



Los diferentes riesgos en la
utilización de las redes sociales por
las personas mayores de catorce
años y menores de dieciocho años.

Universidad de Las Palmas de Gran Canaria

Estructura de Teleformación

Grado de Seguridad y Control de Riesgos

Trabajo Fin de Grado

Alumna: Laura Barrera Macías

Tutora: María Isabel Quintero Verdugo

Fecha de entrega: 15 de Julio de 2018

Los diferentes riesgos en la utilización de las redes sociales por las personas mayores de catorce años y menores de dieciocho años.

Universidad de Las Palmas de Gran Canaria

Estructura de Teleformación

Grado de Seguridad y Control de Riesgos

Trabajo Fin de Grado

Alumna: Laura Barrera Macías

Tutora: María Isabel Quintero Verdugo

Fecha de entrega: 15 de Julio de 2018

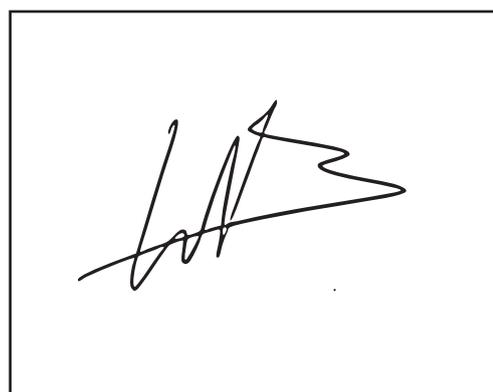
Firma de la tutora:



QUINTERO
VERDUGO
MARIA
ISABEL

Firmado digitalmente por
QUINTERO VERDUGO
MARIA ISABEL

Firma de la alumna:



Los diferentes riesgos en la utilización de las redes sociales por las personas mayores de catorce años y menores de dieciocho años.

Universidad de Las Palmas de Gran Canaria

Estructura de Teleformación

Grado de Seguridad y Control de Riesgos

Trabajo Fin de Grado

Alumna: Laura Barrera Macías

Tutora: María Isabel Quintero Verdugo

Fecha de entrega: 27 de Mayo de 2018

Firma de los miembros del Tribunal:

Calificación obtenida:

AGRADECIMIENTOS

Quiero agradecer a la Universidad de Las Palmas de Gran Canaria por darme la oportunidad de realizar este Trabajo de Fin de Grado, y finalizar así mis estudios en el Grado de Seguridad y Control de riesgos.

A mi tutora, Maria Isabel Quintero Verdugo, por el tiempo dedicado en mí y en mi proyecto, sin su ayuda no lo hubiera hecho realidad. Aportó la luz que necesitaba cuando en ocasiones no encontraba el camino.

Por cada consejo, Gracias.

A los profesores del Grado en Seguridad y Control de Riesgos, a los cuales recordaré siempre por los consejos, y la dedicación puesta en el alumnado.

A mi familia por el apoyo continuo que siempre recibo.

Siempre gracias.

ÍNDICE

INDICE DEL DOCUMENTO

1. RESUMEN/ ABSTRACT	9
2. INTRODUCCIÓN	11
3. OBJETIVOS	13
4. METODOLOGÍA	14
5. CONTENIDOS	15
5.1. Concepto de red social	15
5.2. Origen y evolución de las redes sociales	17
5.3. Las redes sociales más utilizadas	23
5.4. El perfil de los usuarios de las redes sociales	30
5.5. La utilización de las redes sociales por los mayores de catorces años: riesgos posibles	32
5.6. Normativa aplicable al uso de las redes sociales	43
5.6.1. Derecho de Protección de Datos de Carácter Personal	46
5.6.2. Derechos de Propiedad Intelectual	49
5.6.3. Derecho Fundamental al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen	52

5.7. Protección jurídica de los menores de edad en el uso de las redes sociales	55
5.8. Asociaciones españolas dedicadas la seguridad en la utilización de Internet y de las redes sociales.....	58
5.9. Recomendaciones de uso seguro y responsable del uso de las redes sociales.....	63
5.9.1. Recomendaciones básicas.....	64
5.9.2. Recomendaciones dirigidas a los mayores de catorce años	66
5.9.3. Recomendaciones a los padres y tutores.....	68
6. CONCLUSIONES/ CONCLUSION.....	71
7. GLOSARIO.....	76
8. FUENTES.....	78
8.1 Bibliografía.....	78
8.2 Recursos web.....	78
8.3 Legislación.....	83
9. ANEXOS.....	85
9.1 Anexo I.....	85
9.2 Anexo II.....	86

1. RESUMEN

La comunicación es un aspecto imprescindible para el desarrollo del ser humano, ha ido modificando nuestra manera de comunicarnos y relacionarnos gracias a la evolución tecnológica, proporcionan que las comunicaciones 2.0 aporten a la comunicación actual un sello de identidad, las redes sociales.

La mayoría de personas por todo el mundo hace uso de ellas, en constante actualización y cada vez en edades mas tempranas, esto es preocupante, ya que son herramientas de comunicación de las cuales, no existe una enseñanza previa por parte de tutores o padres, o de la misma sociedad y a consecuencia de ello, los menores de edad, hacen un mal uso de ellas en numerosas ocasiones.

Por ello, en el presente proyecto conoceremos que es una red social, de donde surgen y su evolución, destacaremos cuales son las redes sociales mas utilizadas y el perfil de los usuarios mas influyentes, es necesario saber, que Normativa existe en España aplicable al uso de las redes sociales, y la protección jurídica de los menores de edad en el uso de las redes sociales. También conoceremos asociaciones Españolas dedicadas a la seguridad en la utilización de internet y redes sociales.

De los catorce a los dieciocho años se vive en constante cambio personal y por ello social. Las redes sociales deberían ser una herramienta que acompañe en el desarrollo de los menores y no una herramienta que monopolice su desarrollo.

ABSTRACT

The communication is an essential aspect for the development of the human being, it has been modifying our mode to communicate thanks to the technological evolution, they provide that the communications 2.0 contribute to the current communication a seal of identity, the social networks.

Most people around the world use of them, in constant updating and every time at younger ages, this is disturbing, since they are communication tools of which, there is no previous teaching by tutors or parents, or from the same society and as a consequence, minors make a misuse of them on numerous occasions.

Therefore, in this project we will know what is a social network, where they arise and their evolution, we will highlight which are the most used social networks and the profile of the most influential users, it is necessary to know, what regulations exist in Spain applicable to the use of social networks, and the legal protection of minors in the use of social networks. We will also know Spanish associations dedicated to security in the use of internet and social networks.

From the age of fourteen to eighteen, people live in constant personal and therefore social change. Social networks should be a tool that accompanies the development of minors and not a tool that monopolizes their development.

2. INTRODUCCIÓN

Este trabajo de fin de grado pretende contextualizar el uso de las redes sociales en los menores, las consecuencias negativas que se pueden experimentar a partir de un mal empleo de estas herramientas online, da como resultado, la necesidad de un mecanismo de control hacia a los menores, y ese mecanismo de control no es otro que una labor de educación entre padres y educadores. Por ello en el presente trabajo se proporcionan unas medidas de seguridad y consejos básicos con el fin de facilitar las precauciones debidas con las redes sociales y obtener un mayor aprovechamiento y disfrute de ellas.

Las redes sociales han transformado la manera de relación entre las personas, en como nos conocemos y como nos dejamos conocer. Esta nueva forma resulta muchas veces beneficiosa pero otras muchas no resultan el mismo efecto, debido a las posibles consecuencias negativas a las que podemos estar expuestos.

Exponemos nuestra vida en la red, sin apenas conocer que pueden hacer con nuestros datos, quien ve nuestras fotos y que alcance puede llegar a tener la información publicada. Estos aspectos contienen un riesgo incrementado, si los usuarios de los que hablamos son menores de edad.

En el presente proyecto cuando hablemos de menores nos referiremos a los adolescentes entre 14 y 18 años, ya que la edad mínima para acceder a una red social son los 14 años, salvo las redes sociales específicas para menores.

Este y otros sesgos de la sociedad utilizan diariamente diversos dispositivos tecnológicos para acceder a Internet: móviles, tablets, ordenadores, videoconsolas, televisores...utilizando diferentes redes sociales, aplicaciones, juegos,

Es por ello que en estos aparatos se almacenan cantidades de datos personales, como son fotos, nombres de usuarios y claves que deben ser secretas, por consiguiente debemos perseguir una excelente seguridad en nuestros dispositivos ya que la pérdida de dichos datos podrían causar daños y más si tratamos de menores, en el que el descuido es mayor, a partir de ahí, para una mayor seguridad y confort en la red debemos proteger sus dispositivos, y enseñarles un uso adecuado de la red e internet.

Cuando un menor utiliza Internet proporciona gran cantidad de información sensible sobre sí mismo, construyendo la imagen que encontrarán los demás sobre él en la red: su identidad digital.

Es muy importante la prevención en el mundo cibernético, establecer unos hábitos de navegación seguros, extremar la precaución al conversar online, evitar prácticas de riesgo que veremos en el presente proyecto, ser conscientes de los riesgos o peligros que existen en la red forma parte de la prevención en seguridad informática.

La seguridad informática se encarga de crear procedimientos, métodos y normas que logren proteger la infraestructura, identificar y eliminar vulnerabilidades en la información y equipos físicos, así como proteger a los usuarios en las estructuras tecnológicas, zonas de comunicaciones y durante sus gestiones de información. En este sentido, establece normas que minimizan los riesgos a los que se exponen descargando contenidos de sitios web, en sus visitas a los portales o realizando transacciones en ellos.

Los menores si reservan su privacidad, no en redes sociales sino a cualquier adulto que pueda frenar o controlar sus hábitos en el uso de ellas, No miden la importancia de los actos en el mundo online, y las consecuencias que pueden llegar a experimentar. Por ello es de vital importancia recomendar un uso responsable, privado y coherente con el uso de las redes sociales y las infinitas oportunidades que ofrecen.

3. OBJETIVOS

El objetivo principal de este Trabajo de Fin de Grado, es determinar los posibles riesgos a los que se enfrentan los jóvenes cuando utilizan las redes sociales, y los aspectos negativos del uso indebido de las mismas.

Por otro lado, los objetivos secundarios son los siguientes:

- Definir el concepto de red social.
- Establecer las redes sociales mas utilizadas.
- Determinar los riesgos mas comunes en el uso de las redes sociales.
- Establecer la normativa relativa al uso de las redes sociales.
- Proponer unas recomendaciones para un uso seguro y responsable de las redes sociales.

4. METODOLOGÍA

Para lograr los objetivos se llevará a cabo una investigación bibliográfica, este método proporciona los datos tras una revisión exhaustiva de documentos con resultados en estudios reconocidos, utilizando artículos de publicaciones periódicas, monografías, documentos oficiales, recortes de asociaciones, trabajos presentados en conferencias o seminarios, testimonios de expertos, documentales, páginas en web especializadas, etc. En la actualidad, internet ofrece esta herramienta a la que se acceder con facilidad y de manera rápida puedes consultar en profundidad los textos de los diferentes autores frente a una materia determinada.

Por ello, para la realización de este trabajo se ha utilizado dicha metodología en la que todo el material recogido ha sido clasificado, ordenado y expuesto como fuentes de información a lo largo del presente trabajo.

El mayor beneficio del diseño bibliográfico es la amplia variedad de información disponible a través de los diferentes estudios realizados por diferentes profesionales o asociaciones expertas en la materia.

Este método nos será de utilidad para agrupar todo tipo de informaciones, poder extraer las conclusiones acertadas que proporcionen sentido a nuestros objetivos y permita darle a este trabajo una visión fundamentada acerca de los riesgos en las redes sociales.

5. CONTENIDOS

5.1. Concepto red social.

Las redes sociales se han convertido en un fenómeno social, son plataformas de comunidades virtuales que proporcionan información e interconectan a personas con afinidades o intereses comunes. Las redes sociales son uno de las mejores muestras de la Web 2.0 y la construcción de opinión en el entorno digital.

Estas redes, se expanden como sistemas abiertos en constante cambios y evolución de sí mismos, al igual que las personas que las utilizan.

Por otro lado, son disposiciones de interacción social, en la que su mayor característica es el intercambio activo entre personas o grupos, compartiendo información, generando contenido y participando en corrientes sociales mas destacadas a nivel nacional o mundial. Los usuarios de estas redes sociales pueden entablar relaciones por motivos muy diferentes como pueden ser de interés profesional o amistad entre otras.

En el siguiente ítem de este trabajo veremos el origen y evolución de las redes sociales, respecto a ello, la web ha hecho posible la interacción y comunicación virtual y *online* entre las personas, compartiendo conocimientos e intereses comunes a través de las redes y el entorno digital, que favorece la creación de aplicaciones complejas de forma más rápida, a un menor coste.



Figura 1: Características Redes Sociales. Elaboración propia.

5.2. Origen y evolución de las redes sociales.

Antes de conocer el origen y evolución de las redes sociales, debemos hacer un pequeño recorrido en la historia de Internet. Dicha historia se puede dividir en tres etapas: Web 1.0, Web 2.0, y Web 3.0.

La Web 1.0 se caracteriza por la emisión de contenido en webs cerradas y delimitadas, páginas estáticas en las que el usuario no participa en ninguna de las etapas del contenido que se ofrece, por lo que es un sujeto pasivo, simple observador del espacio creado. No se podían incluir comentarios ni nada parecido, y apenas se actualizaban.

Es complejo su fecha de inicio pero se podría datar la web 1.0 alrededor del 1991.

La Web 2.0, aparecen las redes sociales, el usuario pasa a formar parte activa del proceso, es decir, genera contenido para la web, como puede ser, subiendo vídeos a la plataforma de Youtube, fotos a Facebook, Instagram, dejando una opinión tras un artículo, votando por encuestas, o escribiendo en su propio blog. El paso de la web 1.0 a la 2.0 es clave en la historia de Internet, ya que cambió radicalmente los procesos creativos y colaborativos. El usuario se convierte en el autor del contenido publicado. Lo mas fascinante es la forma gradual en la que se produjo el proceso. Fue Tim O'Reilly quien analizó el fenómeno y lo acuñó.

La Web 3.0 es la fase en la que nos encontramos actualmente, datos en la nube, geolocalizaciones, inteligencia artificial y el big data (nuevas formas de procesar cantidades masivas de datos para generar contenido). La expresión Web 3.0 apareció por primera vez en 2006 en un artículo de Jeffrey Zeldman. Actualmente existe aún la controversia alrededor de lo que significa Web 3.0, y cuál es la definición más adecuada.

Buena parte de las ideas de la 3.0 siempre han estado ahí. No hay un gran cambio sino que en el fondo hablamos de una Web 2.0 mejorada.

Para continuar con la contextualización de las redes sociales, haremos una cronología de los hechos mas destacados del fenómenos que son.

En el año 1969, se realizó la primera conexión entre los ordenadores de Standford y UCLA, cuando también nació ARPANET. (Base del desarrollo de la actual Internet).

Dos años mas tarde, en 1971, Ray Tomlinson envió el primer e-mail y aparece el primer virus Creeper.

En el año 1973, se usa por primera vez la palabra internet en una transimisión de control de protocolo.

En el 1978, Ward Christensen y Randy Suess crean el BBS (Bulletin Board Systems) para informar a sus amigos sobre reuniones, publicar noticias y compartir información.

En el 1982, el gran auge de los emoticonos, cambió la forma de expresión hasta el día de hoy.

En 1991, el creador de la World Wide Web (WWW), el inglés Tim Berners-Lee, subió a Internet la primera página a través de su computadora.

En el año 1994, se lanza GeoCities, un servicio que permite a los usuarios crear sus propios sitios web y alojarlos en determinados lugares según su contenido y también en dicho año se funda Yahoo.

En 1995, la Web alcanza el millón de sitios web, y The Globe ofrece a los usuarios la posibilidad de personalizar sus experiencias on-line, mediante la publicación de su propio contenido y conectando con otros individuos de intereses similares. En este mismo año, Randy Conrads crea Classmates, una red social para contactar con antiguos compañeros de estudios. Classmates es para muchos el primer servicio de red social, principalmente, porque se ve en ella el germen de Facebook y otras redes sociales que nacieron, posteriormente, como punto de encuentro para alumnos y ex-alumnos. En este mismo año Microsoft lanza Internet Explorer.

Dos años más tarde en 1997 se produce el lanzamiento de AOL Instant Messenger, que ofrece a los usuarios el chat, al tiempo que comienza el blogging y se lanza Google. También se inaugura Sixdegrees, red social que permite la creación de perfiles personales y listado de amigos, algunos establecen con ella el inicio de las redes sociales por reflejar mejor sus funciones características. Sólo durará hasta el año 2000.

Fue en 1998, cuando nace Google, el mayor de los buscadores de Internet. Aparece Friends Reunited, una red social británica similar a Classmates. Asimismo, se realiza el lanzamiento de Blogger.

En el cambio de siglo, año 2000, estalla la “Burbuja de Internet”. En este año se llega a la cifra de setenta millones de ordenadores conectados a la Red.

Wikipedia aparece en el año 2001, en el 2002 se lanza el portal Friendster, que alcanza los tres millones de usuarios en sólo tres meses. Y nace LinkedIn, red social con intereses laborales por excelencia.

El 2003, fue un año importante por las redes sociales que se dan a conocer como MySpace, Skype y Facebook, aunque la fecha de esta última no está clara puesto que llevaba gestándose varios años. Creada por el conocido Mark Zuckerberg, Facebook se concibe inicialmente como plataforma para conectar a los estudiantes de la Universidad de Harvard. A partir de este momento nacen muchas otras redes sociales como Hi5 y Netlog, entre otras.

Fue en 2004 cuando se lanzan Digg, como portal de noticias sociales, en ese mismo año aparece Gmail, Flickr y Vimeo.

En 2005, otra de las grandes Youtube, comienza como servicio de alojamiento de vídeos, y MySpace se convierte en la red social más importante de Estados Unidos.

Un año mas tarde, en 2006 se inaugura la red social de microblogging Twitter. Google cuenta con 400 millones de búsquedas por día, y Facebook sigue recibiendo ofertas multimillonarias para comprar su empresa. En España se lanza Tuenti, una red social enfocada al público más joven. Este mismo año, también comienza su actividad Badoo.

Es en 2008, cuando Facebook se convierte en la red social más utilizada del mundo con más de 200 millones de usuarios, adelantando a MySpace, en ese mismo año nace Tumblr como red social de microblogging para competir con Twitter y aparece Chrome de Google. Daniel Ek y Martin Lorentzon crean Spotify.

En 2009, gracias a Jam Koum, creador de WhatsApp, Facebook alcanza los 400 millones de miembros, y MySpace retrocede hasta los 57 millones. Mismo año en el que el éxito de Facebook es imparable.

Un 6 de octubre de 2010 se lanzó en Apple App Store una de las redes sociales más famosas del mundo entero. Instagram fue creado por los jóvenes Kevin Systrom y Mike Krieger. Dicha aplicación se pensó en principio solamente para Iphone, Ipad y Ipod. Ese mismo año, Google lanza Google Buzz, su propia red social integrada con Gmail, en su primera semana sus usuarios publicaron nueve millones de entradas. También se inaugura otra nueva red social, Pinterest. Los usuarios de Internet en este año se estiman en 1,97 billones, casi el 30% de la población mundial. Las cifras son asombrosas: Tumblr cuenta con dos millones de publicaciones al día; Facebook crece hasta los 550 millones de usuarios: Twitter computa diariamente 65 millones de tweets, mensajes o publicaciones de texto breve; LinkedIn llega a los 90 millones de usuarios profesionales, y Youtube recibe dos billones de visitas diarias.

En el 2011, MySpace y Bebo se rediseñan para competir con Facebook y Twitter. LinkedIn se convierte en la segunda red social más popular en Estados Unidos con 33,9 millones de visitas al mes. En este año se lanza Google+, otra nueva apuesta de Google por las redes sociales. La recién creada Pinterest alcanza los diez millones de visitantes mensuales. Twitter multiplica sus cifras rápidamente y en sólo un año aumenta los tweets recibidos hasta los 33 billones.

Es en el año 2012, cuando Facebook ha superado los 800 millones de usuarios, Twitter cuenta con 200 millones, y Google+ registra 62 millones. La red española Tuenti alcanzó en febrero de este año los 13 millones de usuarios.

Es en 2013 cuando nace Vine, permitía crear y publicar vídeos cortos en forma de loop (reproducción continua), de una duración máxima de 6 segundos, límite que posteriormente se amplió a 140 segundos el 20 de junio de 2016. Estos podían ser compartidos a través de la red social Vine o mediante Facebook, Twitter, etc. La plataforma de microvideos anunció que dejaba de desarrollar la aplicación para móviles e impedía volver a subir videos a la red social Vine el 27 de octubre de 2016.

Nace desde Canarias, en el año 2016, The Gaming Experience (TGX) es una red social que ha aparece en versión de pruebas (beta). La plataforma, TGX.es nace con el objetivo de ser reconocida por todo el mundo en la nueva moda de los deportes en red y la temática que les envuelve. La página se distingue como una red social ya que ofrece a jugadores amateur como profesionales los servicios necesarios para interactuar con éxito con sus adversarios, así como les ofrece contenido en noticias, clanes y torneos. En la actualidad, triunfan mas que nunca el contenido audiovisual de los videos. también en este año se percibe mas que el año pasado el auge de los chatbot, software de inteligencia artificial cuya función es la de atención al cliente. Es capaz de simular una conversación con una persona a través de Internet. Esta herramienta es de gran utilidad para empresarios y clientes ya que es en directo y 24 horas.

5.3. Las redes sociales más utilizadas

En el contexto online hay diferentes valoraciones a la hora de clasificar las diferentes redes sociales de internet. Hoy en día no hay una visión común y unificada. Algunos análisis sobre los diferentes tipos de redes sociales destacan unas clasificaciones complejas, diferenciándolas en base a:

- 1.- El público objetivo y la temática: diferencia entre las redes horizontales y verticales.
- 2.- El sujeto principal: las clasifica entre redes humanas, de contenidos y de objetos.
- 3.- La localización geográfica: diferencia entre redes sociales sedentarias y nómadas.
- 4.- La plataforma: las diferencia entre la Red Social MMORPG y Metaversos y la red social web.

Dentro de las clasificaciones en este proyecto las catalogamos de la siguiente manera:

1. Según su público objetivo y temática: dentro de las redes sociales On-Line podemos dividir las en: redes sociales horizontales y redes sociales verticales.
 - Las redes sociales horizontales: son aquellas que no tienen una temática definida y que están diseñadas para todo tipo de público. Son de entrada y participación libre. Ejemplos de este tipo de red son: Facebook, twitter, Google +.

- Las redes sociales verticales: se centran en un eje temático definido y su objetivo principal es el de juntar a un grupo de personas en torno a ésta temática. Blablacar, wallapop, son verticales, centran su contenido en una materia.

Dentro de las redes sociales verticales coexisten las profesionales y de ocio:

- Redes sociales verticales profesionales: que están dirigidas a unir grupos de personas y generar relaciones profesionales, como por ejemplo: LinkedIn, o Xing.
- Redes sociales verticales de ocio: que su objetivo es juntar a gente que desarrolle actividades de ocio, deporte, etc. Hay ejemplos como: Minube o TripAdvisor.

2. Según el tema principal:

Podemos diferenciar, en redes sociales humanas y de contenidos.

- Las redes sociales humanas: son aquellas que fomentan las relaciones entre las personas uniéndolas según su perfil, es decir, según sus intereses, sentimientos, actividades de ocio o trabajo. Ejemplo de ellas: eDarling, Meetic.
- Las redes sociales de contenidos: se unen perfiles según el contenido publicado o el contenido que cada persona publique en su perfil. Encontramos Youtube, la grande del contenido audiovisual, Instagram, Flickr, Vimeo como redes sociales de contenidos.

3. Según su localización geográfica: Diferenciamos las redes sociales sedentarias y las nómadas.

- Las redes sociales sedentarias: son un tipo de red que van cambiando e innovando según las relaciones entre las personas, los contenidos o los eventos creados. Blogger es una de ellas.
- Las redes sociales nómadas: Este tipo de redes se van construyendo a medida que los sujetos comparten su localización geográfica, de manera que publican donde se hallan, que lugares han visitado o aquellos a los que tengan previsto acudir. Ejemplo de ellas es Foursquare.

4. Según su plataforma web : en la encontramos las redes sociales mas diferentes, son:

- MMORPG (sigla en inglés de massively multiplayer online role-playing game): videojuegos de rol que permiten a miles de jugadores introducirse en un mundo virtual de forma simultánea a través de internet e interactuar entre ellos.
- Metaversos: espacio virtual colectivo y compartido con frecuencia creado por convergencia y compatibilización con un aspecto de la realidad externa. Los metaversos son entornos donde los humanos interactúan social y económicamente a través de su avatar, por medio de un soporte lógico en un ciberespacio. La red social MMORPG y Metaversos generalmente están construidas sobre una base técnica cliente-servidor como por ejemplo WOW (World Of Warcraft) o Second Life, pero no siempre. Travian o Habbo: Habbo es una comunidad virtual dirigida a jóvenes a partir de 14 años, pueden crear un personaje y diseñar sus propias salas. Conocer nuevos amigos, chatear, organizar fiestas, cuidar y entrenar mascotas virtuales, realizar retos, crear y participar en múltiples juegos.

- La red social web: Su plataforma de desarrollo está basada en una estructura típica de web.

Actualmente hay más de 2.000 millones de usuarios en el mundo con un perfil en alguna red social, según datos de Statista, el portal estadístico por excelencia. El uso de las redes sociales en España ha mostrado una tendencia estable con tendencia al crecimiento, con porcentajes de uso superiores al 80% a partir de 2014, siendo el 86% recogido en el pasado año 2017.

Según el estudio anual de Redes Sociales de 2017 por Interactive Advertising Bureau (IAB Spain). Asociación que representa al sector de la publicidad y la comunicación digital en España.

IAB Spain, reúne a los diferentes pilares del mundo de la publicidad online: agencias de medios, agencias creativas, anunciantes, soportes, redes, empresas de mobile marketing, de vídeo, de e-mail marketing, buscadores, consultoras, observadores, medios de comunicación y proveedores tecnológicos.

El presente estudio, que IAB Spain realiza anualmente desde el 2009, tiene como objetivos:

- Cuantificar la evolución de la penetración de las redes sociales y el perfil de los usuarios.
- Entender el conocimiento y uso de las redes sociales.
- Evaluar la percepción sobre saturación de la publicidad en redes sociales y la vinculación con las marcas.

Según dicho estudio, Facebook sigue siendo la red social más utilizada, seguida de WhatsApp, Youtube y Twitter.

Instagram asciende en números de usuarios seguida de Spotify. Con menos presencia, linkedIn, Google+, Pinterest, entre otras.

Destacar que la plataforma de YouTube alcanzó una importante cifra a mediados de 2017, 1.500 millones de usuarios registrados inician sesión en la plataforma cada mes. El número de usuarios que visitan el sitio en total probablemente sea más alto, pues esta cifra solo cuenta los que se *loggean* (registran).

Todos los días los usuarios de YouTube miran mil millones de horas de vídeos a través de miles de millones de visualizaciones. La empresa también se jacta de que YouTube llega a más de 88 países y está disponible en 76 idiomas diferentes para que el 95% de los usuarios de Internet puedan entenderles.

A continuación, en el siguiente gráfico se observan los datos expuestos.

Porcentajes de las Redes Sociales más visitadas

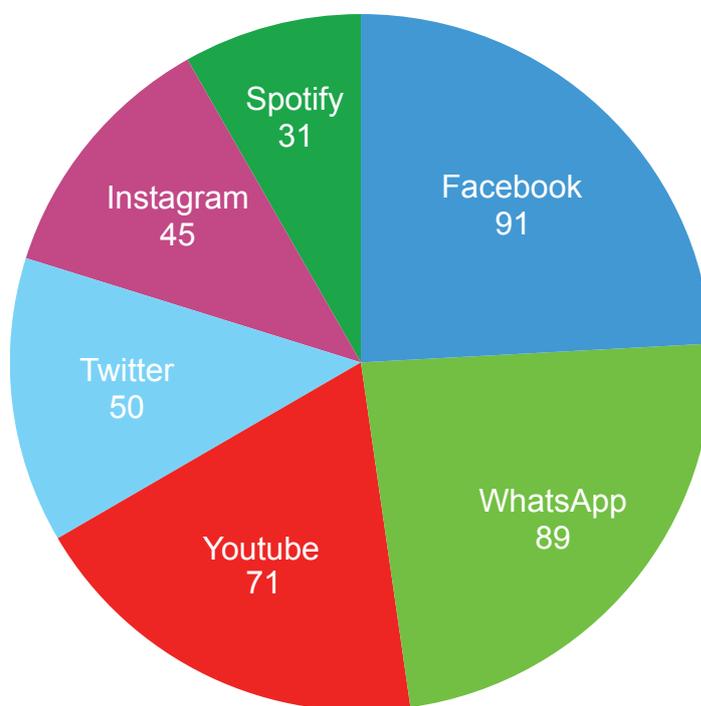


Figura 2: Diagrama sectorial de las RR.SS mas visitadas. Elaboración propia.

Según el mismo estudio, la frecuencia de uso en horas semanales, la aplicación WhatsApp destaca sobre todas las redes sociales, en 5 horas 13 minutos de promedio, seguido por Twitch, Spotify, Facebook, Youtube con 3 horas semanales e instagram.

Como hemos podido ver, la red social Facebook lidera las estadísticas, siendo de las mas importantes para los adultos, pero los adolescentes se declinan por otras Redes Sociales más frescas y dinámicas, que les aporten otro tipo de contenido y dinámicas de expresarse, es por ello que refieren comunicarse de manera más rápida e instantánea y así conocer a más personas e incrementar

sus números de seguidores. Las redes mas populares entre los jóvenes son: Instagram, Youtube, Twitter.

Instagram es la red social mas destacada por los adolescentes, quienes prefieren compartir fotos con cierta regularidad y las “*stories*” (vídeos de corta duración que perduran 24h en la red social) de su día a día. En esta red social podemos seguir las marcas mas de moda, ídolos y personajes famosos, seguir su vida de una manera mas cercana, eso atrapa la curiosidad de los adolescentes.

La red social Twitter es la mas instantánea para escribir y publicar frases de 140 caracteres en un principio y en la actualidad a 280. Es la red social donde nacen por primera vez los *Hashtags* y luego se utilizaron en todas las demás redes.

Por otro lado, la red social Youtube posee una acogida significativa entre los más jóvenes, ya que la plataforma de contenido audiovisual mas destacada, es para muchos sustitutiva de la televisión, ofreciendo un contenido de mayor volumen, mucho mas variado y les permite ver aquello que desean como y cuando quieran. Hay usuarios que de ser meros visualizadores o usuarios de la plataforma, se convierten en creadores de contenido para Youtube, suben a la red vídeos sobre temas de actualidad, tutoriales, humor, viajes, experimentos, *gameplays*, e incluso hay una corriente que graba su vida, día a día, llamados *dailys*, de los que obtienen unos seguidores como público fiel y constante.

5.4. El perfil de los usuarios de las redes sociales.

En España según el estudio anteriormente citado, el anual de Redes Sociales de 2017 por Interactive Advertising Bureau (IAB Spain) un 86% de los internautas de entre 16 y 65 años utilizan redes sociales, lo que supone más de 19 millones de usuarios en nuestro país.

Entre esos millones de usuarios, destacan la generación entre 1980 y 2000, los llamados *millenials*, son los que mas utilizan las redes sociales. Esta generación ha crecido alrededor de la informática, y por ello, Internet es su mayor fuente de información e inspiración, no hay realidad sin Internet.

Las generaciones mas adultas también se involucran en esto de las redes sociales, sim embargo dependiendo de las edades, gustos y preferencias, se hace un uso mas o menos frecuente y diferente de las redes.

Según IAB Spain, obtenemos las características de los usuarios que formas parte de estas plataformas, son las siguientes.

- No existe prácticamente diferencia por sexo. Un 51% son mujeres y un 49% son hombres.
- La edad de uso de las plataformas es cada vez superior ya que hay una mayor concentración entre las edades de 31 a 45 años, siendo la edad promedio 39 años.
- En relación a la formación académica, un 46% de los usuarios posee estudios universitarios y un 35% estudios secundarios.

Como vimos anteriormente, acerca de las redes sociales con mayores visualizaciones, los usuarios mas jóvenes, entre 12 y 18 años, optan por Youtube e Instagram, suben sus fotos mejor retocadas aplicando los mejores filtros y siguen a las celebridades e *influencers* con mas seguidores. Lo prefieren antes que Facebook o Twitter, aun siendo líderes mundiales, son redes que consideran mas serias y para un público mas mayor como veremos a continuación.

La siguiente generación se sitúa entre los 18 y 30 años, prefieren Facebook, es en esa aplicación en la que muchos de la generación se estrenaban en las redes sociales. Considerándola una aplicación mas completa, en la que encontrar amigos de la infancia, compartir fotografías, estados y contenido interesante, así como seguir páginas que destaquen la actualidad en sus publicaciones para mantenerse informados constantemente.

La red social Twitter, también forma parte de sus preferidas, donde pueden buscar noticias de actualidad, opiniones y debates entre los *tweets* mas destacados del día.

Esta generación es también muy activa en Instagram, red social con mas éxito en el último año, la utilizan para publicar sus fotografías con mas retoques y seguir a las personalidades que les interesan.

Por otro lado, la red social Youtube triunfa en todos los rangos de edad, posee contenido para todas las edades, aunque en música, esta generación prefiere Spotify para escuchar sus listas de reproducciones, y sigue consumiendo televisión convencional.

Los adultos con edades entre los 30 y 55 años también prefieren entre sus redes sociales a Facebook y Twitter. Su presencia en redes como Instagram, es menor, pero sin embargo en redes como LinkedIn son más activos debido a su formato profesional. Es considerada como la mejor para estar conectados en el mundo laboral.

Las redes sociales no las solemos relacionar con la tercera edad, sin embargo un estudio realizado en Argentina, "Evaluación del uso de Redes Sociales en la Tercera Edad". Destaca que cada vez más el uso de redes sociales incrementa el rango de edades debido a la mayor disponibilidad que existe para acceder a Internet desde cualquier dispositivos y lugar, y de esta generación destaca su uso para mantener el contacto con seres queridos desde Facebook y Skype para llamar a los familiares del extranjero.

En conclusión, existen redes sociales afines a cada tipo de persona según su edad, gustos o necesidades. El amplio abanico es infinito en donde llevar a cabo tu perfil en las redes.

5.5. La utilización de las redes sociales por los mayores de catorce años: riesgos posibles.

Los niños y adolescentes pasan una cuantía de horas frente a los aparatos electrónicos conectados a Internet, cada vez a edades más tempranas, pese a que la mayoría de redes sociales requieran de una edad mínima de 14 años o una autorización paterna o de un tutor.

En 2010, el 11,9% de los niños de 9 y 10 años tienen un perfil en una red social, entre los 11 y 12 años el porcentaje subía a un 43%, al 75,2% entre los 13 y 14 años y al 88,9% entre los 15 y 16 años, según el estudio de EU Kids Online. Grupo de investigación referente en el estudio de menores y nuevos medios.

La red EU Kids Online se propone proporcionar continuamente evidencia empírica sobre las experiencias en línea de niños y jóvenes, las oportunidades y riesgos relacionados. Ahora, EU Kids Online hará un seguimiento de la encuesta de 2010, que se realizará en tantos países como sea posible. Los preparativos para la recopilación de datos ya han comenzado en 11 países, hasta el verano de 2018, donde se obtendrán datos mas actualizados.

Por otra parte estudiamos el informe de Net Children Go Mobile para España. Proyecto que analiza los riesgos y oportunidades en internet y uso de dispositivos móviles entre menores españoles (2010-2015). Este Proyecto en España lo realiza la Universidad del País Vasco.

Como dato precedente, este informe evidencia que la edad de inicio en el uso de Internet es cada vez más temprana. Así, los niños y niñas de 9-10 años se iniciaron por término medio a los 7 años mientras los adolescentes de 15-16 lo hicieron a los 10 años.

Compararemos los datos del anterior estudio con los de mayor actualidad hasta el momento.

La comunicación online se incrementa cada vez entre los adolescentes, mantener el contacto con los amigos es parte importante en su vida diaria, y esta comunicación se establece a través de las redes sociales. Cuando el acceso a estas es a través de los smartphone, y por tanto siempre está al alcance, es delicado establecer el equilibrio entre privacidad e intimidad en el contacto con las personas que se llegan a conocer a través de internet. Por ello, tratamos de analizar el uso de redes sociales en los menores, la gestión de las peticiones de amistad, la configuración de la privacidad y la información personal disponible en los perfiles.

Según los datos que nos proporciona el informe de Net Children Go Mobile, el 19% de los menores tienen más de 100 contactos. Este dato se incrementa entre los niños (22%), los adolescentes de 15-16 años (21%) y, es más notable, entre los de 13-14 años (25%). El número de contactos online varía dependiendo de los filtros de privacidad que estén activados, el 52% de niños y niñas aceptan solicitudes de contactos solo si son conocidos. Siete de cada diez niños y niñas aceptan nuevos contactos solo si los conocen (52%), el 23% acepta solicitudes de amistades con las que comparte amistad en la vida real, por último, sólo el 9% dice aceptar todas las peticiones.

En función de la privacidad en los perfiles, debemos diferenciarlo por edades, destacando la existencia de perfiles públicos entre los menores de 9 a 10 años, correspondiente a un 35% y entre los de 13 a 14, con un 38%, Sin embargo, a medida que la edad sube, la privacidad aumenta, por mayor conciencia en la privacidad o mayores habilidades informáticas.

En este contexto, el interés sobre la privacidad en los perfiles de los menores, también se relaciona con la información que publican en

sus perfiles. La mayoría de los menores y usuarios en la red, se pueden encontrar tecleando sus nombres y apellidos, en la que aparecerá su perfil con una imagen normalmente del rostro. Es también muy común entre los adolescentes, indicar el centro de enseñanza al que acuden y el 90% de los adolescentes comparten su número de teléfono y solo el 1% su dirección postal.

Otra tendencia entre los menores es mentir con la edad, la mayoría de las veces engañan para burlar el mínimo permitido en la red social, (14 años), o por aparentar ser mas mayor, es el 44% de los menores quienes mienten con la edad.

Antes de presentar los riesgos a los que se exponen los menores, señalar que la investigación del informe de Net Children Go Mobile, quiso averiguar la percepción general del riesgo y el daño, mostrando si los menores habrían sufrido experiencias online que les hubieran molestado. Como resultado, en general, el 18% de los y las menores dicen que se han sentido molestos por algo que han visto en internet a lo largo del año pasado. Aunque sigue siendo una minoría, este porcentaje es mayor que el constatado por la encuesta EU Kids Online de 2010.

En conclusión, se puede afirmar que mientras el uso del internet aumente, los menores van a poder disfrutar de mayores oportunidades, pero también se expondrán a mas experiencias de riesgo, si no existe una previa enseñanza dedicada a las normas y formas de relación e intercambio con otros usuarios de las redes sociales en el mundo digital.

Al respecto, el Instituto Nacional de Ciberseguridad de España , en adelante INCIBE, muestra y enseña a detectar los principales

riesgos posibles de una mala gestión de la información personal en Internet y por tanto, en las redes sociales, que puede acarrear diversas consecuencias perjudiciales para los menores.

Los riesgos posibles son los siguientes:

- La pérdida de privacidad es el principal riesgo al compartir información privada, donde la intimidad del menor es expuesta públicamente. Cuando hay datos publicados en la red, es bastante costoso eliminar ese contenido.
- Reputación dañada. La publicación de datos privados puede originar una imagen errónea que los demás usuarios podrán ver a través de la red.
- Perfiles falsos, suplantación de identidad. Publicar datos personales y privados puede originar que otros usuarios se hagan perfiles con esos datos y acarrear diversos problemas.
- Riesgos para la seguridad personal. Publicar datos de localizaciones de centros de estudios, domicilios, a través de redes sociales, pueden conducir a problemas reales de seguridad personal ya que se podría geolocalizar al menor en este caso.
- Ciberacoso o Cyberbullying. Los datos íntimos o no, publicados en redes sociales, pueden ocasionar situaciones de acoso en los centros escolares o fuera de ellos entre los menores, con el objetivo de hacer daño.
- Sexting. Esta es una práctica de riesgo, ya que trata de compartir con otra persona contenidos íntimos generalmente sexual a través de Internet, como imágenes o vídeos, perdiendo en ese momento el control sobre los mismos.
- Grooming. Problema relativo a la seguridad del menor, consiste en acciones deliberadas por un adulto que trata de establecer

relación con un menor a través de Internet por medio de las redes sociales, teniendo intenciones de carácter sexual, el acercamiento suele proceder con extorsión y chantaje.

- Dependencia y uso excesivo. La preocupación de que los menores lleguen a perder el control de su actividad en las redes es clave para los informes sobre seguridad y riesgos de los menores en la red. Según los datos del estudio de EU Kids online, el smartphone se usa de manera muy extendida como una herramienta para ayudar a “pasar el rato” y combatir el aburrimiento. De hecho, la gran mayoría de los y las menores que poseen estos dispositivos considera que es “un poco cierto” (35%) o “muy cierto” (51%) que gracias a su smartphone se sienten menos aburridos. Esta afirmación no presenta una mínima preocupación acerca del uso excesivo, sin embargo datos como que, uno de cada dos menores están de acuerdo con la afirmación “He sentido un fuerte impulso de comprobar mi teléfono para ver si había pasado algo nuevo muy o bastante a menudo”, si es preocupante. Alrededor de uno de cada tres menores afirman sentirse “muy” o “bastante” a menudo molestos cuando no han podido usar su teléfono por estar en una zona sin cobertura, y casi uno de cada cuatro afirma que utiliza su móvil en sitios u ocasiones en las que no es apropiado.

Estos datos nos reflejan que hay niños y adolescentes que están mas predispuestos a usar en exceso sus smartphones precisamente por las características de éstos: en primer lugar, igual que ocurrió con los teléfonos móviles previamente, los smartphones son percibidos por niños y adolescentes como una parte mas de su

propio cuerpo, que transportan fácilmente en un bolsillo durante todo el día.

A continuación, expondremos con mayor detalle dos de los riesgos anteriormente citados, por su riesgo mas frecuente y dañino. En concreto, el ciberacoso y sexting.

- 1.Ciberacoso: el Instituto Nacional de Ciberseguridad de España, lo define como una realidad en las aulas, y que cada vez se publican mas casos, en los que los perjudicados son niños, niñas y jóvenes de edades y contextos diferentes. Es un tipo de acoso que se origina entre menores y en el que se utilizan los medios digitales para hacer daño a la víctima, conscientemente y de forma repetida en el tiempo, forman parte de sus características:
 - Daño intencional: el acoso se puede proporcionar de múltiples variantes, como burlas, humillaciones, insultos, difusión de mentiras y rumores, hacerse pasar por la víctima con el objetivo de ridiculizar, denunciar las cuentas en los perfiles de las redes sociales, coaccionar al resto de compañeros con la intención de hacerle daño psicológica, emocional y socialmente.
 - Repetido: el daño se produce de manera habitual, pudiendo llegar a ser algo cotidiano y rutinario. No se trata de incidentes aislados, o peleas ocasionales.
 - Entre menores: el acoso es realizado por un menor hacia otro o por un grupo de menores hacia un menor.
 - Medios digitales: utilizan como herramienta los móviles, las redes sociales, fotos, vídeos, juegos online, correo electrónico, foros y cualquier otra aplicación móvil o servicio de Internet en la que la víctima tenga un perfil.

Cada historia de acoso y ciberacoso es diferente dependiendo de las personas, como lo hayan vivido o sufrido. Por lo general estas vivencias ocasionan secuelas psicológicas graves, perjudicando el normal desarrollo del menor con el resto de personas, afectando su autoestima, e incluso originar depresiones e ideas o actos suicidas.

Además, el cyberbullying presenta algunas singularidades respecto al acoso físico que agravan sus consecuencias.

La diferencia con el acoso o bullying, es el uso de dispositivos tecnológicos que producen una desinhibición en el comportamiento y esto origina que los acosadores se permitan actuar de manera agresiva cuando no lo harían en persona. Las singularidades son:

- El anonimato de la red genera una incorrecta percepción de ausente responsabilidad e impunidad.
- Al realizar el acoso a través de los dispositivos, la percepción del daño no es la misma, aunque la mayoría de acosos llevan implícitamente el ciberacoso.
- La inmediatez de las comunicaciones permite respuestas rápidas e impulsivas que pueden empeorar los conflictos.
- La ausencia de normas claras de comportamiento y mecanismos de regulación social en Internet permiten que aparezcan conductas que no se darían de la misma manera en persona.

Asimismo, debido a los sistemas de comunicaciones actuales, el móvil es un dispositivo 24 horas activo, por lo que el ciberacoso puede ser llevado a cabo en cualquier momento. Además de ello al compartir ciertos abusos, imágenes, desprecios o cualquier acto abusivo a través de las redes, puede hacerse viral y ser compartido por muchísimas personas en un corto espacio de tiempo.

En cualquier caso, las motivaciones pueden ser de diferente clase como son las siguientes:

- Creencia por parte de padres o profesores que es una pelea o broma entre niños. No debe ser una realidad cotidiana en el aula ni fuera de ella.
- Falta de habilidades sociales en la resolución de problemas, ocasionando generar daños a otra persona.
- Deficiencia de autoestima del acosador, quien trata de ocultarlo abusando de otras personas con el fin de parecer superior.
- La presión social por ser líderes de un grupo entendido como necesario humillar al resto para destacar.

Por todo ello, cualquiera puede ser víctima en un caso de ciberacoso, aunque existan una serie de características mas afines a un determinado tipo de perfil, como puede ejemplo: no ser como el resto, en cualquier aspecto (nacionalidad, color de piel, orientación sexual, gustos, físico, forma de ser), y entre los aspectos mas personales y emocionales destacan como puede ser, tener la autoestima baja, inseguridad en tus acciones y unas escasas habilidades sociales que entorpece una buena comunicación y acercamiento con los demás. Con esto recalcar en la necesidad de educar en tolerancia y respeto. Dichas singularidades o características no disculpan cualquier tipo de acoso.

Según los datos del Informe de Net children Go Mobile, muestra que el 32% de los y las menores han experimentado alguna forma de bullying online.

La experiencia del bullying está levemente sesgada por género; es más probable entre las chicas haberlo experimentado (35%) y haberse disgustado por ello (26%) que entre los chicos (de los cuales el 29% respondió haberlo sufrido, y el 22% haberse disgustado).

La incidencia general del cyberbullying aumenta muy progresivamente, a medida que lo hace la edad de los y las adolescentes. Es en la franja de 15 y 16 años donde se sufren con más frecuencia los casos de bullying mediante redes sociales, mensajería instantánea, llamadas o mensajes que se reciben en teléfono móvil.

En cuanto al sexting:

- 2. El sexting, es una práctica cada vez mas usual entre personas con dispositivos móviles con cámara, prácticamente todo el mundo, no es un problema de seguridad en sí mismo, sino una práctica de riesgo, sobre todo cuando implica a los menores de edad.

El sexting consiste en el intercambio de imágenes o vídeos de contenido sexual a través de dispositivos móviles. El riesgo de esta práctica se formaliza una vez el contenido producido ha sido enviado a otra persona, ya que se pueden ser utilizados para un mal fin o incluso la extorsión.

Esta práctica se caracteriza por las siguientes particularidades:

- Voluntariedad. El contenido enviado es creado y compartido por uno mismo para otras personas. En situaciones de robo o pérdida de móvil también es posible que se produzca un envío involuntario o sin consentimiento.

- Carácter sexual. Los contenidos tienen una clara connotación sexual: desnudez, así como muestra o descripción de actividades sexuales.
- Uso de dispositivos tecnológicos. Actualmente cualquier persona dispone de un teléfono móvil o tablet con cámara.

Los riesgos de esta práctica comienzan con la difusión de estas imágenes o vídeos entre personas que no eran los destinatarios. Dichos receptores del contenido pueden utilizar el chantaje o la extorsión para obtener un beneficio. Al tratarse de contenidos íntimos, su difusión conlleva sin duda una pérdida de privacidad, de tal modo que se produce un daño en la reputación de la víctima, deteriorando su imagen pública. El sentimiento de humillación y traición que implica puede provocar falta de confianza en futuras relaciones, además de problemas psicológicos como ansiedad, depresión, etc.

Asimismo, el contacto con personas desconocidas, constituye una situación de riesgo que puede darse entre los más jóvenes en redes sociales, datos del estudio de Net children afirman que, uno de cada cinco menores (21%) ha contactado online con personas que nunca había visto cara a cara.

Si bien se aprecian ciertas variaciones en función del género, donde realmente se aprecian diferencias es entre franjas de edad: el contacto online con personas desconocidas se incrementa con los años. De manera notable, en el paso de los 11-12 a los 13-14 años, el porcentaje de menores que contactan online con alguien a quien no conocen se triplica.

Tras un contacto online, la probabilidad de encontrarse offline con contactos online se incrementa con la edad, del 2% registrado en la franja de 9 y 10 años al 25% para la franja de 15 y 16 años.

Si comparamos los datos del estudio de 2010 de EU Kids Online, con el informe de Net Children Go Mobile, se observa un incremento significativo en los menores que contactaron con personas que habían conocido online.

AÑO	Niños	Niñas	13-14 años	15-16 años
2010	9 %	9 %	8 %	17 %
2015	12 %	11 %	18 %	25 %

Tabla 1: Comparación en menores que contactaron con personas que habían conocido online (%). Evolución 2010- 2015. Elaboración propia.

Es evidente la preocupación social que resulta de esta situación ya que la podemos ver reflejada en los diferentes artículos periodísticos que se incluyen en el Anexo II del presente trabajo.

5.6. Normativa aplicable al uso de las redes sociales.

Las principales leyes que regulan el uso de las redes sociales , así como los derechos de los usuarios de las mismas son las siguientes.

- La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, actualmente en revisión tras la aplicación del Reglamento General de Protección de Datos (UE) 2016/679 del Parlamento Europeo y del Consejo.

- Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia

En relación a las redes sociales, la normativa jurídica es un elemento esencial a considerar dentro de la rama de las nuevas tecnologías, dado el crecimiento, evolución, e incidencia social que están experimentando.

Por ello, vamos a analizar los principios básicos que se recogen en la citada normativa sobre el Derecho de Protección de Datos de Carácter Personal, el Derecho de Propiedad Intelectual y el Derecho Fundamental al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

En este sentido, a modo de contextualizar los derechos mencionados anteriormente, se va realizar un breve resumen de cada uno de los siguientes apartados que a continuación se exponen.

- El Derecho de Protección de Datos de Carácter Personal. El principio básico del funcionamiento de las redes sociales se encuentra en el hecho de que los usuarios proporcionan y hacen públicos sus datos y perfiles de usuarios, permitiéndoles

interrelacionarse con otros usuarios, según los perfiles y datos publicados por éstos. Este hecho conlleva que la normativa de protección de datos de carácter personal cuente con una especial trascendencia, dado que todos los perfiles de los usuarios son tratados con diferentes finalidades por parte de las redes sociales, sin que se cumpla rigurosamente con la normativa vigente. La Protección de Datos en España es un derecho fundamental, lo que significa que como tal está reconocido en la Constitución Española y merece especial protección en las leyes. Es un derecho con el contamos todas las personas, y que nos da la facultad para poder controlar en cualquier momento el uso que se haga de nuestros datos personales, para evitar que se traten de manera que se pueda obtener información sobre nosotros mismos que nos perjudique nuestra intimidad y otros derechos fundamentales y libertades públicas.

- El Derecho de Propiedad Intelectual. Uno de los principales usos más comunes y extendidos en las redes sociales es la distribución y el intercambio de contenidos. En este sentido, y dada la cantidad de normativa aplicable a los derechos de propiedad intelectual y la especial protección existente en Europa, esta acción supone el choque constante entre los derechos de los autores (en muchas ocasiones usuarios también de las redes sociales) y uno de los fundamentos básicos de Internet y de las redes de este tipo, que es el hecho de compartir, el intercambio constante de información, con independencia del formato o tipo de información intercambiada.
- El Derecho al Honor, Intimidad Personal y Familiar y a la Propia Imagen. Este derecho está relacionado con el derecho a la protección de datos de los usuarios, toda persona tiene derecho a

la intimidad personal y familiar. El propio concepto de red social, tal y como son entendidas en la actualidad, conlleva la renuncia por parte de los usuarios de cierta parte de ese derecho fundamental. Aunque se trata de una renuncia completamente voluntaria por parte de los usuarios.

A continuación desarrollaremos mas detalladamente los derechos anteriormente expuestos.

5.6.1. Derecho de Protección de Datos de Carácter Personal.

El Derecho de Protección de Datos de Carácter Personal en el ámbito Europeo. Es reciente el inicio de la aplicación del Reglamento General de Protección de Datos (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. (GDPR), Este reglamento entró en vigor en 2016, pero su aplicación se formalizó el pasado 25 de mayo de 2018.

El GDPR es un Reglamento de aplicación directa, lo que quiere decir que sus artículos son aplicables en los diferentes Estados de la Unión Europea, sin necesidad de adaptarlos mediante una norma nacional, ya que el objetivo es unificar los criterios de protección de datos. Sin embargo, este Reglamento reconoce a los países miembros la facultad para elaborar una ley nacional que aplique dicho Reglamento.

Este Reglamento trata de proveer mayor seguridad de los datos personales a los usuarios, de manera que las redes sociales como WhatsApp, Facebook, Twitter se han visto en la obligación de modificar las políticas de privacidad y seguridad con el objetivo de que el usuario conozca de manera detallada la información que se recopila, como es su uso y como se comparte. Esto se consigue a través del consentimiento, que obtienen con un “click” en la casilla de “He leído y acepto los términos y condiciones de uso” tras la exposición de dicho procedimiento relatado en cientos de páginas que pocos usuarios leen y comprenden, pero que sin ese consentimiento no te permiten el uso de la aplicación, por lo que cada usuario vuelve a aceptar las condiciones sin conocerlas.

En España, la protección de datos de carácter personal se ha regulado por la Ley Orgánica 15/1999, de 13 de diciembre. En el caso de los menores y su consentimiento, está regulado en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

El Artículo 13 del Real Decreto 1720/2007, de 21 de diciembre en el Capítulo II, Consentimiento para el tratamiento de los datos y deber de información, se detalla el consentimiento de los menores de edad. De tal forma que el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años y por el contrario, el tratamiento de los datos de los menores de trece años sólo será permitido si figura el consentimiento de los padres o tutores.

En el ámbito de las redes sociales, son las mismas las que ofrecen el nivel de protección, seguridad y privacidad, cada usuario puede elegir quien puede ver el contenido publicado, y que contenido es el publicado. Para una cuenta de uso personal, el nivel de privacidad debe ser la que mejor nos convenga, recomendando privatizarla, de manera que solo tus contactos puedan ver tu perfil o por el contrario, si es pública, tu perfil está al alcance de cualquier usuario de la red social.

Por otro lado, al margen de responsabilizarnos del contenido publicado en nuestro perfil, puede ser que terceros publiquen contenido relacionado con nosotros, es por lo cual, La Agencia Española de Protección de Datos expone nuestro derecho a que se elimines los datos publicados en sitios web que no hayan obtenido con nuestro consentimiento, así como el Reglamento General de Protección de Datos reconoce a los usuarios el derecho de supresión. La Agencia Española de Protección de Datos se hará cargo de ese derecho cuando previamente el afectado haya comunicado su intención al responsable por un método que pueda probarlo, acreditando su identidad y el contenido que desea eliminar, una vez pasado el plazo establecido, (un mes) el afectado podrá establecer una reclamación ante la Agencia Española de Protección de Datos respectivamente.

El derecho de supresión únicamente puede ser solicitado por el afectado, al tratarse de menores de 14 años, serán sus padres o tutores legales.

Las redes sociales mas reconocidas ofrecen métodos establecidos para que los usuarios comuniquen las vulneraciones de sus datos mediante sus formularios y enlaces de denuncias.

5.6.2. Derechos de Propiedad Intelectual.

El Derecho de Propiedad Intelectual se regula en el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Los derechos de la Propiedad Intelectual se regulan por el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

En el Artículo 1 de la citada ley se define la propiedad intelectual como “la propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el solo hecho de su creación”.

La normativa en materia de propiedad intelectual tiene como finalidad proteger los derechos de los autores sobre sus obras, integrando derechos de carácter personal y patrimonial, establecidas en la legislación vigente.

El titular de estos derechos puede autorizar o no cualquier reproducción, transmisión de una obra suya.

En este sentido, las redes sociales y páginas web como ya hemos indicado a lo largo de este proyecto, basan su esencia en el intercambio de información y de contenidos. Son un gran número de usuarios de este tipo de redes que introducen en ellas sus nuevas obras musicales o contenido multimedia como documentos fotográficos y vídeos con la finalidad de autopromoción de forma viral entre los millones de usuarios de la red, lo que ha provocado que la violación de derechos de autor pase a ser en los últimos tiempos una de las cuestiones que, junto con la protección de datos y la protección de la intimidad de los usuarios, uno de los aspectos jurídicos principales en las redes sociales, debido a que el contenido se percibe en formato digital y su copia y distribución resulta muy sencilla, sin embargo su descubrimiento o comprobación por parte del autor una ardua tarea. ya que son millones de usuarios compartiendo contenido simultáneamente.

Por estos motivos son por los que cada usuario debe configurar rigurosamente la seguridad de su perfil así como prestar atención a las condiciones de registro y políticas en materia de propiedad intelectual y privacidad que la red social haya regulado. Las redes sociales deben considerar en alta estima la protección de los derechos de propiedad intelectual de los usuarios y de los terceros para el funcionamiento legítimo de sus plataformas.

A continuación se muestra algunas de las condiciones de la red social Facebook en relación con la protección del derecho de Propiedad Intelectual:

FACEBOOK

“Tus compromisos con Facebook y nuestra comunidad. Permisos que nos concedes:

Para proporcionar nuestros servicios, necesitamos que nos concedas determinados permisos:

1. Permiso para usar contenido que creas y compartes: El contenido que creas y compartes en Facebook y los demás Productos de Facebook te pertenece, y ninguna disposición incluida en estas Condiciones anula los derechos que tienes sobre él. No obstante, para proporcionar nuestros servicios, debemos contar con ciertos permisos de uso por tu parte.

En concreto, cuando compartes, publicas o subes contenido que se encuentra protegido por derechos de propiedad intelectual (como fotos o vídeos) en nuestros Productos, o en relación con ellos, nos concedes una licencia mundial, no exclusiva, transferible, sublicenciable y exenta de pagos por derechos de autor para alojar, usar, distribuir, modificar, mantener, reproducir, mostrar o comunicar públicamente y traducir tu contenido, así como para crear contenido derivado (de conformidad con tu configuración de privacidad y de la aplicación). En otras palabras, si compartes una foto en Facebook, nos das permiso para almacenarla, copiarla y compartirla con otros (de conformidad con tu configuración), como proveedores de servicios que nos ayudan a proporcionar nuestros servicios u otros Productos de Facebook que usas.

Puedes eliminar el contenido o tu cuenta en cualquier momento para dar por finalizada esta licencia. En cualquier caso, debes saber que, por motivos técnicos, el contenido que elimines puede permanecer en la plataforma en copias de seguridad durante un tiempo limitado, aunque los demás usuarios no podrán verlo. Asimismo, el contenido que elimines puede seguir siendo visible si lo has compartido con otras personas y estas no lo han borrado.”

fuelle: [facebook.com](https://www.facebook.com)

Este permiso de la red social Facebook viene a demostrar que los derechos de propiedad intelectual pueden no estar suficientemente protegidos una vez que el usuario comparta sus archivos en la citada red social.

5.6.3. Derecho Fundamental al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

El Derecho Fundamental al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen se regula en la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

Esta Ley establece Orgánica es la encargada de salvaguardar los Derechos al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

Esta ley establece la protección civil frente a todo tipo de intromisiones no legítimas y desautorizadas expresamente por el titular y que afecten de forma directa a su honor, intimidad personal y familiar, así como a la propia imagen.

A propósito de ello, debemos citar el artículo 20 de la Constitución Española, en el que “se reconocen y protegen los derechos:

- a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.
- b) A la producción y creación literaria, artística, científica y técnica.
- c) A la libertad de cátedra.
- d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades”.

Del mismo modo que el derecho a la protección de datos, el derecho a la propiedad intelectual, el derecho al honor, a la intimidad personal y familiar y a la propia imagen se encuentra relacionada con las redes sociales, ya que el objetivo principal de éstas como ya se ha expresado se centra en el intercambio de información, y contenido audiovisual, propio o sobre terceros.

En la actualidad, existen múltiples aplicaciones de edición de fotografía y vídeo que posibilitan retocar las imágenes de manera que aparezcan situaciones que no son reales, modificar ciertos aspectos que posteriormente al publicarlo por terceros pueda dañar la imagen de cierta persona, eso unido a la gran repercusión que generan ciertos contenidos colgados en la red, hacen que resulten fácilmente disponibles por millones de usuarios desde cualquier parte del mundo. Esta situación se da en multitud de ocasiones en el ciberbullying, en la cual fotografían a una persona y por medio de la edición en la que incluyen imágenes o mensajes ofensivos, obtienen un contenido que publican en las redes sociales y consiguen provocar una situación indeseable para nadie.

Por ello, es importantísimo la necesidad de proteger nuestra privacidad e intimidad con las herramientas que nos ofrecen las redes sociales, ya que está al alcance de cualquiera publicar una foto en la que aparezcas o en la que sin aparecer seas etiquetado en contenido que no es de tu interés, por ello es recomendable modificar los ajustes de manera que requieran de nuestro consentimiento para las publicaciones en las que aparezca nuestro usuario o imagen. De todas formas, no siempre se consiga el nivel de privacidad que podemos exigir ya que como vimos anteriormente

en las condiciones de Facebook, cuando un usuario quiere eliminar su cuenta, es posible que aún ejecutando dicha acción, permanezcan datos, imágenes y contenido en general nuestro en copias de seguridad, por lo que son accesibles desde los diferentes buscadores de Internet.

Otro obstáculo hacia preservar nuestra intimidad en las redes, es la posibilidad que tienen estas plataformas de ubicar geográficamente al usuario a través de la dirección IP esta opción puede resultar peligrosa de manera que se podría llegar a realizar un seguimiento de las rutinas de los usuarios y atacar de esa manera a la intimidad, hay que decir que esta opción la ofrece la red social pero es el usuario el que decide publicar su geolocalización o no.

Tanto el derecho a la intimidad como el derecho a la imagen son vulnerados diariamente en Internet, agrediendo de esta forma la intimidad de las personas.

Las redes sociales tienen gran parte del compromiso u obligación en lo referido a la protección de la intimidad de sus usuarios. El adecuado diseño de la plataforma y de las herramientas puestas al servicio del usuario deben ser suficientes para evitar o minimizar los problemas relacionados con la privacidad, intimidad, imagen u honor. Las redes sociales deberían coartar ciertas actitudes de sus usuarios de manera que no fuera posible la publicación de comentarios ofensivos o actos que vulneren la intimidad y privacidad de las personas, debiendo expulsar de la red a quien no cumpla las normas, esta medida es posible en las redes ya que cualquier usuario puede denunciar a otro por un comentario, imagen

inapropiada o similar, una vez denunciado la red social dependiendo de la cantidad de denuncias sobre el mismo hecho y análisis de sus normas de convivencia accederá o no a la expulsión de ese usuario.

Como conclusión, es difícil solucionar las posibles vulneraciones de los derechos referidos ya que cualquiera utilizando otra cuenta de usuario y perfil aleatorio podría invadir la esfera de la intimidad personal igualmente.

5.7. Protección jurídica de los menores de edad en el uso de las redes sociales.

La protección jurídica específica de los menores en redes sociales se regula en las leyes que a continuación se especifican:

- La Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.
- Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia.

En la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil, en su artículo 5 se especifica el Derecho a la información, se describe como los menores tienen derecho a buscar, recibir y utilizar información acorde a su etapa evolutiva, por ello se presta mayor atención al ámbito digital, de manera que les permita la

utilización de las nuevas tecnologías con seguridad e identificando situaciones de riesgo.

Los padres o tutores deben cuidar que la información recibida sea la adecuada a su edad y desarrollo.

Así como las Administraciones Públicas estimularán la difusión de materiales informativos a los menores que faciliten de esta manera el acceso de los menores a los servicios de información, y por consiguiente se cerciorarán de que los medios de comunicación apuesten por una información que promueva valores de igualdad, solidaridad, diversidad y respeto.

Por ello, “la difusión de información, utilización de imágenes o nombre de los menores en los medios de comunicación, que puedan implicar una intromisión ilegítima en su intimidad, honra o reputación, o que sea contraria a sus intereses, determinará la intervención del Ministerio Fiscal, que instará de inmediato las medidas cautelares y de protección previstas en la Ley y solicitará las indemnizaciones que correspondan por los perjuicios causados”.

Por otro lado en la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, también se hace referencia en el apartado 3 del artículo 5, la importancia de las Administraciones Públicas en inculcar la producción y difusión del material informativo respetuoso, destinado a los menores, de la misma forma que faciliten su acceso a los diferentes servicios culturales de información, bibliotecas y demás oferta de ocio y cultura en Internet junto con la debida concienciación sobre la defensa de la propiedad intelectual.

Otra defensa del menor respecto al manejo de sus datos personales en redes sociales se hace efectiva en las citadas leyes, Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil, como en la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia. Establecen en su artículo 21 dedicado al Acogimiento residencial, un apartado que establece la importancia de constituir medidas educativas y de control que protejan y aseguren la protección de los datos personales del menor cuando acceda a las tecnologías de la información y redes sociales.

En este apartado es conveniente distinguir las dos situaciones de tutela en las que se pueden encontrar los menores:

- a) Cuando están bajo la custodia de sus padres: en este caso los padres serán los responsables de adoptar las medidas para un uso correcto y seguro de las redes sociales por los menores, por ejemplo, por medio de la activación del control parental en los dispositivos informáticos que utilicen los menores.
- b) Cuando la tutela de los menores la ejerzan las Administraciones Públicas competentes, será las mismas las que deberán adoptar esas medidas de control respecto a la utilización de las redes sociales por los menores.

Igualmente para cuando los menores se hallen en los centros de educación primaria o secundaria, serán los tutores los encargados de que los alumnos hagan un uso responsable y seguro de las redes sociales en el ámbito del centro escolar.

5.8. Asociaciones españolas dedicadas la seguridad en la utilización de Internet y de las redes sociales.

En la actualidad, la utilización de internet como herramienta ha transformado el modo en el que la sociedad establece las relaciones, la manera de comunicarnos y el medio que utilizamos, así como Internet es la herramienta fundamental en la vida de cualquier niño, las nuevas tecnologías son su medio natural.

No obstante debemos ser conscientes de que simultáneamente los privilegios y ganancias que aporta el uso genérico de Internet y en concreto las redes sociales, los niños pueden resultar vulnerables en este contexto virtual.

Por estas causas y debido al rápido proliferamiento del avance tecnológico sobre las redes sociales, diferentes organizaciones, asociaciones e instituciones pretenden concienciar tanto niños, jóvenes, padres y tutores sobre la importancia de proteger la privacidad, el acceso y el material que se publica en estas plataformas, así como un uso responsable de sus datos en la red.

A continuación, las asociaciones e instituciones españolas dedicadas a la seguridad en la utilización de Internet y de las redes sociales son las siguientes:

En primer lugar, se debe destacar la labor de La Agencia Española de Protección de Datos. (en adelante AEPD).

Desde la AEPD proponen resaltar la importancia del papel activo que deben asumir los padres, tutores y profesores en recordar a los niños que sus datos personales son importantes, que deben protegerlos y cuidarlos, y concienciarles de que deben hacer un uso responsable de sus datos en internet.

La Agencia ha puesto en marcha un correo electrónico, y un número de teléfono con servicio WhatsApp para resolver las dudas que puedan plantearse en relación con el tratamiento de datos de los menores de edad.

Además, la AEPD dispone de la web Tú decides en internet, un proyecto dirigido a concienciar tanto a jóvenes como a padres y profesores sobre la importancia de proteger la privacidad, y que incorpora guías tanto para menores como para padres y profesores, vídeos, juegos y diversos contenidos de interés.

En segundo lugar, INCIBE se dedica a consolidar la confianza digital, proporcionar un nivel superior en la ciberseguridad, la resiliencia y contribuir al uso seguro del ciberespacio en España.

A través de INCIBE, accedemos a la Oficina de Seguridad del Internauta en adelante OSI, dedicada a la ayuda del usuario de internet, por lo que su labor es proporcionar la información y el apoyo necesarios para evitar y resolver los diversos obstáculos o inconvenientes en temas de seguridad que pueden existir al navegar por Internet.

Su objetivo principal es aumentar y fomentar la confianza y tranquilidad en el espacio cibernético por medio de los procesos formativos en materia de ciberseguridad.

Para ello establecen tres formas de trabajar para la consecución de sus objetivos, que son las siguientes:

- Inculcar en los usuarios buenos hábitos de seguridad que deben de interiorizar.
- Concienciar de la responsabilidad de cada usuario en relación con la ciberseguridad.
- Ayudar y contribuir a minimizar los casos y la trascendencia de las incidencias de seguridad experimentadas por el usuario.

En el portal de la Oficina de Seguridad del Internauta, se encuentra información genérica sobre la ciberseguridad y el material necesario para navegar mas seguro.

OSI pone a disposición un canal de avisos para estar actualizado de las últimas alertas en seguridad virtual y a través de las redes sociales, Facebook, Twitter, Google+, Youtube. Además el centro de atención telefónica ayuda con las consultas y problemas de seguridad.

El Instituto Nacional de Ciberseguridad (INCIBE), crea el Centro de Seguridad para menores de edad en España, Internet Segura for Kids (IS4K) y tiene por objetivo el fomento del uso de Internet de manera segura y responsable así como de las nuevas tecnologías entre los niños y adolescentes. Sus principales labores son las siguientes:

- Aportar formación a los menores, jóvenes, familias, y profesionales que trabajen con menores, así como sensibilizarlos por medio de diferentes talleres, campañas, iniciativas a nivel nacional.
- Dedicar un servicio de ayuda con el que poder aconsejar, advertir e informar a menores, familias, educadores y profesionales sobre los riesgos en Internet hacia los menores.

Este Centro de Seguridad en Internet para menores es coordinado por la Secretaría de Estado para la Sociedad de la Información y Agenda Digital (SESIAD), sus servicios son realizados a través del INCIBE, en colaboración con otras entidades del sector. De la misma forma, está presente en la red paneuropea INSAFE de Centros de Seguridad en Internet y está cofinanciado por la Comisión Europea. Este centro de seguridad en internet para menores de edad ofrece diferentes líneas de contacto para dudas y propuestas a través de sus perfiles en redes sociales como Facebook, Twitter y su página web.

Otro de los proyectos mas destacados en el ámbito español, es el realizado por Pantallas Amigas,

Esta sociedad la conforma un equipo profesional multidisciplinar especializado en la educación, la pedagogía, la psicología, la sociología, la informática, la comunicación y el diseño. Pantallas Amigas es una iniciativa empresarial que nace por la necesidad de promocionar e impulsar el uso seguro y responsable de las redes y nuevas tecnologías, así como obtener una ciudadanía digital comprometida con la protección en la infancia y adolescencia. Sus tres líneas de actuación con las siguientes:

- Internet seguro, evitando los riesgos en la medida de lo posible y/o reducir sus consecuencias.
- Internet saludable, buscar una relación satisfactoria con las nuevas tecnologías tanto de forma individual como colectivo.
- Ciberciudadanía, conseguir una ciudadanía comprometida con la causa.

El proyecto de Pantallas Amigas, elaboran y participan en intervenciones en centros escolares nacionales, participan en la formación de formadores en prevención del cibercrimen, coordinan y organizan congresos y jornadas de difusión, realizan estudios sobre menores y el uso de tecnologías, así como participan en eventos internacionales sobre la seguridad de los menores en el uso de las nuevas tecnologías.

El diseño de las intervenciones son constituidas bajo los siguientes cinco objetivos claves:

- Comunicación educativa a través de estrategias multicanal.
- Mejora de habilidades sociales, empatía, pensamiento crítico y control de emociones.
- Fomentar valores universales como respeto, responsabilidad, justicia, solidaridad, cooperación, participación, equidad, igualdad de oportunidades y cuidado de las demás personas.

Esta iniciativa de Pantallas Amigas participa activamente en todas las redes sociales recomendando el uso seguro que promulga y fomenta. Ayuda a madres y padres y realizan apoyos en centros educativos de todo el país. Ofrece un formulario de denuncia online y la sensibilización y prevención son sus mayores objetivos, al margen de las intervenciones, dedican sus esfuerzos a la creación

de materiales didácticos, edición de artículos de opinión y divulgación, diseño y organización de jornadas de difusión, como lo son las intervenciones en municipios y centros educativos.

Uno de los mayores éxitos de Pantallas amigas es su canal de Youtube, con mas de 48 millones de visualizaciones y mas de 100 mil suscriptores, esta iniciativa alberga mas de 10 años aportando contenido a la plataforma, con una serie de videos de animación, alertando de los posibles riesgos sin un uso responsable de las redes, situaciones incómodas, recomendaciones, denuncias y consejos.

Por último, hablamos de EMICI, (Equipo Multidisciplinar de Investigación del Cyberbullying) es un grupo de trabajo que tiene como misión el desarrollo de aportaciones de alto valor añadido y carácter social a diferentes fenómenos asociados al uso de las TIC (Tecnologías de la Información y la Comunicación) y relacionados con el cyberbullying por parte de la infancia y la adolescencia con una aproximación rigurosa y multidisciplinar.

5.9. Recomendaciones de uso seguro y responsable del uso de las redes sociales.

Una vez conocido las mayores redes sociales del mundo de los internautas, los posibles riesgos a los que podemos estar expuestos sin una determinada prevención y uso seguro y responsable de las

redes, la normativa que la sustenta, y las asociaciones e instituciones que velan por un empleo óptimo de las tecnologías.

Facilitamos una serie de recomendaciones para un excelente uso de las redes.

5.9.1. Recomendaciones básicas.

A continuación definiremos una serie de recomendaciones básicas de uso seguro y responsable en las redes e internet de manera general, basándonos en los expuesto anteriormente.

Escoger la red social apropiada.

No todas las redes sociales son para todos los públicos.

Leer las condiciones generales de uso y políticas de datos de la red social.

La red social se manifiesta en el uso que hace de los datos que le proporcionan, junto con la declaración de derechos y responsabilidades.

Fortalecer las contraseñas.

- Utilizar diferentes usuarios y contraseñas en las diferentes redes sociales.
- Utilizar contraseñas de mas de 8 caracteres alfanuméricos, utilizando mayúsculas y minúsculas con símbolos de puntuación.

- No marcar la casilla de “Recordar contraseña” ni “Recordar usuario”, algunos servicios de Internet pueden tener esta opción de manera automática.
- Cerrar la sesión de manera segura.

Proteger la privacidad.

Configurar la privacidad en el apartado de ajustes de las redes, sin facilitar datos personales salvo los necesarios.

Confirmar los contactos.

- No aceptar cualquier petición de amistad que no conozcas.
- Bloquear si no hay buena relación o te produce incomodidad.
- No ceder a chantajes.
- Denunciar o pide ayuda si no sabes como actuar.

Realizar un control sobre el contenido publicado. (fotos y vídeos).

- No subir imágenes o material comprometido propio y menos si es ajeno.
- No publicar contenido sin autorización de las personas que aparecen en el.
- Saber que cualquiera puede obtener tus imágenes.
- No difundir imágenes violentas, humillantes o desgarradoras.

Navegar con respeto y ser responsable cada uno de sus actos.

5.9.2. Recomendaciones dirigidas a los mayores de catorce años.

A continuación ampliaremos los consejos y recomendaciones anteriormente descritos, acentuando en la importante labor de concienciación y fomento del uso seguro y responsable de las redes hacia los mayores de catorce años.

Seguridad con los smartphones.

- Tener siempre contraseña de acceso al smartphone
- Mantener desactivado el Bluetooth, GPS, wifi utilizarlos solo cuando lo necesites.
- Cuidado con el contenido que almacenas en el teléfono, (imágenes, contraseñas...)

Seguridad en las webs.

- Las webs visitadas, los vídeos vistos, consultas en buscadores, publicaciones, comentarios, los *likes*, son informaciones que dejan rastro, todo lo que se hace en internet se registra como huella digital que habla de cada usuario.
- Decidir quien ve tu contenido.

Privacidad y Seguridad.

- Comprobar en tu navegador, que estás en la página web deseada. Los hackers aprovechan para crear direcciones parecidas pero con fines diferentes, robar cuentas, datos o contenido dañino que perjudique a los dispositivos

- Evita conectarte a redes wifi gratis o sin clave. No son seguras y podrán robarte datos y contraseñas.
- Instalar siempre los antivirus. Los virus estropean los dispositivos o los inutilizan.
- No abrir correo electrónico de desconocidos, ni acceder a enlaces.
- Tapa las cámaras de tus dispositivos, al hackearlas pueden acceder a ella.

Convivencia en la red.

- No facilitar información a desconocidos.
- No hacer lo que en la vida real no harías, no faltes el respeto y no trates de ofender a nadie.
- No participes en el acoso de otra persona, al compartir imágenes , vídeos, que puedan herir a otros, es acoso.
- No participes en las cadenas de mensajes.
- Si recibes mensajes o llamadas que desconoces, te molestan con comentarios, es acoso, pide ayuda y denúncialo.
- No polemizar a través de la red, pueden dar a malentendidos.
- No usar el móvil ni las redes de manera obsesiva, que no controlen tu tiempo.

5.9.3. Recomendaciones a los padres y tutores.

Las recomendaciones y consejos siguientes dirigidos a padres y tutores, se enfocan desde una finalidad conjunta entre ambos, para hacer de Internet y las redes, comunidades en las que prevalezca el respeto, la tolerancia y la capacidad de empatía.

Estas recomendaciones quieren cumplir con el objetivo de enseñar a los mas pequeños a crecer con las herramientas tecnológicas propias de su edad, haciendo uso de manera responsable y segura de las redes sociales.

- El ordenador debe estar en una zona común de la casa, es cierto que en la actualidad el contacto con internet no es exclusivo del ordenador de mesa de casa, sino en múltiples dispositivos por lo que utilizar herramientas que nos den a conocer las rutas de navegación del menor no es excesivo.

- Los padres y tutores deben estar actualizados en utilidades y posibilidades de las plataformas, de esta manera se podrá educar en su utilización de manera mas experta.

- El control parental es importante, así como establecer el correo del adulto responsable como cuenta secundaria a la cuenta del menor. De esta manera se podrán verificar movimientos o visitas a páginas inadecuadas.

- En casa se debe establecer horarios sobre el uso de Internet y redes sociales, evitando de esta manera un uso excesivo y perjudicial.

- Verificar el control de edad, el acceso a redes sociales se permite a partir de los 14 años, con menos edad es necesario la autorización de los padres o tutores.

- Los menores deben ser informados sobre la seguridad en la red. La educación es importante, cuando pretendemos inculcar aspectos básicos sobre la navegación segura en el mundo virtual.

- Informar y reforzar a los menores de los riesgos de publicar contenido como imágenes, fotografías o vídeos, a través de las redes sociales, cerciorar que son conscientes del funcionamiento de las redes y sus fines así como las cámaras web. Darles herramientas para que sepan gestionarse sin que pueda suponer algún riesgo.

- Explicar que los menores no deben quedar con personas desconocidas o conocidas en el mundo online, y de tener interés en conocer a esa persona, contar con la compañía de los padres o tutores.

- Controlar la información que el menor publica en redes, a quien hace pública esa información, conociendo que sus contactos son similares a su edad. Además revisar y ayudarle con las condiciones de privacidad de su perfil.

- Comprobar que no utiliza el nombre y apellidos completos así como asegurarse de que accede a páginas recomendadas para su edad.

Las recomendaciones orientadas a padres y tutores sobre el uso de las redes sociales se basan en establecer y mantener una comunicación continua con los menores respecto a su relación con Internet.

Además es conveniente profundizar en este apartado, ya que creemos que para saber constituir cualquier tipo de relación, estipulada en el mundo real o en digital, se debe hacer con educación, ya que engloba una serie de valores como el respeto, la tolerancia, la cordialidad, amabilidad, que por contraposición en las redes sociales escasea.

Resulta de gran ayuda y fundamental la concienciación y formación de los menores, se les debe informar utilizando el diálogo como herramienta sobre los peligros y riesgos existentes en el mundo online. Como ya hemos apuntado anteriormente, las redes sociales pueden ser muy beneficiosas para la vida social de los menores y adolescentes, pero es importante controlar y limitar el tiempo que éstos pasan delante del ordenador.

No se trata de prohibir, ni infundir miedo, se trata de acompañar a los menores en su descubrimiento por el espacio online, por las redes sociales en particular, y por Internet, en general.

Es por ello, que deben tener una actitud empática y con predisposición hacia las actividades de los menores en Internet, enseñándoles a observar lo que descubren desde una visión crítica, así como con quienes contactan, comprobando que todo es normal.

El uso de estas recomendaciones aseguraría un uso seguro de las redes sociales y de esta manera podremos disfrutar de haber inculcado un uso responsable y seguro de las oportunidades que las redes sociales aportan a todos los usuarios. Proporcionándoles las herramientas útiles para desenvolverse en la vida online con responsabilidad y ante todo seguridad.

6. CONCLUSIONES/ CONCLUSIONS

En este trabajo, se han tratado de exponer los riesgos presentes en la utilización de los nuevos métodos de comunicación como son las redes sociales, por los mayores de catorce años, pero menores de dieciocho años.

Además, en este proyecto se describen las funciones de las diferentes asociaciones y organismos públicos y privados encargados de la promoción de un uso seguro y responsable de Internet, fomentando mecanismos de autoprotección con el objeto de que los usuarios de las redes sociales se conciencien de la existencia de una serie de riesgos que pueden afectar principalmente a su intimidad personal y en algunas ocasiones a su imagen. Por otro lado, se ha destacado la normativa que regula la protección de los derechos que pueden verse vulnerados cuando se utilizan las redes sociales de forma no segura, como los derechos a la intimidad personal y familiar, a la propia imagen, o el derecho de propiedad intelectual.

Igualmente, se han propuesto una serie de recomendaciones que pueden servir de guía para una utilización segura de las redes sociales, diferenciándose los destinatarios de dichas recomendaciones, ya que algunas van dirigidas a los menores de edad, mientras que otras van destinadas a los padres y a los tutores de los mismos, puesto que, en definitiva, son éstos últimos los responsables directos de que sus hijos o tutelados utilicen de forma segura las redes sociales.

Asimismo, hemos podido comprobar como los riesgos en las redes son reales y constituye un problema social que requiere para su solución la implicación de diferentes agentes sociales, y es que se trata de un tema que cuando aparece crea una evidente alarma social y para ello, solo hay que fijarse como con cierta frecuencia la prensa nacional publica casos en los que algún menor ha sufrido una violación de su intimidad personal por medio de las redes sociales.

Una vez expuesto lo anterior, parece claro que una primera conclusión podría ser la de que pese a que los distintos agentes sociales, pensemos en los Centros Educativos y demás Administraciones Públicas, puedan contribuir a difundir la información necesaria para que los menores utilicen las redes sociales de forma responsable y lo más segura posible, no se puede obviar el hecho de que la educación en el ámbito familiar es de suma importancia para que los menores conozcan los riesgos a los que se enfrentan cuando están utilizando las redes sociales, y en este punto es en el que los progenitores adquieren suma relevancia, ya que sin

tener que prohibir a sus hijos el uso de las redes sociales, deben informarles, enseñarles y orientarles hacia un camino seguro cuando aquéllos utilizan Internet, puesto que, no se puede olvidar de que las redes sociales aportan beneficios en la vida cotidiana de los menores, estimulando su creatividad y fomentando diferentes habilidades sociales, y a modo de ejemplo, se puede reseñar, la capacidad de convocatoria que poseen las redes sociales de generar movimientos masivos de solidaridad ante una situación de crisis de carácter social.

Como segunda conclusión y a modo de cierre, debemos hacer hincapié en la papel fundamental que la educación tiene en este ámbito, y es que debemos insistir en que la información de los riesgos del uso de las redes sociales debe tener su origen en los propios hogares de los menores porque el uso responsable de Internet debe ser inculcado por las personas responsables de los menores, padres o tutores, imponiéndoles un control de ese uso, como por ejemplo, limitándoles el tiempo que emplean ante el ordenador, vigilando el contenido de las redes sociales que visitan, y que tipo de información personal están compartiendo, pues no debemos olvidar que en este caso se trata de menores en proceso de formación que aún no han desarrollado todas sus capacidades intelectivas y volitivas, capacidades que en su caso deben ser completadas por sus padres en los que recae la tan importante responsabilidad de contribuir al desarrollar integral de la personalidad de sus hijos, y ello, sin perjuicio de que el resto de operadores sociales contribuyan a que el uso de las redes sociales por los menores sea más seguro y responsable.

CONCLUSIONS

In this document, it has been tried to expose the risks present in the use of new communication methods such as social networks, for those over fourteen years of age, but under eighteen years of age.

In addition, this project describes the functions of the different associations and public and private organizations responsible for the promotion of a safe and responsible use of the Internet, promoting self-protection mechanisms in order to make users of social networks aware of the existence of a series of risks that may mainly affect your personal privacy and sometimes in your image. On the other hand, it has highlighted the regulations governing the protection of rights that may be violated when social networks are used in an unsafe mode, such as the rights to personal and family privacy, to one's own image, or the right to intellectual property.

Evenly, a series of recommendations have been proposed that can serve as a guide for the safe use of social networks, differentiating the recipients of these recommendations, since some are aimed at minors, while others are intended for parents and the tutors of the same, since, ultimately, the latter are directly responsible for their children or guardians to use social networks safely.

Likewise, we have been able to verify how the risks in social networks are real and constitute a social problem that requires the involvement of different social agents for its solution, and that it is a subject that seems to create a simple social alarm and for that. Only

hay that resembles the frequency of the national press publishes cases in which the minor has suffered a violation of their personal privacy through the medium of social networks.

Once exposed the above, it seems clear that a first conclusion could be that despite the different social agents, think of the Educational Centers and other Public Administrations, can contribute to disseminate the necessary information for children to use social networks in a responsible use as safe as possible, we can not ignore the fact that education in the family is of the very importance for children to know the risks they face when they are using social networks, but that is not why the message is, and at this point, the one that the parents acquire high relevance that you do not have to prohibit your children from using social networks, that you must inform them, teach them and guide them to a safe place when they use the Internet, that you can't forget that social networks provide benefits in the daily lives of minors , stimulating their creativity and fostering social skills, what can be called, the ability to call social networks to generate mass movements of solidarity in the face of a crisis of a social nature.

In conclusion, we must emphasize the fundamental role that education has in this area, and we must insist that the information of the risks of the use of social networks must have its origin in the homes of the minors because the responsible use of the Internet must be inculcated by the people responsible for the minors, parents or guardians, imposing a control on that use, such as limiting the time they use to work, monitoring the content of the social networks they visit, and what kind of personal information they are sharing, therefore, do not forget that this is the case of a minor in a training

process who has not yet developed all his intellectual and volitional capacities, the capacities that in his case must be completed by his parents, contributing to the integral development of the personality of their children, and this, notwithstanding that the rest of the social operators contribute to making the use of social networks by minors safer and more responsible.

7. GLOSARIO

Cyberbullying: El uso de los medios telemáticos (Internet, telefonía móvil y videojuegos online principalmente) para ejercer el acoso psicológico entre iguales, se incluye actuaciones de chantaje, vejaciones e insultos.

Daily blog: Blog diario, los creados de contenido de Youtube que “suben” videos con su vida cotidiana diariamente.

Gameplays: Vídeo donde se reproduce una partida grabada por un jugador.

Grooming: Es una práctica de acoso y abuso sexual en contra de niños y jóvenes que, en la mayoría de los casos, sucede a través de las redes sociales.

Hashtags: Etiquetas, se utilizan con el símbolo (#) en las publicaciones realizadas en redes sociales.

IP: Número que identifica un dispositivo en la red.

Likes: gustos, en las redes sociales se añaden “likes” o “me gusta” a las publicaciones que son de tu agrado.

Login: Registrarse, se utiliza en las redes sociales para poder acceder a ellas mediante una identificación.

Microblogging: Microblogueo, microblog, permite a los usuarios enviar publicaciones con pequeños textos. El más conocido es la red social Twitter.

Millennials: Se refiere a la llamada generación del milenio, personas nacidas a partir de los 80, identificados como generación digital, multiconectada y con altos valores sociales y éticos.

MMORPG: “Massively multiplayer online roleplaying game”, videojuego de rol multijugador masivo en línea.

Offline: Desconectado

Online: En línea.

Sexting: Se usa para referirse al acto de enviar mensajes explícitos de contenido sexual desde un dispositivo móvil.

Stories: Historias, es una función de la red social Instagram en la que los usuarios pueden crear vídeos de máximo de duración 15 segundos, que permanecen en la red social durante 24h desde su publicación.

Tweet: Publicación o actualización de estado realizado en la red social Twitter. Mensaje de máximo 140 caracteres.

8. FUENTES

8.1. Bibliografía

- Freire Obregón, David, Quesada Arencibia, Alexis y Santos Espino, J. Miguel (2012). *Informática Aplicada*. Las Palmas de Gran Canaria: Vicerrectorado de Profesorado y Planificación Académica Universidad de Las Palmas de Gran Canaria.
- Ocón Carreras, A , Rosa Remedios, C (2011) *Apuntes de Emergencias Tecnológicas*. Vicerrectorado de Ordenación Académica y EEES. Estructura de Teleformación ULPGC. Universidad de las Palmas de Gran Canaria.

8.2. Recursos web

- Ponce, I. (2012). Monográfico: Redes Sociales. Ministerio de Educación, Cultura y Deporte. Extraído el 10 de diciembre, 2017 de: <http://recursostic.educacion.es/observatorio/web/ca/internet/web-20/1043-redes-sociales>
- Costa-Sanchez, C., Piñeiro-Otero, T. (2012). Activismo social en la web 2.0. Revista de Comunicación Vivat Academia. Extraído el 11 de diciembre, 2017 de: <http://webs.ucm.es/info/vivataca/numeros/n117E/PDFs/Varios7.pdf>

- Universitat Politècnica de València. Blog Historia de la Informática. (2011). Extraído el 13 de diciembre, 2017 de: <http://histinf.blogs.upv.es/2011/12/20/redes-sociales/>
- Ruiz, A. Historia de la web. Extraído el 13 de diciembre, 2017 de: <http://www.postgradomarketingonline.com/blog/en-que-grandes-fases-se-divide-la-historia-de-internet/>
- González, G. Genbeta. El estado de las redes sociales en 2017 (2017). Extraído el 14 de diciembre, 2017 de: <https://www.genbeta.com/a-fondo/el-estado-de-las-redes-sociales-en-2017>
- Urretabizkaia, B. (2012): Clasificación y tipos de redes sociales. Extraído el 15 de diciembre, 2017 de: <https://comunidad.iebschool.com/marketingenredessociales/clasificacion-y-tipos-de-redes-sociales/>
- Mesa, F. (2016). ELDIA.es. Nace en Canarias The Gaming Experience (TGX), una red social para “gamers”. Extraído el 15 de diciembre, 2017 de: <http://eldia.es/tecnologia/2016-04-08/2-Nace-red-social-gamers-Canarias-The-Gaming-Experience-TGX.htm>
- Garmendia, M. Jiménez, E., Casado, M.A. y Mascheroni, G. (2016). Net Children Go Mobile: Riesgos y oportunidades en internet y el uso de dispositivos móviles entre menores españoles (2010-2015). Madrid: Red.es/Universidad del País Vasco/Euskal Herriko Unibertsitatea. Extraído el 20 de diciembre, 2017 de: <https://www.ehu.eus/documents/1370232/0/>

[Informe+NET+CHILDREN+RED.ES+España+2016.pdf/626251bc-f3f1-47ee-a06b-8401b91352df](#)

- UNODC. Oficina de las Naciones Unidas contra la Droga y el Delito. (2015) Mini guía de seguridad informática. Extraído el 15 de enero, 2018 de: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Safety_Guide_Spanish.pdf
- IT Digital Security (2018). Seguridad online en 2018: El internet de las cosas esconde grandes riesgos potenciales. Extraído el 25 de enero, 2018 de: <http://www.itdigitalsecurity.es/opinion/2018/01/seguridad-online-en-2018-el-internet-de-las-cosas-esconde-grandes-riesgos-potenciales>
- INCIBE Instituto Nacional de Ciberseguridad de España (2017). INCIBE lanza un teléfono de ayuda para aconsejar sobre los riesgos de Internet para los menores. Extraído el 26 de enero, 2018 de: <https://www.incibe.es/sala-prensa/notas-prensa/incibe-lanza-telefono-ayuda-aconsejar-los-riesgos-internet-los-menores>
- INCIBE Instituto Nacional de Ciberseguridad de España (2017). El centro de seguridad en internet para menores ayudará a niños y adolescentes a prevenir riesgos en la red. Extraído el 30 de enero, 2018 de: <https://www.incibe.es/sala-prensa/notas-prensa/el-centro-seguridad-internet-menores-ayudara-ninos-y-adolescentes-prevenir>

- OSI Oficina de Seguridad del Internauta.(2016) Guía de privacidad y seguridad en Internet. Extraído el 2 de febrero, 2018 de: <https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet>
- Youtube. OSIsseguridad (7 de octubre de 2016). Privacidad y seguridad en Whatsapp.[Archivo de Video]. Extraído el 2 de febrero, 2018 de: <https://www.youtube.com/watch?v=RpwRtQN9iv0>
- IS4k Internet Segura For Kids. Privacidad. Extraído el 3 de febrero, 2018 de: <https://www.is4k.es/necesitas-saber/privacidad>
- IS4k Internet Segura For Kids. Sexting. Extraído el 3 de febrero, 2018 de: <https://www.is4k.es/necesitas-saber/sexting>
- IS4k Internet Segura For Kids. Ciberacoso escolar. Extraído el 3 de febrero, 2018 de: <https://www.is4k.es/necesitas-saber/ciberacoso-escolar>
- IS4k Internet Segura For Kids. Grooming. Extraído el 3 de febrero, 2018 de: <https://www.is4k.es/necesitas-saber/grooming>
- IS4k Internet Segura For Kids. Uso y configuración segura. Extraído el 3 de febrero, 2018 de: <https://www.is4k.es/necesitas-saber/uso-configuracion-segura>
- Acebes, B., Montanera R. y Raigón J. (2017): Estudio Anual Redes Sociales 2017. IAB Spain. Elogia. Recuperado el 5 de febrero, 2018 de: https://iabspain.es/wp-content/uploads/iab_estudioredessociales_2017_vreducida.pdf

- Flores Fernández, J. Pantallas Amigas (2009). Seguridad en las Redes Sociales. Extraído el 7 de febrero, 2018 de: <http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/seguridad-en-las-redes-sociales.shtm>
- AEPD Agencia Española de Protección de Datos. Eliminar fotos y vídeos de internet. Extraído el 10 de febrero, 2018 de: <https://www.aepd.es/areas/internet/eliminar-fotos-y-videos-de-internet.html>
- Comisión Europea. Reforma de 2018 de las normas de protección de datos de la UE. Extraído 20 de febrero, 2018 de: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_es#sobreelreglamentoylaproteccindedatos
- Facebook. Condiciones de Servicio. Extraído 3 de Marzo, 2018 de: <https://www.facebook.com/legal/terms>
- Rubio, I. (27 de febrero 2018). Uno de cada tres menores españoles ha recibido mensajes sexuales a través de Internet. El País. Extraído el 4 de marzo, 2018 de: https://elpais.com/tecnologia/2018/02/27/actualidad/1519741239_756059.html
- El País. (9 de marzo de 2018). La Comunidad Valenciana registra 240 denuncias por ciberacoso en nueve meses. Extraído el 5 de marzo, 2018 de: https://elpais.com/ccaa/2018/03/09/valencia/1520619949_271112.html

- Gálvez, J.J. (3 de abril, 2018). Cuando el infierno sigue fuera del aula: “Ahora no hay escapatoria para las víctimas”. El País. Extraído el 5 de marzo, 2018 de: https://politica.elpais.com/politica/2018/04/01/actualidad/1522594895_713952.html
- ACN Barcelona (3 de febrero, 2016). ‘Ciberbullying’ en niños de nueve años. La Vanguardia. Extraído el 5 de marzo, 2018 de: <http://www.lavanguardia.com/local/girona/20160203/301865681908/ciberbullying-ninos-girona-whatsapp.html>

8.3. Legislación.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE núm. 298 de 14 de diciembre de 1999. Extraído el 6 de marzo, 2018 de: <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750>
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. BOE núm 97, de 22/04/1996. Extraído el 6 de marzo, 2018 de: <https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930>
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. BOE núm 115, de 14/05/1982. Extraído el 7 de marzo,

2018 de: <https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196>

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) DOUEL núm. 119 de 04 de Mayo de 2016. Extraído el 7 de marzo, 2018 de: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE núm. 17, de 19/01/2008. Extraído el 8 de marzo, 2018 de: <https://www.boe.es/buscar/act.php?id=BOE-A-2008-979>
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. BOE núm.97, de 22/04/1996. Extraído el 8 de marzo, 2018 de: <https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930>
- Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil. BOE núm. 15, de 17/01/1996. Extraído el 8 de marzo, 2018 de: <https://www.boe.es/buscar/act.php?id=BOE-A-1996-1069>

- Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia. BOE núm. 180, de 29/07/2015. Extraído el 8 de marzo, 2018 de: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-8470>

9. ANEXOS

9.1 Anexo I

9.2 ANEXO II

Artículo periodístico 1: Periódico EL PAIS, 27 de Febrero de 2018

Uno de cada tres menores españoles ha recibido mensajes sexuales a través de Internet

Los niños acceden a la web a los siete años y a los ocho ya tienen teléfono móvil

Uno de cada tres menores españoles de entre 11 y 16 años ha recibido mensajes sexuales a través de Internet. Las chicas envían más fotografías sugerentes, mientras que los chicos recurren con mayor frecuencia a fotos comprometidas y explícitas que muestran sus genitales. Pese a que un 94,5% de los jóvenes admite que se trata de una práctica peligrosa, casi la mitad opina que es parte del juego erótico o sexual y uno de cada cuatro que mejora las relaciones de pareja.

Esta práctica, denominada sexting, aumenta a medida que los menores crecen: si el 20% de los niños entre 11 y 12 años admite haberlo practicado, el porcentaje sube al 42% entre los jóvenes de 15 y 16. Los niños son quienes reciben más mensajes sexuales, un

35% frente a un 28% de las chicas, ya que también son los que más los demandan. Estas son algunas de las conclusiones del libro *Entre selfies y whatsapps. Oportunidades y riesgos para la infancia y la adolescencia conectada*, que recopila 17 artículos científicos de investigadores europeos y latinoamericanos y que ha sido presentado este martes en la sede de la Comisión Europea en Madrid.

Para Maialen Garmendia, directora del equipo de investigación EU Kids Online de la Universidad del País Vasco, el problema de estos mensajes sexuales es lo que se conoce como sexting secundario, es decir, "cuando esa imagen se reenvía a todos los estudiantes del instituto". Pero este no es el único riesgo al que se enfrentan los menores al conectarse a la web.

El ciberacoso ha aumentado notablemente en los últimos años, según una encuesta realizada a 500 menores españoles de entre nueve y 16 años y a sus progenitores. No obstante, la prevalencia del tipo de acoso "cara a cara" sigue siendo mayor que el que se realiza a través de Internet o por el móvil. "No debemos culpar a la tecnología", señala Garmendia. Por ello, los datos que se ofrecen en la investigación hacen referencia a los menores que han sufrido tanto bullying como ciberbullying. La incidencia del acoso entre usuarios de 9 a 16 años se ha doblado en menos de una década: mientras que en 2010 un 15% declaraba haberlo sufrido, ahora la cifra se ha elevado al 31%.

Además, los datos recogidos en el libro ponen de manifiesto que son los niños de entre nueve y 10 años quienes se sienten "más disgustados" ante una situación de acoso o ciberacoso. Después, a medida que la edad aumenta, son capaces de gestionar mejor esta

situación. Solo un 6% de los jóvenes de entre 15 y 16 años que ha sufrido esta situación manifiesta haberse sentido "muy disgustado".

Acceso al móvil

La implicación del profesorado y la supervisión de los progenitores son imprescindibles para detectar el ciberacoso, sobre todo teniendo en cuenta que la edad de acceso a Internet y a los smartphones es cada vez más temprana. Mientras que en España hace seis años los menores accedían por primera vez a la web a los diez años y tenían móvil a los 11, ahora disponen de su primer smartphone a los ocho y se conectan a la red a los siete. En algunos países como Reino Unido, uno de cada cuatro menores de dos años y el 36% de los niños de tres a cinco tienen su propia tableta, según el regulador Ofcom.

Garmendia ha subrayado que el hecho de que los niños empiecen antes a usar las nuevas tecnologías es inevitable y no tiene por qué ser negativo: "Tenemos que ser proactivos y generar unos hábitos de supervisión desde que son muy pequeños". Este control también es importante en las redes sociales. El 35% de los niños españoles de 11 y 12 años y el 74% entre 13 y 14 tienen algún perfil en una red social. Esto incumple la normativa legal, ya que por ejemplo Facebook requiere que los usuarios tengan una edad mínima de 14 años para crear una cuenta.

Uso abusivo de las nuevas tecnologías

La Estrategia Nacional de Adicciones, aprobada hace tres semanas por el Consejo de Ministros, incluye por primera vez las adicciones sin sustancia, como las nuevas tecnologías. El 18% de jóvenes entre 14 y 18 años en España usa de manera abusiva las nuevas tecnologías, según anunció el delegado del Gobierno para este plan nacional, Francisco Babín.

Los datos del libro *Entre selfies y whatsapps* revelan que el 39% de los jóvenes se ha sentido aburrido al no poderse conectar a Internet y el 10% ha sido incapaz de controlar el tiempo que pasaba en la red. Los datos son más alarmantes en cuanto al uso de los smartphones. Más de la mitad de los participantes ha sentido un fuerte impulso de comprobar su teléfono. Pero para Garmendia, los menores no son los únicos que deben limitar el uso de los teléfonos móviles. “Si preguntáramos a los adultos, no creo que los resultados fueran muy distintos”, ha afirmado.

Artículo periodístico 2: Periódico EL PAIS, 9 de Marzo de 2018

La Comunidad Valenciana registra 240 denuncias por ciberacoso en nueve meses.

La policía organiza un seminario sobre la figura del menor como víctima y autor de delitos.

La Comunidad Valenciana registró en 2017 un total de 98 denuncias por acoso escolar, 240 por ciberacoso a través de las redes sociales, móvil y el ordenador y 85 por violencia de género en las aulas. El dato ha sido ofrecido este viernes en la clausura del Seminario

Jurídico, Policial y Social sobre la figura del menor organizado por la Jefatura Superior de Policía por el delegado del Gobierno en la Comunidad Valenciana.

Las cifras de acoso escolar, a pesar de no abarcar el último trimestre, superaron las de todo 2016, cuando se contabilizaron 87 denuncias. En este mismo periodo se registraron un total de 254 denuncias por ciberacoso y 62 por violencia de género.

El seminario, que jefatura organiza con la colaboración de la Universidad Católica de Valencia, el Decanato de los Juzgados de Valencia y la División de Formación y Perfeccionamiento de la Dirección General de la Policía se ha clausurado, entre otras intervenciones, la fundación Anar y Universidad de Valencia.

Artículo periodístico 3: Periódico EL PAIS, 3 de Abril de 2018.

Cuando el infierno sigue fuera del aula: “Ahora no hay escapatoria para las víctimas”

Los casos de ciberacoso a menores en España aumentan un 65% y suman ya más de 6.500 en el último lustro.

Ana se enfrentó al infierno cuando solo tenía 12 años. Primero, en forma de insultos y empujones en clase. Después, a través de toda una campaña de acoso liderada por una de sus compañeras del colegio de Pamplona donde estudiaba. "Putas asquerosas. Eres una fácil. Eres una guarra", le gritaba una chica en la escuela. "Muérete, no quiero ni que respires el mismo aire", le decía, mientras instaba a otros alumnos a emular una cacería que duró casi cuatro años. En ese tiempo, los episodios humillantes se sucedieron: como cuando le sacaron de la mochila la ropa de educación física y empezaron a tirarla al aire mientras exclamaban: "¡Cuidado, que el virus se contagia!"; o como cuando impedían que otros chavales se le acercaran en el patio para que estuviera siempre sola. Un martirio de burlas constante que no acababa cuando dejaba atrás las aulas. Seguía en casa. A través de las redes sociales.

El ciberacoso a menores detectado en España ha aumentado un 65% en el último lustro. De los 824 casos de todo 2012 se ha pasado a los 1.364 registrados entre enero y octubre de 2017, según los datos recogidos en el Sistema Estadístico de Criminalidad del Ministerio del Interior y facilitados en una respuesta parlamentaria al PSOE. En total, el Gobierno ha contabilizado casi 6.500 victimizaciones en los últimos cinco años. "Los niños tienen acceso, cada vez antes, a unas armas muy potentes y a un mundo sin reglas como es Internet", subraya Carmena del Moral, analista jurídica de Save the Children, que alerta de que la dimensión del problema es mayor que lo que reflejan las cifras oficiales.

"Una gran parte de casos no se denuncian y quedan ocultos", continúa la técnica de la ONG, que en 2016 publicó un estudio —elaborado con los testimonios de 21.500 jóvenes de 12 a 16 años—

que concluía que el 6,9% de los chavales admite haber sufrido un episodio de ciberacoso. "La extrapolación de los datos implica que unos 82.000 menores estarían padeciéndolo", añade Del Moral sobre un informe que también detalla que un 4,2% de las víctimas cree que le atacaban por su orientación sexual; un 5% por su color de piel, cultura o religión; y un 16% por sus características físicas.

A través del WhatsApp, de los foros en Internet, de las redes sociales, del e-mail... Las herramientas usadas por los ciberacosadores se multiplican a medida que su uso se populariza entre los adolescentes. Y el móvil se ha convertido en su aliado más perverso. Según el informe Sociedad digital en España 2017, un 86% de los jóvenes de entre 15 y 24 años posee un móvil y lo usa como dispositivo de referencia para mensajería instantánea (81,7%) y acceso a redes sociales (77,5%). "En comparación con el acoso tradicional, en el que los niños se encontraban en un entorno seguro cuando volvían a casa, ahora nos enfrentamos a un fenómeno que se sufre las 24 horas del día y los siete días de la semana. Ahora no hay escapatoria para las víctimas", sentencia la analista de Save the Children.

Fue el caso de Arancha, una menor de 16 años que se suicidó en 2015 en Usera (Madrid). "Guarra, ¿qué dices de mí? Voy a ir a pegarte con mis primas. Me cago en tus muertos. Me vas a dar 50 euros o voy a ir con mis primas y más gente a pegarte", rezaba el mensaje que recibió de uno de sus acosadores en el teléfono. Uno de los muchos textos amenazantes y audios que acumuló. "El móvil es la herramienta más habitual para acosar telemáticamente y, dentro de este medio, el WhatsApp es la aplicación más utilizada: afecta al 81% de las víctimas", advierte otro estudio de la Fundación Anar. Según este documento, el bullying a través de otras redes

sociales se produce en el 36,2% de los casos. Y el fenómeno se encuentra en pleno auge.

"Los supuestos de acoso se suceden, más aún si cabe que en las aulas, fuera de ellas", resalta la última memoria de la Fiscalía General del Estado, que muestra su preocupación ante el avance del problema: "Responde a que el inicio en las nuevas tecnologías se produce a edades cada vez más tempranas", recalca el documento del ministerio público, donde ya se alerta del archivo judicial de muchos casos porque los autores no superan los 14 años, la edad mínima penal.

Violencia machista

Pero el ciberacoso a menores no se limita al entorno escolar. Los investigadores resaltan que ha proliferado en las relaciones sentimentales entre adolescentes, vinculado al control de la pareja y a la violencia machista. "Los casos que más se repiten en las sesiones con estudiantes de la ESO son los de personas desconocidas con perfiles falsos que comienzan a acosar a los menores pidiendo fotos íntimas", apostilla Diego Lucena, coordinador de un proyecto de prevención del ciberbullying en 10 institutos y 18 colegios de la comunidad de Madrid, en colaboración con la Asociación de Futbolistas Españoles (AFE).

Ana (nombre ficticio) no aguantó más y en 2016 dejó de ir a la escuela. Antes, el centro no había detectado nada. Pero el daño ya estaba hecho. Los insultos y ataques de sus compañeros le provocaron ansiedad y depresión. Necesitó tratamiento psicológico y farmacológico, según consta en la sentencia que condenó a su acosadora a 14 meses de libertad vigilada y le impuso una orden de alejamiento de 300 metros. Esta vez, la víctima denunció.

Artículo periodístico 4: Periódico LA VANGUARDIA 3 de Febrero de 2016.

‘Ciberbullying’ en niños de nueve años

Ensenyament tiene que actuar después de que los padres de los acosadores amenazaran al colegio con denuncias.

Un nuevo caso de ‘ciberbullying’ ha obligado a actuar al Departament d’Ensenyament de Catalunya. Tres menores de un colegio de Girona acosaban a otro en las horas lectivas y fuera del centro a través de mensajes de Whatsapp.

La dirección del CEIP Aldric de Cassà de la Selva (Girona), una de las dos escuelas públicas que hay en el municipio, decidió expulsar durante una semana a los tres acosadores. A pesar de cursar 4º de Primaria (9-10 años) el asedio sobre su compañero era constante y el colegio se vio obligado a tomar cartas en el asunto.

La expulsión no gustó a los padres afectados, que en lugar de culpar a sus hijos la tomaron con la dirección de la escuela. Los progenitores cuestionan la actuación de los profesores hasta el punto de amenazar con interponer denuncias al colegio.

Ante semejante problemática, el Departament d'Ensenyament de Catalunya activó los protocolos establecidos para este tipo de casos. No se han querido dar detalles de lo ocurrido, porque desde Ensenyament aseguran que son hechos que se enmarcan estrictamente dentro del ámbito del centro y donde, además, están implicados menores. Aunque el niño que sufría el 'ciberbullying' tendría los mensajes amenazantes como prueba.

Los niños acosadores ya han vuelto a la escuela tras su semana de castigo, pero este caso vuelve a activar el debate de si es necesario un mayor control de los padres sobre sus hijos con las nuevas tecnologías. Menores de solo 9 años hacían la vida imposible a otro compañero por Whatsapp y los padres no tenían constancia de lo que hacían sus hijos con el teléfono móvil. Y no solo eso, una vez descubierto el caso culparon al profesorado en lugar de a ellos mismos.

Pese a todo, Ensenyament ha dejado claro que, a pesar de su intervención, el conflicto se va a resolver desde el centro ya que se considera una cuestión interna. Según explica la agencia Europa Press, desde el centro se ha querido dejar claro que la expulsión respondió a una situación de convivencia en la escuela, y ha asegurado que están trabajando con el departamento para resolver el caso.

PROPUESTA TRABAJO FIN DE GRADO

GRADO EN SEGURIDAD Y CONTROL DE RIESGOS

CURSO 2017/18

LAURA BARRERA MACÍAS

LAS PALMAS DE GRAN CANARIA 21 DE OCTUBRE DE 2017

INDICE

1. Datos básicos.....	3
2. Título del tema propuesto.....	4
3. Antecedentes.....	4
4. Objeto del Trabajo de Fin de Grado.....	5
5. Contenido del Trabajo de Fin de Grado.....	6
5.1 Contenido global de los diferentes aspectos a tratar.....	6
5.2 Futuro índice del TFG.....	11
6. Asignaturas relacionadas con la titulación.....	12
7. Firmas del estudiante y firma o documento de aceptación del tutor.....	14

1. DATOS BÁSICOS

a. Titulación

Grado en Seguridad y Control de Riesgos.

b. Nombre completo del alumno y tutor

- **Alumna:** Laura Barrera Macías

- **Tutora:** María Isabel Quintero Verdugo

c. Duración máxima aproximada del TFG

La duración máxima aproximada será de 350 horas, siendo el tiempo estimado de 25 horas por los 14 créditos que consta el TFG.

Pasos de la Temporalización del TFG	HORAS
Búsqueda de información	85
Índice de contenidos	10
Resumen	10
Abstract	5
Enfoque del TFG	25
Introducción	15
Contextualización	15
Objetivos	30
Análisis y estudio de los contenidos	60
Propuesta	30
Conclusiones	20
Glosario	10
Referencias y Bibliografía	20
Anexos	15

TOTAL	350
--------------	------------

2. TITULO DEL TEMA PROPUESTO.

a. “Los diferentes riesgos en la utilización de las redes sociales por los mayores de catorce años y menores de dieciocho años ”

3. ANTECEDENTES DEL TEMA PROPUESTO

a. Las redes sociales son plataformas digitales de comunicación global que ponen en contacto a un gran número de usuarios.¹ Estos usuarios reúnen diferentes objetivos por los que pertenecer a una red social, como puede ser un objetivo de simple entretenimiento, un objetivo social, profesional, o incluso económico.

Debemos hacer un recorrido breve en la historia de Internet para localizar el inicio y origen de las redes sociales.

Dicha historia se puede dividir en tres fases o etapas: (web 1.0, web 2.0 y web 3.0)²

Web 1.0 s.(XX): Se caracterizaba principalmente por ser unidireccional, eran páginas con contenido estático y con un fin divulgativo. No se actualizaban por lo que su contenido quedaba rápidamente anticuado u obsoleto.

Web 2.0 s.(XXI): Las conexiones a internet evolucionan al ADSL con lo que mejoran las herramientas y servidores. Es en esta etapa donde nacen las

¹<http://dle.rae.es/?id=VXs6SD8>

²<https://goo.gl/LJWDe6>

REDES SOCIALES, blogs, wikis, foros..ya que el fin de la web 2.0 es el intercambio del conocimiento, la interacción de los usuarios entre sí y conectar a todo el mundo a través de la red.

Web 3.0 se habla de esta etapa en la actualidad, en la que existen documentos en la nube, aplicaciones y los multidispositivos, no solo disponemos de ordenadores para conectarnos a Internet, los smartphones y tablets nos proporcionan mayor facilidades.

La inclusión de Internet y en este caso las redes sociales en nuestros día a día, ha supuesto un cambio en las costumbres de manera global.

Conectarse y compartir información es más fácil que nunca gracias a las redes sociales, por ello con mayor asiduidad los jóvenes publican y dan a conocer datos de su vida privada en la red. Aunque hablando de seguridad en la red, el riesgo nunca es 0, es cierto que si hacemos un uso responsable de la redes sociales no tiene porqué ser un problema, pero por lo contrario si no está claro donde ponemos los límites, la información que se proporciona a la red se puede volver en contra, suponiendo un riesgo mayor para la protección de sus datos personales y su privacidad, y por ello nuestra seguridad en internet se puede ver afectada.

A este respecto, la Agencia Española de Protección de Datos y Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, responden ante las cuestiones de legalidad o ilegalidad en el mundo cibernético.

Sobre los riesgos que pueden suponer para los usuarios mas jóvenes, un uso indebido o irresponsable de las redes sociales es de lo que tratara este TFG.

4. OBJETO DEL TEMA DEL TFG.

El objeto de este trabajo será determinar los riesgos a los que se enfrentan los jóvenes cuando utilizan las redes sociales, conocer cuáles son los riesgos a los que se exponen y cuáles son sus consecuencias. En este punto, haremos referencia a los aspectos de privacidad, intimidad y libertad de ese tipo de usuarios de las citadas redes, en relación con la normativa vigente, destacando la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, como principales normas sobre la materia.

5. CONTENIDO DEL TFG.

5.1. Contenido global de los diferentes aspectos a tratar

En el presente TFG se analizarán las redes sociales, su origen y evolución hasta nuestros días y como hemos cambiado nuestra forma de relacionarnos con la sociedad en la que vivimos a través de las redes sociales cada vez más popularizadas entre los jóvenes, cómo se relacionan en ese ámbito y las medidas de protección que se pueden articular para proteger a los mismos frente a los distintos riesgos que pueden existir.

En cada red social en principio se exige una edad mínima para acceder a las mismas, en caso de no cumplir este requisito el perfil creado podría ser eliminado. En España, el acceso a las plataformas sociales está regulado en el artículo 13 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de

diciembre, de protección de datos de carácter personal.³ Dicho precepto establece el consentimiento para el tratamiento de datos de menores de edad.

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Por lo tanto, no es legal el uso de estas redes por menores de 14 años y está prohibido su registro sin el consentimiento de los tutores legales.

Por otro lado, debida a la importancia y lo avanzado de la normativa española en todo lo relacionado con la protección de datos personales, la protección de la intimidad y la propiedad intelectual, así como la protección de menores e

³ <https://www.boe.es/buscar/act.php?id=BOE-A-2008-979>

incapaces, se hace esencial determinar cuáles son los elementos necesarios para que una red social se encuentre sometida a la legislación española.⁴

Estos requisitos son:

- Que el prestador de servicios de la sociedad de la información, responsable del sitio web, se encuentre establecido en España.

- Que el sitio web, a pesar de ser propiedad y alojarse en servidores externos a la Unión Europea, dirijan sus servicios específicamente al territorio español.

- Que el prestador, a pesar de encontrarse en otro Estado, ofrezca sus servicios a través de un establecimiento permanente situado en España.

Las normativas presentes desde un punto de vista jurídico, en las redes sociales son las siguientes divididas en cinco apartados.

- Servicios de la Sociedad de la Información:

Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico.

Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

- Protección de Datos Personales:

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley 25/2007 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.

⁴ http://www.policiaronda.com/index_htm_files/guia_redes_sociales_y_menores_internet.pdf

- Protección de la Privacidad, Honor, Intimidad y Propia Imagen:

Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

- Protección de la Propiedad Intelectual:

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

- Protección de Consumidores y Usuarios:

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

Ley 44/2006, de 29 de diciembre, de Mejora de la Protección de los Consumidores y Usuarios.

- Protección de menores e incapaces:

Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.

Ley1/1995, de 27 de enero, de Protección del Menor.

Ley11/1985, de 13 de junio, de Protección de Menores.

Ley10/1989, de 14 de diciembre, de Protección de Menores.

Ley 8/2002, de 27 de mayo, de modificación de la Ley 37/1991, de 30 de diciembre, sobre Medidas de Protección de los Menores Desamparados y de la Adopción, y de Regulación de la Atención Especial a los Adolescentes con Conductas de Alto Riesgo Social.⁵

⁵ http://www.policiaronda.com/index_htm_files/guia_redes_sociales_y_menores_internet.pdf

En lo que concierne a la seguridad en redes sociales se detallará en este TFG, Las redes sociales tienen una parte de la responsabilidad en lo referido a la protección de la intimidad de sus usuarios. El diseño de la plataforma y de las herramientas de las que dispone el usuario pueden ser suficientes para evitar o minimizar los problemas relacionados con la intimidad y privacidad.

Y tener un hábito responsable en el uso de las redes sociales es responsabilidad de los usuarios y en caso de menores, los tutores legales deben vigilar y restringir el espacio web disponible hacia ese menor.

Según un estudio de Panda Security, empresa española especializada en la creación de soluciones de seguridad informática.

Hasta el 10% de los mensajes entre adolescentes en redes sociales se identifican como ciberacoso.

Entre el 5 y el 10 por ciento de las interacciones que tienen lugar entre adolescentes a través de las redes sociales contienen mensajes que podrían identificarse como 'ciberbullying', una preocupación de los padres que, en algunos casos, se encuentran además sin saber si sus hijos son víctimas o acosadores en esa interacción.⁶

Es por todo ello, por lo que se debe apostar por una cultura mas asertiva en las redes, inculcando valores de respeto a la intimidad y a la privacidad, denunciando las actuaciones irregulares que conlleven su correspondiente penalización.

⁶ <http://www.eleconomista.es/tecnologia/noticias/8597938/09/17/Hasta-el-10-de-los-mensajes-de-adolescentes-en-redes-sociales-se-identifican-como-ciberacoso.html>

5.2. Índice

1. RESUMEN/ ABSTRACT

2. INTRODUCCIÓN

3. OBJETIVOS

4. METODOLOGÍA

5. CONTENIDOS

5.1. Concepto de red social

5.2. Origen y evolución de las redes sociales

5.3. Las redes sociales más utilizadas

5.4. El perfil de los usuarios de las redes sociales.

5.5. La utilización de las redes sociales por los mayores de catorce años: riesgos posibles.

5.6. Normativa aplicable al uso de las redes sociales.

5.6.1. Derecho de Protección de Datos de Carácter Personal.

5.6.2. Derechos de Propiedad Intelectual.

5.6.3. Derecho Fundamental al Honor, a la Intimidad

Personal y Familiar y a la Propia Imagen.

5.6. Protección jurídica de los menores de edad en el uso de las redes sociales.

5.7. Asociaciones españolas dedicadas la seguridad en la utilización de Internet y de las redes sociales.

5.8. Recomendaciones de uso seguro y responsable del uso de las redes sociales.

5.8.1. Recomendaciones básicas.

5.8.2. Recomendaciones dirigidas a los mayores de catorce años.

5.8.3. Recomendaciones a los padres y tutores.

6. CONCLUSIONES**7. GLOSARIO****8. FUENTES****8.1 Bibliografía****8.2 Recursos web****8.3 Legislación.****9. ANEXOS****6. ASIGNATURAS DE LA TITULACIÓN CON EL QUE EL TEMA PROPUESTO TIENE RELACIÓN.**

Asignatura	Relación	Unidades de Aprendizaje
Informática Aplicada	ALTA	Unidades de Aprendizaje: <ol style="list-style-type: none"> 1. CONCEPTOS básicos de la informática. 2. Redes de computadores y servicios distribuidos 3. Fundamentos de las bases de datos. 4. Sistemas de información geográfica. 5. Fundamentos de la seguridad informática. 6. Legislación y normativa de la seguridad informática.

Asignatura	Relación	Unidades de Aprendizaje
Emergencias Tecnológicas	ALTA	Unidades de Aprendizaje: 1.- De la Seguridad Digital a la Seguridad de la Información: una visión integral. 2.- Fundamentos en Seguridad Digital 3.- Emergencias Tecnológicas: Riesgos, Amenazas y Ataques 4.- Mecanismos de Defensa 5.- Instrumentos para la Gestión de la Seguridad de la Información 6.- Buenas Prácticas y Normativa en Seguridad de la Información
Sociología Aplicada a la Seguridad y el Control de Riesgos	ALTA	Unidades de Aprendizaje: 2: Interacción social y seguridad. 3: La violencia humana y sus formas esenciales. 4: Sociología de la desviación. 5: La sociedad de la información y del riesgo social. 6: El orden y la entropía sociales.
Seguridad humana	ALTA	Unidades de Aprendizaje: 2: La seguridad humana como un derecho emergente. 3: Seguridad humana: marco conceptual. 4: Seguridad de las capacidades humanas. 5: Prevención y Regulación en el gobierno de la seguridad humana. 6: Seguridad humana y acción comunitaria.
Idioma Moderno	ALTA	Unidades de Aprendizaje: Unit 2: Health and First Aid Unit 3: Accidents Unit 4: Security Unit 5: Natural Disasters Unit 6: Fire

Asignatura	Relación	Unidades de Aprendizaje
Introducción al Desarrollo de Proyectos	ALTA	Unidades de Aprendizaje: 1:El proceso de investigación. 2:Metodologías cuantitativas. 3:Metodologías cualitativas. 4:Medición y construcción de instrumentos. 5:Análisis de datos. 6:Elaboración de Proyectos.
Derecho Constitucional	ALTA	Unidades de Aprendizaje: 2: La Constitución, el ordenamiento jurídico y las fuentes del ordenamiento jurídico. 3: Derechos Fundamentales (I). 4: Derechos Fundamentales (II). 5: Los Poderes y los órganos del Estado. 6:La organización territorial del Estado.
Medios de Comunicación social en la seguridad y control de riesgo	ALTA	Unidades de Aprendizaje: 1.¿Qué es comunicación? 2. Historia y modelos de comunicación. 3.Comunicación del riesgo. 4. Los medios de comunicación y la percepción de la seguridad. 5.Análisis de los efectos. La comunidad institucional pública. La comunicación en la seguridad y el control de riesgos.
La información en la Seguridad y el Control de riesgos	ALTA	Unidades de Aprendizaje: 1. El milenio de la información. 2. La información especializada y la gestión de la información. 3. Seguridad de la información. Explotación y confidencialidad.

7. FIRMA DEL ESTUDIANTE Y FIRMA O DOCUMENTO DE ACEPTACIÓN DEL TUTOR.

FIRMA ALUMNA: Laura Barrera Macías



FIRMA TUTORA: Doña María Isabel Quintero Verdugo

QUINTERO
VERDUGO MARIA
ISABEL - 10867697J

Firmado digitalmente por
QUINTERO VERDUGO MARIA
ISABEL - 10867697J
Fecha: 2017.10.22 16:56:43
+02'00'