargar archivos de fuentes no fiables.

Spam

El correo masivo consiste en la recepción de una gran cantidad de correo electrónico no solicitado, que invade y puede incluso bloquear las cuentas de correos que utilizamos.

[50] https://es.wikipedia.org/wiki/Rootkit

Solución posible y forma de evitarla por parte de los padres

Utilice los sistemas antispam de su proveedor de Internet o del programa de correo electrónico.

No abra nunca archivos adjuntos de un correo desconocido y borre el que no le parezca conocido.

Troyano

Es un programa informático más potente que el virus. El troyano afecta al sistema de tal modo que otra persona puede remotamente controlarlo.

Es un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero al ejecutarlo ocasiona daños. El término troyano proviene de la historia del caballo de Troya mencionado en la Ilíada de Homero. Fuente: Wikipedia[51].

Solución posible y forma de evitarla por parte de los padres

- Instalación de antivirus y antispyware, así como programas que eliminen programas malintencionados.
- Evitar descargar archivos de fuentes no fiables.

6.2. Consejos y programas informáticos que nos pueden ayudar

A continuación, se van a explicar, por un lado, algunas **malas prácticas** que es bueno desterrar a la hora de navegar por Internet y, por otro lado, aplicaciones que nos pueden ayudar, tanto a evitar los **contagios** que afecten a nuestro ordenador (Antivirus), como a controlar los **tiempos de uso** del mismo (WinOff).

[51] https://es.wikipedia.org/wiki/Troyano_(inform%C3%A1tica)

En el tema de la seguridad, las herramientas informáticas, tales como Antivirus o programas de control de acceso, son necesarias, pero lo fundamental es **evitar hábitos de riesgo**. La propagación de amenazas es el resultado de la falta de cautela.

Acciones que no se deben realizar

- Abrir correos de desconocidos con asuntos llamativos o sospechosos.
- Desactivar el antivirus u otras medidas de seguridad para poder acceder a determinados servicios.
- Compartir programas a través de las redes P2P (Emule, Ares, Kazaa, etc.) sin comprobar antes que no están infectados.
- Dar la dirección de email a desconocidos.
- Agregar contactos desconocidos a los programas de mensajería instantánea ICQ[52], Facebook Messenger[53], etc.).
- Pulsar enlaces que aparecen repentinamente en las conversaciones.

Los antivirus y antiespías

Los antivirus nacieron durante la década de 1980 como una herramienta simple, cuyo objetivo era **detectar y eliminar virus informáticos**.

Con el transcurso del tiempo y la aparición de sistemas operativos más avanzados e Internet, los antivirus han **evolucionado** hacia programas más avanzados capaces de, no solo buscar o detectar virus informáticos, sino también de bloquearlos, desinfectar los equipos y prevenir una futura infección de los mismos.

[52] https://www.icq.com/es
[53] https://www.messenger.com/

Actualmente, ya son capaces de reconocer otros tipos de ***malware***. El *malware* (malicious software) es el término empleado para referirse a las aplicaciones informáticas que han sido programadas intencionadamente con el objetivo de colarse en los equipos informáticos con el propósito de dañarlos o, simplemente, causar cualquier tipo de incordio no esperado por el usuario.

El **funcionamiento** de un antivirus varía de uno a otro, aunque su comportamiento normal se basa en contar con una lista de virus conocidos y su forma de reconocerlos (las llamadas firmas o vacunas). El programa analiza constantemente los archivos almacenados o transmitidos desde y hacia un ordenador teniendo en cuenta esa lista de virus.

Adicionalmente, muchos de los antivirus actuales han incorporado funciones de **detección proactiva**, que no se basan en una lista de malware conocido, sino que analizan el comportamiento de los archivos o comunicaciones para detectar cuáles son potencialmente dañinas para el ordenador.

El objetivo primordial de cualquier antivirus actual es **detectar** la mayor cantidad de amenazas informáticas que puedan afectar a un ordenador y bloquearlas antes de que la misma pueda infectar un equipo, o poder eliminarla tras la infección. Actualmente hay una **gran variedad** de antivirus.

Los **antiespías** funcionan de modo similar a los programas antivirus, pero analizan el sistema en busca de programas espías y los eliminan. Estos programas son complementarios de los antivirus. Teniendo ambos instalados en nuestro ordenador estaremos mejor protegidos contra posibles intrusiones en nuestro sistema.

Tipos de antivirus

Hay dos tipos de antivirus diferentes:

- Los antivirus de escritorio. Se instalan en los ordenadores y dispositivos para protegerlos en todo momento de cualquier posible infección, ya sea al navegar por Internet, recibir algún correo infectado o introducir en el equipo algún dispositivo extraíble (USB, CD…) que esté infectado. No es necesario que el dispositivo esté conectado a Internet para que funcionen,

pero sí que es necesario actualizarlos frecuentemente para que sean capaces de detectar las últimas amenazas de virus.

- Antivirus online: que son útiles para analizar el ordenador o dispositivo móvil con un segundo antivirus cuando sospechamos que el equipo puede estar infectado. Para su ejecución es necesario acceder a una página de Internet.

  Si bien son muy útiles para realizar un escaneo del ordenador y, de este modo, comprobar que no está infectado, no sirven para prevenir infecciones, esto solo lo hacen los antivirus de escritorio.

Cortafuegos

En general un cortafuegos es un programa que restringe las conexiones TCP/IP, es decir, las transmisiones de información que puede iniciar o recibir un ordenador conectado a una red.

Hay varios **tipos de cortafuegos:**

- Los cortafuegos perimetrales, los más clásicos, hacen de pasarela entre una red local de una organización e Internet. Dejan entrar y salir solo el tráfico que definan los administradores de la red, y habitualmente hacen traducción de direcciones de red (NAT o también llamado enmascaramiento) y escanean el tráfico en busca de virus y otros programas maliciosos.
- Los cortafuegos personales que están diseñados para ser instalados en un ordenador o dispositivo personal o en una pequeña empresa conectado directamente a Internet. Son especialmente recomendables para conexiones con dirección IP fija, como el ADSL.

Análisis de ficheros

En algunos casos es posible que nuestra herramienta antivirus no sea capaz de detectar ficheros infectados por lo que es recomendable analizar ficheros en los siguientes casos:

- Cuando recibimos ficheros de procedencia desconocida a través de correos electrónicos.
- Cuando intercambiamos archivos a través de redes P2P.
- Cuando descargamos alguna aplicación o fichero desconocido desde Internet.

Mataemergentes o pop-up killers

Existen unas molestas ventanas que aparecen cuando navegamos en alguna página web que se denominan pop-ups. Hay muchos programas que anulan a estas, denominados mataemergentes (pop-up killers), tanto gratuitos como de pago.

- Un sistema no ejecuta el código que las abre; son muy eficaces, pero pueden fallar si se abre con otros métodos, como desde una película de Flash.
- Reconoce la ventana emergente y la cierra. Suelen ser aplicaciones independientes del navegador que reconocen la ventana por su título, su tamaño, la URL que cargan u otros parámetros y la cierran. Son menos eficientes, pero más fiables puesto que no dependen del mecanismo de apertura de la ventana.

Métodos de contagio más habituales

De entre todos los tipos de **malware** mencionados anteriormente, son sobre todo dos los más habituales: los **virus**, cuya instalación o ejecución acepta el usuario en un momento dado de manera inadvertida y los **gusanos**, con los que el programa malicioso actúa replicándose a través de las redes.

En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de **comportamientos anómalos o no previstos**. Dichos comportamientos son los que dan la traza del problema y tienen que permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).
- Ingeniería social; mensajes como: «Ejecute este programa y gane un premio».
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software que pueda contener uno o varios programas maliciosos.
- Unidades extraíbles de almacenamiento (USB).

07. Actividades prácticas

Este último capítulo propone una serie de actividades prácticas que te pueden ayudar a consolidar algunos de los conceptos más importantes explicados a lo largo de este manual. Te invitamos a que realices estos y otros ejercicios. ¡Recuerda que cuanto más practiques, más aprenderás!

7.1. Seguridad en Internet. Protección para sus hijos

1) Asesor de contenidos

Introducción

El navegador web Internet Explorer permite establecer unos parámetros de protección que aseguran la navegación segura en Internet.

Ejercicio práctico

Accede al **"Asesor de contenidos"** del navegador Internet Explorer y habilítalo si no lo está ya. A continuación, realiza las siguientes operaciones:

1. Establece una "Contraseña de supervisor".
2. Añade la dirección de un sitio web (el que quieras) al listado de sitios web bloqueados y acepta todos los cambios.
3. Escribe la dirección del sitio web que has bloqueado y comprueba que solo es posible visitarlo insertando la contraseña del supervisor.

Si tienes dudas, puedes consultar el capítulo 1.4 de la guía que se entrega a los alumnos que asisten a este taller. Además, puedes consultar la información que aparece en el sitio web oficial de Windows[54].

[54] https://support.microsoft.com/es-es/windows

2) Historial de navegación

Introducción

Los navegadores web almacenan información acerca de los sitios web que visitamos mientras navegamos por Internet en el denominado historial de navegación.

Ejercicio práctico

Accede al **"Historial de navegación"** de tu navegador y revisa cuáles son los sitios web que se han visitado durante los últimos dos días desde tu ordenador.

La manera de consultar el "Historial de navegación" dependerá de la versión que tengas del navegador. Por ejemplo, en Internet Explorer 9, puedes acceder desde el menú: **Ver** > **Barras del explorador** > **Historial**.

3) Consultar las descargas realizadas

Introducción

Desde Internet podemos descargar multitud de documentos y ficheros de todo tipo: imágenes, vídeos, canciones, documentos PDF, etc. En el caso de los menores, conviene comprobar la idoneidad de estos contenidos y verificar que son apropiados para ellos.

Ejercicio práctico

Consulta qué documentos se han descargado recientemente desde tu ordenador. Para ello, debes acceder a la opción Ver descargas de tu navegador web.

La manera de consultar las descargas dependerá de la versión que tengas del navegador. Por ejemplo, en Internet Explorer 9, puedes acceder mediante el menú: Herramientas > Ver descargas.

7.2. El correo electrónico

1) Creación de una cuenta de Gmail

Introducción

Gmail es el cliente de correo electrónico desarrollado por la compañía Google. Existen muchos otros clientes de correo (Yahoo, Outlook, AOL, etc.), pero Gmail se ha hecho tremendamente popular en los últimos años por su integración con multitud de servicios web de Google y por ser el correo que se utiliza en los dispositivos móviles con sistema operativo Android.

Ejercicio práctico

Accede a la página de Gmail[55] y crea una nueva cuenta de correo. Esta cuenta la utilizarás para completar algunas de las actividades prácticas de este curso. La puedes eliminar cuando finalices el curso, si quieres.

Una vez que tengas la cuenta creada, envíale un correo al tutor del curso con el asunto “Cuenta Gmail creada” e indícale tu nombre y apellidos en el cuerpo del mensaje.

El tutor te responderá, enviándote un listado con las direcciones de correo de algunos de tus compañeros de curso. Envía un correo a cada uno de ellos con una breve presentación de ti y guarda estas direcciones de correo en tu libreta de contactos para poder interactuar con ellos durante la realización de este curso.

2) Marcar un correo como spam

Introducción

Con el término **spam**, nos referimos a aquellos correos electrónicos no solicitados y que, normalmente, contienen publicidad engañosa. Estos correos intentan convencernos de comprar productos que no hemos pedido, de dudosa calidad y en sitios web de procedencia desconocida.

[55] https://mail.google.com/

Ejercicio práctico

De entre todos los correos que hayas recibido de otros compañeros de curso:

1. Escoge uno y respóndele, diciéndole que quieres comprobar el funcionamiento del filtro antispam de Gmail y que, para ello, necesitas que te envíe otro correo.

2. Marca como spam el correo que habías escogido en paso anterior.

3) Crear filtros de mensaje

Introducción

Los filtros de mensaje son una utilísima herramienta que nos permite administrar el flujo de mensajes entrantes, de manera que podemos especificar qué queremos hacer con ellos: archivarlos, borrarlos, moverlos a una determinada carpeta, reenviarlos, etc.

Ejercicio práctico

Para poder comprender mejor cómo funcionan los filtros de mensaje, vamos a crear uno que cumpla la siguiente funcionalidad: Todos los correos que te lleguen de un determinado compañero de curso (escoge el que quieras) serán marcados por Gmail como "**Destacados**".

Una vez que hayas creado el filtro de mensaje, escribe a esa persona y pídele que te mande un correo para poder comprobar que el filtro funciona correctamente.

> **Nota:** Los correos destacados aparecen marcados en Gmail con una estrella amarilla.

7.3. Mensajería instantánea

1) Creación de una cuenta de Skype y búsqueda de contactos

Introducción

Skype es un sistema de mensajería instantánea adquirido por Microsoft que permite enviar y recibir mensajes, además de realizar llamadas y videollamadas a través de Internet.

Ejercicio práctico

Accede a la web de Skype[56] y crea una nueva cuenta de usuario. Una vez que la hayas creado, añade a tu libreta de contactos, al menos, a tres de tus compañeros de curso (el tutor del curso te mandará sus datos por correo electrónico).

Una vez que ellos te hayan correspondido y también te hayan incluido en su libreta de direcciones, ya podrás contactar con ellos. Compruébalo mandándoles un mensaje de texto a través del sistema de mensajería instantánea de Skype.

2) Bloquear a un contacto en Skype

Introducción

Es posible que, por el motivo que sea, queramos bloquear a un usuario de Skype para que no nos moleste con mensajes o con llamadas.

[56] https://www.skype.com/es/

Ejercicio práctico

Accede a la web de Skype[57] y crea una nueva cuenta de usuario. Una vez que la hayas creado, añade a tu libreta de contactos, al menos, a tres de tus compañeros de curso (el tutor del curso te mandará sus datos por correo electrónico).

De los 3 contactos que has añadido a tu cuenta de Skype en la actividad anterior, escoge uno y bloquéalo.

A continuación, mándale un correo a través de vuestras cuentas de Gmail. El correo tendrá el asunto "Bloqueo en Skype" y en el cuerpo del mensaje, debes explicarle que le has bloqueado en Skype y que quieres que intente hacerte una videollamada. Esta persona no debería poder realizar dicha videollamada. Pídele que te responda por correo con el resultado de la prueba.

3) Consultar el registro de actividad en Skype

Introducción

Skype registra nuestra actividad: llamadas de voz realizadas o recibidas, mensajes de texto, etc. En el caso de que tengas menores a tu cargo que usen este programa, puede ser interesante consultar este registro para ver con qué otros usuarios interactúan los menores.

Ejercicio práctico

Consulta tu registro de actividades recientes: llamadas y videollamadas realizadas y recibidas, mensajes mandados, intercambio de archivos realizados, etc.

[57] https://www.skype.com/es/

7.4. Redes sociales

1) Creación de una cuenta de Facebook y búsqueda de contactos

Introducción

El principal objetivo de Facebook es estar en contacto con nuestros amigos, familiares, conocidos, vecinos, etc. Para ello, es necesario que primero nos registremos y después enviemos una solicitud de amistad a cada una de esas personas.

Ejercicio práctico

Crea una nueva cuenta de Facebook. Busca al menos a 3 de tus compañeros de curso y solicítales que te agreguen como amigo. Puedes localizarlos a través de sus nombres, usando el buscador de Facebook.

2) Creación de una lista de contactos

Introducción

En el momento de darte de alta en Facebook, se crean unas listas con el objetivo de que clasifiques en ellas a tus contactos y te sea más fácil comunicarte con ellos: familia, mejores amigos, conocidos, etc. Además, tenemos la posibilidad de crear nuevas listas y administrarlas.

Ejercicio práctico

Crea una lista llamada "Curso Navegar" y, una vez que tus compañeros hayan aceptado tu solicitud de amistad, asócialos a esta lista.

Escribe un comentario en tu biografía y personaliza el ámbito de la publicación de manera que solo la lista "Curso Navegar" pueda ver dicho comentario.

3) Consultar el registro de actividad

Introducción

Al igual que ocurre en Skype, también en Facebook es posible consultar la actividad reciente de un usuario. Estas verificaciones pueden ser interesantes cuando se está al cargo de menores y estos usan Facebook, ya que permiten estar al tanto de las relaciones sociales que estos menores tienen en Internet.

Ejercicio práctico

Comprueba las siguientes cuestiones de tu perfil:

1. Últimas actualizaciones del estado.
2. Mensajes recibidos y enviados recientemente.
3. Actividad más reciente de la biografía.

4) Bloquear a una persona

Introducción

También en Facebook es posible bloquear a personas o aplicaciones para que no nos molesten ni puedan tener acceso a nuestra privacidad.

Ejercicio práctico

Escoge a una de las personas que has metido en la lista "Curso Navegar" y bloquéala. Después, comprueba que ya no puede interactuar con tu perfil de usuario.

08. Anexo.

8.1. Enlaces y referencias

- Webs utilizadas en la guía:
  - Filtro SafeSearch de Google[58].
  - Vikidia[59].
  - Banco de imágenes y sonidos del INTEF[60].
  - Khan Academy[61].
  - PequeNet[62].
  - iTunes Educación[63].
  - Podcasts para niños y familias[64].
  - Página del INTEF[65].
  - Internet Segura ForKids[66].
  - Educación 3.0[67].
  - Kid and teens online[68].
  - Skype[69].

58 https://support.google.com/websearch/answer/510?hl=es&p=adv_safesearch
59 https://es.vikidia.org/wiki/Vikidia:Portada
60 https://procomun.intef.es/
61 https://es.khanacademy.org/
62 http://www.pequenet.com/
63 https://www.apple.com/es/education/k12/
64 https://music.apple.com/es/genre/m%C3%BAsica/id34
65 https://intef.es/
66 https://www.is4k.es/
67 https://www.educaciontrespuntocero.com/
68 https://kidsandteensonline.com/
69 https://www.skype.com/

- Mozilla Thunderbird[70].
- Outlook[71].
- Facebook[72].
- X (antes Twitter[73]).
- Pinterest[74].
- MySpace[75].
- Hi5[76].
- Flickr[77].
- LinkedIn[78].
- VLC media player[79]
- Aula 365[80]
- Qustodio[81].
- INCIBE(Instituto Nacional de Ciberseguridad)[82].
- WhatsApp[83].
- Skype[84].

[70] https://www.thunderbird.net/es-ES/
[71] https://www.microsoft.com/es-es/outlook-com/
[72] https://www.facebook.com/
[73] https://x.com/?lang=es
[74] https://pinterest.com/
[75]https://myspace.com/
[76] https://www.hi5.com/
[77] https://www.flickr.com/
[78] https://es.linkedin.com/
[79] https://www.videolan.org/vlc/index.es.html

[80] https://www.aula365.com/
[81] https://www.qustodio.com/es/
[82] https://www.incibe.es/
[83] https://web.whatsapp.com/
[84] https://www.skype.com/es/

- Protección y seguridad en Skype y en Internet[85].
- Gmail[86].
- Yahoo[87].
- ICQ[88].
- Microsoft Outlook[89].
- Virus informático (Wikipedia) [90].
- Troyanos y gusanos (Wikipedia) [91].
- Spyware (Wikipedia) [92].
- Toolkit (Wikipedia) [93].

8.2. Imágenes

- Todas las imágenes de la guía son de creación propia mediante capturas de pantalla u otros.

[85] https://www.skype.com/es/security/?intsrc=client-_-windows-_-7.4-_-go-security&setlang=es
[86] https://mail.google.com/mail/u/0/#inbox
[87] https://es.yahoo.com/
[88] https://www.icq.com/es
[89] https://outlook.live.com/owa/
[90] https://es.wikipedia.org/wiki/Virus_inform%C3%A1tico
[91] https://es.wikipedia.org/wiki/Troyano_(inform%C3%A1tica)
[92] https://es.wikipedia.org/wiki/Spyware
[93] https://es.wikipedia.org/wiki/Rootkit