etsinf

PFC:

Seguridad y privacidad de los menores en las redes sociales

Autor: David Correcher Alacreu

Director: Juan Vicente Oltra Gutiérrez

ÍNDICE

OBJETO Y OBJETIVOS

El **objeto** del presente Proyecto de Fin de Carrera es la obtención del título de Ingeniero Técnico en Informática de Gestión, expedido por la Universidad Politécnica de Valencia.

Los **objetivos** de este proyecto, son dar a conocer los peligros a los que se enfrentan los menores al utilizar las redes sociales y dar las directrices a seguir, para minimizar estos riesgos, así como analizar las condiciones de servicio y medidas de seguridad de las dos redes sociales más utilizadas en España, Facebook y Tuenti.

Además, ofrecer a los usuarios información útil para conocer que es una red social, como funciona, cuales son sus elementos, sus beneficios y los riesgos que puede conllevar su utilización, especialmente para los menores de edad, haciendo hincapié en el cumplimiento de la legislación vigente en España.

INTRODUCCIÓN

Hoy en día, las redes sociales son unas de las principales herramientas de comunicación, utilizadas por los internautas. Están sustituyendo a otras herramientas, como el correo electrónico, los clientes de mensajería instantánea, así como los chats.

En los últimos años, en número de usuarios se ha incrementado de una manera espectacular, debido a la gran cantidad de utilidades que le podemos dar a estas redes, que pueden servir tanto para que los usuarios se comuniquen, compartan contenidos, ideas y demás, como para que las empresas se promocionen o mejoren su imagen, y la comunicación con sus clientes sea más fluida, lo que les permite mejorar.

Debido a que gran parte de la gente, a día de hoy, utiliza las redes sociales, esta pensando en utilizarlas en un futuro, o por lo menos tiene una idea general de para que sirven, es necesario dar a conocer como funcionan estas y a que peligros podemos enfrentarnos en ellas.

Y en cuanto a peligros, los que más expuestos a ellos están son los menores, por eso es necesario crear una guía para orientar tanto a los padres (o tutores), como a los menores,

y dar a conocer que es una red social y de que tipos existen (Cap. 1 y 2), además de que riesgos conlleva su utilización(Cap. 3).

Cuanta más información tengan los usuarios, mejor podrán utilizar las redes sociales, y menos riesgos van a correr, sobre todos los menores, que son los mas desprotegidos, la mayoría de veces por no tener los conocimientos necesarios o por acceder a internet sin la supervisión de un adulto.

Es necesario centrarse en las dos redes sociales utilizadas en España, Facebook y Tuenti, y dar a conocer sus condiciones de uso (Cap. 8 y 9),así como exponer los controles parentales que las los tutores pueden utilizar (Cap. 10) para minimizar los riesgos que puedan correr los menores al utilizar las redes sociales.

En lo sucesivo, se tratará de arrojar un poco de luz sobre aquellos aspectos de las redes sociales que no siempre son conocidos por sus usuarios, y que deben tenerse en cuenta para utilizarlas de la forma más satisfactorio posible.

METODOLOGÍA Y HERRAMIENTAS

1.-¿QUÉ ES UNA RED SOCIAL?, ELEMENTOS QUE LA CONFORMAN

Las **redes sociales** son estructuras sociales compuestas de grupos de personas, las cuales están conectadas por uno o varios tipos de relaciones, tales como amistad, parentesco, intereses comunes o que comparten conocimientos.

Toda red social se fundamenta en la "teoría de los seis grados de separación" propuesta por el húngaro Frigyes Karinthy en 1929, por la que cualquier individuo puede estar conectado con otra persona en el planeta a través de una cadena de conocidos que no supera en más de seis el número intermediarios. El concepto está basado en la idea que el número de conocidos crece exponencialmente con el número de enlaces en la cadena, y sólo un pequeño número de enlaces son necesarios para que el conjunto de conocidos se convierta en la población humana entera.

Las redes sociales son espacios virtuales en los que cada usuario cuenta con un perfil público, que refleja datos personales, estado e información de uno mismo. A su vez dispone de herramientas que permiten interactuar y conocer al resto de usuarios, por ejemplo mediante la creación de grupos de interés.

El origen de las redes sociales se produce a mediados de los años 90, si bien en 2003 se produce el despegue de las mismas, con la creación de MySpace (portal cuyo enfoque principal estaba dirigido hacia grupos de música y fans) y Facebook (una red social creada en sus inicios para estudiantes universitarios y que hoy supera los 600 millones de usuarios

Las nuevas plataformas y herramientas colaborativas han producido un cambio desde una

Web 1.0 basada en páginas estáticas, meramente informativas, sin capacidad de generar una participación del usuario, hacia una Web dinámica donde se produce una interrelación que genera una suma de conocimientos y/o experiencias. Es decir, la Web 2.0 o *Web Social* son personas colaborando, compartiendo y participando en un canal multidireccional abierto que permite lograr la máxima interacción entre los usuarios y les ofrece nuevas posibilidades de colaboración, expresión y participación.

Entre los diferentes elementos que conforman el concepto de red social, cabe destacar los siguientes: sociológico, tecnológico y jurídico.

Respecto al **elemento sociológico**, se puede afirmar que la facilidad y rapidez de interconexión a través de la Red, así como la descentralización que implica que todos los servicios sean prestados de forma remota, suponen un auténtico avance en lo que respecta a la facilidad para iniciar o aumentar el inicio de las relaciones sociales entre los usuarios.

Cualquier persona con una conexión a Internet puede formar parte de este tipo de redes sociales, comenzando así a entablar comunicación con los millones de contactos que las conforman, con absoluta independencia del lugar o dispositivo desde el que se accede, así como del momento en que se interacciona con el resto de usuarios.

El segundo es el **elemento tecnológico**, considerado probablemente el pilar esencial gracias al cual las redes sociales han podido evolucionar y crecer de manera exponencial con la rapidez con la que lo han hecho.

Los avances en las telecomunicaciones y especialmente la difusión de las conexiones de alta velocidad -ADSL, Cable, 3G- han permitido el desarrollo de redes cada vez más completas y complejas. Todo ello, unido a la rápida e incesante evolución y abaratamiento de los dispositivos y hardware de conexión, han hecho que el número de usuarios de este tipo de plataformas sea cada vez más elevado y, sobre todo, más recurrente en el empleo de estas redes.

El tercer elemento esencial a considerar dentro del concepto de red social, es el **elemento jurídico**. Dada la entidad, tamaño e incidencia social que están tomando las

redes sociales, existen gran cantidad de acciones y actos que las diferentes plataformas están realizando sin conocer o al menos sin cumplir principios básicos de la normativa española de protección de datos de carácter personal, de protección de la intimidad, la publicidad y la protección de la propiedad intelectual e industrial respecto a los contenidos creados y alojados por los usuarios en sus perfiles de usuarios.

Algunos aspectos esenciales respecto de las repercusiones jurídicas que implican las redes sociales son los siguientes:

-Protección de Datos de Carácter Personal:

El fundamento 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.

-Intimidad:

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, no obstante, existen ciertos indicios y aspectos que podrían permitir una interpretación entendida como una renuncia ciertamente *"viciada"*, sin contar con todos los elementos necesarios para que el consentimiento resulte completamente válido.

-Propiedad Intelectual e Industrial:

Uno de los 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 redes sociales) y uno de los fundamentos básicos de Internet y de las redes de este tipo, el intercambio constante de información, con independencia del formato o tipo de información intercambiada.

2.-TIPOS DE REDES SOCIALES

Según la **temática** que desarrollan, toda red social puede clasificarse según el tipo de temática tratada por sus usuarios, existiendo redes sociales dedicada al desarrollo artístico, hasta redes sociales dedicadas a la mera puesta en contacto de amigos y perfiles, así como redes dedicadas a la información y recomendación respecto a la compra de artículos de consumo.

Según el **público objetivo** al que van destinadas, entendiendo que *"público objetivo"* hace referencia al tipo de usuarios que el creador de la redes quiere que utilicen y desarrollen la red social. Dentro de este segundo grupo, observamos la existencia de dos grandes grupos de redes sociales, que son las de tipo Generalista-ocio y las Profesionales.

Las redes sociales profesionales tienen como objeto principal fomentar, incentivar y aumentar las relaciones entre profesionales, tanto de un mismo sector, como de sectores diferentes. Como principales particularidades, se pueden destacar las siguientes:

- Cuentan con una doble finalidad. Realizar búsqueda de posibles candidatos para puestos de trabajo o bien buscar entidades u oportunidades laborales.

- Dependiendo de la cualificación y nivel del usuario, la red puede ser empleada como plataforma para la toma de contacto inicial ante posibles negocios entre titulares de compañías.

- Permite la creación de una identidad digital profesional, siendo ésta completamente pública en la Red.

- Al ser un punto de encuentro entre profesionales del sector, permite al profesional mantenerse al día de las novedades del mismo.

A pesar de los muchos beneficios que supone el uso de este tipo de redes profesionales y la diversidad de aspectos positivos que pueden derivarse, existen ciertos ***peligros*** que conviene conocer para poder evitarlos. Así, especialmente relacionado con la protección de datos de carácter personal, está el hecho de que los usuarios cuelgan datos personales en la Red, que *animan* la proliferación de los denominados *"coleccionistas de contactos"* o *"social spammers",* dedicados a recabar contactos disponibles en las redes sociales, en principio sin otra finalidad que la de figurar como usuarios con más contactos en dicha red social.

A pesar de que la finalidad no parezca en principio dañina para los usuarios ni para la propia red social, aquella situación supuso un grave problema para una de las más importantes redes sociales profesionales del mundo, ya que desembocó en que la compañía propietaria de la plataforma tuviera que cambiar completamente el modo de interrelación entre los diferentes usuarios, exigiendo para poder realizar contactos directos, que previamente ambos usuarios hubieran aceptado la existencia de una *relación de confianza mutua*.

En las redes sociales profesionales, este requisito inicialmente no era exigido, dado que lo que pretendían era la puesta en contacto del mayor número de profesionales posibles, con la finalidad de lograr el mayor grado posible de *"networking"* (contactos) entre los usuarios. No osbtante, y dados los gravísimos problemas que este tipo de situaciones podrían llegar a suponer, todas las redes sociales han decidido exigir un cierto grado de confianza, cercanía y/o relación para poder ser *"amigo"* o *"contacto"* entre dos miembros de la red.

De otro lado, se encuentran las **redes sociales generalistas o de ocio,** cuyo principal objetivo es facilitar y potenciar las relaciones personales entre los usuarios que la componen. El grado de crecimiento de este tipo de redes ha sido el más destacado en los últimos años, llegando a formarse plataformas que alcanzan los 100 millones de usuarios, como son Myspace y Facebook.

Este tipo de redes han pasado en muchos casos, y especialmente entre el colectivo de usuarios más jóvenes, a complementar e incluso a sustituir otros medios de comunicación, tales como la mensajería instantánea. Esto se debe principalmente a que

todas las redes sociales generalistas o de ocio son redes caracterizadas por los siguientes aspectos:

- Ofrecen gran cantidad de aplicaciones y/o funcionalidades que permiten a los usuarios prescindir de aplicaciones de comunicación externas, poniendo a su disposición una plataforma que integra todas las herramientas en una misma pantalla.

- Ofrecen y fomentan que los usuarios no se centren únicamente en operar de forma online, sino que este medio sea la plataforma a través de la que convocar y organizar aspectos de la vida offline.

- Ponen a disposición de la comunidad de usuarios parte del código abierto, mediante el que ha sido programada la plataforma, de modo que los usuarios puedan desarrollar aplicaciones propias que sean ejecutadas dentro de la red, o aplicaciones externas que se interconecten con la plataforma, logrando así el aumento de la viralidad.

A pesar de existir varios tipos de Redes Sociales, todas ellas tienen un gran número de **puntos comunes** como los que se exponen a continuación:

- Tienen como finalidad principal **poner en contacto e interconectar a personas**, de tal forma que a través de la plataforma electrónica se facilite la conexión de forma sencilla y rápida.

- Permiten la **interacción** entre todos los usuarios de la plataforma, ya sea compartiendo información, contactando o facilitando contactos de interés para el otro usuario.
- Permiten y fomentan la posibilidad de que los usuarios inicialmente contactados a través del mundo online, **acaben entablando un contacto real**, del que muy probablemente nacerán nuevas relaciones sociales.

- Permiten que el contacto entre usuarios sea **ilimitado**, en la medida en la que el concepto espacio y tiempo se convierte en relativo al poder comunicar *desde* y *hacia* cualquier lugar, así como en cualquier momento, con la única condicición de que ambas

partes acepten relacionarse entre sí.

- Fomentan la **difusión viral de la red social**, a través de cada uno de los usuarios que la componen, empleando este método como principal forma de crecimiento del número de usuarios.

3.-PRINCIPALES RIESGOS DE LAS REDES SOCIALES

A pesar de las cifras de los millones de usuarios registrados y del alto grado de crecimiento de este tipo de redes, éstas cuentan con un nivel de riesgo superior al de las redes profesionales, dado que los usuarios exponen no sólo sus datos de contacto o su formación, sino que hacen públicas sus vivencias, gustos y experiencias, lo que provoca que, en muchas ocasiones, sean aún más los datos expuestos en este tipo de redes, que en las de tipo profesional, suponiendo un riesgo mayor para la protección de sus datos personales y su privacidad.

3.1.-Protección de datos de carácter personal

Uno de los principales aspectos jurídicos que debe ser analizado dentro de las redes sociales es el cumplimiento de la normativa de **protección de datos de carácter personal**, regulada mediante Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y su reglamento de desarrollo, 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 (RLOPD).

El derecho a la protección de datos en España ha sufrido en los últimos años una gran evolución, perfeccionando el sistema regulatorio, así como las medidas que los responsables de tratamiento deben adoptar a la hora de tratar datos de carácter personal. No obstante, la evolución de la protección de datos en España no ha estado exenta de situaciones y problemas que son cada vez más acuciantes derivados del uso y explotación de nuevos servicios online.

Durante el año 2000, poco tiempo después de la publicación de la LOPD, el Tribunal Constitucional, en Sentencia 292/2000, reconoció el *Habeas Data* como un auténtico derecho fundamental, derivado de lo dispuesto en el art. 18.4 de la Constitución Española, con entidad y autonomía independiente respecto al derecho al honor, intimidad y propia imagen, lo que supuso un clarísimo punto de inflexión en la mejora y perfección de la

normativa vigente.

El propio concepto de red social conlleva la puesta a disposición de toda la red de contactos de gran cantidad de datos personales. Este hecho hace que las redes sociales se conviertan en grandes fuentes de información sobre sus miembros, lo que, a su vez, hace que el cumplimiento de la normativa, prerrogativas y medidas de seguridad respecto a la protección de datos personales se conviertan en esenciales para su correcto funcionamiento, así como para la protección de sus miembros.

Se observa como frecuentemente los procesos llevados a cabo no se encuentran plenamente adecuados a las exigencias legales dispuestas en la normativa española o europea. En este sentido, cuenta con especial trascendencia el cumplimiento de la normativa española de protección de datos de carácter personal, tanto en el momento iniciar de la obtención de los datos de los usuarios, como durante su tratamiento. No obstante, se ha de tener en cuenta que el modelo de creación y crecimiento empleado por este tipo de redes y, en general, por el modelo denominado web 2.0, no es el responsable del sitio web el que determina y aloja los contenidos en el mismo, sino que son los propios usuarios los que voluntariamente publican sus datos personales en la red.

En este sentido, y dado que la red social está formada esencialmente por tres elementos principales: software, datos personales e información sobre los usuarios, estas plataformas pueden presentar diversos riesgos en lo que respecta a la protección de datos personales, que se detallan a continuación:

• En ocasiones, los datos personales tratados por la red social pueden ser **comunicados, cedidos o puestos a disposición de terceros** por diversos motivos, desde su mantenimiento por servicios de hosting**16**, hasta su almacenaje o comunicación a terceros para llevar a cabo acciones de marketing directo.

•A pesar de que aparezcan publicados textos legales relativos a la protección de datos de los usuarios, es muy frecuente observar como dichos **textos legales no son comprensibles para un ciudadano medio** que no cuente con experiencia o formación jurídica. Los textos, además, suelen ser publicados en lugares de la plataforma de difícil localización y acceso.

Debe tenerse en cuenta lo ya expuesto por la Agencia Española de Protección de Datos (AEPD) en su *Informe sobre buscadores de Internet*, publicado el día 1 de diciembre de 2007**17**, donde se establecía la necesidad y la obligación por parte de los prestadores de servicios de la Sociedad de la Información, de facilitar a los usuarios una información real y efectiva respecto al cumplimiento de las obligaciones legalmente dispuestas.

Esta información debe destacarse suficientemente en las páginas de inicio y en las fases de registro como usuario, así como en las políticas de privacidad. Además debe advertirse cuáles son las consecuencias más relevantes sobre el uso y tratamiento de datos personales, así como el almacenamiento de estos datos en el ordenador a través de cookies.

Debido a que esta información se recoge en textos legales de gran complejidad, haciéndose inteligible para un usuario medio, ha llevado a la generalización entre los usuarios del hecho de que los avisos legales y políticas de privacidad no sean leídos en la gran mayoría de casos y, en aquellos casos en los que son revisados por los usuarios, no son realmente comprendidos, por lo que no cumplen su objetivo principal, que es que el usuario conozca absolutamente toda la información relativa a la finalidad del tratamiento de sus datos personales y la gran cantidad de implicaciones que conlleva el tratamiento de los datos personales.

Por último, es importante destacar el hecho de que las principales redes sociales utilizadas en España no llevan a cabo el tratamiento de los datos personales en España o en la Unión Europea, sino que trasladan la información a terceros estados sobre los que la AEPD considera que no cumplen con los requisitos de seguridad exigidos por la legislación nacional.

En lo que concerniente a las **redes sociales**, y por lo que respecta al cumplimiento de la normativa en materia de protección de datos y siempre que se puedan encuadrar los servicios de aquellas en los ámbitos de aplicación de la LSSI-CE y/o de la LOPD, se establecen **las siguientes recomendaciones:**

-Se recomienda someter la plataforma online, así como el tratamiento de datos

personales de los usuarios a una auditoría que garantice la adecuación plena del sitio web a la normativa vigente, así como que se someta el tratamiento de datos personales a una auditoría que garantice que dicho tratamiento es completamente legal.

-Disponer de una Política de Protección de Datos que sea claramente visible, completamente accesible y comprensible para los usuarios.

-Que la Política sobre Protección de Datos se pueda imprimir o, en su caso, descargar.

-Que los usuarios deban aceptar expresamente la Política de Privacidad antes de que sus datos personales sean enviados al responsable de la Web y sean publicados en su perfil.

-Inscribir el fichero o ficheros que contengan datos personales recabados a través del sitio web en el Registro de la Agencia Española de Protección de Datos.

-Proporcionar medios gratuitos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de sus datos de carácter personal.

-Si se ceden o comunican los datos de carácter personal, se debe hacerlo cumpliendo con lo dispuesto en la LOPD**.**

En lo que respecta a los usuarios, considerados en todo caso como la parte más débil en esta relación, las **recomendaciones** van orientadas en dos sentidos:

- Si se desea saber de qué datos dispone la red social sobre nosotros, o se desean actualizar o eliminar, se deberá ejercitar los derechos de Acceso, Rectificación, Cancelación Oposición (ARCO).

- Si en el plazo de 10 días, o de 30 días en el caso del derecho de acceso, no hubiera sido atendida la solicitud o ésta no hubiera sido satisfactoria, se deberá proceder a denunciar ante la AEPD este hecho, siendo la Agencia la encargada de analizar y determinar el incumplimiento o no de la plataforma.

• Si recibe publicidad o información no deseada, o si por alguna circunstancia considera que sus datos han sido comunicados o cedidos a terceros sin su autorización, deberá ponerlo en conocimiento de la AEPD para que determine la existencia o no del incumplimiento de la obligación dispuesta en los artículos 19 a 22 de la LSSICE.

3.2.-Derecho a la intimidad y propia imagen

En segundo lugar, y según el grado de incidencia, se encuentra otro derecho fundamental, independiente del derecho a la protección de datos personales, aunque estrechamente relacionado, como es el derecho a la Intimidad y a la propia imagen que toda persona tiene.

La protección del Derecho Fundamental al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen**20** se encuentra regulada por 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, cuya finalidad es la protección civil frente a todo género de intromisiones ilegítimas y no autorizadas expresamente por el titular y que afecten de forma directa a su honor, intimidad propia o familiar, así como a su imagen.

Al igual que en la materia de protección de datos, la intimidad y la protección de la imagen de las personas se encuentra íntimamente relacionada con las redes sociales y otros sitios web colaborativos, dado que el objeto principal de éstos se centra en el intercambio de información, en muchas ocasiones personal y también relativa a terceras personas.

El aumento de las herramientas y aplicaciones para la publicación de material gráfico (fotografías y vídeos), así como la gran capilaridad y capacidad de viralidad de dichos contenidos, provocan que, una vez alojados en el medio digital, éstos sean inmediatamente accesibles por miles o incluso millones de usuarios.

La Ley Orgánica 1/1982 regula desde el punto de vista civil la protección de un derecho que, a pesar de encontrarse directamente relacionado con la protección de datos, cuenta con una regulación mucho menos amplia y compleja que ésta, pero que sin embargo

dispone de un desarrollo jurisprudencial muy amplio y desarrollado.

A pesar de que en la parte final de la guía se tratarán los aspectos relativos a los menores de edad, la Ley Orgánica 1/1982 es específica en lo que respecta a este colectivo, indicando que exclusivamente sus representantes legales serán los que autoricen por escrito cualquier publicación de su imagen, debiendo notificarlo de forma previa a la Fiscalía de Menores**.**

Las redes sociales tienen gran parte de la responsabilidad 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 pueden ser suficientes para evitar o minimizar los problemas relacionados con la privacidad.

•La red social debe concienciar a sus usuarios de la importancia de ser respetuoso con el resto de usuarios y de no llevar a cabo actos que puedan vulnerar la intimidad de los mismos.

•De igual forma, la red social debe sancionar de forma ejemplar las acciones que vulneren la intimidad de cualquier tercero. Este tipo de actos deben sancionarse con la expulsión inmediata del usuario infractor.

• Toda red social debe establecer los canales necesarios de denuncia de contenidos para recibir las solicitudes de retirada.

•El canal de denuncia debe ser además efectivo, garantizando la atención de las solicitudes en un plazo de tiempo razonable, siendo más que recomendable la automatización del mismo si esto resulta posible.

•Igualmente, es recomendable facilitar medios de control de comentarios, de tal forma que para que los comentarios que se remitan aparezcan de forma pública sea necesaria la validación previa de los mismos por parte del titular del perfil.

•Por último, también es interesante facilitar sistemas de bloqueo de cuentas y usuarios, de tal forma que los propios usuarios de las redes sociales puedan evitar insultos o

comentarios inadecuados bloqueando a aquellos usuarios con los que pueda tener cualquier conflicto.

•Los servidores donde se albergue la información sensible deberán contar con las medidas tecnológicas y organizativas que sean oportunas para garantizar que ésta no es accesible por ningún tercero no autorizado.

Por su parte, **el usuario que vea vulnerada su derecho a la intimidad debe actuar de la siguiente forma:**

• En primer lugar, de forma inmediata debe ponerse en contacto con los administradores a través de los sistemas de denuncia con los que cuente la red social para que el video o la fotografía en los que aparezca el usuario sean eliminados inmediatamente, al no existir permiso expreso por parte del titular para su publicación. Del mismo modo, deberá solicitar la retirada del comentario o texto que atenta contra su intimidad.

• En segundo lugar, deberá ponerse en contacto con los buscadores que hayan indexado el contenido, para que procedan a su bloqueo o retirada, de tal forma que deje de aparecer dentro de los resultados en el momento de hacer las búsquedas.
• Por último, puede iniciar las actuaciones judiciales pertinentes ante los Tribunales Civiles, y en su caso, denunciar ante la Agencia Española de Protección de Datos el incumplimiento de la normativa de protección de datos de carácter personal. En cualquier caso, se recomienda preconstituir prueba mediante depósito notarial de todos los contenidos mostrados a través de la web.

3.3.-Propiedad intelectual

La normativa en materia de propiedad intelectual tiene por objeto principal proteger los derechos de los autores sobre las obras artísticas, científicas o literarias que les correspondan por su mera creación**25**, integrando derechos de carácter personal y patrimonial, que atribuyen al autor la plena disposición y el derecho exclusivo a la explotación de estas obras, sin más limitaciones que las establecidas en la legislación vigente.

El titular de estos derechos puede autorizar o no cualquier reproducción, puesta a disposición o transmisión de una obra de su repertorio, estando dicha autorización únicamente limitada por las excepciones dispuestas legislativamente**27** y que abarcan el derecho de cita, los trabajos de actualidad o las reproducciones provisionales y copias privadas, entre otras.

Los sitios web como las redes sociales son plataformas centradas básicamente en el intercambio y puesta en común de información y contenidos.

Es la gran viralidad de estas redes y el fomento para la creación de plataformas de generación de contenidos multimedia, especialmente fotografías y vídeos, lo que ha provocado que la propiedad intelectual 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.

Son muchos los usuarios de este tipo de redes que alojan en éstas sus obras musicales o fotográficas con la única finalidad de promocionarlas de forma viral entre los millones de usuarios de la red y considerables los casos en los que importantes grupos musicales han sido parte implicada en situaciones jurídicas planteadas ante controversias respecto de la explotación de sus propias obras.

En este sentido, todos los usuarios deben atender a las condiciones de registro y especialmente a la regulación que en éstas se disponga en materia de propiedad intelectual e industrial, observando el tipo de cesiones de derechos que realizan y a favor de quién se realizan.

Las **redes sociales** deben considerar los derechos de propiedad intelectual de los usuarios y de los terceros para el funcionamiento normal de sus plataformas. Para ello deben seguir estas recomendaciones:

• Informar debidamente y hacer conscientes a los usuarios a través de las condiciones generales de registro, preguntas frecuentes y avisos espontáneos mostrados previamente al alojamiento de imágenes, vídeos y contenidos susceptibles de protección de los

derechos de propiedad intelectual, de la naturaleza de los derechos de autor y de la importancia que tiene respetarlos.

• Facilitar a los autores la protección de sus derechos mediante sistemas de denuncia internos que garanticen la efectividad y rapidez de la comunicación.

• Ejecutar de forma inmediata a la hora de eliminar o, en su caso, bloquear contenidos protegidos por derechos de autor.

Por su parte, **los autores,** en caso de que entiendan que algún usuario o incluso que la red social ha vulnerado alguno de sus derechos de propiedad intelectual, deberá seguir las siguientes recomendaciones:

•Iniciar, de forma inmediata, la puesta en contacto con la red social en cuestión, denunciando el hecho, notificándolo de forma fehaciente, indicando el contenido protegido, la naturaleza y titularidad del mismo, exigiendo la cesación instantánea de la infracción**.**

• En su caso, acudir a los órganos jurisdiccionales que resulten oportunos requiriendo la cesación inmediata de la infracción, así como las medidas cautelares indicadas por la Ley.

Riesgos generales de las Redes Sociales

Dentro de los riesgos existentes en las comunicaciones colaborativas, el componente tecnológico juega un papel fundamental. La capacidad actual del malware o código malicioso para aprovechar vulnerabilidades y fallos de seguridad de las plataformas colaborativas, multiplican los posibles efectos de sus ataques en la información de los perfiles y en los equipos y programas de los usuarios:

•**Infección y/o alteración de los equipos, aplicaciones y programas**, tanto del usuario como de su red de contactos.

• **Robo de información personal**, como nombres de usuarios y contraseñas, fotografías, aficiones, números de tarjetas..., información que puede ser utilizada con fines lucrativos o

publicitarios.

• **Suplantación de la identidad del usuario**, bien creando cuentas falsas en nombre de otros usuarios, bien robando datos de acceso a los perfiles para sustituir al verdadero usuario.

A continuación, se incluyen algunas de las técnicas utilizadas para llevar a cabo los ataques de seguridad y privacidad en plataformas colaborativas.

•**Social Spammer y Scammer**. El uso de estas plataformas es una oportunidad para el envío de correos electrónicos no deseados, tanto si la finalidad es meramente publicitaria (spam), como si implica fraude o lucro indebido (scam).

•**Tabnabbing**. Esta técnica se basa en aprovechar el sistema de navegación por pestañas o *tabs*. Cuando el usuario va de una pestaña a otra, la que permanece en segundo plano se transforma en una página de acceso a servicios y plataformas (como Gmail, Youtube, Facebook, etc.). El usuario, al no percatarse, introduce los datos de acceso a estos servicios, y por tanto, está facilitando estos datos al propietario de la página falsa.

•**Pharming**. Este ataque informático consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de la plataforma Web 2.0. Al escribir el nombre de la plataforma en la barra de direcciones, el navegador redirige automáticamente al usuario a otra dirección IP, donde se aloja una web falsa. Al intentar acceder al servicio, el usuario está facilitando sus datos de acceso al ciberatacante.

Tanto el phishing como el pharming están muy explotados por los delincuentes para lograr la obtención de datos personales de los usuarios de Internet, así como datos de carácter sensible o relativos a aspectos económicos (tarjetas de crédito, PIN de usuarios, etc.).

•**Clickjacking**. En este caso, al hacer *click* en “Me gusta” (botones para compartir opiniones sobre un contenido), se actualizan en el estado del usuario frases que redirigen hacia webs de spam o malware. También se pueden encontrar mensajes que enlazan hacia webs fraudulentas, como en el siguiente ejemplo en Twitter:

En este sentido, en Twitter se está extendiendo el uso de acortadores de URL (dadas las limitaciones de caracteres por mensaje) que enlazan a páginas web maliciosas.

•**Gusanos**. Los gusanos constituyen una de las amenazas con mayor repercusión, ya que disponen de variantes diseñadas para diferentes plataformas Web 2.0, como es el caso del gusano Koobface y sus variantes para las principales redes sociales. Este tipo de malware utiliza cuentas de usuarios ya comprometidas para propagarse, colocando enlaces infectados en los que fácilmente pinchan los contactos del usuario víctima.

• **Instalación y uso de cookies sin conocimiento del usuario**. Otro riesgo relacionado con la participación del usuario en las plataformas radica en la posibilidad de que el sitio web utilice cookies que permitan a la plataforma conocer cuál es la actividad del usuario dentro de la misma. Mediante estas herramientas pueden conocer el lugar desde el que el usuario accede, el tiempo de conexión, el dispositivo desde el que accede (fijo o móvil), el sistema operativo utilizado, los sitios más visitados dentro de una página web, el número de *clics* realizados, e infinidad de datos respecto al desarrollo de la vida del usuario dentro de la Red.

4.-PAUTAS DE PRIVACIDAD A SEGUIR EN LAS REDES SOCIALES

Vistos los posibles riesgos de la Web 2.0, se proporcionan a continuación una serie de pautas de privacidad, dirigidas a cada colectivo implicado.

Usuarios

-En la Web 2.0 los usuarios deben respetar unas normas de privacidad, tanto en lo relativo a datos propios, como si la información que difunden es de terceros.

-Los usuarios deben proteger su información. Por ello, es necesario leer las políticas de privacidad, estableciendo unos límites sobre quién puede o no acceder a la información publicada.

-Una buena práctica es recurrir al uso de seudónimos o *nicks* personales permitiéndole disponer así de una "identidad digital".

-No se debe publicar información excesiva de la vida personal y familiar, esto es, información que no se difundiría en entornos no tan cercanos.

-Es necesario tener especial cuidado al publicar contenidos audiovisuales y gráficos, especialmente si son imágenes relativas a terceras personas.

-Antes de publicar una foto es recomendable considerar si es adecuado colgarla o si dicha acción puede traer consecuencias, involucrando a gente del trabajo, colegio, universidad o del entorno cercano o personal.

-Si se desea utilizar o reproducir cualquier obra en la Red (gráfica o no), se debe acudir al aviso legal de la página web donde se encuentre y ver las condiciones de reproducción de la misma.

-Acudir a la Agencia de Protección de Datos, AEPD (www.agpd.es), para ejercer los derechos que otorga la LOPD en relación a la protección de los datos de carácter personal. En el sitio de la AEPD se puede descargar un modelo de reclamación.

Administradores y moderadores

En este grupo, las pautas de privacidad están relacionadas con la protección de datos e informaciones de carácter personal de los usuarios, así como con la defensa de la legalidad por parte de los usuarios de la plataforma que gestionan.

Según se establece en la LOPD, toda persona que trate datos de carácter personal (asociados a buscadores, a perfiles, etc.) debe cumplir unas obligaciones y atender a los afectados de dicho tratamiento. Entre otras, debe haber un titular que realice un tratamiento de datos:

-Debe inscribir el fichero en el Registro de la AEPD y adecuarlos ficheros a la normativa vigente (LOPD y Reglamento de desarrollo).

-Está obligado a informar a los usuarios sobre la Política de Privacidad de la página web, así como de la finalidad para la que se recaban datos de carácter personal.

-Debe recabar el consentimiento inequívoco del afectado para difundir los datos de este.

-Permite a los usuarios el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición.

-Es importante ejercer de una forma efectiva las labores de supervisión y control, sobre los participantes y sus informaciones. Ante comentarios o informaciones incorrectas o ilícitas, mediar en el debate y/o eliminar los comentarios.

-Hay que implementar medidas tecnológicas que permitan conocer la edad de los usuarios, tales como: el uso de certificados reconocidos de firma electrónica o de

aplicaciones que detecten el tipo de sitio web visitado y los servicios más demandados.

-Es un deber colaborar con las Fuerzas y Cuerpos de Seguridad del Estado para identificar usuarios que cometen hechos ilícitos.

Empresas que prestan servicios de intermediación de la sociedad de la información

Los datos que los usuarios introducen en la Red son almacenados por parte de los prestadores de servicios de intermediación de la sociedad de la información (buscadores, formularios de registro, utilización de datos cruzados, etc.). Las actuaciones en materia de privacidad deben encaminarse al adecuado tratamiento de datos personales de usuarios de las plataformas.

-Al igual que en el caso de los Administradores, cumplir las obligaciones que establece la LOPD en relación al tratamiento de datos de carácter personal.

-Además, la ley prohíbe enviar "comunicaciones publicitarias" por correo electrónico u otro medio de comunicación electrónica "que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios".

-No retener datos de carácter personal de forma excesiva o injustificada, salvo que esta actuación responda a una colaboración con las Fuerzas y Cuerpos de Seguridad del Estado.

Por último, deberán facilitar información a sus usuarios acerca de las posibles responsabilidades en que puedan incurrir por la vulneración de derechos de propiedad intelectual e industrial.

PAUTAS DE SEGURIDAD A SEGUIR EN LAS REDES SOCIALES

Las amenazas de seguridad en la Web 2.0 tienen un potencial de expansión superior al de otros medios, debido a su propia estructura en red. Por ello, todos los actores deben

seguir unas pautas de seguridad.

Usuarios

Los usuarios son los principales perjudicados por los ataques de malware, que pueden afectar tanto a la información contenida en las plataformas colaborativas, como a sus propios equipos y dispositivos. Para evitarlo, se recomienda:

-Mantener actualizado el equipo, tanto el sistema operativo como cualquier aplicación que tenga instalada. Ello es fundamental dado que un navegador actualizado incorporara filtros de bloqueo frente a nuevas amenazas e intrusiones no deseadas.

-Utilizar contraseñas seguras para acceder a los diferentes perfiles.

-Comprobar la legitimidad de los sitios web a los que se quiere acceder, vigilando las URLs en la ventana del navegador.

-Durante la navegación, sólo se deben descargar ficheros o aplicaciones de fuentes confiables, a fin de evitar códigos maliciosos o malware. Se recomienda igualmente analizar con un antivirus los elementos descargados antes de ejecutarlos.

Administradores y moderadores

Se recomienda a estos actores de las plataformas de la Web 2.0:

-Disponer internamente de herramientas encaminadas a reducir los casos de suplantación de identidad de usuarios dentro de la Red, permitiendo a los legítimos titulares de los servicios que puedan autenticar su verdadera identidad, para así recuperar y bloquear el acceso al usuario que ilegítimamente utilizó el perfil del otro.

-Integrar sistemas que detecten el nivel de seguridad de las contraseñas elegidas por los usuarios en el momento de registro, indicándole si es o no segura e informándole de los mínimos recomendables.

Empresas que prestan servicios de intermediación de la sociedad de la Información

Los prestadores de servicios de la sociedad de la información ligados a las plataformas colaborativas deben tener en cuenta que estos servicios se basan en grandes bases de datos, con datos personales de los usuarios que las utilizan. Por ello, deben:

-Garantizar que la Red es segura frente a posibles ataques de terceros y, que impide, o al menos reduce, la posibilidad de éxito de éstos.

-Es vital la correcta elección por parte de la plataforma, de un prestador de servicios de Internet (*Internet Service Provider* o ISP) que cuente con un nivel de seguridad alto.

En este sentido, se recomienda que el ISP garantice en todo momento, al menos, los siguientes aspectos:

-Los servicios prestados por los ISP a este tipo de plataformas se centrarán en servidores seguros, centros de respaldo, accesos seguros, etc.

-En los servidores y en la propia aplicación se deben utilizar herramientas destinadas a detectar, evitar y bloquear códigos maliciosos. En este sentido, se recomienda el fomento de acuerdos estratégicos con empresas de seguridad.

-Emplear aplicaciones de seguridad encaminadas a garantizar, o en su caso minimizar, la posibilidad de recepción de mensajes comerciales no deseados a través de la plataforma (spam/scam).

-A su vez deben informar sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan

resultar nocivos para la juventud y la infancia.

5.-¿CÓMO AFECTAN LAS REDES SOCIALES A LA SEGURIDAD DE LOS MENORES?

Para empezar, conviene señalar que las Redes Sociales no son las culpables, como se tiende a apuntar, no en último extremo. Se trata simplemente de una evolución de Internet donde confluyen una serie de servicios que ya venían existiendo, como la mensajería instantánea y la edición de blogs (con Messenger y Fotolog a la cabeza). Cierto es que hay otras opciones nuevas de alto valor añadido y potencia, pero en esencia estamos hablando de datos personales, de contacto con otras personas y de edición de contenidos. Nada nuevo antes de las Redes Sociales. Internet no es sino una gran Red Social y éstas subconjuntos a medida de la misma.

Lo que sí es cierto es que, por su finalidad, estas plataformas invitan a la participación activa, esto es, a conocer otras personas (formando la Red), a "subir" contenidos (cada vez más audiovisuales) tanto propios como ajenos, que además van trazando los perfiles e intereses de cada cual. Y en demasiadas ocasiones priorizan "su negocio" frente al de sus usuarios, en especial, de los menores, buscando tener más datos para vender y cruzar, intensificando al extremo las opciones de "conectarse con otra persona" incluso de forma transparente para el usuario, imponiendo condiciones de uso abusivas, potenciando indiscriminadamente las afiliaciones automáticas para ganar impactos publicitarios por volumen de usuarios. Y en este punto habría que sacar a colación el "interés superior del menor" promovido por la Convención de los Derechos del Niño y la responsabilidad legislativa de las instituciones, junto con términos como Responsabilidad Social Corporativa que las entidades, con legítimo ánimo de lucro, sería deseable observaran… Pero establecer los límites es un largo debate y volveríamos a usar la controvertida palabra 'autorregulación'.

Podemos decir que sí han intensificado las probabilidades de riesgo a tenor de las características que les son comunes a la mayoría:

Pérdida del criterio de referencia. Promueven más las relaciones entre personas a través de otras personas, por lo que se pierde el control directo de la referencia y el criterio de

selección o confianza usado se diluye según los nodos se distancian. Ampliar relaciones es en sí positivo, pero el efecto negativo es más probable cuando no se ha podido usar el propio criterio de filtrado, sino uno inducido, digamos “transitivo”. Ejemplo: por cortesía o costumbre abro mi Red a cualquier amigo de un amigo que me lo pide… y resulta que me tengo que remontar tres niveles para ver cómo entró en mi red, y con ello, el criterio de filtrado se ha desvirtuado varias veces.

Exceso de operatividad sin intervención directa y consciente del usuario. Disponen de demasiadas funciones automáticas que el usuario novato desconoce. Ayudan a crecer a la Red, y en teoría a la función relacional de la misma buscada por los propios usuarios, pero también a potenciar la propia plataforma. Ejemplo: me doy de alta en la Red X y salvo que preste atención para impedirlo (si es que conozco que lo hace) serán invitados de manera automática a unirse a mi red (lo hagan o no ya saben, cuando menos, que yo me he dado de alta) todas las personas que tenía anotadas en mi servicio de webmail (tipo hotmail, gmail…) si es que las compañías respectivas llegaron a ese acuerdo al que yo les autoricé, seguro, aceptando sus condiciones generales que no llegué a leer.

Funciones demasiado potentes y de efectos desconocidos a priori. Existen posibilidades en exceso avanzadas para compartir todo tipo de cosas. Estas ‘gracias’ que el programa nos prepara pueden ser un grave problema, sobre todo para quien desconoce su funcionamiento. Ejemplo: si te etiquetan en una fotografía (cosa que tú desconocías que se pudiera hacer) y tienes el perfil más o menos abierto, es como si la pusieras tú mismo a la vista de mucha gente. Significa esto que alguien ha decidido por ti qué hacer público y, además, compartirlo, porque sale o no, contigo, en esa fotografía.

Concentran el universo de relaciones de manera intensiva. De sobra es conocida la escasa perspectiva que tienen los menores de la repercusión y alcance de lo que publican (lo dice quien ha hablado con muchos cientos). Cualquier cosa en la Red puede tener un eco brutal. Si eso afecta directamente a ‘mi red’, el efecto puede ser demoledor, como el de un veneno concentrado, selectivo. Ejemplo: una calumnia en una página web puede tener más o menos eco, pero si se vierte en el contexto de tu Red, el efecto es mucho más rápido y doloroso, aunque no lo pueda ver tanta gente.

Guardan, explícitamente o no, información muy precisa. Basan las relaciones en el perfil, intereses y actividad de los usuarios por lo que les requieren muchos datos y les registran sus acciones dentro de la propia Red. El usuario es víctima de un rastreo intensivo (atención, como lo es en los videojuegos y otras muchas actividades online que requieren identificación previa) que adecuadamente tratado puede crear una información de mucho más valor que la explicitada. Ejemplo: desde que entro en la Red pueden quedar registrados mis movimientos e intereses de todo tipo más allá de la información del perfil que de forma voluntaria proporcioné (dónde pincho, con quién hablo, cuánto tiempo dedico…).

Presentan al usuario las opciones de manera demasiado interesada, lo que suele implicar pérdida de privacidad. Tras una supuesta intención de ayudar y agilizar, suele ser política común de las plataformas de Redes Sociales ayudarse a sí mismas. Así, pondrán muy poco énfasis en que el usuario configure las opciones de privacidad de los datos y, sin embargo, insistirán en que completemos los perfiles con todo tipo de cuestiones. Ejemplo: al darme de alta me preguntan datos de lo más variado sin los que no me dejarían registrarme, tras lo cual podré empezar a utilizar la Red sin haber configurado de forma explícita con quién y qué tipo de datos personales o de actividad quiero compartir.

Estos son los principales factores diferenciales en materia de uso seguro de Internet producidos por la irrupción de las Redes Sociales. No he querido abordar temas genéricos como el control de las edades, las medidas de seguridad, la supervisión de los datos y las comunicaciones… que, como digo, ya eran cosa de la Internet anterior a las Redes Sociales, donde ya se prodigaban efectos en forma de ciberbullying y grooming.

6.-RIESGOS PARA LOS MENORES EN LAS REDES SOCIALES

Al hablar de riesgos, hay ciertos parámetros que se deben considerar para su graduación:

- La gravedad y la naturaleza de sus consecuencias.
- La probabilidad de que se produzcan.
- La posibilidad de implementar las medidas preventivas
- Las opciones de paliar o evitar sus consecuencias, una vez afectados.
- La facultad de intervención de los adultos en las diferentes fases: prevención, supervisión y asistencia.

Parece obvio que los riesgos más graves son aquellos que afectan a la integridad, tanto física como emocional, de los menores, en especial el ciberbullying y el grooming. No es fácil evitarlos, no son infrecuentes y, por último, los adultos son los últimos en enterarse, normalmente, cuando el daño ha sido ya muy grande.

Se debe tener bien presente que, aunque no se produzca agresión física por parte de los acosadores (ciberabusones y depredadores sexuales), los efectos sobre la víctima pueden ser tan devastadores como si la hubiera habido. Las políticas europeas por una Red más segura así lo constatan poniendo estos fenómenos en su punto de mira.

Por otro lado, constituyen un claro ejemplo de cómo hay problemas transversales, independientes del canal tecnológico, que se pueden iniciar o desarrollar tanto en Internet como a través del teléfono móvil y los videojuegos online.

6.1-Ciberbullying:

¿Qué es el Ciberbullying?

Se trata del acoso sicológico realizado entre menores en ese que constituye su nuevo y relevante entorno de socialización: el ciberespacio. Adquiere las más diversas manifestaciones alentadas por las incesantes novedades tecnológicas y la ilimitada imaginación de los menores. No hace falta ser más fuerte, ni dar la cara, ni coincidir con la víctima, ni conocerle. Además, no presenciar el sufrimiento puede contribuir a infligirlo en mayores dosis.

¿Qué no es el ciberullying?

Por tanto tiene que haber menores en ambos extremos del ataque para que se considere ciberbullying: si hay algún adulto, entonces estamos ante algún otro tipo de ciberacoso.
Tampoco se trata de **adultos que engatusan a menores** para encontrarse con ellos fuera de la Red o explotar sus imágenes sexuales. Aunque hay veces en que un/a menor comienza una campaña de ciberbullying que puede acabar implicando a adultos con intenciones sexuales.

¿Cuándo estamos ante un caso de ciberbullying?

Estamos ante un caso de ciberbullying cuando un o una menor atormenta, amenaza, hostiga, humilla o molesta a otro/a mediante Internet, teléfonos móviles, consolas de juegos u otras tecnologías telemáticas.

Según el Estudio sobre hábitos seguros en el uso de las TIC por los menores publicado por el INTECO en Marzo de 2009 el ciberbullying se define como acoso entre iguales en el entorno TIC, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños.

¿Qué tiene que ver el ciberbullying con el bullying o acoso escolar?

No son tan similares como podría pensarse. En ambos se da un abuso entre iguales pero poco más tienen que ver en la mayoría de los casos. El **ciberbullying** atiende a otras

causas, se manifiesta de formas muy diversas y sus estrategias de abordamiento y consecuencias también difieren.

Sí es bastante posible que el bullying sea seguido de **ciberbullying**. También es posible que el **ciberbullying** pueda acabar también en una situación de bullying, pero desde luego esto último sí que es poco probable.

¿Por qué es especialmente grave el ciberbullying?

El anonimato, la no percepción directa e inmediata del daño causado y la adopción de roles imaginarios en la Red convierten al ciberbullying en un grave problema.

¿Cómo se manifiesta el ciberbullying?

El *ciberbullying* se caracteriza por los siguientes aspectos:

1. Que la situación de acoso se dilate en el tiempo. Quedan excluidas las acciones puntuales. Sin restar importancia a estos sucesos, que pueden tener serios efectos para el afectado y constituir un grave delito, un hecho aislado no sería ciberacoso.

2. Que la situación de acoso no cuente con elementos de índole sexual. En caso de que la situación de acoso cuente con elementos y connotaciones de carácter sexual, la situación se considera *grooming*.

3. Que víctimas y acosadores sean de edades similares.

4. Que víctimas y acosadores tengan relación o contacto en el mundo físico. Es necesario que ambas partes tengan algún tipo de relación previa al inicio del acoso electrónico. Con frecuencia, la situación de acoso comienza en el mundo real, siendo el medio electrónico una segunda fase de la situación de acoso.

5. Que el medio utilizado para llevar a cabo el acoso sea tecnológico. En este sentido, puede tratarse de Internet y cualquiera de los servicios asociados a ésta; telefónica móvil, redes sociales, plataformas de difusión de contenidos, etc.

Las formas que adopta son muy variadas y sólo se encuentran limitadas por la pericia tecnológica y la imaginación de los menores acosadores, lo cual es poco esperanzador.

Algunos **ejemplos** concretos podrían ser los siguientes:

-Colgar en Internet una imagen comprometida (real o efectuada mediante fotomontajes) datos delicados, cosas que pueden perjudicar o avergonzar a la víctima y darlo a conocer en su entorno de relaciones.

-Dar de alta, con foto incluida, a la víctima en un web donde se trata de votar a la persona más fea, a la menos inteligente… y cargarle de puntos o votos para que aparezca en los primeros lugares.

-Crear un perfil o espacio falso en nombre de la víctima, en redes sociales o foros, donde se escriban a modo de confesiones en primera persona determinados acontecimientos personales, demandas explícitas de contactos sexuales…

-Dejar comentarios ofensivos en foros o participar agresivamente en chats haciéndose pasar por la víctima de manera que las reacciones vayan posteriormente dirigidas a quien ha sufrido la usurpación de personalidad.

-Dando de alta la dirección de correo electrónico en determinados sitios para que luego sea víctima de spam, de contactos con desconocidos…

-Usurpar su clave de correo electrónico para, además de cambiarla de forma que su legítimo propietario no lo pueda consultar, leer los mensajes que a su buzón le llegan violando su intimidad.

-Provocar a la víctima en servicios web que cuentan con una persona responsable de vigilar o moderar lo que allí pasa (chats, juegos online, comunidades virtuales…) para conseguir una reacción violenta que, una vez denunciada o evidenciada, le suponga la exclusión de quien realmente venía siendo la víctima.

-Hacer circular rumores en los cuales a la víctima se le suponga un comportamiento reprochable, ofensivo o desleal, de forma que sean otros quienes, sin poner en duda lo que leen, ejerzan sus propias formas de represalia o acoso.

-Enviar menajes amenazantes por e-mail o SMS, perseguir y acechar a la víctima en los lugares de Internet en los se relaciona de manera habitual provocándole una sensación de completo agobio.

Análisis jurídico del acoso a menores a través de medios electrónicos

El *ciberbullying* puede plasmarse en diferentes tipos de actuaciones, cuya trascendencia, desde el punto de vista jurídico, varía en gran medida dependiendo de cuál se trate, pudiendo lllegar un mismo acto a ser constitutivo de varios delitos al mismo tiempo.
Así, el *ciberbullying* puede ser constitutivo de un delito de:

1. Amenazas:

Se encuentran reguladas en los artículos 169 a 171 del Código Penal, donde se dispone que la comisión de este tipo de delitos requiere del cumplimiento de los siguientes elementos:

-Que exista una amenaza.
-Que la amenaza consista en causar un mal (sea delito o no).
-Que exista una condición para no causar dicho mal.

En la mayor parte de los casos, las amenazas constituyen la situación de acoso vivida por la víctima en la vida física (centros escolares, normalmente), encontrándose indefenso el menor ante el ataque reiterado por parte del acosador.

El mal con el que se amenaza a la víctima puede ser constitutivo de delito o no, pero debe destacarse cómo la amenaza más empleada en Internet se encuentra directamente relacionada con el honor y la intimidad del afectado, existiendo casos en los que el coaccionador intimida a su víctima con la publicación de imágenes o vídeos que pueden situarlo en una posición comprometida respecto a terceros.

Con frecuencia esta situación es ocultada por parte del menor afectado, a pesar de contar con la regulación y protección jurídica específica, por temor a las represalias que pudieran derivarse.

2. Coacciones:

Se encuentran reguladas en los artículos 172 y 173 del Código Penal, donde se dispone que la comisión de este delito requiere del cumplimiento de los siguientes elementos:

-Que se obligue a un tercero a hacer o dejar de hacer algo.
-Que dicha obligación se lleve a cabo mediando violencia.

Por tanto, es posible que durante el acoso se produzca un delito de coacción, siempre y cuando exista violencia.

En este sentido, el elemento *violencia* debe ser entendido en sentido amplio, comprendiendo tanto la violencia física como psíquica, y aplicada sobre las personas o sobre las cosas.

3. Injurias:

Aparecen reguladas en los artículos 206 a 210 del Código Penal, donde se dispone que la comisión de este tipo de delito requiere del cumplimiento de los siguientes elementos:

-Que exista una acción o expresión.
-Que se lesione la dignidad, fama o propia estimación.

La acción constitutiva de injuria es normalmente una expresión, consistente tanto en imputar hechos falsos, como en formular juicios de valor, que pueden realizarse verbalmente y por escrito, o de un modo simbólico por “caricaturas”, “emblemas”, etc.
No obstante, esta acción también puede ser entendida como un acto de omisión que conlleve una desatención, que a su vez implique una acción lesiva para la dignidad, fama o estimación propia de la persona.

En relación con la trascendencia que adquieren este tipo de conductas en el mundo online, deben tenerse en cuenta situaciones y conductas que ya existían previamente en el mundo físico y que causaban importantes daños a los afectados. No obstante, con la introducción del elemento electrónico y con el aumento de la difusión que conlleva el daño provocado a los usuarios afectados es más elevado que el que podría derivarse en el mundo físico.

4. Calumnia:

Se regula en el artículo 205 del Código Penal, donde se dispone que la comisión de este tipo de delito requiere del cumplimiento de los siguientes elementos:

-Que exista la imputación de un delito.
-Que la imputación sea falsa.
-Que la imputación del delito sea sobre un hecho concreto.
- Que la imputación se realice sobre una persona determinada o determinable.

Aunque suele ser menos frecuente entre los acosos realizados a través de medios online, es perfectamente posible que junto a las injurias, se asocie la imputación de delitos falsos que no se han cometido.

Los delitos expresados anteriormente conforman todo el abanico de actos que pueden ser resultado de las conductas de *ciberbullying*. Lo más habitual es que se centre en las primeras conductas. Además de estos tipos penales, se puede incluir el resarcimiento de los daños y perjuicios que cualquier afectado puede reclamar en vía civil o como responsabilidad derivada del delito.
Especial relevancia tiene desde el punto de vista electrónico el hecho de que la publicación de este tipo de contenidos de injurias, calumnias, amenazas y coacciones se encuentran en sitios web públicos y que pueden ser libremente indexados por los buscadores de Internet. Este hecho supone que la accesibilidad y visualización de estos contenidos aumenta exponencialmente, agravándose así el daño a los derechos de los usuarios.

Responsabilidad penal del menor por Ciberbuying.

Desde el punto de vista jurídico, la principal implicación a considerar, cuando los actos son realizados por menores, es la que hace referencia a la responsabilidad penal del menor.

En este sentido, es prioritario discernir cuándo un menor es considerado sujeto inimputable –no responsable de sus actos por no disponer del grado de madurez necesario- o cuándo se considera que dispone de una madurez suficiente, de forma que pueda ser juzgado.

A este respecto, la regulación penal aplica las siguientes normas en función de la edad del sujeto autor del delito:

- Ley Orgánica 10/1995, de 23 de noviembre, por la que se aprueba el Código Penal. Esta norma es de aplicación a sujetos mayores de edad y, excepcionalmente, a sujetos menores en edad comprendidos entre los dieciséis y dieciocho años.

- Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores (en adelante, LORPM). Esta norma señala en su art. 1 que *"se aplicará para exigir la responsabilidad de las personas mayores de catorce años y menores de dieciocho por la comisión de hechos tipificados como delitos o faltas en el Código Penal o las leyes penales especiales"*. Esta norma reduce la edad para que un sujeto sea considerado imputable y penalmente responsable.

En ambas normas también se establece que: *"al mayor de dieciocho años y menor de veintiuno que cometa un hecho delictivo, podrán aplicársele las disposiciones de la Ley que regule la responsabilidad penal del menor en los casos y con los requisitos que esta disponga**17**"*. La LORPM añade que ello se hará cuando los jueces así lo consideren, por tanto, a los denominados por la doctrina penalista como 'jóvenes adultos' se les puede aplicar la normativa de menores.

Como establece la Exposición de Motivos de la LORPM la respuesta de Derecho Penal de Menores ha de revestir doble dimensión :

• Carácter sancionador: medida judicial frente a la conculcación de una norma penal, lo que fomenta la adquisición de responsabilidad en el menor, sujeto de derechos y obligaciones.

• Carácter educativo: prima el superior interés del menor y la prevención especial de educación en el menor, frente a la intención retributiva y de prevención especial propia del derecho penal de adultos.

Así, por aplicación de esta norma, algunas conductas puede que no lleguen a ser castigadas pese a estar tipificadas en el Código Penal por considerarse contraproducente para los menores, o en su caso, por ser realizadas por sujetos menores de 14 años, considerándose estos sujetos inimputables a los efectos de responsabilidad criminal.

6.2-Grooming

Se conoce así a la estrategia de empatía y engatusamiento que utilizan depredadores sexuales para ganarse la confianza del menor y acabar, mediante chantaje emocional o de otro tipo, obteniendo gratificaciones de índole sexual que pueden ir desde el envío de imágenes o vídeos a propuestas de encuentros en persona.

En el lenguaje de seguridad_informática, se conoce como grooming a cualquier acción que tenga por objetivo minar y socavar moral y psicológicamente a una persona, a fin de conseguir su control a nivel emocional. Si bien esta actividad puede producirse en cualquier instancia, es particularmente grave en los casos en los que una persona lleva a cabo este tipo de coacciones y presiones emocionales en contra de un menor, con el objeto de obtener algún tipo de favor sexual.

Este tipo de chantajes suelen producirse habitualmente a través de servicios de chat y mensajería instantánea, y deben ser denunciados de forma inmediata.

Aunque no se tienen datos concretos, son abundantes los casos que se van conociendo públicamente y muchos más aún los que permanecen ocultos bien en el entorno familiar o bien que ni siquiera llegan al conocimiento de los padres. La lucha es muy desigual. Se

trata de un adulto especializado en la caza de menores contra un niño o adolescente que, de pronto, se encuentra inmerso en una situación que no puede controlar ni compartir.

Principales conductas que pueden ser englobadas dentro del acoso a menores a través de medios electrónicos:

El *grooming* se pueden diferenciar varios elementos o fases del acoso:

1. Inicio de la fase de amistad. Hace referencia a la toma de contacto con el menor de edad para conocer sus gustos, preferencias y crear una relación de amistad con el objeto de alcanzar la confianza del posible afectado.

2. Inicio de la fase de relación. La fase de formación de la relación incluye con frecuencia confesiones personales e íntimas entre el menor y el acosador. De esta forma, se consolida la confianza obtenida del menor y se profundiza en información sobre su vida, gustos y costumbres.

3. Componente sexual. Con frecuencia incluye la descripción de términos específicamente sexuales y la petición a los menores de su participación en actos de naturaleza sexual, grabación de imágenes o toma de fotografías.

Si bien el *ciberbullying* es una amenaza clara que puede desembocar en situaciones que pongan en riesgo los aspectos de naturaleza psíquica y física del menor, el *grooming* es, en principio, una modalidad de acoso que conlleva situaciones de peligro más latentes para los menores de edad, ya que como se señalaba anteriormente, mientras que el rasgo característico del *ciberbullying* es la existencia de un acoso entre iguales, en el *grooming* el acosador es un adulto y existe una intención sexual explícita o implícita.
En este sentido, las Administraciones Públicas y diferentes organizaciones y entidades sin ánimo de lucro han puesto en marcha campañas online**8** para informar a menores y adultos sobre los posibles riesgos de la Red, las características para su detección y los medios disponibles para poner fin al acoso.

Análisis jurídico del acoso a menores a través de medios electrónicos

El *grooming* puede ser considerado como un delito englobado dentro del denominado exhibicionismo, difusión y corrupción de menores, regulado expresamente en los artículos 185, 186 y 189 del Código Penal, donde se dispone que la comisión de este tipo de delito requiere del cumplimiento de los siguientes elementos:

1. Para el delito de **exhibicionismo**, se establece como necesarios los siguientes requisitos:
-Exhibición obscena y de carácter sexual.
-Ante menores o incapaces.

2. Por lo que respecta a la **difusión de contenidos pornográficos**, para que ésta se produzca, deben acontecer las siguientes circunstancias:

-Que se venda o difunda a través de un medio directo. o Que los destinatarios sean menores o incapaces. o Que sean materiales idóneos para producir daños psicológicos.
Por último, la **corrupción de menores** es un tipo penal complejo, en el que se recoge un gran número de actuaciones dentro del ámbito sexual.

Así, se tipifican conductas delictivas específicas en relación con menores e incapaces, como son el favorecimiento de la prostitución y la utilización de los menores o incapaces con fines o en espectáculos exhibicionistas o pornográficos, entendiéndose que este tipo de actos pueden venir directamente derivados de actos llevados a cabo a través de medios electrónicos.

Como regla general para las tres conductas, se debe considerar que en ningún momento se establece la necesidad de que la exhibición sea llevada a cabo de forma presencial, sino que basta con que el menor o incapaz visione este tipo de exhibiciones para que sea constitutivo de delito.

Así, la mera exhibición a través de una cámara web o de un chat privado de imágenes o conversaciones de índole sexual o pornográficas son constitutivas de este tipo de delitos, en la medida en que objetivamente puedan afectar a la indemnidad del menor o incapaz.

6.3-Sexting

Es una práctica que supone el envío de imágenes o vídeos de contenido erótico-pornográfico por parte de menores o jóvenes, principalmente, por medio del teléfono móvil (Sexting = Sex + Texting).

En sí mismo, incluso en un contexto de privacidad adecuado, puede suponer problemas ligados a la pornografía infantil. Otro incidente se produce cuando esas imágenes salen del ámbito privado, haciéndose públicas, suponiendo el menoscabo de la intimidad y el honor de la persona y, en muchos casos, el comienzo de despiadadas campañas de ciberbullying. Es una práctica emergente porque los adolescentes lo relacionan con ligue y diversión, dos razones de mucho peso que contrarrestar a esas edades.

La práctica del sexting implica diversos riesgos de carácter psicológico, legal e incluso de la integridad física de los participantes. Muchos de sus practicantes son menores de edad y no son conscientes de ellos: es el deber de los padres y educadores advertirlos.

Riesgo de exposición a pederastas y otros acosadores o chantajistas.

Un/a menor que se fotografía en actitudes sexuales puede sugerir una precocidad sexual a ciertas personas a las cuales les llegue la fotografía o vídeo, y provocar el deseo de un encuentro lo que implica un posible abuso o corrupción del/a menor o exponerles a un chantaje de tipo sexual relacionado con el denominado *grooming*.

Los menores y también los adultos que practican sexting corren el riesgo de que dichas imágenes acaben siendo usadas para una sextorsión por parte de sus destinatarios o de terceras personas que se hagan con las mismas por diversos métodos (acceso ilegal al ordenador, al teléfono móvil por Bluetooth, etc.).

Responsabilidad penal.

La imagen de una persona está protegida por la Constitución y por leyes como la Ley de Protección de Datos o el Código Penal. Además, ciertas imágenes producidas o

trasmitidas por menores podrían ser consideradas *pornografía infantil* y derivar consecuencias penales. En los Estados Unidos ya ha habido sentencias que condenan a menores por esta cuestión o por otras vinculadas, como explotación de menores, ya que la cuestión de agrava cuando se graban y difunden imágenes de otros menores. Recomendamos ampliar información en e-Legales, nuestro web de referencia sobre las implicaciones legales de las actividades online de los menores y en los casos legales relacionados con el sexting que incluimos en este mismo web.

Riesgos psicológicos.

Una persona cuya imagen o vídeo erótico es distribuido sin control puede verse humillada públicamente y acosada (ciberbullying si es entre menores), y sufrir graves trastornos a causa de ello. Ya se ha producido al menos un caso de suicidio originado en el sexting y muchos casos de ansiedad, depresión, pérdida de autoestima, trauma, etc. Algunos expertos sostienen que el *riesgo social* es mayor en localidades pequeñas. Hay incluso quien advierte de los riesgos a nivel neurológico por la simple práctica del sexting. Las repercusiones psicológicas pueden verse agravadas si existe sextorsión a partir de las fotos o vídeos de sexting.

Además desde 2009 están proliferando las webs dedicadas a recopilar y explotar comercialmente las fotos y los vídeos creados mediante sexting (en la miniatura puede verse una captura de uno de estos webs).

Cualquier imagen sexual que salga de tu teléfono, de tu webcam o de tu email, puede acabar en uno de estos webs y proporcionarle beneficios económicos a terceros y alimentar las fantasías eróticas de miles de internautas.

Si la foto es de un/a menor, estaríamos hablando de webs que podrían ser considerados de pornografía infantil según la legislación de numerosos países (la policía del Estado norteamericano de Utah afirma que el 25% de las imágenes de pornografía infantil que detectan, son originadas mediante sexting). En casi todos los casos, aunque las fotos sean de adultos, suelen vulnerar la privacidad ya que no cuentan con permiso de las personas fotografiadas para su difusión y por tanto son webs ilegales.

Desde los primeros tiempos del porno en Internet son numerosos también loswebs dedicados a recopilar fotos de ex-novias o ex-esposas, habitualmente desnudas, sólo en ocasiones distorsionadas para no reconocer su rostro, y que sus ex-parejas envían generalmente por despecho o venganza.

Aunque estas fotos al comienzo no tenían su origen en el sexting sino en fotos realizadas y compartidas privadamente por parejas, con la extensión de las capacidades multimedia de los dispositivos móviles, ambos modos de generar imágenes eróticas (autorrealizadas y enviadas, o directamente obtenidas por la pareja) están ya muy mezclados y en los webs porno dedicados a las ex-novias son cada vez más comunes las fotos generadas mediante sexting.

Recomendaciones dirigidas a los menores:

1. Se recomienda a todos los usuarios recurrir al uso de seudónimos o *nicks* personales con los que operar a través de Internet, permitiéndoles disponer de una auténtica **identidad digital** que no ponga en entredicho la seguridad de su vida personal y profesional. De esta forma, únicamente será conocido por su círculo de contactos que saben el *nick* que emplea en Internet.

2. Ser cuidadoso con los datos personales que se publican. Es recomendable no publicar demasiados datos personales en Internet: redes sociales, plataformas, blogs o foros. Estos datos podrían ser utilizados contra el menor o su entorno.
Es recomendable no publicar más datos de los necesarios y, en caso de datos como el correo electrónico o teléfono móvil, hacerlo de la forma más privada posible.

3. Se recomienda a los usuarios tener especial cuidado a la hora de publicar contenidos audiovisuales y gráficos, dado que en este caso pueden estar poniendo en riesgo la privacidad e intimidad de personas de su entorno.
Siempre que se vayan a alojar contenidos de este tipo o información relativa a terceros,

se recomienda notificar previamente a ese tercero para que lo autorice o, en su caso, filtre los contenidos que desea publicar y los que no.

4. No aceptar ni agregar como contacto a desconocidos. Es recomendable que el menor se asegure de si la persona que va a agregar es realmente un conocido. Para asegurarse, en caso de que el nombre de usuario no sea reconocible, puede preguntar a sus contactos si es conocido por ellos (amigos comunes, compañeros de colegio, campamento, vacaciones, etc.). En caso de detectar discrepancias entre el perfil declarado y el real, o si se identifica alguna conducta malintencionada, la mejor opción es bloquear el contacto de forma inmediata. En función de la gravedad de la situación, es recomendable ponerlo en conocimiento de la plataforma y de las autoridades competentes, si se considera necesario.

En estos casos, siempre conviene que lo comunique a sus amigos para que estén prevenidos ante ese contacto.

5. Evitar el envío de imágenes o vídeos a usuarios en los que no se confía.
En caso de que un contacto desconocido intente involucrarse de forma muy temprana en nuestra vida social y al poco tiempo solicita que se le envíe una foto o encender nuestra cámara web, es mejor dudar y, en un momento posterior disculparse, que ser afectado de alguna de las conductas mencionadas en otros puntos de la guía.

6. Comunicarlo a los padres o tutores. En el momento en que se detecte una situación de riesgo, o en la que un tercero comience a solicitar temas relacionados con aspectos sexuales, se debe comunicar inmediatamente a los padres o tutores legales.

Recomendaciones dirigidas a padres y tutores legales:

1. Involucrarse en el uso que los menores hacen de Internet. La brecha digital existente entre adultos y niños puede hacer que los padres se mantengan alejados de la realidad virtual en la que viven los menores y adolescentes, para los cuales el uso de las herramientas de la web 2.0 es parte de su vida cotidiana. Esto provoca que, en ocasiones,

los padres no consigan comprender las consecuencias que un mal manejo de la tecnología puede tener para sus hijos.

2. Instalar los ordenadores en zonas comunes. Es importante que el ordenador se encuentre en algún sitio común de la casa, permitiendo de esta forma que los padres puedan conocer, en cierto modo, el uso que los menores hacen de la web: utilización de servicios, acceso a determinados contenidos, frecuencia de conexión, duración de las sesiones, etc; sin que esto implique una intromisión en la intimidad del menor.

3. Establecer un horario al uso de Internet y del ordenador. Los menores y adolescentes pasan horas frente al ordenador: una media de 14,5 horas a la semana, según el *Estudio sobre hábitos de seguridad en el uso de las TIC por niños y adolescentes y e-confianza de sus padres* del Observatorio de la Seguridad de la Información de INTECO Las nuevas tecnologías han cambiado la forma de comunicación entre jóvenes: las redes sociales y plataformas colaborativas son puntos de encuentro públicos y masivos. Los niños se aproximan a Internet de un modo natural. No lo hacen necesariamente con una finalidad, simplemente "están" en Internet, "viven" allí, y lo utilizan para estudiar, charlar o escuchar música. I

Internet constituye una herramienta básica de relación social y de identidad y, como tal, la presencia de los niños en Internet es una realidad básica e inexorable, y el aprovechamiento que hacen del mismo apoya esta certeza. Asumiendo este aspecto como una realidad, es necesario no obstante determinar unas pautas de utilización claras sobre duración o momento de la conexión, servicios utilizados, etc.

4. Impulsar el uso responsable de la cámara web. Este servicio es una herramienta de comunicación muy utilizada por los usuarios de Internet. Un uso inadecuado puede posibilitar una puerta de entrada para usuarios malintencionados.

Conviene establecer un control por padres y tutores que garantice información acerca de con qué usuarios y en que ámbitos se comunican los menores.

5. Uso de imágenes. Para los menores y adolescentes, las fotografías e imágenes constituyen la principal vía de presentación ante los demás.

En ese sentido, es fundamental plantearles que no deben enviar fotos ni vídeos

personales a ningún desconocido, ya que éste le puede dar un mal uso en la Red.

6. Supervisión. Basta con mantener un control sobre el ordenador o las cuentas de los menores y ver el historial de búsquedas y del navegador. No se trata de que se sientan controlados y coartados: este control debe ser realizado de la forma menos intrusiva posible en su intimidad.

7. Comunicación. Establecer un diálogo permanente con los menores y adolescentes es tarea fundamental de los padres y tutores. La comunicación debe abordar tanto los aspectos positivos del uso de la tecnología como los posibles riesgos que Internet puede implicar. Sólo con un conocimiento riguroso de las situaciones que pueden tener lugar en Internet es posible estar preparado para responder a ellas.

8. Autoprotección. Es necesario plantear a los menores y adolescentes la necesidad de ser cuidadosos con los datos que facilitan en Internet, publican en las redes sociales o proporcionan a través de los servicios de mensajería instantánea. Los niños deben comportarse con responsabilidad, respeto y sentido común en la Red, igual que lo hacen en el mundo físico.

En el caso de ser consciente de la **existencia de alguna de estas conductas,** es recomendable adoptar las siguientes medidas:

• No destruir las evidencias del acoso en cualquiera de sus modalidades (mensajes de texto, correo electrónico, contenidos multimedia, etc.).

• Tratar de identificar al acosador (averiguar su dirección IP, recurrir a especialistas en informática y a las Fuerzas y Cuerpos de Seguridad del Estado).

• Contactar con la compañía del medio empleado para cometer el acoso (compañía de teléfono, propietario del dominio o sitio web, etc.).

• Denunciar el acoso a las Fuerzas y Cuerpos de Seguridad del Estado que disponen de unidades de delitos informáticos (Policía Nacional, Guardia Civil y Policías Autonómicas).

• En caso de *ciberbullying*, si éste procede del entorno escolar, habrá que tomar tres medidas adicionales:

-Informar a la escuela, director y al orientador del centro, para recibir el apoyo necesario.

-Contactar con los padres del agresor.

-Recurrir a organizaciones especializadas en acoso escolar.

7.-PROTECCIÓN JURÍDICA DE LOS MENORES EN LAS REDES SOCIALES

Según el Informe de abril de 2007, Teens, Social Networks & Safety de Pew Internet and American life Project32, el 93% de los norteamericanos de entre 12 y 17 años utilizan Internet, de los cuales un 55% utiliza las redes sociales.

Por otro lado, es esencial destacar que el 77% de los menores que utilizan redes sociales tienen visible su perfil público, de los cuales un 59% afirma que sólo pueden ver su perfil sus amigos.
Una cifra preocupante, si se tiene en cuenta que se han detectado en los últimos tiempos redes de pedofília que emplean las redes sociales como plataformas para contactar con menores de edad.

De conformidad con lo dispuesto en el artículo 12 de la Constitución Española, la mayoría de edad se establece a partir de los 18 años.

De igual forma, el artículo 39 establece que *"los niños gozarán de la protección prevista en los acuerdos internacionales que velan por sus derechos",* lo que se refleja en la incorporación al ordenamiento jurídico español de la Convención del 20 de noviembre de 1989 sobre los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas.

Por su parte, la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, que modifica parcialmente el Código Civil y la Ley de Enjuiciamiento Civil, establece que los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones.

A su vez, 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, honor, propia imagen, 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, tales como la retirada o bloqueo inmediato de los contenidos, solicitando inmediatamente las indemnizaciones que correspondan por los perjuicios causados.

Por otro lado, los menores gozan del derecho a la libertad de expresión en los términos constitucionalmente previstos extendiéndose este derecho a los casos de publicación y difusión de sus opiniones, entre otros casos. Esta libertad de expresión tiene también su límite en la protección de la intimidad y la propia imagen del menor.

Los menores tienen derecho a recibir de las Administraciones Públicas la asistencia adecuada que permita el efectivo ejercicio de sus derechos y que garantice su respeto. Así, para la defensa y garantía de sus derechos, el menor tiene la posibilidad de:

• Solicitar la protección y tutela ante el Defensor del Menor, la Fiscalía de Menores y la Consejería de Asuntos Sociales, así como de los Cuerpos y Fuerzas de Seguridad del Estado en los casos en los que sea necesario.

• Poner en conocimiento del Ministerio Fiscal las situaciones que considere que atentan contra sus derechos, con el fin de que éste promueva las acciones oportunas.
• Plantear sus quejas ante el Defensor del Pueblo. A tal fin, uno de los Adjuntos de dicha institución se hará cargo de modo permanente de los asuntos relacionados con los menores.

• Solicitar los recursos sociales disponibles de las Administraciones Públicas.

A su vez, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, establece en el artículo 22.3 que, en el orden civil, los juzgados y tribunales españoles serán competentes en materia de incapacitación y de medidas de protección de la persona o de los bienes de los menores o incapacitados, cuando éstos tuviesen su residencia habitual en España.
Otra manera de proteger al menor en las redes sociales es a través de un correcto manejo de sus datos personales. Según la Agencia Española de Protección de Datos, los mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismos, el tratamiento automatizado de sus datos de carácter personal.

Al respecto, el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, es claro al establecer en su artículo 13 que se podrá proceder 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.

Es importante anotar que, 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.

El Reglamento también establece que, 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.

El análisis de varias redes sociales, muestra que, si bien para acceder a las mismas hay que indicar la edad y el contenido de la casilla de seguridad, algunas no establecen ninguna otra medida para verificar la edad.

Este hecho conlleva una primera barrera para la efectividad de las medidas de control, ya que en las redes sociales que no tienen como público objetivo a usuarios mayores de edad, se han fijados límites de edad más bajos, como por ejemplo los 13 años en el caso Facebook ó 14 años en el caso de Wamba33. La mayoría tiene la posibilidad de configurar sus opciones de privacidad, pudiendo elegir qué datos aparecen y el tipo de usuarios para los que estarán disponibles.

En todo caso, y como puede imaginarse, la problemática que se deriva de la posibilidad de uso de estas plataformas por cualquier usuario, sea éste mayor o menor de edad, y de la posibilidad de falsear respecto de la edad, genera una expectativa bastante razonable de peligro en lo referido al tratamiento de los datos de carácter personal tanto propios del

menor como de sus familiares y allegados.

8.-FACEBOOK

8.1-Declaración de derechos y responsabilidades (Terminos de uso)

Esta Declaración de derechos y responsabilidades ("Declaración") tiene su origen en los Principios de Facebook y rige nuestra relación con los usuarios y con todos aquellos que interactúan con Facebook. Al utilizar o acceder a Facebook, muestras tu conformidad con la presente Declaración.

1. **Privacidad**

   Tu privacidad es muy importante para nosotros. Hemos diseñado nuestra Política de privacidad para ayudarte a comprender cómo puedes usar Facebook para compartir información con otras personas y cómo recopilamos y usamos tu información. Te animamos a que leas nuestra Política de privacidad y a que la utilices para poder tomar decisiones fundamentadas.

2. **Compartir el contenido y la información**

   Eres el propietario de todo el contenido y la información que publicas en Facebook, y puedes controlar cómo se comparte a través de la configuración de privacidad yaplicaciones. Además:

   1. Para el contenido protegido por derechos de propiedad intelectual, como fotografías y vídeos (en adelante, "contenido de PI"), nos concedes específicamente el siguiente permiso, de acuerdo con la configuración de privacidady aplicación: nos concedes una licencia no exclusiva, transferible, con posibilidad de ser sub-otorgada, sin royalties, aplicable globalmente, para utilizar cualquier contenido de PI que publiques en Facebook o en conexión con Facebook (en adelante, "licencia de PI"). Esta licencia de PI finaliza cuando eliminas tu contenido de PI o tu cuenta (a menos que el contenido se ha compartido con terceros y éstos no lo han eliminado).

   2. Cuando eliminas contenido de PI, éste es borrado de forma similar a cuando vacías la papelera o papelera de reciclaje de tu equipo informático. No obstante, entiendes que es posible que el contenido eliminado permanezca

en copias de seguridad durante un plazo de tiempo razonable (si bien no estará disponible para terceros).

3. Cuando usas una aplicación, tu contenido e información se comparte con ella. Exigimos que las aplicaciones respeten tu privacidad y tu acuerdo con esa aplicación controlará el modo en que la aplicación puede usar, almacenar y transferir dicho contenido e información. (Para obtener más información sobre la plataforma, lee nuestra Política de privacidad y la página Acerca de la plataforma.)

4. Cuando publicas contenido o información con la configuración "Todos", significa que permites que todos, incluidas las personas que son ajenas a Facebook, accedan y usen dicha información y la asocien a ti (es decir, tu nombre y foto del perfil).

5. Siempre valoramos tus comentarios o sugerencias acerca de Facebook, pero debes entender que podríamos utilizarlos sin obligación de compensarte por ello (del mismo modo que tú no tienes obligación de ofrecerlos).

3. Seguridad

Hacemos todo lo posible para hacer que Facebook sea un sitio seguro, pero no podemos garantizarlo. Necesitamos tu ayuda para lograrlo, lo que implica los siguientes compromisos:

1. No enviarás ni publicarás de ningún otro modo comunicaciones comerciales no autorizadas (como correo no deseado) en Facebook.
2. No recopilarás contenido o información de otros usuarios, ni accederás de otro modo a Facebook, utilizando medios automáticos (como harvesting bots, robots, arañas o scrapers) sin nuestro permiso.
3. No participarás en marketing multinivel ilegal, como el de tipo piramidal, en Facebook.
4. No cargarás virus ni código malintencionado de ningún tipo.
5. No solicitarás información de inicio de sesión ni accederás a una cuenta perteneciente a otro usuario.

6. No molestarás, intimidarás ni acosarás a ningún usuario.
7. No publicarás contenido que resulte hiriente, intimidatorio o pornográfico, que incite a la violencia o que contenga desnudos o violencia gráfica o injustificada.
8. No desarrollarás ni harás uso de aplicaciones de terceros que contengan, publiciten o promocionen de cualquier otro modo contenido relacionado con el consumo de alcohol o de naturaleza adulta (incluidos los anuncios) sin las restricciones de edad apropiadas.
9. No ofrecerás ningún concurso, regalo ni apuesta (colectivamente, "promoción") sin nuestro consentimiento previo por escrito. Si damos nuestro consentimiento, tendrás completa responsabilidad de la promoción y seguirás nuestras Normas de las promociones y cumplirás todas las leyes aplicables.
10. No utilizarás Facebook para actos ilícitos, engañosos, malintencionados o discriminatorios.
11. No realizarás ninguna acción que pudiera inhabilitar, sobrecargar o afectar al funcionamiento correcto de Facebook, como, por ejemplo, un ataque de denegación de servicio.
12. No facilitarás ni fomentarás la violación de esta Declaración.

4. Seguridad de la cuenta y registro

Los usuarios de Facebook proporcionan sus nombres e información reales y necesitamos tu colaboración para que siga siendo así. Éstos son algunos de los compromisos que aceptas en relación con el registro y mantenimiento de la seguridad de tu cuenta.

1. No proporcionarás información personal falsa en Facebook, ni crearás una cuenta para otras personas sin su autorización.
2. No crearás más de un perfil personal.
3. Si inhabilitamos tu cuenta, no crearás otra sin nuestro permiso.
4. No utilizarás tu perfil personal para obtener ganancias comerciales (como vender tu actualización de estado a un anunciante).

5. No utilizarás Facebook si eres menor de 13 años.
6. No utilizarás Facebook si has sido declarado culpable de un delito sexual.
7. Mantendrás la información de contacto exacta y actualizada.

8. No compartirás la contraseña (o en el caso de los desarrolladores, tu clave secreta), no dejarás que otra persona acceda a tu cuenta, ni harás cualquier cosa que pueda poner en peligro la seguridad de tu cuenta.
9. No transferirás la cuenta (incluida cualquier página o aplicación que administres) a nadie sin nuestro consentimiento previo por escrito.
10. Si seleccionas un nombre de usuario para tu cuenta, nos reservamos el derecho a eliminarlo o reclamarlo si lo consideramos oportuno (por ejemplo, si el propietario de una marca comercial se queja por un nombre de usuario que no está relacionado estrechamente con el nombre real del usuario).

5. Protección de los derechos de otras personas

Respetamos los derechos de otras personas y esperamos que tú hagas lo mismo.

1. No publicarás contenido ni realizarás ninguna acción en Facebook que infrinja o viole los derechos de otros o que viole la ley de algún modo.
2. Podemos retirar cualquier contenido o información que publiques en Facebook si consideramos que viola esta Declaración.
3. Te proporcionaremos las herramientas necesarias para ayudarte a proteger tus derechos de propiedad intelectual. Para obtener más información, visita nuestra página Cómo informar de presuntas infracciones de los derechos de propiedad intelectual.
4. Si retiramos tu contenido debido a una infracción de los derechos de autor de otra persona y consideras que ha sido un error, tendrás la posibilidad de apelar.
5. Si infringes repetidamente los derechos de propiedad intelectual de otra persona, desactivaremos tu cuenta si es oportuno.
6. No utilizarás nuestros copyrights o marcas registradas (incluidos Facebook, los logotipos de Facebook y F, FB, Face, Poke, Wall y 32665) ni ninguna marca que se parezca a las nuestras sin nuestro permiso por escrito.

7. Si recopilas información de usuarios: deberás obtener su consentimiento previo, dejar claro que eres tú (y no Facebook) quien recopila la información y publicar una política de privacidad que explique qué datos recopilas y cómo los usarás.

8. No publicarás los documentos de identificación ni información financiera de nadie en Facebook.
9. No etiquetarás a los usuarios ni enviarás invitaciones de correo electrónico a quienes no sean usuarios sin su consentimiento.

6. Móvil

1. Actualmente ofrecemos nuestros servicios de móviles de forma gratuita pero ten en cuenta que se aplicarán las tarifas normales de tu operadora, por ejemplo, las tarifas de mensajes de texto.
2. En caso de que cambies o desactives tu número de teléfono móvil, actualizarás la información de tu cuenta de Facebook en un plazo de 48 horas para garantizar que los mensajes no se le envíen por error a la persona que pudiera adquirir tu antiguo número.
3. Proporcionarás todos los derechos necesarios para permitir que los usuarios sincronicen (incluso a través de una aplicación) sus listas de contactos con cualquier información básica y de contacto que puedan ver en Facebook, así como tu nombre y foto del perfil.

7. Pagos

Si realizas un pago en Facebook o utilizas los créditos de Facebook, aceptas nuestras Condiciones de pago.

8. Disposiciones especiales aplicables a los enlaces compartidos

Si incluyes en tu sitio web nuestro botón para compartir enlaces, debes tener en cuenta los siguientes términos adicionales:

1. Te damos permiso para utilizar el botón de compartir enlaces de Facebook para que los usuarios puedan publicar enlaces o contenido de tu sitio web en Facebook.
2. Nos das permiso para utilizar dichos enlaces y el contenido en Facebook, y para permitir que otros los utilicen.

3. No pondrás un botón de compartir enlaces en ninguna página que incluya contenido que pueda violar esta Declaración si se publica en Facebook.

9. Disposiciones especiales aplicables a desarrolladores u operadores de aplicaciones y sitios web

Si eres un desarrollador u operador de una aplicación o sitio web de la Plataforma, deben aplicarse los siguientes términos adicionales:

1. Eres responsable de tu aplicación, de su contenido y del uso que hagas de la Plataforma. Esto incluye la necesidad de asegurar que tu aplicación o uso de la Plataforma cumplen nuestros Principios y políticas del desarrolladory nuestras Normas de publicidad.
2. El acceso a la información que recibes de Facebook y su utilización por tu parte se limitarán de la siguiente forma:

    1. Sólo podrás solicitar los datos que necesites para hacer funcionar tu aplicación.
    2. Dispondrás de una política de privacidad que indique a los usuarios qué datos de usuario utilizarás, además de la forma en que los utilizarás, mostrarás, compartirás o transferirás. También incluirás la dirección web de la política de privacidad en la aplicación para desarrolladores.
    3. No utilizarás, mostrarás, compartirás ni transferirás datos de un usuario de un modo que resulte incoherente con la configuración de privacidad.

4. Eliminarás todos los datos que recibas de nosotros relacionados con un usuario si éste te pides que los elimines, y facilitarás un mecanismo para que los usuarios puedan realizar dicha solicitud.
5. No incluirás datos que recibas de nosotros en relación con un usuario en ningún mensaje publicitario.
6. No transferirás, directa o indirectamente, los datos que recibas de nosotros a (ni los usarás en conexión con) ninguna red publicitaria, intercambio de anuncios, agente de datos u otro conjunto de herramientas relacionado con la publicidad, incluso si un usuario consiente en dicha transferencia o uso.
7. No venderás los datos de los usuarios. Si un tercero compra tu empresa o si la fusionas con otra, podrás seguir utilizando los datos de los usuarios en la aplicación, pero no podrás transferirlos fuera de ella.
8. Podemos solicitar que elimines datos de usuarios si los utilizas de un modo que no responde a las expectativas de los usuarios.
9. Podemos limitar tu acceso a los datos.
10. Cumplirás todas las demás restricciones incluidas en nuestros Principios y políticas del desarrollador.

3. No nos proporcionarás información que recopiles independientemente de un usuario ni el contenido de un usuario sin su consentimiento.
4. Facilitarás a los usuarios la eliminación o desconexión de tu aplicación.
5. Facilitarás a los usuarios el modo de ponerse en contacto contigo. También podemos compartir tu dirección de correo electrónico con los usuarios y otras personas que afirmen que has infringido o violado sus derechos.
6. Proporcionarás atención al cliente para tu aplicación.
7. No mostrarás anuncios de terceros o casillas de búsqueda en la web en Facebook.
8. Te concedemos todos los derechos necesarios para usar el código, las API, los datos y las herramientas que recibes de nosotros.
9. No venderás, transferirás ni sublicenciarás nuestro código, API (interfaces de programación de aplicaciones) o herramientas a nadie.
10. No falsearás tu relación con Facebook ante otros.

11. Puedes utilizar los logos disponibles para desarrolladores o hacer público un comunicado de prensa o cualquier otra declaración pública siempre que cumplas nuestros Principios y políticas del desarrollador.

12. Podemos publicar un comunicado de prensa que describa nuestra relación contigo.

13. Cumplirás todas las leyes aplicables. En particular, deberás (si procede):

1. tener una política de eliminación de contenido infractor e inhabilitación de los infractores que sea conforme a la ley estadounidense de protección de los derechos de autor (Digital Millennium Copyright Act).
2. cumplir la ley de protección de la privacidad de vídeo (Video Privacy Protection Act, "VPPA") y obtener el consentimiento necesario de los usuarios para que se puedan compartir en Facebook los datos de usuario de acuerdo con la VPPA. Declaras que cualquier notificación que nos hagas no incidirá en el transcurso normal de tu negocio.

14. No garantizamos que la Plataforma será siempre gratuita.

15. Nos concedes todos los derechos necesarios para habilitar tu aplicación para que funcione con Facebook.

16. Nos concedes el derecho a enlazar a tu aplicación, o a incluirla en un marco, y a colocar contenido, incluidos anuncios, alrededor de ella.

17. Podemos analizar tu aplicación, contenido y datos para cualquier propósito, incluido el comercial (por ejemplo, para la segmentación de anuncios o el indexado de contenido para búsquedas).

18. Para garantizar que tu aplicación es segura para los usuarios, podríamos realizar una auditoría.

19. Podemos crear aplicaciones que ofrezcan funciones y servicios similares a los de tu aplicación, o que de algún modo compitan con ella.

10. Acerca de los anuncios u otro contenido comercial servido u optimizado por Facebook

Nuestro objetivo es ofrecer anuncios que no sólo sean valiosos para los anunciantes, sino también para ti. Para lograrlo, aceptas lo siguiente:

1. Puedes utilizar tu configuración de privacidad para limitar cómo se puede asociar tu nombre y fotografía de perfil al contenido comercial, patrocinado o similar (como una marca que te gusta) que sirvamos u optimicemos. Nos das permiso para utilizar tu nombre y foto de perfil en conexión con ese contenido, de acuerdo con los límites que tú establezcas.
2. No proporcionamos tu contenido o información a anunciantes sin tu consentimiento.

3. Entiendes que es posible que no siempre identifiquemos las comunicaciones y los servicios pagados como tales.

11.Disposiciones especiales aplicables a anunciantes

Puedes dirigirte a un público específico comprando anuncios en Facebook o en nuestra red de editores. Los siguientes términos adicionales son aplicables si realizas un pedido a través de nuestro portal de anuncios en línea ("Pedido"):

1. Cuando realices un pedido, nos indicarás el tipo de anuncio que deseas comprar, la cantidad que deseas gastar y tu puja. Si aceptamos tu pedido, entregaremos los anuncios cuando el inventario esté disponible. Al entregar tus anuncios, hacemos lo posible por mostrárselos al público que has indicado, aunque no podemos garantizar que sea así en todas las ocasiones.
2. Es posible que ampliemos los criterios de segmentación que indiques en los casos en los que consideremos que puede ayudar a la efectividad de tu campaña publicitaria.
3. Pagarás los pedidos de acuerdo con nuestras Condiciones de pago. La cantidad debida se calculará en base a nuestros mecanismos de seguimiento.
4. Tus anuncios cumplirán nuestras Normas de publicidad.
5. Nosotros determinaremos el tamaño, ubicación y colocación de tus anuncios.

6. No garantizamos la actividad que tendrán tus anuncios, por ejemplo, el número de clics que recibirán.
7. No podemos controlar el modo en el que la gente interactuará con tus anuncios y no somos responsables de los clics fraudulentos ni de otras acciones impropias que afecten al coste de los anuncios activos. No obstante, disponemos de sistemas para detectar y filtrar determinadas actividades sospechosas. Infórmate aquí.

8. Puedes cancelar el pedido en cualquier momento a través de nuestro portal en línea, pero podrían transcurrir 24 horas hasta que desactivemos el anuncio. Será tu responsabilidad cubrir el coste de estos anuncios.
9. Nuestra licencia para mostrar tu anuncio finalizará cuando hayamos completado tu pedido. Entiendes, sin embargo, que si los usuarios han interactuado con tu anuncio, éste podría seguir activo hasta que el usuario lo elimine.
10. Podemos utilizar tus anuncios y contenido e información relacionados con propósitos de marketing o promocionales.
11. No publicarás ningún comunicado de prensa ni harás declaraciones públicas acerca de tu relación con Facebook sin permiso por escrito.
12. Podríamos rechazar o retirar cualquier anuncio por cualquier motivo. Si colocas anuncios en nombre de un tercero, tendremos que asegurarnos de que tienes permiso para hacerlo, incluido lo siguiente:
    1. Garantizas que tienes la autoridad legal para vincular al anunciante a esta Declaración.
    2. Aceptas que si el anunciante al que representas viola la presente Declaración, podríamos hacerte responsable de dicha violación.

12. Disposiciones especiales aplicables a páginas

Si creas o administras una página en Facebook, aceptas nuestras Condiciones de las páginas

13. Enmiendas

1. Podemos cambiar esta Declaración si te lo notificamos (mediante la publicación del cambio en la página Facebook Site Governancee) y te ofrecemos la posibilidad de hacer comentarios. Para obtener notificaciones de los cambios futuros a esta declaración, visita nuestra página Facebook Site Governancey hazte fan.
2. Para cambios en las secciones 7, 8, 9 y 11 (secciones relacionadas con pagos, desarrolladores de aplicaciones, operadores de sitios web y anunciantes), la notificación se hará con un mínimo de tres días de antelación. Para todos los demás cambios daremos aviso con un mínimo de siete días de antelación. Dichos comentarios se deben realizar en la página Facebook Site Governance.
3. Si más de 7.000 usuarios envían comentarios acerca del cambio propuesto, también te daremos la oportunidad de participar en una votación en la que se te ofrecerán alternativas. El voto será vinculante para nosotros si más del 30% de todos los usuarios registrados activos en la fecha de la notificación votan.
4. Podemos realizar cambios por razones legales o administrativas, o bien para corregir una declaración incorrecta, tras notificación sin posibilidad de comentarios.

14.Terminación

Si infringes la letra o el espíritu de esta Declaración, o de algún otro modo provocas riesgo o que quedemos expuestos legalmente, podríamos dejar de proporcionarte todo o parte de Facebook. Te notificaremos por correo electrónico o la próxima vez que intentes acceder a tu cuenta. También puedes eliminar tu cuenta o desactivar tu aplicación en cualquier momento. En tales casos, esta Declaración cesará, pero las siguientes disposiciones continuarán vigentes: 2.2, 2.4, 3-5, 8.2, 9.1-9.3, 9.9, 9.10, 9.13, 9.15, 9.18, 10.3, 11.2, 11.5, 11.6, 11.9, 11.12, 11.13 y 14-18.

15.Conflictos

1. Resolverás cualquier demanda, causa de acción o conflicto (colectivamente, "demanda") que tengas con nosotros surgida de o relacionada con la presente Declaración o con Facebook exclusivamente en un tribunal estatal

o federal del condado de Santa Clara. Las leyes del estado de California rigen esta Declaración, así como cualquier demanda que pudiera surgir entre tú y nosotros, independientemente de las disposiciones sobre conflictos de leyes. Aceptas dirigirte a la competencia por razón de la persona de los tribunales del condado de Santa Clara, California, con el fin de litigar dichas demandas.

2. Si alguien interpone una demanda contra nosotros relacionada con tus acciones, tu contenido o tu información en Facebook, te encargarás de indemnizarnos y nos librarás de la responsabilidad por todos los posibles daños, pérdidas y gastos de cualquier tipo (incluidos los costes y tasas legales razonables) relacionados con dicha demanda.

3. INTENTAMOS MANTENER FACEBOOK EN FUNCIONAMIENTO, SIN ERRORES Y SEGURO, PERO LO UTILIZAS BAJO TU PROPIA RESPONSABILIDAD. PROPORCIONAMOS FACEBOOK "TAL CUAL" SIN GARANTÍA ALGUNA EXPRESA O IMPLÍCITA, INCLUIDAS, DE MANERA ENUNCIATIVA PERO NO LIMITATIVA, LAS GARANTÍAS DE COMERCIABILIDAD, ADECUACIÓN A UN FIN PARTICULAR Y NO CONTRAVENCIÓN. NO GARANTIZAMOS QUE FACEBOOK SEA SEGURO. FACEBOOK NO SE RESPONSABILIZA DE LAS ACCIONES, EL CONTENIDO, LA INFORMACIÓN O LOS DATOS DE TERCEROS Y POR LA PRESENTE NOS DISPENSAS A NOSOTROS, NUESTROS DIRECTIVOS, EMPLEADOS Y AGENTES DE CUALQUIER DEMANDA O DAÑOS, CONOCIDOS O DESCONOCIDOS, DERIVADOS DE O DE ALGÚN MODO RELACIONADOS CON CUALQUIER DEMANDA QUE TENGAS INTERPUESTA CONTRA TALES TERCEROS. SI ERES RESIDENTE DE CALIFORNIA, NO SE TE APLICA EL CÓDIGO CIVIL DE CALIFORNIA §1542 , SEGÚN EL CUAL: "UNA RENUNCIA GENERAL NO INCLUYE LAS DEMANDAS QUE EL ACREEDOR DESCONOCE O NO SOSPECHA QUE EXISTEN EN SU FAVOR EN EL MOMENTO DE EJECUCIÓN DE LA RENUNCIA, LA CUAL, SI FUERA CONOCIDA POR ÉL, DEBERÁ HABER AFECTADO MATERIALMENTE A SU RELACIÓN CON EL DEUDOR". NO SEREMOS RESPONSABLES DE NINGUNA PÉRDIDA DE BENEFICIOS, ASÍ COMO DE OTROS DAÑOS RESULTANTES, ESPECIALES, INDIRECTOS O INCIDENTALES DERIVADOS DE O RELACIONADOS CON

ESTA DECLARACIÓN DE FACEBOOK, INCLUSO EN EL CASO DE QUE SE HAYA AVISADO DE LA POSIBILIDAD DE QUE SE PRODUZCAN DICHOS DAÑOS. NUESTRA RESPONSABILIDAD CONJUNTA DERIVADA DE LA PRESENTE DECLARACIÓN O DE FACEBOOK NO PODRÁ SOBREPASAR LA CANTIDAD MAYOR DE CIEN DÓLARES (100 $) O LA CANTIDAD QUE NOS HAYAS PAGADO EN LOS ÚLTIMOS DOCE MESES. LAS LEYES APLICABLES PODRÍAN NO PERMITIR LA LIMITACIÓN O EXCLUSIÓN DE RESPONSABILIDAD POR DAÑOS INCIDENTALES O CONSECUENCIALES, POR LO QUE LA EXCLUSIÓN DE LIMITACIÓN ANTERIOR PODRÍA NO SER APLICABLE EN TU CASO. EN TALES CASOS, LA RESPONSABILIDAD DE FACEBOOK SE LIMITARÁ AL GRADO MÁXIMO PERMITIDO POR LA LEY APLICABLE.

16. Disposiciones especiales aplicables a usuarios que se encuentran fuera de EEUU

Nos esforzamos por crear una comunidad global con normas coherentes para todos, pero también por respetar la legislación local. Las siguientes disposiciones se aplicarán a los usuarios que se encuentran fuera de Estados Unidos:

1. Das tu consentimiento para que tus datos personales sean transferidos y procesados en Estados Unidos.
2. Si te encuentras en un país bajo el embargo de Estados Unidos o que forme parte de la lista SDN (Specially Designated Nationals, Nacionales especialmente designados) del Departamento del Tesoro de Estados Unidos, no participarás en actividades comerciales en Facebook (como publicidad o pago) ni utilizarás una aplicación o sitio web de la Plataforma.
3. Determinados términos específicos que se aplican únicamente a los usuarios de Alemania están disponibles aquí.

17.Definiciones

1. El término "Facebook" se refiere a las funciones y servicios que proporcionamos, incluidos los que se ofrecen a través de (a) nuestro sitio web en www.facebook.com y cualquier otro sitio web con marca o marca compartida de Facebook (incluidos los subdominios, versiones internacionales, widgets y versiones móviles); (b) nuestra Plataforma; (c) plugins sociales, como el botón "Me gusta", el botón para compartir y otros elementos similares y (d) otros medios, software (como la barra de herramientas), dispositivos o redes ya existentes o desarrollados con posterioridad.
2. El término "Plataforma" se refiere al conjunto de API y servicios que permiten que otras personas, incluidos los desarrolladores de aplicaciones y los operadores de sitios web, recuperen datos de Facebook o nos los proporcionen a nosotros.
3. El término "información" se refiere a los hechos y otra información sobre ti, incluidas las acciones que realizas.
4. El término "contenido" se refiere a todo lo que publicas en Facebook que no se incluye en la definición de "información".
5. El término "datos" se refiere al contenido y la información que pueden recuperar terceros de Facebook o proporcionan a Facebook a través de la plataforma.
6. El término "publicar" significa publicar en Facebook o proporcionarnos contenido de otro modo (por ejemplo, mediante una aplicación).
7. Por "usar" se entiende utilizar, copiar, reproducir o mostrar públicamente, distribuir, modificar, traducir y crear obras derivadas.
8. El término "usuario registrado activo" se refiere al usuario que ha entrado en Facebook al menos una vez en los últimos 30 días.
9. El término "aplicación" significa cualquier aplicación o sitio web que usa la plataforma o accede a ella, así como cualquiera que recibe o ha recibido datos de nosotros. Si ya no accedes a la plataforma pero no has eliminado todos los datos que te hemos proporcionado, el término "aplicación" continuará siendo válido hasta que los elimines.

18.Otros

1. Si resides o tienes tu ubicación de actividad comercial en EE.UU. o Canadá, esta Declaración constituye el acuerdo entre Facebook, Inc y tú. De lo contrario, esta Declaración constituye el acuerdo entre Facebook Ireland Limited y tú. Las menciones de "nosotros" o "nos" se refieren a Facebook, Inc. o Facebook Ireland Limited, según corresponda.
2. Esta Declaración constituye el acuerdo completo entre las partes en relación con Facebook y sustituye cualquier acuerdo previo.
3. Si alguna parte de esta Declaración no puede hacerse cumplir, la parte restante seguirá teniendo validez y efecto completos.
4. Si no cumpliéramos alguna parte de esta Declaración, no se considerará una exención.

5. Cualquier corrección a o exención de esta Declaración deberá hacerse por escrito y estar firmada por nosotros.
6. No transferirás ninguno de tus derechos u obligaciones bajo esta Declaración a ningún tercero sin nuestro consentimiento.
7. Todos nuestros derechos y obligaciones según esta Declaración son asignables libremente por nosotros en conexión con una fusión, adquisición o venta de activos o por efecto de ley o de algún otro modo.
8. Nada en esta Declaración nos impedirá el cumplimiento de la ley.
9. Esta Declaración no otorga derechos de beneficiario a ningún tercero.
10. Cuando accedas a Facebook o lo uses deberás cumplir todas las leyes aplicables.

Política de privacidad de Facebook

1. Introducción

Preguntas. Si tienes alguna pregunta o duda sobre nuestra política de privacidad, ponte en contacto con nuestro equipo de privacidad a través de esta página de ayuda. También puedes contactar con nosotros por correo ordinario en 1601 S. California Avenue, Palo

Alto, CA 94304.

Programa TRUSTe. Facebook ha obtenido la certificación TRUSTe Privacy Seal. Esto significa que TRUSTe ha verificado que esta política de privacidad y nuestras prácticas cumplen los requisitos del programa TRUSTe. Si tienes alguna duda o queja sobre nuestra política de privacidad o nuestras prácticas, contáctanos por correo ordinario en la siguiente dirección: 1601 S. California Avenue, Palo Alto, CA 94304 o a través de esta página de ayuda. Si no te satisface nuestra respuesta, puedes ponerte en contacto con TRUSTe. Esta política de privacidad se aplica al sitio web www.facebook.com. El programa TRUSTe sólo incluye la información recopilada a través de este sitio web, y no comprende otros datos, como información que pudiera recopilarse a través de software descargado de Facebook.

Safe Harbor. Facebook también cumple el marco Safe Harbor de la Unión Europea desarrollado por el Departamento de Comercio de Estados Unidos en cuanto a recopilación, uso y retención de datos pertenecientes a la Unión Europea. Como parte de nuestra participación en Safe Harbor, nos comprometemos a resolver todos los posibles conflictos que puedan surgir en relación con nuestras políticas y prácticas a través de TRUSTe. Asimismo, responderemos a las solicitudes de acceso dentro de un plazo de tiempo razonable. Para ver nuestra certificación, entra en el sitio web del programa Safe Harbor del Departamento de Comercio de los Estados Unidos.

Ámbito. La presente política de privacidad incluye Facebook al completo. No obstante, no es aplicable a entidades que no sean propiedad o no se encuentren bajo el control de Facebook, incluidos los sitios web y aplicaciones que utilicen la plataforma. Si utilizas o accedes a Facebook, estarás aceptando las prácticas de privacidad aquí definidas.

No se acepta información de niños menores de 13 años. Si tienes menos de 13 años, no intentes registrarte en Facebook ni nos facilites ningún dato personal. Si descubrimos que hemos recibido información de un niño menor de 13 años, borraremos esa información lo más rápido posible. Si crees que podría obrar en nuestro poder información procedente de un niño menor de 13 años, ponte en contacto con nosotros a través de esta página de ayuda.

Participación de los padres. Recomendamos encarecidamente que los menores de edad, a partir de los 13 años, pidan permiso a sus padres antes de enviar información sobre sí mismos a través de internet, y animamos a los padres a que enseñen a sus hijos prácticas seguras para el uso de internet. Encontrarás material de ayuda acerca de cómo los padres pueden hablar con sus hijos sobre un uso seguro de internet en esta página de ayuda.

2. Información que recibimos

Información que nos envías:

Información sobre ti. Cuando te registras en Facebook, nos facilitas tu nombre, correo electrónico, sexo y fecha de nacimiento. Durante el proceso de registro, te ofrecemos la posibilidad de conectarte a tus amigos, centros educativos y empleados. También podrás añadir una foto. En algunos casos podríamos pedirte información adicional por motivos de seguridad o para ofrecerte servicios específicos. Una vez registrado puedes proporcionar otra información sobre ti relacionada, por ejemplo, con tu ciudad de residencia, ciudad de origen, familia, relaciones, redes, actividades, intereses y lugares. También puedes indicar tu ideología política o tus creencias religiosas.

Contenido:

Una de las finalidades principales del uso de Facebook es compartir contenido con los demás, por ejemplo, actualizar tu estado, cargar o hacer una foto, cargar o grabar un vídeo, compartir un enlace, crear un evento o un grupo, hacer un comentario, escribir algo en el muro de alguien, escribir una nota o enviar un mensaje. Si no deseas que guardemos los metadatos asociados al contenido que compartes en Facebook (como las fotografías) elimina los metadatos antes de cargar el contenido.

Información sobre transacciones. Podemos guardar los datos de las transacciones o pagos que realices a través de Facebook. Si no deseas que almacenemos el número de cuenta de origen de tu pago, puedes eliminarlo a través de la página de pagos.

Información sobre amigos. Te ofrecemos herramientas de importación de contactos para ayudarte a cargar las direcciones de tus amigos para que puedas encontrarlos en

Facebook e invitar a unirse a aquellos contactos que todavía no usen Facebook. Si no deseas que almacenemos esta información, entra en esta página de ayuda. Si nos das tu contraseña para obtener estos contactos, no la guardaremos una vez cargada la información de los contactos.

Información que recopilamos cuando interactúas con Facebook:

Información sobre la actividad en el sitio web. Realizamos un seguimiento de las acciones que llevas a cabo en Facebook, como añadir conexiones (incluido unirte a un grupo o añadir un amigo), crear un álbum de fotos, enviar un regalo, dar un toque a otro usuario, indicar que "te gusta" una publicación, asistir a un evento o conectarte a una aplicación. En algunos casos, también estás llevando a cabo una acción cuando nos proporcionas información o contenido. Por ejemplo, si compartes un vídeo, además de almacenar el contenido real que has actualizado, podemos registrar el hecho de que lo hayas compartido.

Acceso a la información del dispositivo y del navegador. Cuando accedes a Facebook desde un ordenador, teléfono móvil u otro dispositivo, podemos obtener información de dicho dispositivo sobre tu tipo de navegador, ubicación y dirección IP, así como las páginas que visitas.

Información sobre cookies. Utilizamos "cookies" (datos que almacenamos en tu ordenador, teléfono móvil u otro dispositivo durante un período de tiempo prolongado) para que Facebook sea más fácil de usar, para que nuestra publicidad sea mejor y para proteger tanto a ti como a Facebook. Por ejemplo, las empleamos para guardar tu nombre de usuario (pero nunca tu contraseña) de modo que te resulte más sencillo iniciar sesión cada vez que quieras entrar en Facebook. También utilizamos las cookies para confirmar que estás conectado a Facebook, y para saber cuándo estás interactuando con aplicaciones y sitios web de la plataforma Facebook, nuestros widgets, botones de compartir y nuestros anuncios. Puedes eliminar o bloquear las cookies mediante la configuración de tu navegador, pero en algunos casos puede influir en tu capacidad de uso de Facebook.

Información que recibimos de terceros:

Plataforma de Facebook. No poseemos ni operamos las aplicaciones o sitios web que utilizas a través de la plataforma de Facebook (como juegos y otros programas). Cuando te conectes a un sitio web o una aplicación de la plataforma, nos suministrarán información, incluida la información acerca de las acciones que realizas. En algunos casos, es posible que recibamos una cantidad limitada de información antes de que te conectes a la aplicación o sitio web para poder personalizar el proceso de conexión.

Información procedente de otros sitios web:

-Podemos establecer programas con socios publicitarios y otros sitios web en los que éstos comparten información con nosotros:

- Podemos solicitar a los anunciantes que nos indiquen cómo nuestros usuarios han respondido a los anuncios que les mostramos (y, con fines comparativos, cómo han actuado en su página otros usuarios que no habían visto los anuncios). Esta compartición de datos, denominada comúnmente "seguimiento de conversión" nos ayuda a medir la efectividad de nuestra publicidad y a mejorar la calidad de los anuncios que ves.
- Podemos recibir información sobre si has visto o no, o si has interactuado con determinados anuncios de otros sitios, para medir la efectividad de dichos anuncios.

Si en cualquiera de estos casos recibimos datos que todavía no tenemos, les otorgaremos el carácter de "anónimos" en un plazo de 180 días, lo cual significa que no asociaremos la información con ningún usuario en particular. Si establecemos dichos programas, sólo haremos uso de la información según se explica en la sección "Cómo utilizamos tu información" expuesta a continuación.

Información procedente de otros usuarios:

-Podemos recopilar información acerca de ti a partir de otros usuarios de Facebook (como cuando un amigo te etiqueta en una foto, un vídeo o un lugar, proporciona detalles de vuestra amistad o indica su relación contigo).

3. Compartir información en Facebook

En esta sección se explica cómo funciona la configuración de la privacidad , y cómo se comparte tu información en Facebook. Antes de compartir información en Facebook debes tener en cuenta tu configuración de la privacidad.

-Nombre y foto del perfil.

Facebook ha sido diseñado para que te resulte sencillo encontrar y conectarte a otros. Por este motivo, tu nombre y la foto de tu perfil carecen de configuración de privacidad. Si no quieres compartir la foto de tu perfil, debes eliminarla (o no añadir ninguna). También puedes controlar quién puede encontrarte al buscar en Facebook o en motores de búsqueda públicos utilizando la configuración de la privacidad de las aplicaciones y los sitios web.

Información de contacto.

La configuración de tu información de contacto (disponible en la configuración de la privacidad) controla quién puede ponerse en contacto contigo en Facebook y quién puede ver tu información de contacto (por ejemplo, tu dirección de correo electrónico y número de teléfono). Recuerda que esta información no es obligatoria (excepto la dirección de correo electrónico) y que no tienes por qué compartir tu dirección de correo electrónico con nadie.

Información personal

La configuración de tu información personal controla quién puede ver tu información personal (por ejemplo, tus tendencias políticas y creencias religiosas) si decides añadirla. Recomendamos compartir esta información utilizando la opción "amigos de amigos".

Mis publicaciones.

Puedes seleccionar una configuración de privacidad para cada publicación que realices usando el editor de nuestro sitio. Tanto si vas a cargar una foto como a publicar una actualización de estado, puedes controlar exactamente quién puede verla en el momento de crearla. Cada vez que compartas algo, busca el icono del candado. Si haces clic en el candado se mostrará un menú que te permite elegir quién podrá ver tu publicación. Si

decides no seleccionar tu configuración en el momento de publicar el contenido, dicho contenido se compartirá en consonancia con la configuración de "Mis publicaciones" (disponible en la configuración de la privacidad).

Sexo y fecha de nacimiento.

Además del nombre y la dirección de correo electrónico, requerimos que nos facilites tu sexo y fecha de nacimiento durante el proceso de registro. Te pedimos la fecha de nacimiento para comprobar que eres mayor de 13 años y, así, poder limitar mejor el acceso a contenidos y anuncios que no sean adecuados para ciertas edades. Puesto que tu fecha de nacimiento y sexo son obligatorios, no puedes eliminarlos. Sin embargo, puedes editar tu perfil para ocultar todo (o parte) de dichos campos para que no los vean otros usuarios.

Otras indicaciones que debes recordar:

- Parte del contenido que compartes y de las acciones que llevas a cabo se mostrarán en las páginas de inicio de tus amigos y en otras páginas que visiten.

- Si otro usuario te etiqueta en una foto, vídeo o lugar, puedes eliminar la etiqueta. También puedes limitar quién puede ver que has sido etiquetado en tu perfil desde la configuración de la privacidad.

- Incluso tras haber eliminado la información de tu perfil o tras haber borrado tu cuenta, es posible que alguna copia de dicha información permanezca visible en algún otro lugar si ha sido compartida con otros, ha sido distribuida de algún otro modo según tu configuración de la privacidad o ha sido copiada o almacenada por otros usuarios.

- Debes entender que la información puede ser compartida a su vez o copiada por otros usuarios.

- Algunos tipos de comunicaciones que envías a otros usuarios no pueden eliminarse, como por ejemplo los mensajes.

- Cuando publicas información en el perfil de otro usuario o realizas un comentario en la publicación de otro usuario, dicha información queda sujeta a la configuración de la privacidad del otro usuario.

- Si utilizas una fuente externa para publicar información en Facebook (como una aplicación móvil o un sitio web de Connect) debes comprobar la configuración de privacidad de dicha publicación, puesto que la establece la fuente externa.

Información de “Todos”.

La información configurada como “todos” está disponible públicamente, como tu nombre, foto de perfil y conexiones. Dicha información permanece accesible y visible para todo aquel que entre en internet (incluidas las personas no registradas en Facebook), queda sujeta a indexación por parte de motores de búsqueda de terceros y puede ser importada, exportada, distribuida y redistribuida por nosotros y otros sin limitaciones de privacidad. Dicha información puede asociarse contigo, incluido tu nombre y fotografía de perfil, incluso fuera de Facebook, por ejemplo, en motores de búsqueda públicos y cuando visites otros sitios de Internet. La configuración de privacidad predeterminada para ciertos tipos de información que publicas en Facebook está establecida en “todos”. Puedes revisar y modificar la configuración predeterminada en tu configuración de la privacidad. Si eliminas el contenido compartido con "todos" previamente publicado en Facebook, lo borraremos de tu perfil de Facebook, pero no podemos controlar su uso fuera de Facebook.

Menores.

Nos reservamos el derecho de aplicar métodos de protección especial para menores (como proporcionarles un contenido adecuado a su edad) y aplicar restricciones a la capacidad que tienen los adultos para compartir y conectarse a menores, reconociendo que esto puede suponer para los menores una experiencia más limitada en Facebook.

4. Información que compartes con terceros

Platforma de Facebook.

Como ya hemos mencionado, no operamos los sitios web y aplicaciones que utilizan la plataforma de Facebook ni somos sus propietarios. Esto significa que al utilizar estas aplicaciones y sitios web, tu información de Facebook no está sólo disponible para Facebook. Antes de permitir el acceso a cualquier información sobre ti, les requerimos que acepten una serie de condiciones que limitan su uso de tu información (puedes consultar estas condiciones en la sección 9 de nuestra Declaración de derechos y responsabilidades) y ponemos en práctica medidas técnicas para garantizar que sólo obtienen información autorizada. Para obtener más información sobre la plataforma, visita la página Acerca de la plataforma.

Conexión a una aplicación o sitio web:

Cuando te conectas a una aplicación o sitio web, éstos tendrán acceso a Información general sobre ti. El término Información general incluye tu nombre y los nombres de tus amigos, fotografías de perfil, sexo, identificador de usuario, conexiones y cualquier contenido compartido usando la configuración de privacidad “Todos”. Para ayudar a estos sitios web y aplicaciones a poner en práctica medidas de seguridad y controlar la distribución de contenido apropiado a usuarios de diferentes edades, podemos poner a su disposición otra información, como datos técnicos, la localización de tu equipo informático o dispositivo de acceso, así como tu edad. Asimismo, las aplicaciones o sitios web que aceptan créditos pueden acceder a tu saldo de créditos. Si la aplicación o el sitio web desea acceder a otros datos, tendrá que pedirte permiso.

Te proporcionamos herramientas para controlar cómo compartes tu información con aplicaciones y sitios web que utilizan la plataforma. Por ejemplo, puedes bloquear completamente el acceso a tus datos de todos los sitios web y aplicaciones, o bien bloquear aplicaciones específicas en la configuración de la privacidad de las aplicaciones y los sitios web, o en la página "Acerca de" de la aplicación. También puedes utilizar tu configuración de la privacidadpara limitar qué parte de tu información está disponible para “todos”.

Aconsejamos que leas siempre las políticas de los sitios web y las aplicaciones de terceros para cerciorarte de que estás de acuerdo con el modo en el que usan la información que compartes con ellos. Facebook no puede garantizar que estos sitios web

o aplicaciones cumplirán nuestras normas. Si encuentras alguna aplicación o sitio web que infringe nuestras normas, infórmanos de este incumplimiento en esta página de ayuday tomaremos las medidas oportunas.

Cuando tus amigos utilizan la plataforma.

Si tu amigo se conecta a una aplicación o sitio web, éstos podrán acceder a tu nombre, fotografía del perfil, sexo, ID de usuario y aquella información que hayas compartido con "todos". También podrán acceder a tus conexiones, pero no podrán acceder a tu lista de amigos. Si ya te has conectado a ese sitio web o aplicación (o dispones de otra cuenta en estos lugares), es posible que éstos también puedan conectarse con tu amigo a través de ese sitio web o aplicación. Si la aplicación o el sitio web desean acceder a cualquier otro contenido o información tuya (incluida tu lista de amigos), tendrá que obtener permiso específico de tu amigo. Si tu amigo concede permiso a la aplicación o al sitio web, sólo podrán acceder a contenido e información sobre ti a la que tu amigo pueda acceder. Además, sólo podrán utilizar dicho contenido y dicha información en conexión con ese amigo.

Te proporcionamos una serie de herramientas para controlar cómo se comparte tu información cuando tu amigo se conecta a una aplicación o sitio web. Por ejemplo, puedes utilizar la configuración de privacidad de tus aplicaciones y sitios web para limitar qué información pueden poner tus amigos a disposición de las aplicaciones y los sitios web. Puedes bloquear el acceso a tu información de todas las aplicaciones y sitios web de la plataforma, o de aplicaciones o sitios web concretos. Puedes utilizar tu configuración de la privacidad para limitar los amigos que pueden acceder a tu información o limitar qué parte de tu información está disponible para "todos". También puedes desconectarte de un amigo si no estás de acuerdo con el modo en que utiliza tu información.

Sitios web y aplicaciones de terceros aprobados previamente.

Para proporcionarte experiencias sociales útiles fuera de Facebook, en ocasiones necesitamos proporcionar Información general sobre ti a sitios web y aplicaciones de terceros aprobados previamente que utilizan la plataforma cuando los visitas (si aún tienes una sesión iniciada en Facebook). Del mismo modo, cuando uno de tus amigos visita un sitio web o aplicación aprobados previamente, recibirá información general sobre

ti para que podáis conectaros también a través de ese sitio web (si también dispones de una cuenta en dicho sitio web). En estos casos, requerimos que estos sitios web y estas aplicaciones se sometan a un proceso de aprobación y participen en diferentes acuerdos con el objetivo de proteger tu privacidad. Por ejemplo, estos acuerdos incluyen disposiciones relativas al acceso y eliminación de tu Información general, así como la posibilidad de rechazar la participación en la experiencia ofrecida. Puedes inhabilitar la personalización instantánea de todos los sitios web y aplicaciones aprobados previamente mediante la configuración de la privacidadde las aplicaciones y los sitios web. También puedes bloquear un sitio web o una aplicación que han recibido autorización previa haciendo clic en "No, gracias", que verás en la barra de color azul de la aplicación o sitio web concreto. Además, si cierras la sesión de Facebook antes de visitar un sitio web o aplicación aprobados previamente, éstos no podrán acceder a tu información.

Exportación de información.

Puedes (al igual que todos aquellos a cuya disposición has puesto tu información) utilizar herramientas como fuentes RSS, aplicaciones de libretas de direcciones del teléfono móvil o funciones de copiar y pegar, para obtener y exportar (y en algunos casos, importar) información de Facebook, incluida tu propia información y todos los datos sobre tu persona. Por ejemplo, si compartes tu número de teléfono con tus amigos, éstos pueden utilizar aplicaciones de terceros para sincronizar dicha información con la libreta de direcciones de sus teléfonos móviles.

Publicidad.

En ocasiones, los anunciantes que presentan publicidad en Facebook emplean métodos tecnológicos para medir la efectividad de sus anuncios y personalizar el contenido publicitario. Puedes renunciar a la fijación de cookies de numerosos anunciantes haciendo clic en el enlace correspondiente. También puedes usar la configuración de cookies de tu navegador para limitar o evitar la fijación de cookies por parte de redes publicitarias. Facebook no comparte con los anunciantes información que te identifica personalmente salvo si obtenemos tu autorización.

Enlaces.

Al hacer clic en algunos enlaces de Facebook, es posible que te lleven fuera de nuestro sitio web. No nos hacemos responsables de las políticas de privacidad de otros sitios web, y te animamos a que leas sus normas de privacidad.

5. Cómo utilizamos tu información

Utilizamos la información que recopilamos para tratar de ofrecerte una experiencia segura, eficaz y personalizada. A continuación, incluimos algunos datos sobre cómo lo hacemos:

Para gestionar el servicio.

Utilizamos la información que recopilamos para ofrecerte nuestros servicios y funciones, evaluarlos y mejorarlos y prestarte servicio técnico. Empleamos la información para impedir actividades que podrían ser ilegales y para aplicar nuestra Declaración de derechos y responsabilidades. También utilizamos una serie de sistemas tecnológicos para detectar y ocuparnos de actividades y contenido en pantalla anómalos con el fin de evitar abusos como el correo basura. Estos esfuerzos pueden provocar, en ocasiones, el fin o la suspensión temporal o permanente de algunas funciones para algunos usuarios.

Para ponernos en contacto contigo.

Ocasionalmente, podemos ponernos en contacto contigo para informarte de anuncios relativos a servicios. Puedes optar por no recibir ninguna comunicación salvo actualizaciones esenciales en la página de notificaciones de la cuenta. En los mensajes de correo electrónico que te enviemos, podemos incluir contenido que veas en Facebook.

Para ofrecerte anuncios personalizados.

No compartimos información tuya con anunciantes sin tu consentimiento. (Un ejemplo de consentimiento sería que nos pidieses que suministrásemos tu dirección de envío a un anunciante para recibir una muestra gratuita.) Permitimos a los anunciantes elegir las características de los usuarios que verán sus anuncios y podemos utilizar cualquiera de los atributos que hayamos recabado que no te identifiquen personalmente (como

información que puedas haber decidido no mostrar a otros usuarios, por ejemplo, el año de nacimiento) para seleccionar el público apropiado para dichos anuncios. Por ejemplo, podríamos utilizar tu interés por el fútbol para mostrarte anuncios de equipamiento de fútbol, pero no le decimos a la empresa que vende el equipamiento quién eres. Puedes consultar los criterios que pueden seleccionar los anunciantes visitando nuestra página de publicidad. Aunque no compartimos tu información con anunciantes sin tu consentimiento, cuando hagas clic en un anuncio o interactúes de otro modo con éste, existe la posibilidad de que el anunciante pueda colocar una cookie en tu navegador y tomar nota de que cumple los criterios que ha seleccionado.

Para ofrecer anuncios sociales.

En ocasiones, emparejamos los anuncios que ofrecemos con información pertinente que poseemos sobre ti y sobre tus amigos para que los anuncios resulten más interesantes y se adapten mejor a ti y a tus amigos. Por ejemplo, si te conectas a la página de tu grupo de música favorito, podemos mostrar tu nombre y la foto de tu perfil al lado de un anuncio de dicha página que verán tus amigos. Sólo compartimos la información personal visible en el anuncio social con el amigo que puede ver el anuncio. Puedes optar por que tu información no sea utilizada en anuncios sociales en esta página de ayuda.

Para complementar tu perfil.

Podemos utilizar información acerca de ti que recabemos de otros usuarios de Facebook para completar tu perfil (por ejemplo, cuando se te etiqueta en una foto o se te menciona en una actualización de estado). En tales casos, generalmente te permitimos eliminar el contenido (por ejemplo, permitiéndote eliminar la etiqueta de una foto tuya) o limitar la visibilidad de tu perfil.

Para hacer sugerencias.

Utilizamos tu información, incluidas las direcciones que importas a través de las herramientas de importación de contactos, para hacerte sugerencias a ti y a otros usuarios de Facebook. Por ejemplo, si otro usuario importa la misma dirección de correo electrónico que tú, podemos sugeriros a ambos que añadáis al otro a vuestra lista de amigos. También, si un amigo tuyo carga una foto en la que apareces, podemos sugerirle que te etiquete en ella. Para hacer esto, comparamos las fotos de tu amigo con

información recopilada de las fotos en las que se te ha etiquetado. También podemos sugerirte que uses herramientas o funciones concretas, según lo que utilicen tus amigos. Para controlar si podemos sugerir o no a otro usuario que te añada como amigo, ve a la opción "Buscarte en Facebook" de tu configuración de privacidad. También puedes controlar si sugerimos o no a otros usuarios que te etiqueten en una foto haciendo clic en "Personalizar la configuración" en la página de configuración de la privacidad.

Para ayudar a tus amigos a encontrarte.

Permitimos a otros usuarios utilizar información de contacto que tengan sobre ti (como tu dirección de correo electrónico) para encontrarte, incluso a través de herramientas de importación y búsqueda de contactos. Puedes impedir que otros usuarios utilicen tu dirección de correo electrónico para encontrarte en la sección de búsquedas de tu configuración de la privacidad.

Software descargable.

Algunas aplicaciones de software descargables y applets que ofrecemos, como las barras de herramientas del navegador y las herramientas para cargar fotos, nos transmiten datos. Podemos no realizar ninguna declaración formal si creemos que la recopilación y uso de información por nuestra parte es el fin obvio de la aplicación, por ejemplo, el hecho de recibir fotografías cuando se utiliza la herramienta para cargar fotos. Si creemos que no resulta obvio que estemos recopilando o utilizando dicha información, te avisaremos la primera vez que nos facilites la información, de tal manera que puedas decidir si deseas utilizar esa función.

Cuentas in memoriam.

Si se nos notifica que un usuario ha fallecido, podemos convertir su cuenta en una cuenta conmemorativa. En tales casos, restringimos el acceso al perfil a los amigos confirmados y permitimos a éstos y a los familiares que escriban en el muro del usuario en recuerdo suyo. Podemos cerrar una cuenta si recibimos una solicitud formal de un pariente del usuario u otra solicitud legal pertinente para hacerlo.

6. Cómo compartimos la información

Facebook se basa en compartir información con otros (amigos y personas de tu entorno) al tiempo que se te ofrece una configuración de la privacidadque puedes utilizar para restringir el acceso de otros usuarios a tu información.. Compartimos tu información con terceros cuando creemos que dicha acción está permitida por ti, que es razonablemente necesaria para ofrecer nuestros servicios o cuando se nos exige legalmente que lo hagamos. Por ejemplo:

Cuando realizas un pago.

Cuando realices transacciones con otras personas o efectúes pagos en Facebook, sólo compartiremos la información de la transacción con los terceros que sean necesarios para completar la transacción. Requeriremos que los terceros acuerden respetar la privacidad de la información.

Cuando invitas a un amigo a que se una a Facebook.

Cuando nos pides que invitemos a un amigo a que se una a Facebook, le enviaremos un mensaje de tu parte, usando tu nombre. La invitación también puede contener información sobre otros usuarios que tu amigo pueda conocer. También le enviamos hasta dos recordatorios en tu nombre. Puedes ver quién ha aceptado tus invitaciones, enviar recordatorios y eliminar las direcciones de correo electrónico de tus amigos en la página del historial de invitaciones. Si tu amigo no quiere que conservemos su información, la eliminaremos a petición suya en esta página de ayuda.

Cuando eliges compartir tu información con comerciantes.

Puedes elegir compartir información con comerciantes o proveedores de comercio electrónico no asociados con Facebook a través de ofertas en el sitio web. Esto será a tu entera discreción y no le suministraremos información tuya a dichos comerciantes sin tu consentimiento.

Para ayudar a tus amigos a encontrarte.

De forma predeterminada, incluimos cierta información que has colocado en tu perfil en los resultados de búsqueda de Facebook para ayudar a tus amigos a encontrarte. Sin embargo, puedes controlar quién puede ver alguna de esta información, así como quién puede encontrarte en búsquedas, a través de la configuración de la privacidad. También colaboramos con proveedores de mensajería instantánea y correo electrónico para ayudar a sus usuarios a identificar cuáles de sus contactos son usuarios de Facebook, de forma que podamos promocionar Facebook a dichos usuarios.

Para dar a los motores de búsqueda acceso a información públicamente disponible.

En general, restringimos el acceso de los motores de búsqueda a nuestro sitio web. Podemos permitirles acceder a información configurada con la opción "todos" (junto con tu nombre y fotografía de perfil) y a la información de tu perfil que sea visible para todos. Puedes cambiar la visibilidad de parte de la información de tu perfil en la sección de personalización de la configuración de la privacidad. También puedes impedir que los motores de búsqueda sometan a indexado tu perfil en la configuración de la privacidad de las aplicaciones y los sitios web.

Para ayudar a mejorar o promocionar nuestro servicio.

A veces compartimos datos agregados o anónimos con terceros para ayudar a mejorar o promocionar nuestro servicio. Sin embargo, sólo lo hacemos de tal manera que no se pueda identificar a ningún usuario en particular ni vincularse a éste con ninguna información o acción específica.

Para prestarte servicios.

Podemos ofrecer información a proveedores de servicios que nos ayudan a facilitarte los servicios que ofrecemos. Por ejemplo, podemos utilizar a terceros para alojar nuestro sitio web, enviar actualizaciones por correo electrónico acerca de Facebook, eliminar información repetitiva de nuestras listas de usuarios, procesar pagos u ofrecer enlaces o resultados de búsqueda (lo que incluye enlaces promocionados). Estos proveedores de servicios pueden tener acceso a tu información personal para utilizarla durante un período de tiempo limitado, pero cuando esto ocurre, implantamos sistemas de protección técnicos y contractuales razonables para restringir su uso de dicha información a la ayuda que nos prestan para ofrecer el servicio.

Para publicitar nuestros servicios.

Podemos pedir a anunciantes ajenos a Facebook que muestren anuncios para promocionar nuestros servicios. Podemos pedirles que entreguen dichos anuncios basándose en la presencia de una cookie, pero al hacerlo, no se compartirá ninguna otra información.

Para ofrecer servicios conjuntos.

Podemos prestar servicios de forma conjunta con otras empresas, como se el caso del servicio de clasificados del Marketplace de Facebook. Si utilizas estos servicios, podemos compartir tu información para facilitar dicho servicio. Sin embargo, identificaremos al socio y te presentaremos la política de privacidad del proveedor de servicios conjuntos antes de que utilices dicho servicio.

Para responder a requerimientos legales y evitar daños.

Podemos revelar información con arreglo a citaciones, órdenes judiciales u otros requerimientos (incluidos asuntos civiles y penales) si creemos de buena fe que la ley exige dicha respuesta. Esto puede incluir respetar requerimientos de jurisdicciones ajenas a los Estados Unidos cuando creamos de buena fe que las leyes locales de tal jurisdicción exigen dicha respuesta, son aplicables a usuarios de dichas jurisdicción y resultan coherentes con estándares internacionales generalmente aceptados. También podemos compartir información si creemos de buena fe que resulta necesario para impedir un fraude u otra actividad ilegal, evitar un daño físico inminente o protegernos tanto a nosotros como al usuario de personas que infrinjan nuestra Declaración de derechos y responsabilidades. Esto puede incluir compartir información con otras empresas, abogados, tribunales u otras entidades gubernamentales.

Transferencia en caso de venta o cambio de control. En tal caso, tu información seguiría estando sujeta a las promesas efectuadas en la Política de privacidad preexistente.

7. Cómo puedes cambiar eliminar información

Edición de tu perfil.

Puedes cambiar o eliminar la información de tu perfil en cualquier momento yendo a la página de tu perfil y haciendo clic en “Editar mi perfil”. La información se actualizará de inmediato.

Eliminar los contactos cargados.

Si utilizas nuestra herramienta para importar contactos con el fin de cargar direcciones, después puedes eliminar la lista en esta página de ayuda. Puedes eliminar las direcciones de correo electrónico de amigos que hayas invitado a unirse a Facebook en tu página del historial de invitaciones.

Desactivación o eliminación de la cuenta.

Si quieres dejar de utilizar tu cuenta, puedes desactivarla o eliminarla. Cuando desactivas una cuenta, ningún usuario podrá verla, pero no será eliminada. Guardamos la información de tu perfil (conexiones, fotos, intereses, etc.) por si más tarde decides volver a activarla. Muchos usuarios desactivan sus cuentas por motivos temporales y al hacerlo, nos piden que mantengamos su información hasta que vuelvan a Facebook. Seguirás pudiendo reactivar la cuenta y restaurar tu perfil en su totalidad. Cuando eliminas una cuenta, se borra de forma permanente. Sólo deberías eliminar tu cuenta si estás seguro de que nunca querrás reactivarla. Puedes desactivar la cuenta en la página de configuración de la cuentao eliminar tu cuenta en esta página de ayuda.

Limitaciones sobre la eliminación.

Incluso después de eliminar información de tu perfil o eliminar tu cuenta, pueden permanecer copias de dicha información visibles en otro lugar en la medida en que se haya compartido con otros, se haya distribuido de otro modo conforme a tu configuración de la privacidad, o haya sido copiada o almacenada por otros usuarios. Sin embargo, tu nombre dejará de estar asociado con dicha información en Facebook. (Por ejemplo, si publicas algo en el perfil de otro usuario y después eliminas tu cuenta, dicha publicación podría permanecer, pero atribuirse a un “Usuario de Facebook anónimo.”) Asimismo, podemos conservar cierta información para evitar el robo de identidades y otras conductas inadecuadas, incluso si se ha solicitado la eliminación. Si has facilitado a aplicaciones o sitios web de terceros acceso a tu información, éstos pueden conservar tu información hasta el límite permitido por sus condiciones de servicio o políticas de

privacidad. Sin embargo, después de desconectarte de ellos, ya no podrán acceder a la información a través de nuestra plataforma.

Copias de seguridad.

La información eliminada y borrada puede permanecer en copias de seguridad hasta un máximo de 90 días, pero no estará disponible para los demás.

Información de contacto de no usuarios.

Si un usuario nos facilita tu dirección de correo electrónico, pero no eres usuario de Facebook y quieres que la eliminemos, puedes hacerlo en esta página de ayuda. Sin embargo, esa solicitud sólo se aplicará a las direcciones que tengamos en el momento de la solicitud y no a ninguna dirección que los usuarios nos faciliten posteriormente.

8. Cómo protegemos la información

Hacemos todo lo posible para mantener a salvo tu información, pero necesitamos tu ayuda. Para obtener información más pormenorizada sobre cómo mantener la seguridad en Facebook, visita la página Security Page de Facebook.

Medidas que tomamos para mantener a salvo su información. Mantenemos la información de tu cuenta en un servidor protegido con un firewall. Cuando introduces información confidencial (por ejemplo, contraseñas y números de tarjeta de crédito), la ciframos usando tecnología de capa de socket seguro (SSL). También utilizamos medidas sociales y automatizadas para aumentar la seguridad (como el análisis de la actividad de la cuenta por si hubiera algún comportamiento fraudulento o anómalo de otro tipo), podemos limitar el uso de funciones del sitio web en respuesta a posibles signos de abuso, podemos eliminar contenido inadecuado o enlaces a contenido ilegal, y podemos suspender o desactivar cuentas por si hubiera violaciones de nuestra Declaración de derechos y responsabilidades.

Riesgos inherentes a compartir información.

Aunque te permitimos definir opciones de privacidad que limiten el acceso a tu información, ten en cuenta que ninguna medida de seguridad es perfecta ni impenetrable.

No podemos controlar las acciones de otros usuarios con los que compartas información. No podemos garantizar que sólo vean tu información personas autorizadas. No podemos garantizar que la información que compartas en Facebook no pase a estar disponible públicamente. No somos responsables de que ningún tercero burle cualquier configuración de la privacidad o medidas de seguridad en Facebook. Puedes reducir estos riesgos utilizando hábitos de seguridad de sentido común como elegir una contraseña segura, utilizar contraseñas diferentes para servicios diferentes y emplear software antivirus actualizado.

Informar de incumplimientos.

Deberías informarnos de cualquier incumplimiento de la seguridad en esta página de ayuda.

9. Otras condiciones

Cambios.

Podemos cambiar esta Política de privacidad conforme a los procedimientos señalados en la Declaración de derechos y responsabilidades. Salvo indicación en contrario, nuestra política de privacidad en vigor se aplica a toda la información que tenemos sobre ti y tu cuenta. Si realizamos cambios en esta Política de privacidad, te lo notificaremos publicándolo aquí y en la página Facebook Site Governance. Si los cambios son sustanciales, mostraremos un aviso prominente si las circunstancias lo requieren. Puedes asegurarte de que recibes notificación directamente haciendo clic en el botón "Me gusta" de la página Facebook Site Governance.

Consentimiento para la recopilación y procesamiento en Estados Unidos.

Al utilizar Facebook, das tu consentimiento para que tus datos personales sean transferidos y procesados en Estados Unidos.

Términos definidos.

"Nos," "nosotros," "nuestro," "Plataforma" y "Facebook" significan lo mismo que en la Declaración de derechos y responsabilidades. “Información” y “contenido” se utilizan de forma más general e intercambiable aquí que en la Declaración de derechos y responsabilidadessalvo que el contexto lo limite de otro modo.

8.2-¿Qué es el Facebook Safety Advisory Board (consejo asesor de seguridad de Facebook) y a qué se dedica?

El consejo asesor de seguridad global de Facebook integra cinco de las principales organizaciones de Norteamérica y Europa que se ocupan de la seguridad en Internet. Estas organizaciones asesoran a Facebook en cuestiones relacionadas con la seguridad de la red. A continuación dispones de información sobre ellas:

Childnet International

Childnet International es una organización benéfica con sede en el Reino Unido que desarrolla su actividad tanto en ese país como en el extranjero. Su objetivo consiste en hacer de Internet un lugar seguro para los menores y los adolescentes, al tiempo que se les enseña a usar las tecnologías interactivas con responsabilidad y seguridad. Childnet ha diseñado varios recursos que ayudan tanto a los jóvenes como a los adultos a sopesar y hacer frente a los posibles riesgos de Internet: http://www.childnet.com

NNEDV

El proyecto tecnológico de seguridad en la red de la Red estadounidense para poner fin a la violencia doméstica es la organización líder en seguridad en línea para víctimas de violencia doméstica, abuso en citas de adolescentes, ciberacoso o acoso. Con sede en Washington D.C., es una coalición contra la violencia doméstica que abarca todos los estados y territorios de Estados Unidos y cuyo objetivo es fomentar el uso seguro de la tecnología con organizaciones filiales en todo el mundo.

Connect Safely

ConnectSafely.org es el principal recurso web interactivo para padres, adolescentes y

educadores, es decir, para todos los colectivos interesados en la seguridad de los menores en las redes sociales fijas o móviles: http://www.connectsafely.org

The Family Online Safety Institute (FOSI)

The Family Online Safety Institute trata de mejorar la seguridad del mundo virtual para los menores y sus familias identificando y promoviendo prácticas recomendadas, herramientas y métodos en el ámbito de la seguridad que respeten, al mismo tiempo, la libertad de expresión: http://fosi.org

WiredSafety

WiredSafety es el mayor programa mundial de seguridad en Internet, formación y grupos de ayuda. Ofrece a los usuarios de Internet y de dispositivos móviles de cualquier edad ayuda, información y formación, en particular en relación con el acoso cibernético: http://www.wiredsafety.org y http://stopcyberbullying.org/

Centro de seguridad para familias

Facebook también dispone del llamado Centro de seguridad para familias (http://www.facebook.com/safety), en el que ofrece información muy variada sobre seguridad, tanto para usuarios adultos, menores, así como padres o tutores.

Aquí se explica detalladamente la política de seguridad y privacidad que sigue Facebook y se dan consejos sobre como actuar para protegernos de posibles amenazas.

9.-TUENTI

9.1-Decálogo de Condiciones de Tuenti

1. TUENTI es una plataforma social para usuarios mayores de 14 años.

2. El uso de TUENTI es personal, y bajo ningún concepto podrás utilizarlo con fines económicos o comerciales sin nuestro previo consentimiento.

3. Está prohibido crear perfiles con datos falsos. Los datos han de ser correctos y pertenecientes a personas físicas reales.

4. TUENTI es un intermediario en la utilización del servicio, siendo el usuario el único responsable de las acciones que lleva a cabo, así como de los contenidos que sube.

5. TUENTI se reserva la facultad de retirar o investigar cualquier contenido que atente contra sus Condiciones Generales de Uso.

6. Está TERMINANTEMENTE prohibido:

- Copiar imágenes subidas por otros usuarios para distribuirlas dentro o fuera de TUENTI.
- Alojar y usar de cualquier modo material o información de carácter racista, violento, pornográfico, abusivo, engañoso, ilegal o que atente contra la moral y el orden público.
- Usar el servicio para injuriar, difamar, intimidar, violar la propia imagen o acosar a otros usuarios.
- Utilizar el servicio de manera ilegal o de cualquier forma que pueda perjudicar a TUENTI.
- Introducir cualquier tipo de software que pudiera resultar perjudicial para TUENTI o sus sistemas.
- Utilizar el servicio para realizar envíos de comunicaciones comerciales, envío de mensajes con finalidad publicitaria o captar datos con dicho fin.
- Recopilar direcciones de correo electrónico u otra información de los usuarios para remitir comunicaciones no solicitadas.

7. No se puede suplantar la personalidad de un tercero a través de la creación de un perfil con los datos de ese tercero.

8. Cuando un usuario publica cualquier tipo de contenido, garantiza que tiene todos los derechos necesarios para publicar dicho contenido y licenciar a TUENTI para su uso en la red y que con ello no se vulnera ningún derecho relativo a la intimidad, el honor o la propia imagen de un tercero.

9. TUENTI no será en ningún caso responsable de las interacciones entre los usuarios. Los únicos responsables serán los propios usuarios, independientemente de que TUENTI realice todos los esfuerzos para investigar cualquier acción que no respete las Condiciones de Uso o la legislación vigente.

10. Se prohíbe la publicación de cualquier URL o contenido perteneciente a TUENTI fuera del mismo sin nuestro previo consentimiento escrito.

Para poder ser usuario de TUENTI es completamente imprescindible la lectura y aceptación de las Condiciones Generales de Uso de las que el presente decálogo es un resumen, así como de nuestra política de privacidad.

9.2-Condiciones de uso y política de privacidad de Tuenti

Por favor lee atentamente estas condiciones de uso ya que contienen toda la información relativa a tus derechos y obligaciones como usuario de TUENTI. Aquí podrás ver todo lo que puedes y lo que no puedes hacer en la plataforma social privada de TUENTI, así como todos los procedimientos de reclamación y solución de conflictos.

TUENTI es una plataforma social privada (en adelante, también denominada "Servicio") que facilita un espacio (en adelante "Perfil") a través del que puedes facilitar e intercambiar información y establecer comunicación entre tus amigos y tú. Permite saber

qué cosas están pasando a tu alrededor y te ayuda a conectar con tus amigos y a hacer contactos de todo tipo de redes como el colegio, universidad, trabajo, zonas de marcha y demás. La plataforma social privada de TUENTI es administrada por TUENTI TECHNOLOGIES, S.L. (en adelante "TUENTI" o "nosotros").

Estas Condiciones de uso regulan el acceso y la utilización del Servicio y sitio web alojado bajo los nombres de dominio www.tuenti.com y www.tuenti.es, así como de todos los contenidos que en los mismos se muestre o pongan a disposición de los Usuarios. Cuando accedes o utilizas el sitio web o cualquiera de las utilidades de la plataforma social privada, manifiestas que has leído y aceptas cumplir con todo lo dispuesto en estas Condiciones de uso.

Estas Condiciones de uso también se aplicarán a la versión móvil del sitio web y del Servicio.

TUENTI se reserva el derecho a su elección exclusiva, de revisar las presentes Condiciones de uso en cualquier momento por razones legales, por motivos técnicos o por cambios en la prestación del Servicio o en la normativa, así como modificaciones que pudieran derivarse de códigos tipo aplicables o, en su caso, por decisiones corporativas estratégicas. Cuando esto ocurra te avisaremos de ello a través del sitio web y si, una vez te hemos informado de ello, continúas utilizando el Servicio, entenderemos que has aceptado las modificaciones introducidas. Si no estuvieras de acuerdo con las modificaciones efectuadas, podrás darte de baja en el servicio siguiendo el procedimiento habilitado para ello.

Estas Condiciones de uso podrán ser completadas por TUENTI a través de condiciones particulares que regulen el uso de determinados servicios o productos que se puedan ofrecer en el Sitio Web.

El acceso a ciertos contenidos y la utilización de algunos servicios o productos pueden encontrarse sometidos a determinadas condiciones particulares, que, según los casos, sustituirán, completarán y/o modificarán las presentes Condiciones de uso de TUENTI, y en caso de contradicción, prevalecerán los términos de las condiciones particulares sobre los estipulados en las Condiciones de uso.

La recogida y tratamiento de tus datos personales así como el ejercicio de tus derechos sobre dichos datos, se regirán por estas Condiciones de uso y la Política de Privacidad y Protección de Datos.

ACCESO AL SERVICIO: Personas físicas mayores de 14 años

El acceso al Servicio está PROHIBIDO a los menores de 14 años, por tanto, por la aceptación de estas Condiciones, garantizas que eres mayor de 14 años y te responsabilizas enteramente de esta declaración.

El equipo de TUENTI puede ponerse en contacto contigo, en cualquier momento, para que demuestres tu edad real aportándonos fotocopia de tu DNI o un documento equivalente. Si no nos das esa información dentro del plazo que te digamos, desde TUENTI nos reservamos el derecho a bloquear o cancelar tu perfil.

Los datos del DNI o del documento que se aporte serán utilizados única y exclusivamente por el personal autorizado de TUENTI para realizar esta tarea de identificación, en ningún caso, se tratará para otro fin.

Si tienes entre 14 y 18 años, te recomendamos que informes y consultes con tus padres o tutores legales a la hora de transmitir información a terceros con los que hayas contactado a través del Servicio.

Si somos informados de que un menor de 14 años está registrado como Usuario en TUENTI, adoptaremos las medidas necesarias y podremos eliminar o bloquear el perfil de Usuario.

Te pedimos que cualquier abuso o vulneración de las presentes condiciones que detectes y, en particular, aquellos que afecten a menores, nos lo digas inmediatamente.

Además, tienes que saber que para poder ser Usuario de TUENTI es necesario que antes hayas recibido en tu correo electrónico una invitación de un amigo que ya sea Usuario de TUENTI. Para ver las implicaciones que en materia de protección de datos tiene el envío de invitaciones, consulta el apartado "Invitaciones" en la Política de Privacidad y Protección de Datos.

SEGURIDAD DEL PERFIL

ACEPTAS EXPRESAMENTE que el Servicio y los servicios de TUENTI se ofrecen exclusivamente para tu uso personal, y no puedes utilizarlo para una finalidad económica o comercial sin contar con la previa autorización de TUENTI.

A salvo de lo dispuesto expresamente en las presentes Condiciones de uso, y sin perjuicio de las herramientas publicitarias, de comunicación o de patrocinio que TUENTI pueda poner a tu disposición, las personas jurídicas - sean empresas, asociaciones o cualesquiera otro tipo de entidades - tienen PROHIBIDO tener un Perfil. Asimismo, tampoco podrán tener Perfil las personas físicas que, por si solas, en representación de personas jurídicas o en el ejercicio de actividades profesionales, tengan como finalidad utilizar el Perfil con un fin comercial, publicitario, promocional o para la realización de alguna actividad con finalidad económica.

El acceso al Servicio implica necesariamente que debes facilitar a TUENTI una serie de datos de carácter personal y, por tanto, consentir nuestra Política de Privacidad y Protección de Datos. Queda prohibido el suministro de datos falsos, por tanto, debes identificarte siempre con tu nombre real y con datos correctos. Si TUENTI detecta datos falsos o incorrectos en los perfiles podrá cancelarlo, de acuerdo con lo previsto en estas Condiciones de uso.

Los datos que suministres deberás mantenerlos actualizados en todo momento.

El acceso al Servicio y el uso del perfil implica tu compromiso y obligación de hacer un uso correcto de los mismos, con sujeción a estas condiciones y a la legalidad vigente, sea nacional o internacional, así como a los principios de buena fe, a la moral y al orden público, y con el compromiso de observar diligentemente cualquier instrucción adicional que, en relación con el uso y acceso que hagas, pueda realizarte TUENTI. Tú eres el responsable del uso que hagas del perfil.

RESPONSABILIDADES

Estás obligado a hacer un uso razonable del Servicio y del sitio web y sus contenidos, según las posibilidades y fines para los que está concebido.

En relación al Servicio, TUENTI actúa como mero intermediario que pone a tu disposición su espacio web, asumiendo única y exclusivamente la responsabilidad derivada de la

diligencia que le pudiera ser exigible por ley. TUENTI no asumirá ninguna responsabilidad, ya sea directa o indirecta, derivada del mal uso que hagas del Servicio, del sitio web o de los contenidos allí localizados.

TUENTI hará todo lo razonablemente posible para vigilar la legalidad de los contenidos, imágenes, opiniones y demás información que se comuniquen a través del Servicio y del sitio web. Sin embargo, al no ser posible el control absoluto de aquellos, tú serás el único responsable de la información, imágenes, opiniones, alusiones o contenidos de cualquier tipo que comuniques, alojes, transmitas, pongas a disposición o exhibas a través del sitio web; y, en concreto, serás el único responsable del mantenimiento de tu perfil, y de la información, imágenes, opiniones, alusiones o contenidos de cualquier tipo que comuniques, alojes, transmitas, pongas a disposición o exhibas en tu perfil.

En especial, TUENTI no podrá ser considerado responsable editorial, y declaramos expresamente que no nos identificamos con ninguna de las opiniones que como usuario de TUENTI podáis emitir a través del Servicio, de cuyas consecuencias se hace enteramente responsable el emisor de las mismas.

Podremos limitar el acceso al Servicio de opiniones, informaciones, comentarios, imágenes o dibujos que como usuario de TUENTI nos hagas llegar, pudiendo instalar, si así lo entendiéramos oportuno, filtros a tales efectos. Lo anterior no supone, en modo alguno, la obligación de TUENTI de controlar los contenidos que puedan difundirse a través del Servicio, sino la voluntad de evitar, en la medida de lo posible, que a través de TUENTI puedan difundirse en la Red contenidos u opiniones que puedan ser considerados difamatorios, racistas, sexistas, xenófobos, discriminatorios, pornográficos, violentos o que, de cualquier modo contraríen la moral, el orden público o las buenas costumbres, o resulten claramente ilícitos o ilegales.

USOS NO PERMITIDOS

QUEDA TERMINANTEMENTE PROHIBIDO y, por tanto, sus consecuencias serán de tu exclusiva responsabilidad, el acceso o la utilización del Servicio con fines ilegales o no autorizados, con o sin finalidad económica, y, más específicamente y sin que el siguiente listado tenga carácter absoluto, queda prohibido:

- Alojar, almacenar, divulgar, publicar, distribuir o compartir cualquier contenido que pueda ser considerado como una vulneración en cualquier forma de los derechos fundamentales al honor, imagen e intimidad personal y familiar de terceros y, muy especialmente, de los menores de edad.
- Alojar, almacenar, divulgar, publicar, distribuir o compartir imágenes o fotografías que recojan imágenes o datos personales de terceros sin haber obtenido el oportuno consentimiento de sus titulares.
- Alojar, almacenar, divulgar, publicar, distribuir o compartir cualquier contenido que vulnere el secreto en las comunicaciones, la infracción de derechos de propiedad industrial e intelectual o de las normas reguladoras de la protección de datos de carácter personal.
- Reproducir, distribuir, poner a disposición o de cualquier otro modo compartir, dentro o fuera de la red de TUENTI, fotografías o imágenes que hayan sido puestas a disposición por otros usuarios de TUENTI.
- Alojar, almacenar, divulgar, publicar, distribuir o compartir cualquier material o información que sea ilegal, racista, obscena, pornográfica, abusiva, difamatoria, engañosa, fraudulenta o de cualquier forma contraria a la moral o al orden público.
- Usar el servicio para injuriar, difamar, intimidar, violar la propia imagen o acosar a otros usuarios.
- Hacer un uso del Sitio Web o de cualquiera de los servicios de TUENTI de forma ilegal, o de cualquier otro modo por el cual se pueda dañar, sobrecargar o perjudicar el Servicio o el sitio web.
- Introducir virus informáticos, archivos defectuosos, o alojar, almacenar, distribuir o compartir cualquier otro material o programa informático que pueda provocar daños o alteraciones en los contenidos, programas o sistemas de TUENTI.
- Usar el Servicio para el envío de publicidad o comunicaciones comerciales, para la emisión de mensajes con finalidad publicitaria o para la captación de datos con el mismo fin.
- Usar el Servicio, con independencia de su finalidad, para remitir correos electrónicos con carácter masivo y/o repetitivo no solicitados a una pluralidad de personas, ni mandar direcciones de correo electrónico de terceros sin su consentimiento.

- Captar o recopilar direcciones de correo electrónico u otra información de contacto de otros usuarios a través del Servicio de TUENTI con la finalidad de enviar correos electrónicos u otras comunicaciones no solicitados.
- Alojar, almacenar, divulgar, publicar, distribuir o facilitar publicidad no solicitada o no autorizada, ofrecimientos ilícitos, materiales promocionales, "correo basura", "spam", "cartas encadenadas", o comunicaciones similares.
- Registrar y usar el perfil con una finalidad económica, comercial o publicitaria.
- Crear Perfiles en nombre o para el beneficio de personas jurídicas (empresas entidades administrativas, organizaciones, asociaciones, partidos políticos, sindicatos, ONGs…etc).
- Instar, pedir o solicitar a otros usuarios, a través del Servicio de TUENTI, datos personales o solicitar contraseñas o datos de carácter personal.
- Crear una identidad falsa, suministrar y/o utilizar datos falsos en el perfil, realizar manifestaciones falsas, proporcionar información falsa sobre ti y sobre otras personas y/o tu relación con ellas.
- Registrar un perfil en nombre de otra persona, o cualquier otra modalidad de utilización de identidades ajenas y, en particular, la suplantación de personalidades.
- Usar el Servicio para organizar cualquier tipo de juegos de suerte, envite o azar cuya participación implique dinero u objetos valorables económicamente.
- Impedir el normal desarrollo de un evento, concurso, promoción o cualquier otra actividad disponible a través del Servicio o cualesquiera de sus funcionalidades, ya sea alterando o tratando de alterar ilegalmente su registro y/o, participación, falseando el resultado del mismo y/o utilizando métodos de participación fraudulentos, mediante cualquier procedimiento, técnico o informático, y/o que atente o vulnere en modo alguno las presentes Condiciones de uso. La realización de cualquiera de los anteriores comportamientos por tu parte, con o sin consideración económica, permitirá a TUENTI para, dependiendo de la gravedad y según su criterio, suspender o cancelar tu perfil de forma inmediata y, en su caso, para retirar contenidos en los perfiles que vulneren este catálogo de prohibiciones.

  En el caso de que TUENTI o una entidad patrocinadora/colaboradora de un evento, concurso, promoción o actividad disponible a través del Servicio detecten cualquier

anomalía o actuación fraudulenta o sospechen que un participante está tratando de impedir el normal desarrollo del mismo, podrán de forma unilateral y sin necesidad de previo aviso, eliminar la inscripción de ese participante, así como retirar el evento, concurso, promoción o actividad, y/o declarar el premio desierto.

En aplicación de lo recogido anteriormente, TUENTI podría suspender o cancelar tu perfil automáticamente sin previo aviso, y, en ningún caso, tal suspensión o cancelación te daría derecho a indemnización alguna. A todos estos efectos, te informamos que TUENTI podrá poner en conocimiento y colaborar oportunamente con las autoridades policiales y judiciales competentes si detectase cualquier infracción de la legislación vigente o si tuviera sospecha de delito.

SUPLANTACIÓN DE PERFILES

En relación con los casos de suplantación de personalidades, te advertimos que, en el momento en el que tengamos indicios de que has suplantado la personalidad de un tercero a través de tu perfil, procederemos a comprobar tu identidad y si has suplantado una identidad ajena borraremos tu perfil.

Si realizadas las debidas comprobaciones de tu identidad por parte de TUENTI comprobásemos que efectivamente habías llevado a cabo una suplantación de una identidad ajena y no pudiésemos certificar adecuadamente tu identidad, procederíamos a la cancelación definitiva de tu perfil.

Si en algún momento sabes que hay un perfil que es falso o tienes indicios de que puede ser falso por favor no dudes en enviarnos un correo a soporte@tuenti.com.

A todos estos efectos, te informamos que TUENTI podrá poner en conocimiento y colaborar oportunamente con las autoridades policiales y judiciales competentes si detectase una suplantación de identidad que pudiera implicar la comisión de un delito, en particular, del tipificado en el artículo 401 del Código Penal vigente.

PROPIEDAD INTELECTUAL E INDUSTRIAL DEL SERVICIO

TUENTI es el titular de todos los derechos de propiedad industrial e intelectual relativos al Servicio, a excepción de los contenidos de los Usuarios que les seguirán perteneciendo

conforme a lo establecido en el apartado siguiente, y a excepción de aquellos facilitados por terceros, tales como los juegos. Por las presentes Condiciones de Uso, TUENTI, como propietario del Servicio, te concede una licencia limitada, revocable y no sub-licenciable para usar el Servicio de forma estrictamente personal. A excepción de la licencia referida anteriormente, está prohibida cualquier forma de reproducción, distribución, comunicación pública, modificación y, en general, cualquier acto de explotación de la totalidad o parte de los contenidos (imágenes, textos, diseños, índices, formas, etc.) que integran el sitio web, así como de las bases de datos y del software necesario para la visualización o el funcionamiento del mismo, que no cuente con la expresa y previa autorización escrita de TUENTI.

No podrás, en ningún caso, explotar o servirte comercialmente, de forma directa o indirecta, total o parcial, de ninguno de los contenidos (imágenes, textos, diseños, índices, formas, etc.) que conformen el sitio web sin la autorización previa y por escrito de TUENTI. En caso de que infrinjas la presente licencia, TUENTI cancelará tu perfil, sin perjuicio de otras consecuencias que puedan derivarse de dicha infracción.

CONTENIDOS DE LOS PERFILES DE LOS USUARIOS

Al publicar contenidos en tu perfil -fotos, archivos, textos, vídeos, sonidos, dibujos, logos o cualquier otro material- conservas todos tus derechos sobre los mismos y otorgas a TUENTI una licencia limitada para reproducir y comunicar públicamente los mismos, para agregarles información y para transformarlos con el objeto de adaptarlos a las necesidades técnicas del Servicio. Esta autorización es mundial, no exclusiva (lo que significa que puedes otorgar otra licencia sobre tu contenido a cualquier persona o entidad, además de a TUENTI), por todo el tiempo que tengas vigente tu perfil y con la única y exclusiva finalidad de que TUENTI pueda prestarte el servicio en los términos explicados en estas Condiciones de uso.

La anterior licencia quedará resuelta una vez que elimines tu contenido del Servicio o des de baja tu perfil. A partir de ese momento, TUENTI interrumpirá la comunicación de tu contenido a la mayor brevedad posible.

En relación con el contenido que publiques en el Servicio, garantizas:

- Que eres el propietario o titular de los derechos que te permiten conceder a TUENTI la licencia para su publicación y que, en su caso, has obtenido de terceros el consentimiento necesario para ello.
- Que no vulnera leyes aplicables tales como las relativas al derecho a la intimidad, a la imagen y/o al honor, derechos de propiedad intelectual o industrial o similares ni ningún derecho de un tercero, ya sea una persona o una entidad.
- Que en caso de publiques datos de carácter personal de alguno de tus amigos o de otra persona, les has informado y obtenido previamente su consentimiento para la publicación de dichos datos.

Por ello, responderás frente a TUENTI de la veracidad de lo afirmado, manteniendo indemne a TUENTI ante cualquier demanda o reclamación presentada por un tercero en relación a las anteriores afirmaciones y en relación a cualquier derecho legítimo sobre el contenido que hayas publicado en el Servicio.

NOTIFICACIÓN DE INFRACCIÓN DE DERECHOS

En TUENTI velamos por la protección de los derechos de sus titulares por lo que, si cualquier persona o entidad detecta que sus contenidos han sido publicados en el Servicio sin su consentimiento, generando una infracción de derechos de propiedad intelectual o industrial y/o de derecho al honor, intimidad o a la imagen o de cualquier otro derecho, podrá comunicarlo a TUENTI, enviando un email a soporte@tuenti.com o bien mediante correo postal a la dirección que consta al final de estas Condiciones de Uso y Política de Privacidad Y Protección de Datos Personales (con el asunto en el caso del email o la referencia expresa en correo postal "Infracción de Derechos") y acompañando la siguiente información:

- Identificación del contenido o datos personales o derecho protegido que ha sido vulnerado.
- Identificación del citado contenido de forma suficiente para que en TUENTI podamos ubicarlo dentro del Servicio.
- Identificación suficiente para que TUENTI pueda contactar con el reclamante: correo electrónico y teléfono.

- Copia de su D.N.I, pasaporte o documento oficial similar que permita su identificación.
- Una declaración firmada en la que el reclamante manifieste que la información anterior es veraz y que afirme ser el legítimo titular (o bien que está autorizado a actuar en su nombre) de los derechos presuntamente vulnerados.

CONDICIONES DE USO DE TUENTI SITIOS

- TUENTI Sitios es una funcionalidad que se ofrece de forma gratuita a los usuarios TUENTI para que compartan opiniones y contenidos sobre sitios de ocio tales como restaurantes, bares, comercios, pubs, museos y similares.
- Los usuarios de TUENTI pueden participar en la creación de nuevos “sitios” mediante el proceso de alta desde la página de cualquier sitio o desde "Mi cuenta".
- Los usuarios de TUENTI podrán comentar, publicar fotos y hacer referencias sobre los “sitios” así como valorar las opiniones ya existentes sobre el “sitio”.
- TUENTI no censura ningún tipo de opinion siempre que sea respetuosas y educada. Sin embargo, si TUENTI detecta comentarios o contenidos prohibidos por las Condiciones de Uso y la Política de Privacidad de TUENTI así como algún ilícito, lo eliminará de inmediato.
- TUENTI no se hace responsable de los contenidos, opiniones e imágenes que aparezcan en los “sitios”. En cualquier caso, si TUENTI es informado de que existe cualquier contenido inapropiado o ilícito, procederá a su eliminación de forma inmediata.
- Los usuarios que compartan contenido en “sitios” garantizan que poseen todos los derechos y permisos necesarios para su publicación, manteniendo indemne a TUENTI de cualquier reclamación de tercero en este sentido.
- Los usuarios que compartan contenido en "sitios" consienten de forma expresa que dicho contenido pueda ser visto tanto por usuarios de TUENTI como por terceros, sin qie dichos contenidos sean asociados de manera alguna a datos personales de los usuarios.
- TUENTI Sitios ofrece el servicio de "Checkin" a sus usuarios. Con este servicio, los usuarios de TUENTI podrán determinar su localización mediante dispositivos móviles para poder contactar con sus amigos así como para compartir opiniones y reseñas de los

"sitios" que están visitando. Al acceder a TUENTI Sitios "Checkin", permitirás al TUENTI y a tus amigos conocer tu localización. Esta información es necesaria para el funcionamiento del Servicio. TUENTI no hará seguimiento de tu información de geo-localización.

- TUENTI Sitios podrá facilitar productos, servicios y/o funcionalidades específicas para usuarios que sean propietario/s de un “sitio”.
- Los usuarios que reclamen ser propietarios de un “sitio”, garantizan que poseen todos los derechos y permisos (incluyendo, entre otros, su poder de representación, así como ser mayores de edad) necesarios para la administración del “sitio”, manteniendo indemne a TUENTI de cualquier reclamación de tercero en este sentido. TUENTI podrá solicitar al usuario información adicional para la verificación de su condición de propietario y en caso de no facilitarse dicha información, TUENTI podrá denegar o desvincular al usuario del “sitio”. En caso de que se aporten datos de carácter personal, su tratamiento se regirá por lo dispuesto en la Política de Privacidad y de Protección de Datos Personales de TUENTI.
- Los usuarios con perfil de propietarios de un “sitio”, podrán acceder a diferentes funcionalidades desde su perfil de TUENTI, quedando en todo caso obligados al cumplimiento de las presentes Condiciones particulares y generales de uso, con especial incidencia en las prohibiciones del apartado de usos no permitidos, propiedad intelectual e industrial, perfiles falsos, etc.
- TUENTI Sitios podrá ampliar, modificar, reducir o eliminar en cualquier momento y a su propia discrecionalidad, las funcionalidades de TUENTI Sitios, tanto para usuarios de TUENTI como usuarios propietarios.

CONDICIONES DE USO DE PÁGINAS TUENTI

- TUENTI Páginas es una funcionalidad que se ofrece de forma gratuita a los usuarios TUENTI para interactuar alrededor de sus intereses, actividades y ordenar nuestras preferencias en cuanto a organizaciones, bandas de música o sensibilidades sociales.
- En TUENTI Páginas encontrarás instituciones, marcas comerciales, ONG's y similares administrados por representantes reales que tendrán un espacio de comunicación con los usuarios de TUENTI.

- Adicionalmente, los usuarios de TUENTI podrán crear sus propias Páginas relacionadas con sus intereses para compartir fotografías, comentarios o incluso vídeos.
- TUENTI no se hace responsable de los contenidos, opiniones e imágenes que aparezcan en los "Páginas". En cualquier caso, si TUENTI es informado de que existe cualquier contenido inapropiado o ilícito, procederá a su eliminación de forma inmediata.
- Los usuarios que compartan contenido en "Páginas" garantizan que poseen todos los derechos y permisos necesarios para su publicación, manteniendo indemne a TUENTI de cualquier reclamación de tercero en este sentido.
- Los usuarios que compartan contenido en "Páginas" consienten de forma expresa que dicho contenido pueda ser visto tanto por usuarios de TUENTI.

CONDICIONES DE USO DE TUENTI JUEGOS

TUENTI Juegos es un espacio donde el Usuario puede acceder a juegos ofrecidos por terceros. TUENTI es un mero intermediario respecto a los juegos que se anuncian y están disponibles desde dicho espacio. Los juegos, así como sus funcionalidades, características y, en su caso, la compra de bienes virtuales son provistos y gestionados por terceras empresas, que son los únicos responsables por la prestación de dichos juegos y funcionalidades. TUENTI únicamente ofrece a los Usuarios acceso a dichos juegos y funcionalidades. En particular, los juegos que se anuncian en el espacio de juegos de TUENTI son ofrecidos y operados por Metrogames y Viximo. La empresa que pone a disposición de los Usuarios de TUENTI y gestiona los medios de pago utilizados para la compra de bienes virtuales en los diferentes juegos es Viximo. Al ser los juegos titularidad de estas terceras empresas, el acceso y utilización de los mismos está sujeto a los términos y condiciones de dichas empresas. Por favor, lee sus respectivas condiciones de uso http://www.metrogames.com/terms.html y http://viximo.com/terms_of_service. El acceso a determinados juegos o a determinadas funcionalidades dentro del juego puede estar restringido por estos proveedores para determinados usuarios, tales como menores de edad o aquellos que no cumplan determinados requisitos. En todo caso, la primera vez que accedas a un juego podrás ver el nombre del proveedor de dicho juego, y los términos y condiciones de dicho proveedor que se aplican al juego en cuestión.

La participación en los juegos disponibles desde TUENTI será siempre gratuita. En su caso, el Usuario puede adquirir bienes virtuales en el entorno de TUENTI (los "Créditos TUENTI") que los Usuarios podrán utilizar en conexión con los juegos, en la forma en que cada proveedor de juegos permita. En ningún caso, los Créditos TUENTI serán reembolsables o intercambiables por dinero real. TUENTI simplemente ofrece los "Créditos TUENTI" como puntos que sólo pueden ser utilizados en los juegos disponibles desde TUENTI, y en ningún caso son, ni serán considerados como, dinero real.

Dichos "Créditos TUENTI" y todos los bienes virtuales forman parte inseparable, se adquieren por y para su utilización con y dentro del entorno de TUENTI y/o de los juegos a los que se puede acceder desde el entorno de TUENTI.

En caso de que aceptes los términos y condiciones de uso de los juegos que los proveedores de dichos juegos han puesto a tu disposición, entiendes que TUENTI en ningún caso controla ni puede controlar dichos juegos ni la utilización de Créditos TUENTI dentro de los mismos, y que el respectivo proveedor de juegos es el único responsable de cualquier incumplimiento o fallo que dichos juegos o contenidos asociados puedan sufrir.

TUENTI no se hace responsable de los contenidos, opiniones e imágenes proporcionados por los Usuarios, que aparezcan en los juegos. En cualquier caso, si TUENTI es informado de que existe cualquier contenido inapropiado o ilícito, procederá a su eliminación de forma inmediata.

TUENTI se reserva la facultad de retirar cualquier juego sin previo aviso.

Los Usuarios que soliciten los servicios de juegos, permitirán a los proveedores de juegos el acceso a su información. TUENTI le comunicará y/o permitirá el acceso de Metrogames US Inc. (100 West Evelyn Av., Suite 110; Mountain View, California 940041, US) y de Viximo, Inc. (1 Camp Street Suite 100, Cambridge, MA 02140 USA) a la información de tu perfil, fotografías, la información de tus amigos, tu dirección IP y cualquier otro contenido que se necesite para el funcionamiento de las aplicaciones.

Los usuarios, al registrarse en los juegos, consienten de forma expresa que al permitir el acceso a su información (que contiene datos de carácter personal), ésta podrá ser comunicada a los servidores de los proveedores de servicios ubicados en Estados Unidos de América.

En algunos de los juegos podrás adquirir bienes virtuales (los “Créditos TUENTI”). Estos bienes virtuales podrán ser abonados a través de la pasarela de pago de una tercera empresa, Viximo, cuyas condiciones de uso se mencionan en apartados anteriores. En caso de que aceptes sus condiciones de uso, entiendes que Viximo es el único responsable de cualquier incumplimiento o fallo que dicha pasarela de pago pueda sufrir.

El precio de cada uno de los bienes virtuales vendrá determinado en el juego donde sea exhibido, de acuerdo con lo que cada proveedor de juegos establezca, así como en su caso, los impuestos aplicables. TUENTI no se hace responsable de dicho precio, así como tampoco del valor que se asigne a los "Créditos TUENTI" y demás cuestiones relacionadas con los medios de pago.

Para la adquisición de "Créditos TUENTI" se facilitarán diversas formas de pago a través de la propia pasarela de pago. Tus datos de usuario y de la compra serán introducidos y transmitidos directamente por ti a la entidad titular de la pasarela de pago, Viximo. TUENTI bajo ninguna circunstancia accede, retiene, ni facilita dichos datos a ningún tercero.

Los usuarios, al registrarse en la pasarela de pago de Viximo, consienten de forma expresa que TUENTI facilite o permita el acceso a cierta información (susceptible de contener datos de carácter personal), la cual podrá ser comunicada a los servidores de Viximo en Estados Unidos de América.

Podrás obtener mayor información sobre tus derechos de acceso, rectificación, cancelación u oposición en estas Condiciones de Uso y en la Política de Privacidad y de Protección de Datos Personales.

EVENTOS Y ACTIVIDADES PROMOCIONALES

Dentro de la página dispones de un espacio denominado "Mis eventos" en el que podrás colgar información sobre cualquier acontecimiento tuyo y, además, podrás invitar a tus amigos dentro de la red de TUENTI a que participen en tus eventos personales, por ejemplo, tu fiesta de cumpleaños.

Además de los eventos personales, TUENTI puede realizar actividades promocionales de diversa índole. A título de ejemplo, existen los denominados "eventos patrocinados", que son actividades promocionales realizadas por un profesional o empresa con las que

TUENTI colabora. Estos eventos funcionan de idéntico modo a los eventos personales, con la salvedad de que es TUENTI quien te los propone e invita a que te agregues en virtud de su colaboración con las empresas y profesionales. La participación en estos eventos se regirá por los mismos usos y pautas de comportamiento exigidas en el Servicio y contempladas por estas Condiciones de uso. Cuando señales que vas o que quizás vayas a un evento, debes saber que otros usuarios de TUENTI que pueden ver el evento, se hayan unido o no al evento, podrán saber que vas a ir o, en su caso, que quizás vayas al evento.

En este sentido, la participación en posibles eventos, concursos, promociones o cualesquiera otras actividades disponibles a través del Servicio organizadas por terceras empresas colaboradoras de TUENTI, implicará la aceptación de las condiciones particulares de cada una de dichos eventos, concursos, promociones y/o actividades. Con carácter general se informa de que la participación en estos eventos, concursos, promociones y/o actividades puede estar sujeta a requisitos adicionales de los participantes(edad, lugar de domicilio, etc.), y la entrega de los premios a los ganadores de cualquiera de las promociones organizadas por terceras empresas colaboradoras de TUENTI puede encontrarse supeditada al cumplimientos de determinadas condiciones.

De la misma forma, al actuar TUENTI como simple intermediario, las posibles reclamaciones relacionadas con eventos, concursos, promociones o cualesquiera otras actividades disponibles a través del Servicio organizadas por terceras empresas colaboradoras de TUENTI, deberán dirigirse directamente contra las éstas empresas, no siendo TUENTI responsable, directo o indirecto, en caso de cualquier fallo, error o, en general, incumplimiento de dichas empresas colaboradoras respecto de los eventos, concursos, promociones o cualesquiera otras actividades disponibles a través del Servicio organizadas por las mismas, siendo éstas empresas las exclusivas responsables.

RESPONSABILIDAD POR INTERACCIONES CON OTROS USUARIOS

Tú eres el único responsable de las interacciones que tengas con otros usuarios de TUENTI. Nosotros no controlamos tus relaciones personales, lo que sí te recomendamos es que elijas bien a tus amigos y a las personas que unes a tu red. Por supuesto, si alguien te acosa, molesta o intimida, debes comunicárnoslo inmediatamente para que adoptemos las medidas oportunas.

TUENTI no se hará responsable de aquellos conflictos que pudieras tener con otros usuarios y que no impliquen incumplimiento de las presentes Condiciones de uso por ninguno de vosotros, por ejemplo en el caso de la posible compraventa de productos entre usuarios. TUENTI no estará obligado y no será responsable de ello, pero se reserva el derecho a mediar en los posibles conflictos que surjan.

PUBLICIDAD

Conoces y aceptas que hay publicidad en el Servicio y que, por tanto, desde tu perfil podrás acceder a publicidad que terceras empresas y profesionales contraten con TUENTI.

INVITACIONES, RECUPERACIÓN DE CONTRASEÑAS Y OTRAS NOTIFICACIONES

TUENTI podrá poner a tu disposición un servicio de notificaciones a tu correo electrónico para que conozcas los movimientos que hay en tu perfil y en la red de tus amigos de TUENTI. Siempre tendrás todo el control sobre si recibes o no este tipo de notificaciones desde el parte de "Preferencias" dentro de la página.

Este servicio de notificaciones no afectará a las comunicaciones que TUENTI pueda hacerte para:

- Recuperar tu contraseña, en el caso que haya sido olvidada.
- Enviarte invitaciones para que puedas enviar a nuevos amigos.
- Cambiar tu cuenta de correo electrónico.

Conoces y aceptas que estos tipos de comunicaciones y cualesquiera otras de naturaleza similar son necesarias y, por tanto, forman parte del Servicio.

Como Usuario de TUENTI podrás invitar a amigos para que se unan a TUENTI. Basta con que le envíes una invitación a tu amigo a su correo electrónico a través del sistema de invitación automático de TUENTI. Esta invitación es un simple vehículo que TUENTI pone a tu disposición para que, si quieres, puedas ofrecer a tus contactos la posibilidad de registrarse en TUENTI. El envío de esta invitación no implica que tu amigo aparezca registrado en TUENTI automáticamente.

Tu amigo tendrá que aceptar la invitación y cumplir con el proceso de registro de Usuario de TUENTI.

TUENTI no hará uso de los datos que señales en la invitación y especialmente de la cuenta de correo de tu amigo. Serás tu quien respondas frente a tu amigo si hay cualquier tipo de reclamación contra TUENTI.

Cuando invites a otros a unirse a TUENTI, tú responderás frente al destinatario de tu invitación por cualquier reclamación que éste pudiera efectuar a TUENTI exonerando a esta última de toda responsabilidad que pudiera derivarse de dicha invitación.

USO DE ENLACES

QUEDA PROHIBIDO EL USO de cualesquiera recursos técnicos, lógicos o tecnológicos en virtud de los cuales alguien, usuario o no de TUENTI, pueda beneficiarse, directa o indirectamente, con o sin lucro, de los perfiles y de los contenidos del sitio web.

Nadie podrá insertar en su web, blog, foro, perfil de TUENTI o de cualquier red social, un link, hyperlink, framing o vínculo similar que redireccione a URLs de contenidos de TUENTI y/o perfiles de TUENTI. Si TUENTI detectara algún enlace de estas características que pudiera vulnerar los derechos a la intimidad, el honor y la propia imagen de sus usuarios, estará plenamente legitimada para actuar con el fin de eliminar ese enlace y, en su caso, ponerlo en conocimiento de las autoridades competentes.

SERVICIO MOVIL DE TUENTI

Todo lo dispuesto en estas Condiciones de uso será aplicable a los accesos que hagas al Servicio a través del teléfono móvil.

A este respecto, tienes que tener en cuenta que nosotros no cobramos por el acceso móvil al Servicio, pero que tu operador de telefonía móvil te aplicará la tarifa que tengas contratada para el envío y recepción de datos.

TUENTI no se hace responsable de las restricciones que el operador móvil pueda tener impuestas y que pudieran hacer que el Servicio no funcionara con normalidad. Asimismo,

tú eres responsable de conocer si tu operador móvil, tus servicios contratados y tu terminal móvil son los idóneos para el acceso al Servicio.

MODIFICACIONES

TUENTI podrá sustituir, en cualquier momento, por motivos técnicos o por cambios en la prestación del Servicio o en la normativa, así como modificaciones que pudieran derivarse de códigos tipo aplicables o, en su caso, por decisiones corporativas estratégicas, las Condiciones de uso y la Política de Privacidad y Protección de datos y que, según los casos, sustituirán, completarán y/o modificarán las Condiciones de uso y Política de Privacidad aquí recogidas.

Cuando TUENTI sustituya o modifique las Condiciones de uso o la Política de Privacidad y Protección de datos, te avisaremos de ello a través del sitio web y si, una vez te hemos informado de ello, continúas utilizando el Servicio, entenderemos que has aceptado las modificaciones introducidas. Si no estuvieras de acuerdo con las modificaciones efectuadas, podrás darte de baja en el servicio siguiendo el procedimiento habilitado para ello.

LEY APLICABLE Y JURISDICCIÓN

La normativa vigente determinará las leyes que deban regir y la jurisdicción que deba conocer de las relaciones entre TUENTI y los Usuarios del Sitio Web. Ello no obstante, en aquellos casos en los que dicha normativa vigente prevea la posibilidad para las partes de someterse a un fuero determinado, TUENTI y el Usuario, con renuncia expresa a cualquier otro fuero que pudiera corresponderles, se someten a los Juzgados y Tribunales de la ciudad de Madrid.

POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

Para poder ser Usuario de TUENTI, y tener tu perfil en TUENTI, es necesario que leas nuestra Política de Protección de Datos Personales y nos des tu consentimiento a través de la casilla que aparece en este formulario de registro para que podamos tratar tus datos.

Nuestra Política de Protección de Datos Personales afecta a todos los datos personales que nos aportes al registrarte, así como a todos aquellos que nos facilites durante el tiempo que tengas vigente tu perfil, para acceder a cualquiera de los servicios (presentes y/o futuros) de TUENTI.

USUARIO Y PERFILES

TUENTI es una plataforma social privada que facilita la comunicación entre tus amigos y tú. Permite saber qué cosas están pasando a tu alrededor y te ayuda a conectar con tus amigos y a hacer contactos de todo tipo de redes como el colegio, universidad, trabajo, zonas de marcha y demás.

Para poder ser Usuario de TUENTI es necesario que antes hayas recibido en tu correo electrónico una invitación de un amigo que ya sea Usuario de TUENTI.

Una vez que hayas aceptado la invitación de tu amigo, es necesario que te registres y para ello deberás rellenar el formulario con los siguientes datos personales reales:

- Nombre y Apellidos.
- Si estás en el colegio, en la Universidad o trabajando.
- Fecha de nacimiento.
- Provincia de residencia.
- E-mail.

Si quieres, podrás dar voluntariamente a TUENTI más información relacionada contigo, como, por ejemplo, dirección, teléfono, tus gustos, aficiones, zonas de marcha o similares.

Esta información estará disponible y podrá ser modificada por ti a través de tu perfil.

Tener un perfil en TUENTI supone que tienes que ser tú en todo momento y que no te puedas hacer pasar por nadie. Tienes que ser totalmente responsable y debes introducir tus datos reales y veraces. Desde TUENTI procuraremos comprobar la veracidad de tus datos, y nos reservamos, sin perjuicio de otras acciones, el derecho a no registrarte o a darte de baja si los datos que nos has facilitado son falsos o incompletos. La obligación de tener un perfil real es esencial en TUENTI. Asimismo, te informamos de que en TUENTI, como plataforma social privada, nos reservamos el derecho de admisión, teniendo la

facultad de cancelar unilateralmente los perfiles que no nos parezcan adecuados por su contenido en relación con el Servicio.

Cuando te registras en TUENTI, tienes un perfil TUENTI en el que cuelgas y compartes, como quieras, y con quién desees, tu información personal real. La información personal será compartida en TUENTI con las condiciones de privacidad que tú mismo elijas y bajo tu exclusivo control.

Te corresponde a ti controlar, en todo momento, tu información personal por eso te pedimos y recomendamos que seas cuidadoso con la información personal que compartes y con quién la compartes. Además, como Usuario de TUENTI nos tienes que informar de cualquier cambio que se produzca en los datos que nos has dado. Puedes acceder a "Mi cuenta","Información personal" y realizar los cambios que quieras.

INVITACIONES

Como Usuario de TUENTI podrás invitar a amigos para que se unan a TUENTI. Basta con que le envíes una invitación a tu amigo a su correo electrónico a través del sistema de invitación automático de TUENTI. Esta invitación es un simple vehículo que TUENTI pone a tu disposición para que, si quieres, puedas ofrecer a tus contactos la posibilidad de registrarse en TUENTI. El envío de esta invitación no implica que tu amigo aparezca registrado en TUENTI automáticamente.

Tu amigo tendrá que aceptar la invitación y cumplir con el proceso de registro de Usuario de TUENTI.

TUENTI no almacenará los datos que señales en la invitación, y especialmente de la cuenta de correo de tu amigo, la cual será utilizada única y exclusivamente para lanzar tu invitación. Serás tú quien respondas frente a tu amigo si hay cualquier tipo de reclamación contra TUENTI.

Como Usuario deberás hacer un uso adecuado del sistema de invitaciones de acuerdo con lo previsto en las Condiciones de uso.

EDAD MÍNIMA PARA TENER PERFIL

Es muy importante que sepas que sólo puedes ser Usuario de TUENTI si eres mayor de 14 años. Como mayor de 14 años eres responsable de la edad que dices tener.

El equipo de TUENTI puede ponerse en contacto contigo, en cualquier momento, para que demuestres tu edad real aportándonos fotocopia de tu DNI o un documento equivalente. Si no nos das esa información dentro del plazo que te digamos, desde TUENTI nos reservamos el derecho a bloquear o cancelar tu perfil.

Los datos del DNI o del documento que se aporte serán utilizados única y exclusivamente por el personal autorizado de TUENTI para realizar esta tarea de identificación, en ningún caso, se almacenará o tratará para otro fin.

Si tienes entre 14 y 18 años, te recomendamos que informes y consultes con tus padres o tutores legales a la hora de transmitir información a terceros con los que hayas contactado a través del Servicio.

Si somos informados de que un menor está registrado como Usuario en TUENTI, adoptaremos las medidas necesarias y podremos eliminar o bloquear el perfil de Usuario.

Te pedimos que cualquier abuso o vulneración de las presentes condiciones que detectes y, en particular, aquellos que afecten a menores, nos lo digas inmediatamente a través de soporte@tuenti.com.

NIVELES DE PRIVACIDAD

TUENTI pone a tu disposición niveles de privacidad para garantizar la seguridad de tus datos. De esta manera, serás tú quién, bajo tu exclusiva responsabilidad decidas, por tu cuenta y riesgo, quién tiene acceso a tu información personal.

Como Usuario de TUENTI podrás controlar en todo momento la privacidad de tu perfil y sus diferentes elementos; tus fotos, tu tablón, la recepción de mensajes y/o la visibilidad de tus números de teléfono. A continuación te señalamos cómo controlar tu privacidad en diferentes niveles atendiendo al tipo de contenido y en función de tres categorías. Tú eres el único responsable del nivel de privacidad que elijas.

El primer nivel de privacidad que TUENTI te ofrece afecta a tu perfil y tus fotos y podrás elegir entre estas categorías:

Sólo mis amigos. Supone que sólo los amigos que tú hayas seleccionado tendrán acceso a tus datos e información de tu perfil.

Sólo hasta amigos de mis amigos. Supone que los amigos que tu hayas seleccionado, y los amigos seleccionados por cada uno de ellos, tendrán acceso a tus datos y a la información de tu perfil.

Todos los miembros de TUENTI. Supone que todas las personas con perfil en TUENTI tendrán acceso a tus datos y a la información de tu perfil.

Adicionalmente, te ofrecemos un nivel más de privacidad, donde podrás controlar quién puede enviarte mensajes y postear en tu tablón dentro de las tres categorías anteriormente señaladas: Sólo mis amigos, Sólo hasta amigos de mis amigos o Todos los miembros de TUENTI.

Igualmente, en un nivel de privacidad más, podrás decidir quién puede ver tus números de teléfono dentro de las tres categorías mencionadas: Sólo mis amigos, Sólo hasta amigos de mis amigos o Todos los miembros de TUENTI.

De forma complementaria y compatible con los anteriores niveles de privacidad escogidos, podrás optar por no permitir que nadie que vea tu tablón y/o que nadie pueda descargar tus fotos. Asimismo, tendrás la posibilidad de bloquear a Usuarios no deseados.

En caso de que TUENTI añadiese niveles de privacidad adicionales, serás oportunamente informado de ello conforme a lo aquí establecido. TUENTI no será responsable, en ningún caso, de cualquier reclamación relacionada con los controles de seguridad elegidos y con el acceso a tu información por parte de otros Usuarios.

TUENTI no controla y, por tanto, no asume ninguna responsabilidad en la posible recogida y tratamiento de información de Usuarios por parte de otros Usuarios o por terceros.

Además, tienes que saber que en TUENTI hay un buscador que te permite buscar a otros Usuarios miembros de TUENTI. En las búsquedas generales que los Usuarios registrados realicen por los perfiles de TUENTI, no se tiene acceso a la información del perfil de los Usuarios. En estos casos, la única información que se comparte totalmente y se muestra como presentación será el nombre del Usuario, las redes a las que perteneces, y, en su caso, la foto que el Usuario decida colgar como foto principal. Esta misma información

también será accesible dentro de los eventos, en relación a los usuarios que hubieran indicado su intención de acudir o "quizás acudir" al evento.

TRATAMIENTO DE DATOS PERSONALES Y PUBLICIDAD

Los datos que aportas en el proceso de registro a TUENTI los incluimos en la base de datos de Usuarios de la cual hemos informado a la Agencia Española de Protección de Datos.

Para tu información, la Agencia Española de Protección de Datos es una entidad que se encarga de velar por el cumplimiento de las leyes que protegen los datos personales y garantizar la seguridad y privacidad de los datos.

Si recogemos tus datos y los tratamos es para poder identificarte como Usuario de TUENTI, darte acceso a TUENTI y poner a tu disposición todas las facilidades y aplicaciones de nuestra plataforma social privada. Además, te mantendremos informado a través de la propia red de todas las novedades que surjan sobre TUENTI.

Además, visualizarás en la red información de empresas con las que TUENTI colabora.

También podrás acceder en tu red a eventos patrocinados. Estos eventos, son actividades patrocinadas por una empresa con la que TUENTI colabora y en los que, si estás interesado, puedes participar.

Como Usuario de TUENTI tienes derecho a poder acceder a tus datos personales para saber cómo los tratamos y con que finalidad y decirnos si te opones a que usemos tus datos para una actividad concreta. Además, podrás rectificar tus datos si ves que no son correctos e incluso podrás pedirnos que los cancelemos si no quieres ser Usuario de TUENTI.

Para todo ello tendrás que contactar con nosotros enviándonos un correo electrónico a soporte@tuenti.com. Te informamos que para poder hacer cualquiera de las acciones que te hemos señalado te pediremos el DNI u otro documento que te identifique para asegurarnos y comprobar que eres tú quien se ha puesto en contacto con nosotros.

CONTENIDOS E INFORMACIÓN PERSONAL

Además de datos personales, podrás compartir en tu perfil textos, fotos, vídeos… y otro tipo de información que estará sujeta a las Condiciones de Uso de TUENTI.

TUENTI no controla la información que compartes con otros Usuarios y por tanto no nos hacemos responsable de esa información. No obstante, si sabes que hay una información o contenido en TUENTI que pueda ser indebido y ser contrario a nuestra Política de Protección de Datos Personales y nuestras Condiciones de Uso ponte en contacto con nosotros por correo electrónico a soporte@tuenti.com.

BAJA EN TUENTI

Puedes desactivar de forma temporal tu perfil o bien darlo de baja de forma definitiva siguiendo los siguientes pasos:

- Para desactivar tu cuenta en TUENTI sólo tienes que entrar en "Mi cuenta" > "Preferencias de mi cuenta" y pulsar el botón "Desactivar cuenta" que encontrarás al final de la página.
- Para dar de baja de forma definitiva tu cuenta en TUENTI, entra en la sección de "Ayuda" (en la parte inferior derecha de la página) > "Preferencias de mi cuenta" > "¿Cómo puedo dar de baja mi cuenta?" Ten en cuenta que, si eliges esta opción, perderás toda la información de tu cuenta (amigos, fotos, comentarios en el tablón, etc.).

  Para cualquier duda que tengas puedes contactar con nosotros enviándonos un correo electrónico a soporte@tuenti.com.

COOKIES

Como sabes, las cookies son pequeños ficheros de datos que se alojan en el ordenador del Usuario de TUENTI y que contienen cierta información de la visita que haces a la página web.

TUENTI utiliza cookies con el fin de facilitar tu navegación. En ningún caso, es posible asociar las cookies a tus datos personales concretos, ni identificarte a través de ellas. Además, como Usuario tienes la posibilidad de desactivar las cookies a través de tu navegador.

10.-CONTROLES PARENTALES, COMO VIGILAR A QUE CONTENIDOS DE INTERNET ACCEDEN NUESTROS HIJOS

Las nuevas tecnologías están a la orden del día entre los más pequeños. Tal es así, que no nos sorprendemos al ver a niños1 enseñando a sus mayores a utilizar el DVD, la cámara digital, su nuevo móvil o incluso a navegar por la Red sin que aparentemente nadie les haya enseñado previamente. Nuestros niños y adolescentes son la generación de las nuevas tecnologías. Son la generación de Internet.

Internet se ha convertido en un medio para informarse, para aprender, para comunicarse, para jugar, para acceder a casi una infinitud de archivos, programas, etc. y satisfacer nuestras necesidades de conocimiento y ocio. No obstante, del mismo modo que son innegables los beneficios que nos brinda Internet, existen aspectos menos favorables que debemos conocer y prevenir, y en especial, cuando éstos afectan a los menores.

En este sentido, tanto los padres como los educadores están preocupados por la facilidad con la que los menores pueden acceder a contenidos poco apropiados2. Frente a este *todo vale*, se puede y se debe actuar desde una doble vertiente. Por una parte, luchar desde las instituciones del Estado contra los contenidos ilícitos (que no inapropiados) y los comportamientos delictivos que pululan por la Red. En segundo lugar, desde la educación y concienciación a nuestros menores sobre las claves para una navegación segura y responsable.

Según el estudio *Seguridad infantil y costumbres de los menores en Internet3,* el 54% de los menores no ha recibido formación alguna sobre las normas básicas de seguridad frente a un 45% que afirma conocer dichas reglas. Además, el informe señala que el 86% de los menores usuarios accede a la Red desde ordenadores que no cuentan con ningún sistema de filtrado de contenidos y que entre el 28% y el 38% de los menores, accede a contenidos inconvenientes o nocivos (destacar que el porcentaje aumenta con la edad).

¿A qué tipo de contenidos podrían acceder nuestros hijos?

Hablar con menores de ciertos temas no siempre es una tarea fácil, y todavía menos si tenemos en cuenta que los adolescentes suelen ser muy recelosos cuando se abordan asuntos que, en su foro interno, consideran un ataque contra su intimidad. En particular aquellos que hacen referencia a sus amigos, a qué contenidos acceden, al número de horas que pasan ante el ordenador, con quién se mandan innumerables mensajes, etc.

El pasado mes de octubre se publicó el libro *Cómo controlar lo que hacen tus hijos con el ordenador: Técnicas de hacker para padres5*, de la autora valenciana Mar Monsoriu, según la cual, *"cuando la comunicación falla, la alternativa que le queda a los padres es convertirse en un verdadero espía informático"*. Pero convertirse en espía no es la única solución frente a los contenidos nocivos y/o inapropiados que los menores pueden encontrarse; del mismo modo que tampoco es solución vetarles el acceso.

Pero, ¿a qué tipo de contenidos podrían acceder nuestros hijos? Los ***contenidos ilícitos*** son aquellos contenidos que vulneran la norma penal, es decir, que su publicación en la Red puede llevar (y de hecho lleva) asociado un delito. Como ejemplo de este tipo de contenidos podemos nombrar la pornografía infantil, pederastia, estafa informática, racismo, xenofobia. Todos ellos son contenidos perseguidos por la ley y que por tanto si tenemos noticia de ellos se deben denunciar inmediatamente ante los cuerpos y fuerzas de seguridad del Estado que trabajan en la persecución de este tipo de delincuentes y en la eliminación de la Red de dichos contenidos. No obstante, la acción contra los mismos es complicada pues en numerosas ocasiones, se encuentran alojados en otros países y cada país tiene su propia definición de ilegalidad de contenidos.

Cuando se hace referencia a los ***contenidos inapropiados*** la definición es mucho más sencilla. Si entendemos como contenidos apropiados aquellos comúnmente denominados como "para todos los públicos", por exclusión, los contenidos inapropiados hacen alusión a contenidos que, si bien no vulneran la ley, pueden resultar ofensivos o nocivos para determinadas personas, en este caso menores. Así, son contenidos *no aptos6* (pornografía, drogas, violencia, juegos de azar, etc). En cualquier caso son *per se* difícilmente objetivables ya que ante un mismo caso, lo que para unos padres resulta que no es apropiado para su hijo, otros pueden pensar que su hijo "ya tiene edad para ver

ciertas cosas”. Es por ello que éstos son los contenidos de los que se ocupan las técnicas de filtrado que más adelante se exponen.

Filtrado de contenidos

Para solventar estos problemas, han salido al mercado diferentes sistemas de control parental de los contenidos. Así, sistemas operativos como *Windows Vista* y *Mac OS X 0.5 Leopard* ya cuentan con controles parentales incorporados; ambos, con sus ventajas y con sus limitaciones. Los dos sistemas incorporan, dentro de su ***control parental***, diferentes opciones como son: límites de tiempo y contenidos, determinación de juegos y programas ejecutables,...Además, los diferentes proveedores de Internet, por una pequeña cuota adicional, ofrecen también algún tipo de filtrado de contenidos.

Pero los controles parentales no sólo aparecen en los diferentes sistemas operativos, sino que hay multitud de programas (tanto gratuitos como bajo licencia de pago) que permiten diferentes **técnicas de filtrado**.

1. Control del tiempo: se ofrece la posibilidad de determinar el tiempo que el menor puede estar conectado a Internet; la limitación podemos realizarla por horas y días por semana. Resulta muy útil cuando no queremos que el niño se pase *las horas muertas* delante del ordenador y también ayuda a determinar el tiempo de conexión de los niños que están solos en casa.

2. Bloqueo de palabras clave: Consiste en bloquear las páginas que contengan aquellas palabras que creamos que llevan asociadas contenidos inapropiados (sexo, apuestas, drogas, casino,...). Tiene una pega y es que con ésta técnica se pueden producir numerosos “falsos positivos”, es decir, corremos el peligro de bloquear contenidos que pueden no ser nocivos para los menores ya que se bloquean las palabras aisladamente, sin tener en cuenta el contexto en el que se hayan integradas.

3.Registros: Realiza un recuento de las páginas que han sido visitadas o a las que se ha intentado visitar. Sirve para revisar y comprobar los hábitos de navegación de los menores.

Esta técnica no precisa que el menor sea consciente de que los contenidos están siendo limitados, pero como ya hemos comentado con anterioridad, la base de una navegación segura es el diálogo entre padres/educadores y niños. Además, esta falta de confianza puede derivar en inseguridades y descrédito por parte de los niños hacia sus padres.

4. Bloqueo de programas: Bloqueo de determinada información de servicios del tipo mensajería instantánea, correo electrónico, descarga de programas, etc.

Con el bloqueo de estas páginas, es evidente que se bloquea también un uso incorrecto

de las mismas. Algunas herramientas permiten además, el bloquear la salida de determinada información, ya sea de manera voluntaria o por accidente (nombre, dirección, datos bancarios,...).

5. Listas blancas y negras: Permiten la configuración de listas positivas (blancas), a las que se permite el acceso y listas negativas (negras), a las que se deniega.

Las *listas negras* consisten en determinar las páginas a las que se restringe el acceso; lo cual lleva un peligro asociado, y es la rapidez con la que se añaden cada día contenidos y páginas a la Red y por tanto es prácticamente imposibles tenerlas actualizadas.

Las *listas blancas* son más restrictivas pero aseguran le denegación de acceso a determinados contenidos. Se trata de listas de páginas a las que se permite el acceso por considerarlas apropiadas.

6. Etiquetado de páginas: Todas las páginas contienen una serie de etiquetas de clasificación que determinan el contenido de la misma. Con esta técnica se permite el bloqueo por parte de navegadores y herramientas a páginas que contengan ciertos contenidos determinados por los padres/educadores.

La Plataforma para la Selección de Contenidos de Internet (PICS), desarrollada por el World Wide Web Consortium (W3C), proporciona un medio más eficiente para controlar el acceso a los contenidos. El sistema de etiquetado fue diseñado originalmente para ayudar a los padres y maestros en el control de acceso de los menores a la Red.

Este sistema tiene sus partes positivas y las negativas. Como positivo, señalar que es independiente del idioma, lo que posibilita la restricción de un mayor número de contenidos, y el hecho de que es el propio padre/educador quien bloquea lo que cree oportuno. Lo negativo es que no siempre existe dicha clasificación en ciertas páginas porque no existe un estándar común que sigan los generadores de contenidos y de páginas web.

Pero no sólo existe la posibilidad de establecer un control en Internet, también los móviles y las consolas empiezan a introducir una serie de restricciones en su uso.

Bien es cierto que el uso de Internet, el móvil y los videojuegos muchas veces se solapa. Los menores juegan en línea, se descargan tonos, juegos para la videoconsola o el móvil y, a todo ello hay que sumarle el resto de actividades que ofertan los móviles.

Una de las videoconsolas más populares entre los adolescentes, la X-Box 360, entre sus características en su última versión, incluye la posibilidad de establecer un control

parental. Además, tiene la posibilidad de establecer diferentes tipos de control según el menor esté jugando en línea o sin conexión. En el caso en que el menor esté jugando sin conexión, el control parental se puede configurar para licitar o negar el acceso a juegos en función de la clasificación PEGI8. Si el menor juega conectado a la Red, se puede determinar el acceso a determinados contenidos así como los contactos que establece el menor.

No se puede olvidar el hecho de las adicciones tecnológicas9. Es difícil determinar el porcentaje de menores que está o puede estar desarrollando una adicción a los videojuegos en Red10, pero es una problemática que está ahí y no puede, ni debe, pasar inadvertida.

En lo que respecta a la utilización del móvil, los padres suelen ser más restrictivos; o al menos creen serlo. Y se hace hincapié en el *creen* porque la mayor parte de las veces se auto-convencen de que el hecho de controlar el dinero que invierten en el mismo es suficiente. Pero no lo es. Ya no solo por el hecho de que la tecnología avance de tal forma que ahora podamos conectarnos a la Red desde el móvil, si no porque los peligros a los que los menores se enfrentan desde sus móviles se empiezan a parecer cada vez más a los que se encuentran en la Red.

Cuando nuestros hijos deciden bajarse melodías o conectarse a Internet desde su móvil, la exposición a virus y códigos maliciosos es casi la misma que cuando lo hacen desde el ordenador. Pero ¿con quién hablan?, ¿a quién mandan y de quién reciben los mensajes?, ¿sólo a/de sus compañeros de colegio o hay alguien más? En el correo electrónico se reciben mensajes de personas desconocidas (*spam*), en el móvil sucede lo mismo, pudiéndose recibir mensajes y llamadas de supuestas ofertas, premios, sorteos a los que el usuario no para a preguntarse si sus hijos los omiten o por el contrario, responden.
Desde hace ya algún tiempo, las diferentes compañías ponen a disposición de los padres una serie de controles parentales en los móviles. Con ellos pueden, no sólo de controlar el gasto, sino la restricción de llamadas y mensajes tanto por número como por destinatario (a los contactos de la agenda o a una serie de números determinados), limitar los contenidos a los que acceden (en la Red), o el acceso al servicio *localízame.*

Herramientas gratuitas de control parental

A continuación se exponen algunas herramientas gratuitas que permiten a los padres conocer y controlar los contenidos a los que sus hijos acceden en la Red:

1. Asesor de contenidos de Internet Explorer:

http://www.microsoft.com/spain/windows/ie/using/howto/contentadv/config.mspx

Idioma: Español

Características:

- Es una opción en el navegador Internet Explorer.
- Puede configurarse de tal forma que active diferentes filtros y detecte los contenidos según haya sido etiquetada la página.
- Da la posibilidad de crear listas de páginas “permitidas” para incluir los sitios que consideras adecuados para tus hijos (listas blancas).
- Permite agregar “filtros adicionales” más complejos que simplemente las etiquetas en la página.

2. Parental control bar:

http://www.aboutus.org/ParentalControlBar.org

Idioma: Inglés

Características:

- La instalación se hace de la misma forma que una “barra de herramientas” en los navegadores Internet Explorer, Firefox y Safari en computadoras con sistema operativo Windows 98/ME/2000/XP.
- Cuando se activa el Child Mode, automáticamente se bloquean las páginas etiquetadas con contenidos no aptos, las que no estén clasificadas (esto es configurable) y las que se agreguen a la lista negra.
- Permite la creación de listas de páginas blancas para incluir los sitios que consideras adecuados para tus hijos.
- Permite colocar páginas que estén etiquetadas como aptas dentro de las listas negras si contienen información inadecuada.

- Da la opción de saber en qué páginas ha entrado tu hijo.

3. Naomi:

http://www.naomifilter.org/spanish.html

Idioma: Varios (incluye español)

Características:

- Se instala como una aplicación independiente en Windows NT/ME/2000/XP
- Si detecta un contenido inadecuado, automáticamente cierra el navegador. La detección se realiza por medio de técnicas inteligentes que van más allá del simple etiquetado.
- No se puede configurar. Para dejar pasar páginas aptas que, por defecto han sido bloqueadas, es preciso desactivar el programa.
- Además de bloquear el navegador, bloquea también programas de tipo chat, compartir archivos, etc.

4. Leopard:

http://www.faq-mac.com/noticias/node/26785

Idioma: Español Características:

- Permite la configuración de cuentas de usuario específicas para los niños.
- Permite la restricción de contenidos de tres formas diferentes: acceso ilimitado, limitación selectiva y aprobación selectiva.
- Control del acceso a mail e iChat (aplicaciones de mensajería instantánea relacionadas con MSN aparecerán como otras aplicaciones.)
- Permite un control del tiempo de uso. • Da la opción de saber en qué páginas ha entrado su hijo.

11.-RECOMENDACIONES ORIENTADAS A PADRES Y TUTORES

1.- Eduque al menor sobre los posibles peligros que puede encontrar en la Red.

2.- Acompañe al menor en la navegación cuando sea posible, sin invadir su intimidad.

3.- Advierta al menor de los problemas de facilitar información personal (nombre, dirección, teléfono, contraseñas, fotografías, etc.) a través de cualquier canal.

4.- Aconséjele no participar en charlas radicales (provocadoras, racistas, humillantes, extremistas, etc.) ya que pueden hacerle sentir incómodo.

5.- Infórmele de que no todo lo que sale en Internet tiene que ser cierto, ya que pueden ser llevados a engaño con facilidad.

6.- Preste atención a sus “ciber-amistades” en la misma media que lo hace con sus amistades en la vida real.

7.- Pídale que le informe de cualquier conducta o contacto que le resulte incómodo o sospechoso.

8.- Vigile el tiempo de conexión del menor a Internet para evitar que desatienda otras actividades.

9.- Utilice herramientas de control parental que le ayudan en el filtrado de los contenidos accesibles por los menores.

10.- Cree una cuenta de usuario limitado para el acceso del menor al sistema.

12.-PRUEBAS REALIZADAS

Al registrarse en Facebook:

Facebook solo nos deja registrarnos si ponemos en el formulario de registro que tenemos al menos 14 años, de lo contrario nos dice que no cumplimos los requisitos, pero no nos dice porque. Si volvemos a intentarlo, no nos deja volver a registrarnos a no ser que borremos todos los datos de navegacion del navegador que estemos utilizando o bien gastemos otro navegador con el cual no hayamos tratado de registrarnos antes con una edad menor a 14 años.

Esta protección no nada difícil de saltar, y cualquier uusrio con unos conocimientos medio-bajos de navegación por internet la podría burlar sin ninguna dificultad.

Según los terminos de uso de facebook, las aplicaciones de facebook, deben de distinguir entre los usuarios mayores de edad y los que no lo son, aquellos con una edad comprendida entre 14 y 18. En la práctica hay aplicaciones que respetan este punto y otras muchas que no, esto depende de que los programadores se hayan preocupado de adaptar sus aplicaciones a los menores de edad, o bien de que los propios controladores de Facebook se den cuenta de que alguna aplicación no cumple los terminos de uso, y la eliminen.

Al registrarse en Tuenti:

En la página de registro de Tuenti, de entrada solo podemos elegir un año de nacimiento que sea al menos 14 años menor al año actual, y en caso de poner un mes y día mayor al actual,- lo que quiere decir que tenemos menos de 14 años – no nos deja registrarnos por no ser mayores de 14 años.
Aunque después de avisarnos de que somos demasiado jovenes para registrarnos, nos permite introducir otra edad sin tener que borrar las cookies del navegador o utilizar otro como pasa en Facebook. Esto hace que sea un poco más fácil registrarse en Tuenti siendo menor que en Facebook, aunque en los dos es tan fácil como mentir en la fecha de nacimiento.

CONCLUSIONES

Podemos concluir, que para un menor que navega por internet sin la supervisión de un adulto, es muy fácil saltarse las reglas de registro de las redes sociales, debido a que es tan fácil como mentir en la edad para poder hacerlo.

Los distintos términos de uso que tenemos que aceptar para poder registrarnos, la mayoría de veces , a parte de ser tan extensos que no invitan a su lectura, además suelen estar escritos en un lenguaje farragoso, como si los mismos editores buscaran que evitemos leer el texto por su complejidad y extensión, y así no estemos al tanto de las reglas que rigen la red social, y por lo tanto no podamos enterarnos con facilidad con por ejemplo, que van a hacer nuestros datos o cueles son nuestros derechos y obligaciones.

Lo mejor para que los menores no corran peligro al utilizar las redes sociales, es que las utilicen siempre en presencia de un adulto, para que pueda supervisar lo que el menor hace o deja de hacer. Sabemos que hoy en día debido a las obligaciones laborales de los padres, madres o tutores, es difícil sacar tiempo para esto, por lo que se debería hacer incapie en la educación del menor, y hacerle entender los peligros que puede correr en una red social. Lo principal sería inculcarle que las utilice siempre con sentido común, y que además de todas las cosas buenas y beneficios que se pueden sacar de ellas, también se corren riesgos, que hay que prevenir al utilizarlas.
No estaría de más controlar la navegación mediante algún tipo de software como los que se han expuesto anteriormente, aunque un exceso de control puede producir una reacción adversa en el menor, y que este intente acceder a lo que tiene prohibido desde otro equipo al que pueda tener acceso, como el de algún amigo o familiar.

En mi humilde opinión, lo mejor que se puede hacer hoy en día es educar al menor educadamente para que corra el menor peligro posible al utilizar las redes sociales, ya que con la gran expansión que están teniendo hoy en día, es inevitable que termine teniendo acceso a ellas. Se debería educar, tanto enseñando los peligros , como los beneficios que puede sacar tanto de ellas, como de Internet en general, ya que cada día es mas importante saber manejarse adecuadamente por las redes sociales o por internet,

sea cual sea el ámbito profesional en el que se desarrolle una persona.

BIBLIOGRAFÍA

Para realizar este proyecto, la mayor parte de la información se ha obtenido de la web del Instituto nacional de tecnológias de la información (INTECO, htp://www.inteco.es), consultando los siguientes documentos:

-Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online
-Guía legal, redes sociales, menores de edad y privacidad en la red.
-Guía sobre adolescencia y sexting: qué es y cómo prevenirlo
-Guía legal sobre ciberbullying y grooming.
-Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas.
-Los controles parentales: cómo vigilar a qué contenidos de Internet acceden nuestros hijos.

También se ha consultado el siguiente documento, de la fundación telefónica:

-Menores y redes sociales (Xavier Bringué/Charo Sádaba)
(http://www.ite.educacion.es/es/inicio/ultimas-noticias/149-presentado-el-estudio-qmenores-y-redes-socialesq)

Además de estos dos documentos:

-Implementation of the Safer Social Networking Principles for the EU: Testing of 20 Social Networks in Europe February 2010 (Charo Sádaba, School of Communication of the University of Navarra)

-Evaluation of the Implementation of the Safer Social Networking Principles for the EU Part I: General Report (Elisabeth Staksrud, University of Oslo, & Bojana Lobe, University of Ljubljana)

El resto de la información de ha ido cosechando realizando búsquedas a través de la web, de las cuales se ha considerado contenían información de interés las siguientes páginas y artículos:

-http://www.abc.es/20110121/sociedad/abcp-control-parental-clave-exito-20110121.html

-http://menoresenlastic.fundacionctic.org/

-http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/situacion-de-

los-riesgos-para-los-menores-en-el-uso-de-la-tic.shtm

-http://www.hoytecnologia.com/noticias/riesgo-redes-sociales/47760

-http://www.unblogenred.es/seguridad-en-las-redes-sociales-%C2%BFque-hay-de-nuevo/

-http://www.educaweb.com/

-http://www.unblogenred.es/seguridad-en-las-redes-sociales-%C2%BFque-hay-de-nuevo/