Informe de Amenazas CCN-CERT IA-03/13

Riesgos derivados del uso de Redes Sociales

19 de febrero de 2013

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la *información y software que se indican incluso cuando se advierta de tal posibilidad.*

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. CCN-CERT 5
2. Resumen ejecutivo 6
3. Introducción 7
3.1 ¿Qué son las redes sociales? 7
3.2 Tipología de redes sociales 8
3.3 Principales redes sociales 8
3.4 ¿Para qué se usan las redes sociales? 10
4. Riesgos de seguridad en las redes sociales 12
4.1 Ingeniería social 12
4.2 Suplantación de identidad 13
4.3 Phishing y Pharming 13
4.4 Social Spammer y Spam 14
4.5 Distribución de código dañino 15
4.6 Geolocalización 16
4.7 Privacidad 16
4.8 Falta de control de los contenidos 18
4.9 Sexting 19
4.10 Reputación virtual 19
4.11 Ciberacoso 20
4.12 Grooming 20
5. Buenas prácticas en el uso de redes sociales 21
Anexo A. whatsapp 24
Anexo B. SpotBros 26
Anexo C. Configuraciones básicas de seguridad 27
5.1 Facebook 27
5.2 Twitter 31
5.2.1 Configuración de la cuenta 32
5.3 LinkedIn 38
5.4 Badoo 42
5.5 Instagram 44
5.6 Tuenti 46

5.7 Youtube 49

ANEXO D. Noticias publicadas sobre seguridad en redes sociales 51

ANEXO E. Referencias 54

1. CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó a finales del año 2006 como el CERT gubernamental/nacional y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad.

El CCN-CERT tiene responsabilidad en los ataques procedentes del ciberespacio sobre sistemas clasificados, sistemas de la Administración y empresas pertenecientes a sectores designados como estratégicos.

La misión del CCN-CERT es, por tanto, contribuir a la mejora de la ciberseguridad en España y afrontar de forma activa las nuevas ciberamenazas, siendo el centro de alerta y respuesta nacional responsable de cooperar y ayudar a responder de forma rápida y eficiente a las Administraciones Públicas y a las empresas pertenecientes a sectores estratégicos.

2. Resumen ejecutivo

En la actualidad, para conocer la repercusión y el interés de una noticia se acude al *Trending Topic*[1] de **Twitter**, el índice de popularidad de una persona es fiel reflejo del número de *amigos* de **Facebook** o los *followers* (seguidores) de Twitter, el mercado laboral, con ofertas de trabajo y currículos, giran en torno a **LinkedIn**, mientras que el éxito de un disco se mide por el número de visionados en **Youtube** y las parejas se buscan en **Badoo**.

Además, las manifestaciones reivindicativas, el apoyo a determinadas iniciativas ciudadanas o las campañas publicitarias e institucionales cuentan con las redes sociales como principal caja de resonancia, al tiempo que todos los personajes de la vida pública mantienen vigente su perfil en alguna de estas redes.

Se trata de un fenómeno social que se ha asentado en la vida diaria de millones de personas, se calcula que 1.500 millones de internautas pertenecen a alguna red social en todo el mundo. La magnitud de este proceso ha provocado un cambio en el paradigma de las relaciones interpersonales y de la comunicación.

Las redes sociales no solo han cambiado la manera en que los ciudadanos se informan y se comunican entre sí, sino también la manera en que los Gobiernos y organizaciones transmiten sus mensajes a los ciudadanos y la forma en que estos responden. Comunicarse, compartir información, mantener un contacto por interés o afinidad, relacionarse, formar una identidad y reputación, reivindicarse, protestar, manipular,… son múltiples los objetivos buscados a la hora de utilizar una u otra red social.

No obstante, el éxito alcanzado, las enormes posibilidades que brindan y su uso masivo, las han hecho situarse en el punto de mira de los ciberatacantes que no dudan en explotar los riesgos y vulnerabilidades que tienen tanto las plataformas que sustentan estas redes sociales como las personas u organizaciones que las utilizan. Una vez más, el eslabón más débil de esta cadena vuelve a ser el factor humano por su escasa concienciación y su exceso de confianza a la hora de emplear estas redes.

En este documento se recogen los principales riesgos y amenazas derivados del uso de las distintas redes sociales, así como una guía de buenas prácticas a tener en cuenta en su utilización, junto con las configuraciones básicas de seguridad que deben tenerse en cuenta a la hora de emplear las principales plataformas (Facebook, Twitter, LinkedIn, Tuenti, Badoo e Instagram).

[1] Los temas del momento o tendencias[1] (*trending topics* en inglés), son las palabras o frases más repetidas en un momento concreto en Twitter. Los diez más relevantes se muestran en la página de inicio, pudiendo el usuario escoger el ámbito geográfico que prefiera, mundial o localizado, o personalizadas, en función además de a quién sigue el propio usuario. Tienen su origen en los *hashtag*, etiquetas precedidas por la almohadilla (#) que sirven para organizar tuits sobre un tema concreto en Twitter.

3. Introducción

3.1 ¿Qué son las redes sociales?

Las redes sociales se han convertido en un fenómeno social que está revolucionando el modo en que los usuarios de Internet se comunican y comparten información, intereses y afinidades. Son ya parte de los hábitos cotidianos de navegación de los usuarios.

Pero, ¿qué son las redes sociales? En realidad, son numerosas las definiciones que han ido surgiendo en los últimos años, en función del prisma desde el que se analicen: estructura, herramientas y aplicaciones, servicios y relaciones de sus miembros y/o contenidos.

Lo que sí tienen en común todas ellas es que descansan en Internet y más concretamente en la denominada **Web 2.0,** término acuñado en el año 2004 para referirse a una serie de aplicaciones y páginas de Internet que utilizan la inteligencia colectiva para proporcionar servicios interactivos en red.

La Web 2.0 comprende aquellos sitios Web que facilitan el compartir la información, la interoperabilidad y la colaboración entre los usuarios que son, además, generadores de contenidos frente a los sitios Web estáticos de los años 90 donde los usuarios se limitaban a una observación pasiva.

Podríamos definir entonces las redes sociales como plataformas Web, compuestas por grupos de personas, que forman una comunidad y que, a través de Internet y de distintas herramientas interactivas, pueden relacionarse, comunicarse y compartir contenidos con otros miembros de esa misma comunidad o grupo, de un modo público o semipúblico, en función de las distintas posibilidades de asociación o acceso a la red y de los intereses, propiedades u objetivos comunes de dichos usuarios.

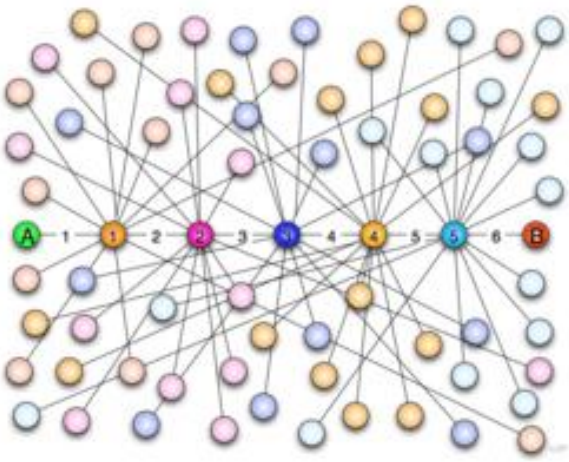


Figura 1. Seis grados de separación

Su funcionamiento se basa en la Teoría de los "***seis grados de separación***" (*véase Figura 1*), que intenta probar que cualquier persona puede estar conectado a otra a través de una cadena de conocidos que no tiene más de cinco intermediarios (conectando a ambas personas con sólo seis enlaces)[2].

[2] La teoría fue inicialmente propuesta en 1930 por el escritor húngaro Frigyes Karinthy en un cuento llamado Chains. Posteriormente, en 1967, el psicólog estadounidense Stanley Milgram ideó una manera de probar la teoría, que denominó "el problema del pequeño mundo". De hecho, en 2011 la empresa Facebook realizó un estudio denominado "Anatomy of Facebook" con todos los usuarios activos de su página en ese momento 721.000.000 miembros (alrededor del 10% de la

De hecho, desde el principio, el modelo de crecimiento de las redes sociales se ha basado en "el boca a boca" o proceso viral, en el que un número inicial de participantes invita o comparte unos contenidos con su grupo. Estos, a su vez, repiten el proceso incrementándose rápidamente el número de miembros o participantes.

3.2 Tipología de redes sociales

Desde un punto de vista general, la primera gran división a la hora de clasificar las redes sociales es en función de si se necesita o no un perfil para acceder a ellas. En base a este criterio, las redes se clasificarían en:

- ✓ Redes sociales **directas**[3]: es necesaria la creación de un perfil por cada uno de los usuarios. Entre ellas cabría una segunda división atendiendo a:
  - La **finalidad**: de ocio (Facebook, Tuenti, YouTube, Twitter…), uso profesional (Facebook, Twitter, LinkedIn…).
  - El modo de **funcionamiento**: de contenidos (YouTube), basada en perfiles personales o profesionales (Facebook, LindekIn…), microblogging (Twitter).
  - El grado de **apertura**: públicas (Facebook, Tuenti, YouTube…) o privadas (Yammer).
  - El nivel de **integración**: vertical (acotado a un grupo de usuarios a los que les une una misma formación, interés o profesión, como Dir&Ge) u horizontal (Youtube, Twitter, LindekIn).
- ✓ Redes sociales **indirectas**: no es necesario la creación de un perfil. En este caso, un usuario propone un tema y los demás pueden comentar o participar de esta aportación. En este apartado contaríamos con Foros y Blogs.

3.3 Principales redes sociales

A principios del año 2012 había en el mundo más de 2.000 millones de internautas (23,2 millones en España)[4]. De ellos, y aunque las cifras cambian a un ritmo trepidante, se calcula que el 75% pertenece al menos a una red social.

Basta citar, a modo de ejemplo, que cada minuto se suben a YouTube 35 horas de grabación o que Facebook contaba a finales del 2012 con 800 millones de usuarios. Como puede apreciarse en la Figura 2[5], son millones las personas que forman parte de alguna red social. De ellas destacan las siguientes:

población mundial) y se analizó el conjunto de amigos en común, para sacar el promedio de cuántos eslabones hay entre un usuario y otro cualquiera. De esta prueba se excluyó a celebridades y famosos. Los resultados mostraron que el 99,6% de pares de usuarios estuvieron conectados por 5 grados de separación. http://es.wikipedia.org/wiki/Seis_grados_de_separaci%C3%B3n

[3] Clasificación recogida en el estudio "Las Redes Sociales en Internet", diciembre de 2011 del Observatorio Nacional de las Telecomunicaciones y de la SI (ONTSI)

[4] Fundación Telefónica, "La Sociedad de la Información en España 2011"

[5] Gráfico elaborado por iRedes (Congreso Iberoamericano de Redes Sociales) http://www.iredes.es/2012/03/iredes-presenta-la-segunda-version-del-mapa-de-las-redes-sociales/

- **Facebook:** 800 millones de usuarios/15 en España. Es un sitio Web formado por muchas redes sociales relacionadas con una escuela, universidad, trabajo, región, etc.

  Se utiliza para mantenerse al día con amigos o compañeros compartiendo fotos, enlaces, vídeos, etc. Cualquier persona puede hacerse miembro de Facebook, lo único que necesitas es una dirección de correo electrónico.

- **YouTube**: 490 millones. Difusión de vídeos.

- **Haboo**: 230 millones. Enfocado a jóvenes y adolescentes, presenta salas de chat con formas de habitaciones de un hotel.

  El registro y la entrada es totalmente gratuito, pero el acceso a servicios adicionales requiere la compra de "Habbo Créditos" con dinero real, que es la moneda dentro del Hotel.

- **Twitter**: 200/4,5 millones en España. Red de microbblogin que permite enviar mensajes de texto plano de corta longitud, con un máximo de 140 caracteres, llamados tuits, que se muestran en la página principal del usuario.

  Los usuarios pueden suscribirse a los tuits de otros usuarios, a esto se le llama "seguir" y a los usuarios abonados se les llama "seguidores"[9] o *tweeps*[10] ('Twitter' + 'peeps').

  Por defecto, los mensajes son públicos, pudiendo difundirse privadamente, mostrándolos únicamente a unos seguidores determinados.

- **LinkedIn:** 135/2 millones en España. Red profesional orientada a negocios, que permite a los usuarios registrados mantener una lista con información de contactos de las personas con quienes tienen algún nivel de relación, llamada Conexión.

- **Google+:** 135 millones. Integra distintos servicios del propio buscador e introduce otros como Círculos, Quedadas, Intereses y Mensajes.

- **Badoo**: 120 millones. Red de contactos.

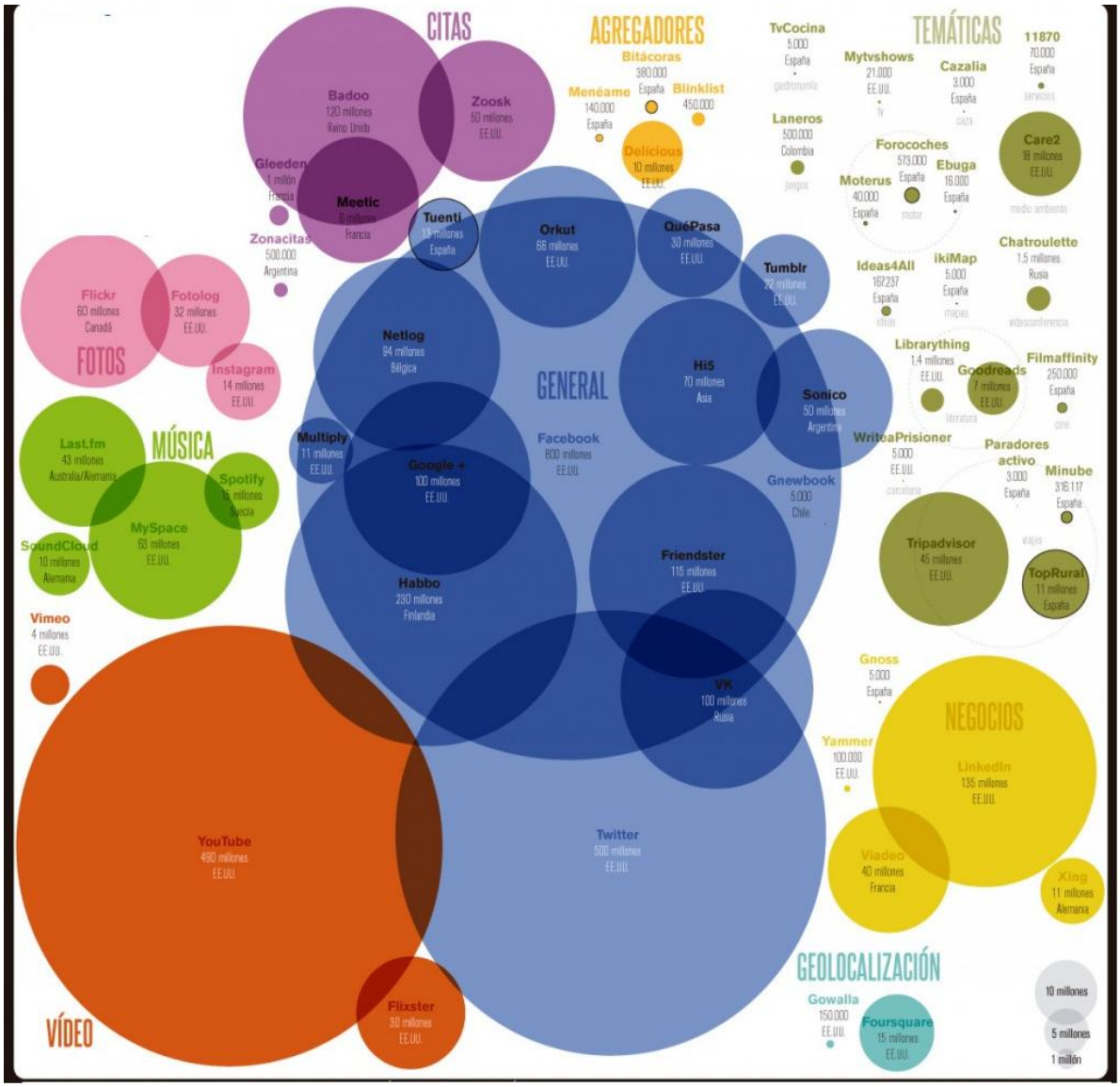


Figura 2. Mapa de Redes sociales con presencia en Iberoamérica

3.4 ¿Para qué se usan las redes sociales?

Ampliación de las relaciones del mundo real, herramienta de comunicación masiva, formación de identidad… Desde que iniciaron su andadura en 1995, tras la creación del sitio Web *classmates.com* por parte de Randy Conrads para mantener contacto con sus ex compañeros de instituto, las redes sociales han registrado un crecimiento vertiginoso, favorecido por el desarrollo de nuevas aplicaciones y soluciones de conectividad (dispositivos móviles).

Así, a medida que se han ido incrementando las capacidades, tanto de la plataforma como de las herramientas, se han ido ofreciendo nuevos servicios a los usuarios, que pueden acceder desde cualquier sitio y con infinidad de dispositivos, convirtiendo a las redes sociales en un medio de comunicación global y poderoso,

utilizado incluso para apoyar acciones militares (por ejemplo en noviembre de 2012, Israel narró la ofensiva sobre Gaza a través de Twitter, contrarrestando minuciosamente cada uno de los mensajes difundidos por grupos propalestinos[6]), convocar actos reivindicativos (basta recordar el papel de las redes sociales en las revueltas de Egipto y Túnez) o actualizar las noticias minuto a minuto.

No obstante, los motivos principales para pertenecer a una red social por lo menos en aquellas donde es necesario crear un perfil, es el mantenerse en contacto con amigos y conocidos (ver Figura 3)[7].

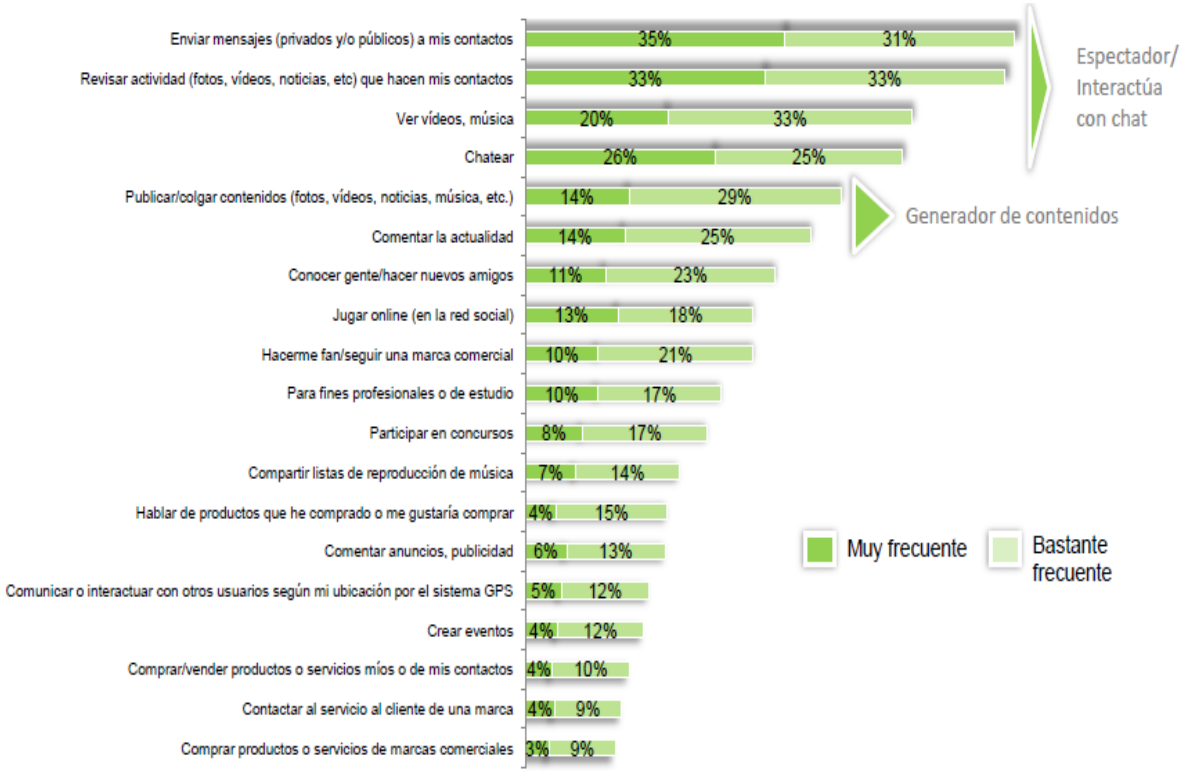


Figura 3. Motivos de pertenencia a redes sociales (estudio iab Spain)

[6] http://internacional.elpais.com/internacional/2012/11/15/actualidad/1353014160_029420.html

[7] Fuente: "Informe de resultados Observatorio de Redes Sociales". The Cocktail Analysis. Cuarta oleada, 2011. Abril 2012

4. Riesgos de seguridad en las redes sociales

Las enormes posibilidades que brindan las redes sociales y su uso masivo llevan aparejados una serie de riesgos de diversa índole, tanto en el ámbito privado como el profesional.

Ante la creciente tendencia a utilizar este tipo de redes como medio para el desarrollo de ciberataques, es de vital importancia estar protegido y utilizar un entorno seguro durante su empleo.

Las vulnerabilidades y fallos que presentan las redes sociales y la excesiva confianza de sus usuarios no hacen sino incrementar estos riesgos y que se hayan convertido en objetivo prioritario para los ciberatacantes. Así, según un reciente informe, en el año 2012[8] las redes sociales, y más concretamente Facebook y Twitter, fueron dos de las plataformas favoritas para propagar código dañino y robar u obtener información.

En general, los riesgos asociados a las redes sociales son los mismos que los del resto de actividades y/o servicios en Internet: grandes dificultades para eliminar la información subida, el acceso futuro por terceros (el derecho a cambiar de opinión es nulo y será muy difícil borrar cualquier opinión, fotografía o vídeo subido a la red) y la dificultad de discernir entre información veraz y propaganda o manipulación.

A continuación se describen algunos de los riesgos de seguridad más habituales en las redes sociales.

4.1 Ingeniería social

La ingeniería social se define como el proceso de manipular a usuarios legítimos para obtener información clasificada o confidencial, con el objetivo de divulgar información, cometer fraude u obtener acceso a un sistema informático.[9] Esta técnica era, y sigue siendo, una de las prácticas más usadas en Internet.

Se busca dirigir/controlar la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en determinados enlaces, introducir contraseñas, visitar páginas Webs, etc.) convencido de que está haciendo un uso correcto cuando realmente está siendo engañado por el ingeniero social[10].

En el caso de las redes sociales, los atacantes disponen de una gran cantidad de información tan sólo con ver el perfil de su víctima (sexo, fecha de nacimiento, aficiones, formación, carrera estudiantil o profesional, etc.), lo que favorece el despliegue y empleo de estas técnicas.

[8] http://eset.es/index.php/rss/398-resumen-de-amenazas-en-diciembre

9 "CCN-CERT IA-03/12 Ingeniería Social". Enero 2012. CCN-CERT

[10] Guía CCN-STIC 401 Glosario de Términos: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-Glosario_y_abreviaturas/401/index.html

De este modo, y desde un perfil inventado por el ingeniero social, se obtiene una confianza que será aprovechada de diversas formas para cliquear en enlaces redirigidos a Webs maliciosas, compartición de archivos con código dañino, phishing y grooming (se explica más adelante).

La ingeniería social se convierte, por tanto, en la antesala de otro tipo de ataques más delicados y de peores consecuencias para la víctima.

4.2 Suplantación de identidad

Se conoce por suplantación de identidad la actividad maliciosa en la que un atacante se hace pasar por otra persona por distintos motivos como cometer un fraude, realizar ciberbullying, grooming, etc. Muchas veces esta acción viene precedida por un proceso de ingeniería social o por el acceso sin permiso de la cuenta del usuario.

Del mismo modo, un gran número de los datos publicados en redes sociales pueden facilitar esta técnica (fecha de nacimiento, fotografías de usuario…).

Suele creerse que esta técnica sólo se emplea con personajes famosos y grandes empresas, pero la verdad es que se utiliza contra todo tipo de víctimas. La finalidad es robar información personal para cometer otros actos delictivos o para actuar bajo el anonimato y hacer daño a terceros.

Cada vez es más frecuente que usuarios que nunca se habían registrado en redes sociales online, comprueben cómo en el momento en el que intentan acceder, su "identidad digital" ya está siendo utilizada[11].

Un ejemplo de esta técnica se produjo en enero de 2011[12], cuando se suplantó la identidad de Mark Zuckerber en Facebook (creador de esta red) y se comenzaron a difundir mensajes públicos desde su "supuesto" perfil contra la propia compañía.

En los casos de suplantación de identidad, cada red social cuenta con sus propios mecanismos de denuncia y prevención, a los que se puede recurrir antes de hacerlo por vía judicial.

4.3 Phishing y Pharming

El *phishing* es un tipo de ataque en el que se utiliza la ingeniería social para obtener fraudulentamente de los usuarios información personal, principalmente de acceso a servicios financieros.

Para alcanzar al mayor número posible de víctimas e incrementar sus posibilidades de éxito utilizan el correo basura ("spam") para difundirse. Una vez que llega el correo al destinatario, intentan engañar a los usuarios para que faciliten datos de carácter personal, normalmente conduciéndolos a lugares de Internet

[11] Estudio sobre la privacidad de los datos y la seguridad de la información en las redes sociales online (INTECO y Agencia Española de Protección de Datos)

[12] http://myspace.wihe.net/hackean-pagina-facebook-mark-zuckerberg/

modificados, páginas Web, aparentemente oficiales, de bancos y empresas de tarjeta de crédito que terminan de convencer al usuario de que introduzca datos personales de su cuenta bancaria como su número de cuenta, contraseña, número de seguridad social, etc.[13].

Por su parte, el *pharming* es un redireccionamiento malintencionado del usuario a un sitio Web falso y fraudulento, mediante la explotación del sistema DNS (se denomina secuestro o envenenamiento del DNS).

Tanto con el phising como con el pharming se buscan datos personales sensibles (tarjetas de crédito, PIN de usuarios, etc.).

La naturaleza de las redes sociales, donde los usuarios comparten detalles personales de sus vidas, correo electrónico, aficiones, información laboral o fechas de cumpleaños, hace que este tipo de ataques sea más fácil de llevar a cabo.

Con toda la información facilitada es relativamente sencillo recuperar cuentas de correo electrónico o acceso a servicios sensibles (banca online, compras…), teniendo en cuenta que estos sistemas permiten resetear la contraseña, realizando una pregunta secreta al usuario que en la mayoría de las ocasiones, tiene relación con su vida personal (nombre de la primera mascota, segundo apellido del padre, primer colegio, profesora favorita, fecha de nacimiento, etc.).

Muchos de estos datos pueden encontrarse en las redes sociales, incluso en la información pública del perfil del usuario.

Asimismo, también se emplean técnicas de phishing suplantando la página de inicio de las plataformas de redes sociales, ya que es habitual compartir el mismo usuario y contraseña en la mayoría de los servicios que ofrece Internet y una vez recopilada esta información se puede intentar acceder a los demás servicios que utiliza la víctima.

4.4 Social Spammer y Spam

El *social spammer* es el uso de las redes sociales como plataformas para el envío de correos electrónicos no deseados, que se envían aleatoriamente en procesos por lotes. Es una eficiente y barata forma de comercializar cualquier producto.

La mayoría de usuarios están expuestos a este correo basura, como evidencian las encuestas que muestran que más del 50% de todos los correos electrónicos son correos basura.

No es una amenaza directa, pero la cantidad de correos electrónicos generados y el tiempo que lleva a las empresas y particulares relacionarlos y eliminarlos representa un elemento molesto para los usuarios de Internet.

[13] Guía STIC CCN-CERT 401 – Glosario de Términos

4.5 Distribución de código dañino

Las redes sociales se están convirtiendo en uno de los principales instrumentos de propagación de código dañino de forma masiva. El gusano *Koobface*[14], un anagrama de Facebook pero al revés, fue una de las primeras grandes amenazas para las redes sociales en 2008.

Este gusano atacaba a usuarios de Facebook, MySpace, Hi5, Bebo, Friendster y Twitter, y se diseminaba enviando un mensaje a las contactos de la persona cuyo ordenador era infectado. El mensaje contenía un asunto atrayente, seguido de un link que redireccionaba a una Web con una supuesta actualización del reproductor Flash de Adobe. Si el archivo era descargado y ejecutado, el ordenador ya estaba infectado y podía obtener información sensible de las víctimas.

Desde entonces hasta la fecha, el abanico de aplicaciones falsas se han multiplicado, con la promesa de enterarse de quién visitó su perfil o ver las respuestas a preguntas que sus amigos han contestado sobre ellos, imágenes divertidas o noticias sorprendentes, los usuarios son atraídos a caer en estos enlaces que terminan con sus cuentas infectadas de software dañino.

A partir de estrategias de ingeniería social, los desarrolladores de malware suelen utilizar las redes sociales para propagarlo. Los principales métodos para infectar con código dañino los diferentes dispositivos son:

- **Enlaces maliciosos.** Estos tipos de ataques suelen aparecer bajo la fórmula "mensaje más enlace" siendo el enlace, el que lleva al usuario al contenido malicioso. En el caso de un ataque en Facebook, por ejemplo, se suele utilizar el muro de la víctima, donde se coloca un mensaje, un privado (inbox) o una foto en la que el usuario aparece etiquetado, entre otros.
- En el caso de **Twitter**, los ataques se realizan a través de una mención, un mensaje privado o con el uso de los acortadores de enlaces que emplean esta plataforma y que son aprovechados en campañas de spam y redireccionamiento.

  Instalar un *plugin* para el navegador que resuelva las direcciones URL cortas y permita ver las originales sin la necesidad de hacerles clic en ellas, como es *LongURL Mobile Expander* puede en muchas ocasiones solucionar este problema.
- **Videos prometedores.** Uno de los "anzuelos" más comunes para un ataque, y al igual que ocurre en el correo electrónico, es la promesa de ver un vídeo impactante, como el que prometía mostrar la muerte de Osama Bin Laden.

  Al cliquear en muchos de estos vídeos, se publica información en el perfil de la red social, publicando este mismo vídeo u otro similar sin el consentimiento de la víctima.

[14] http://www.us-cert.gov/current/archive/2009/03/04/archive.html#malicious_code_targeting_social_networking

Por todo ello, es preferible acudir a una plataforma de gestión de vídeos, como YouTube o Vimeo, introduciendo allí el título antes que pinchar en el enlace que se facilita.

4.6 Geolocalización

Cada vez se desarrollan más servicios en las redes sociales que dependen sustancialmente de la información proporcionada en base a la localización. En otras palabras, no se trata tanto de qué se está haciendo sino desde dónde se hace.

En donde estemos ubicados tendrá una enorme influencia en los contenidos y servicios disponibles, de modo que será inevitable que las redes sociales tomen conciencia de ello.

Facilitar, en muchas ocasiones sin intención, el sitio en el que un usuario está ubicado puede ocasionar ciertos riesgos. Desde una posible intromisión en la casa de la víctima aprovechando su ausencia, hasta el acoso digital.

En ocasiones el usuario facilita directamente su dirección (sobre todo en Twitter) y, otras muchas veces, no es consciente de ello. Hay que tener en cuenta que muchos teléfonos inteligentes (smartphones) etiquetan geográficamente las fotos, por lo que la información se obtiene fácilmente.

Existen direcciones Web que demuestran los riesgos de la geolocalización como *PleaseRobMe.com* o *I Can Stalk U* que tienen como propósito la intención de concienciar a los usuarios de las redes sociales de los peligros que pueden haber al informar sobre el sitio en el que uno se encuentra en todo momento.

4.7 Privacidad

Las redes sociales se han convertido en archivos diarios cargados con riquísima información sobre la vida de sus usuarios. Desde datos básicos y de contacto, hasta información acerca de los amigos, el trabajo, aficiones, rutinas y actividades contadas en fotos y comentarios.

Por tanto, la privacidad se ha convertido en una preocupación frecuente en estas redes, ya que existe el riesgo de compartir (o que otros compartan) demasiada información de uno mismo y sin ningún tipo de control.

En la medida de lo posible hay que evita utilizar máquinas de acceso público para conectarse a Internet, como cibercafés, y, si no queda otro remedio, conectarse tomando las precauciones adecuadas.

Pero además, y con la utilización de cookies por el sitio Web, se puede conocer cuál es la actividad del usuario dentro de la misma, desde qué lugar se accede, el tiempo de conexión, el dispositivo desde el que se accede (fijo, tableta o móvil), el sistema operativo utilizado, la dirección IP, los perfiles visitados, los mensajes recibidos y enviados, los sitios más visitados, el número de clics realizados. Es decir, todo un registro de información personal sobre lo que se ha hecho mientras se estaba en la red social.

Entre las posibles situaciones de riesgos, relacionadas con la privacidad de los usuarios, se encontrarían las siguientes:

- **Mala configuración del perfil** a la hora de darse de alta en la red social, en la medida en que no sea configurado correctamente el nivel de privacidad ofrecido por la propia plataforma. Conviene, de hecho, no elegir las opciones por defecto sino analizar detenidamente cada una de las configuraciones que ofrecen para mostrar según qué contenido.
- **Captación de los datos** de un perfil por un atacante que puede ser empleado en acciones más comprometedoras como preguntas clave para conocer contraseñas, etc… favorecidas por los fallos de seguridad de las propias plataformas.

  Hay numerosos ejemplos de robo de cuentas y publicación de contraseñas, correos y otros datos de las principales redes sociales: Facebook, LinkedIn, Twitter[15]….
- Dificultad de **controlar el perfil** pese a las configuraciones de seguridad y lo que otros "amigos" publican sobre uno. En este sentido, la mayoría de las redes sociales disponen de un perfil completo del usuario, en formato público, de forma que cualquier usuario de Internet o de la red social puede acceder a información de carácter personal ajena sin que el propietario de los datos tenga que dar su consentimiento expreso.

  De igual forma, las redes sociales están incrementando sus servicios con prácticas comprometedoras para la privacidad. Así, por ejemplo, el servicio recién lanzado por Facebook[16] *(Graph Search*) que actúa como un motor de búsqueda sobre la propia red social, permitirá a un usuario conocer de sus conocidos cuatro grandes áreas: personas, fotos, lugares (restaurantes, ciudades, atracciones,…) y actividades (música, cine,…).
- Dificultad de borrar los datos publicados a la hora de **darse de baja de la plataforma,** manteniéndose en muchos casos información personal o imágenes propias publicadas en los perfiles de otros usuarios.
- **Publicidad hipercontextualizada** que, a priori, es una ventaja para los usuarios pero puede ser una práctica ilegal el que, gracias a la información facilitada en las redes sociales, se contextualice y se muestre publicidad relacionada según los datos mostrados y preferencias.
- **Indexación** no autorizada por parte de buscadores de Internet.
- Acceso a la **agenda de contactos** y otros datos sin consentimiento. Este es el caso de WhatsApp, donde los usuarios deben permitir el acceso a su agenda de contados.

[15] http://tecnologia.elpais.com/tecnologia/2013/02/04/actualidad/1359967398_800973.html

[16] "Facebook se convierte en un buscador 'social' para competir con Google". El Mundo 15-01-2013. http://www.elmundo.es/elmundo/2013/01/15/navegante/1358278037.html

De esta forma, todos los números de teléfonos registrados en la tarjeta SIM del cliente se transmiten a la aplicación para facilitar la identificación de otros usuarios. En lugar de borrar el número de teléfono de los no usuarios, se almacenan.

Este hecho ha provocado, por ejemplo, que las autoridades de Holanda y Canadá[17] acusen a esta aplicación de violar varias leyes de protección de información privada.

4.8 Falta de control de los contenidos

Existe una falta de control sobre los contenidos que se alojan en este tipo de redes. De un lado porque una vez que se entrega cierta información a los portales, ésta queda en manos de los propietarios de la red (*véase Figura 4*).

"Usted le otorga a Facebook el derecho irrevocable, perpetuo, no exclusivo, transferible y ***mundial*** *(con la autorización de acordar una licencia secundaria) de utilizar, copiar, publicar, difundir, almacenar, ejecutar, transmitir, escanear, modificar, editar, traducir, adaptar, redistribuir cualquier contenido depositado en el portal".*

Figura 4.: Facebook. Licencia y términos de uso

De otra, porque existen suspicacias sobre cómo son administrados esos datos sensibles por parte de las compañías. Por último, porque, tal y como se ha mencionado en el apartado anterior, todavía existen numerosos fallos de seguridad en estas plataformas, lo que facilita el robo de información sensible.

Asimismo, las políticas de seguridad y privacidad son cambiantes. Facebook, Google o Instagram se han enfrentado a crecientes reclamaciones por cuestiones de privacidad y seguridad de los datos y, en ocasiones, han sufrido la baja airada de sus usuarios ante los cambios de política de privacidad.

De: Instagram <no-reply@instagram.com>
Fecha: 16 de enero de 2013 07:05:40 GMT+01:00
Para: xxxxxxx@gmail.com
Asunto: Instagram Update

Hello,

Our community has grown by many millions of people since we wrote our original Terms of Service and Privacy Policy. As we announced in December, we have updated our Terms of Service and Privacy Policy. These policies also now take into account the feedback we received from the Instagram Community. We're emailing you to remind you that, as we announced last month, these updated policies will be in effect as of January 19th, 2013.

You can read our blog post that highlights some of the key updates. And remember, these updates don't change the fact that you own your photos that you post on Instagram, and our privacy controls work just as they did before.

Thank you,
The Instagram Team

Figura 5. Correo electrónico enviado por Instagram a sus usuarios

[17] http://www.elmundo.es/elmundo/2013/01/28/navegante/1359402509.html

Es paradigmático el caso de la popular red social de fotos **Instagram** que, tras ser comprada por Facebook, en abril de 2012, anunció ocho meses después que modificaba los términos de privacidad (véase Figura 5). Este hecho provocó un descenso en el número de usuarios activos del 50% en un mes. Así, habría pasado de los 16,35 millones de usuarios activos el día el 17 de diciembre a los 7,41 millones el 14 de enero.

4.9 Sexting

El sexting es el envío por Internet, especialmente a través de smartphones (aplicaciones como WhatsApp facilitan esta práctica) de fotografías y vídeos con contenido sexual, tomados o grabados por el protagonista de los mismos. Es una práctica cada vez más común entre jóvenes.

Es preciso recordar que, a partir del momento en que se envía una foto o video, se pierde el control sobre los mismos. No sólo porque el receptor puede difundirlos a su antojo sino porque se puede producir el robo o la pérdida del móvil así como su uso momentáneo por un tercero.

4.10 Reputación virtual

Las personas y las empresas cuentan con una gran cantidad de datos sobre sí mismas publicados en Internet en general y en las redes sociales en particular. Por ello, es muy importante **seleccionar bien la forma y el fondo de los contenidos que se suben** a la red ya sean fotos, videos o comentarios, reflexionando en todo momento sobre la imagen que se está construyendo de sí mismos en la red.

En este sentido, es básico tener claro el objetivo de la información (informar, persuadir, adoctrinar, contrarrestar otra información…), así como el hecho de que en el mismo momento en que algo se sube a la red, en cuestión de segundos se puede volver en contra del emisor.

A ello se añade que, aparte de la publicación personal, la reputación online[18] no está bajo el control absoluto del sujeto o la organización sino que la "fabrican" también el resto de personas cuando conversan y aportan sus opiniones sobre una fotografía, un artículo o un vídeo.

De hecho, en las redes sociales aparecen informaciones erróneas (con y sin un propósito malintencionado), injurias (información que provoca deshonra o descrédito a una persona sabiendo que es falsa) o calumnias (falsa imputación de un delito) sobre una persona, que constituyen un ataque al honor y la reputación de la misma.

Al tratarse Internet de un medio abierto, están apareciendo nuevas amenazas sobre la reputación online de las empresas que posteriormente afectan a su negocio. Las opiniones de exempleados sobre los métodos de actuación de su antigua empresa, las opiniones de consumidores o la competencia sobre dicha empresa o ataques directos a los directivos, gerentes e incluso empleados, puede afectar de

[18] "Guía para usuarios: identidad digital y reputación online" 23/07/2012 INTECO

manera crítica a cómo se verá a esa persona o empresa desde las redes, creando una primera impresión muy negativa.

A pesar de las medidas reactivas que se pueden aplicar (retirada de los comentarios, acciones legales, etc.), la capacidad de difusión en medios sociales aumenta el daño sobre la imagen que tiene la persona de cara a la comunidad internauta.

4.11 Ciberacoso

También llamado cyberbullying, en su traducción al inglés, es el uso de información electrónica y medios de comunicación tales como correo electrónico, redes sociales, blogs, mensajería instantánea, mensajes de texto, teléfonos móviles y Websites difamatorios para acosar a un individuo o grupo mediante ataques personales u otros medios. Puede constituir un delito penal.

En definitiva, se trata del uso de Internet, el teléfono móvil o los videojuegos para humillar, agredir, maltratar, difamar, insultar, amenazar o desprestigiar a compañeros o personas. Incluso, podemos ser víctimas sin darnos cuenta mientras alguien se vale de sus conocimientos informáticos para introducirse en nuestro ordenador y manipular la webcam u obtener información personal (documentos, fotos, vídeos, etc…).

El ciberacoso es obstinado e implica un daño recurrente y repetitivo infligido por medio del texto electrónico. El ciberacoso puede también incluir amenazas, connotaciones sexuales, etiquetas peyorativas, etc…

4.12 Grooming

El cibergrooming[19] es un método basado en un conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza de un menor de edad a través de Internet y las nuevas tecnologías, para conseguir su control a nivel emocional, con el fin último de obtener concesiones de índole sexual.

Se habla entonces de acoso sexual a menores en la Red y el término completo sería child grooming o Internet grooming. Desde un acercamiento lleno de empatía y/o engaños se pasa al chantaje más cruento para obtener imágenes comprometidas del menor y, en casos extremos, pretender un encuentro en persona.

El daño psicológico que sufren niños, niñas y adolescentes atrapados en estas circunstancias es enorme. El rol de los adultos es fundamental para la protección de la infancia, que no deberían de utilizar las redes sociales sin contar con el apoyo de sus padres o cualquier adulto de referencia, incluso los propios maestros.

En este sentido cobran una gran importancia las charlas de concienciación que realizan las Fuerzas y Cuerpos de Seguridad del Estado en los colegios.

[19] "Grooming, acoso a menores en la Red" Oct. 2008 Pantallas amigas

5. Buenas prácticas en el uso de redes sociales

Después de ver los numerosos riesgos que conlleva el uso de redes sociales, los cuales irán incrementándose a medida que aumenten los servicios y el número de usuarios, es preciso ofrecer algunos consejos y sugerencias[20] que minimicen las amenazas presentes en estas redes.

En este punto hay que recordar la importancia que tiene la configuración de seguridad del dispositivo (sistema operativo y navegador) utilizado para conectarse a Internet y, de esta manera, acceder a las redes sociales.

Los dispositivos tipo smartphones y las tabletas añaden a las vulnerabilidades habituales de cualquier equipo informático, las posibilidades de geolocalización a través de los sistemas de localización tipo GPS que llevan asociados.

1. **Creación cuidadosa del perfil. Protección con la configuración de privacidad**
   - No basarse en la configuración por defecto que proporciona la plataforma.
   - Usar opciones orientadas a la privacidad. Comprobar quién puede ver nuestras fotos, quién puede ponerse en contacto con nosotros y quién puede añadir comentarios.
   - Leer con atención y de principio a fin la política de privacidad y las condiciones y términos de uso de la red social que se escoja. Las políticas de privacidad cambian continuamente y pueden afectar a los datos que se tienen publicados.[21]
2. **Reflexión sobre todo lo que se publica**
   - Pensar muy bien que imágenes, vídeos e información se escoge para publicar, teniendo en cuenta que todo lo que se publica deja de tener una connotación privada y pasa a formar parte de los contenidos de la comunidad y de la Red. En este caso, hay que preguntarse si uno se sentiría cómodo si su supervisor, jefe o compañero de trabajo viese la información publicada (ahora o en un futuro).
   - Dar por sentado que todo lo que se sube en una red social es permanente. Aunque se elimine la cuenta, cualquier persona en Internet puede fácilmente imprimir fotografías o texto, guardar imágenes y vídeos publicados en la red.
   - No publicar nunca información que no se compartiría con un desconocido en la calle como DNI, dirección, teléfono, etc. Asumir que cualquier información que se coloque puede hacerse de conocimiento público en cualquier momento.

[20] Algunos de los puntos aquí recogidos se han obtenido del documento: 11 Consejos para protegerse en las redes sociales. Centro de Seguridad y protección de Microsoft

[21] "Facebook modifica la política de privacidad de Instagram y enfada a los usuarios". Diciembre 2012. Cinco Días

- Abstenerse de informar acerca de domicilios particulares propios o ajenos, así como detalles sobre ausencias prolongadas o vacaciones[22].
- Usar un pseudónimo.

3. Escoger cuidadosamente a nuestros amigos

- Hay que ser selectivo a la hora de decidir a quién se acepta como amigo en una red social, los ladrones de identidades pueden crear un perfil falso para obtener información suya. Hay que verificar todos nuestros contactos.
- Tener cuidado con lo que se publica sobre otras personas ya que podemos estar incluyendo información que esa persona puede no aprobar/autorizar para su difusión.

4. No permita que examinen su libreta de direcciones

- Para evitar revelar las direcciones de correo de sus amigos, no permita que los servicios de redes sociales examinen su libreta de direcciones de correo.
- En ocasiones, se recibe una oferta de introducir su dirección y contraseña para saber si sus contactos forman parte de la red. El sitio puede usar la información para enviar mensajes de correo a todas las personas de su lista de contactos e, incluso, a cualquiera que le haya enviado un mensaje.

5. Prestar atención a los servicios basados en la localización y a la información de nuestro teléfono móvil

- Desactivar los servicios basados en la localización geográfica cuando no los estemos usando.
- La geolocalización puede ser utilizada por delincuentes (no solo hackers) ya que aporta información sobre la ubicación exacta del usuario o de las fotos que se etiquetan. Facebook, Twitter, Google+ o Tuenti cuentan con aplicaciones como Google Maps.

6. Precaución con los enlaces

- Evitar hacer clic en hipervínculos o enlaces de procedencia dudosa para prevenir y evitar el acceso a sitios amenaza para los sistemas informáticos. Recuerde que este tipo de enlaces pueden estar presentes en un correo electrónico, una ventana de chat o un mensaje en una red social.

7. Escriba la dirección de su sitio de redes sociales directamente en el explorador

- Si hace clic en un vínculo al sitio a través del correo electrónico u otro sitio Web, podría estar introduciendo su nombre de cuenta y su contraseña en un sitio falso donde se podría robar su información personal.
- Es importante configurar la navegación utilizando el protocolo HTTPS, ya que permite evitar los ataques relacionados con la interceptación de información que viaja en texto claro (legible) a través de las redes. Con el protocolo HTTPS,

[22] Orihuela, José Luis (2011) "Mundo Twitter". Barcelona: Alienta Editorial

todos los datos "no solo el usuario y la contraseña" viajarán cifrados y serán ilegibles, en principio, para cualquier atacante en la red.

8. **Tener precaución de instalar elementos adicionales en su sitio**

   - Muchos sitios relacionados con redes sociales ofrecen la descarga de aplicaciones de terceros que permiten ampliar las funciones de la página personal.
   - Los delincuentes en ocasiones usan estas aplicaciones para robar información personal. Para descargar y usar aplicaciones de terceros de forma segura, hay que tomar las mismas precauciones de seguridad que se toman con cualquier otro programa o archivo que se descarga de Internet.

9. **Revisar la información publicada acerca de uno mismo**

   - Un método común utilizado por los atacantes para obtener información financiera de otras cuentas es haciendo clic en el vínculo "¿Olvidó su contraseña? en la página de inicio de sesión.
   - Para entrar en su cuenta se buscan las respuestas a sus preguntas de seguridad como, por ejemplo, su cumpleaños, su ciudad natal, clase del instituto,…

10. **Seguridad de las contraseñas**

    - Utilice contraseñas con al menos ocho (8) caracteres, complejas que incluyan números, símbolos y signos de puntuación.
    - Es importante no compartir la misma contraseña para todas las redes sociales ni para el resto de servicios que se utilizan en Internet.
    - Se aconseja utilizar un gestor de contraseñas tipo *keepass* para guardarlas y mantenerlas almacenadas de forma segura. Nunca hay que dejarlas escritas en papel o en lugares a los que puedan acceder otras personas.

ANEXO A. WHATSAPP

WhatsApp[23] es una aplicación multiplataforma de mensajería instantánea, gratuita, que permite intercambiar mensajes sin tener que pagar por servicios tipo SMS. En estos momentos está disponible en distintos dispositivos: iPhone, BlackBerry, Android, Windows Phone y Nokia.

Hasta la fecha no se le ha considerado una red social, aunque está evolucionando de tal forma que podría empezar a englobarse en este tipo de plataformas. A través de WhatsApp ya se envían mensajes de texto, fotografías, imágenes, videos, notas de voz, localizaciones, datos de contacto entre los usuarios adscritos al servicio, actualización del estado del usuario, cambios en las fotos de su perfil, creación de grupos de hasta treinta (30) miembros, etc…

No obstante, durante la vida de la aplicación se han ido descubriendo diversas vulnerabilidades y riesgos de cara a los usuarios como la suplantación de identidad, la privacidad o la pérdida de reputación.

En resumen las **principales amenazas** del uso del WhatsApp son las siguientes:

1. Ataques contra el proceso de registro.
2. Cabeceras de mensajes enviadas en texto plano: se ha conseguido enumerar usuarios monitorizando las conversaciones cifradas que se enviaban a través de Internet, ya que las cabeceras de destino se envían en texto plano.
3. Enumeración de usuarios: se ha conseguido mediante una petición Web y de forma anónima, la enumeración de usuarios que se encuentran utilizando WhatsApp.
4. Suplantación de identidad: mediante la extracción de claves de autenticación, un usuario dañino puede realizar ataques contra un usuario suplantando la identidad del mismo. Posibilidad de poder suplantar los teléfonos con sólo conocer el IMEI en sistemas basados en Android.
5. Extracción de conversaciones: se ha conseguido extraer las conversaciones de la base de datos, ya que éstas se almacenan sin cifrado alguno.
6. Extracción de claves de autenticación: se ha conseguido extraer las claves de autenticación necesarias para la suplantación de identidad, ya que éstas se almacenan en una base de datos de caché.
7. Envío de mensajes de spam / phishing: se han conseguido realizar ataques de ingeniería social contra usuarios mediante el envío de mensajes personalizados.
8. Envío masivo de mensajes: se han conseguido realizar envíos masivos de mensajes contra usuarios o grupos de usuarios.

[23] CCN-CERT IA-17/12 Análisis de WhatsApp (Android). Vulnerabilidades. Diciembre 2012. CCN-CERT

9. Ataques de denegación de servicio contra una cuenta específica: mediante la opción de registro, se ha conseguido registrar un número de forma indefinida, causando una denegación de servicio en la cuenta afectada.
10. Sobre los ficheros que almacena WhatsApp: cabe mencionar que los ficheros multimedia no están cifrados, por tanto, se guardan de forma directa en la carpeta de acceso público. Cualquier fichero enviado por WhatsApp reside en el terminal y es de acceso genérico sin ningún tipo de restricción.
11. Whatsapp utiliza el listado de contacto almacenado tanto en el teléfono como en la tarjeta SIM: esto hace que cualquier persona que disponga de nuestro número de teléfono (conocido o no) pueda ponerse en contacto con nosotros (podría solucionarse realizando los bloqueos a usuarios), ver la imagen del perfil y el mensaje de estado que hayamos seleccionado.

En definitiva debido al elevado número de vulnerabilidades descubiertas en la aplicación, unido al elevado tiempo de reacción frente a una vulnerabilidad por parte de los responsables de la misma, se desaconseja el uso de esta herramienta para fines laborales, así como la inclusión de la misma en dispositivos de la Administración.

En todo caso, se recomienda:

- Proteger la tarjeta SIM con un PIN.
- Incluir un patrón, código o contraseña para acceder al dispositivo móvil.
- Las copias de seguridad almacenadas en la tarjeta de almacenamiento han de estar protegidas con contraseña.
- En caso de robo, se debe denunciar a la policía e indicárselo a la operadora para que anulen la SIM.

ANEXO B. SPOTBROS

La aplicación SpotBros es una aplicación de mensajería instantánea muy similar a las actuales del mercado como WhatsApp y Line. Su principal diferencia radica en el envío de las conversaciones de manera cifrada.

Sin embargo, se han detectado ciertas debilidades en la aplicación:

1. La aplicación almacena en claro la contraseña del usuario en un fichero de configuración, siendo un grave error y un potencial peligro en caso de robo de la cuenta.
2. Las conversaciones se almacenan en el propio terminal sin ningún tipo de cifrado. Esto implica que si el móvil se extravía o es robado se puede acceder a las conversaciones que el usuario no hubiera eliminado previamente.
3. Las imágenes y datos adjuntos viajan en claro.
4. Si se cambia la tarjeta SIM del terminal por otra, la aplicación no detecta dicha modificación, funcionando con las credenciales del anterior usuario (suplantación de identidad).
5. Bajo la configuración por defecto, se permite visualizar todos los contactos que posee un determinado usuario de SpotBros, revelando de esta forma con quién se comunica dicho usuario.
6. Se puede acceder sin autorización a los ficheros adjuntos remitidos entre usuarios de forma independiente a la aplicación y sin autenticación.
7. El empleo de este tipo de aplicación puede dar al usuario final una falsa sensación de seguridad.

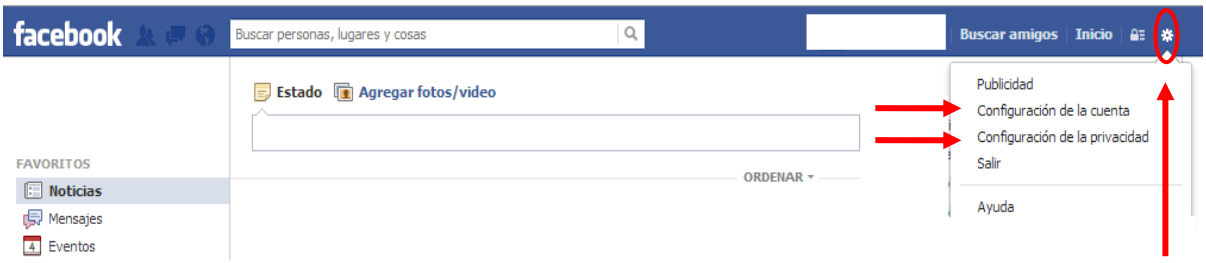
ANEXO C. CONFIGURACIONES BÁSICAS DE SEGURIDAD

El primer consejo recogido en el epígrafe de Buenas prácticas de Seguridad (véase apartado 5) en el uso de redes sociales se fija en la creación cuidadosa del perfil y protección con la configuración de privacidad. No obstante, cada red social cuenta con una política de privacidad y una configuración de seguridad distinta.

Recogemos a continuación la configuración de la privacidad y seguridad de las principales redes sociales implantadas en España.

5.1 Facebook

En la barra superior de navegación del usuario de Facebook, se encuentran el apartado cuenta desde donde se desplegará un menú con diferentes apartados, entre los que se encuentran los que nos interesan en materia de seguridad "**Configuración de la cuenta**" y "**Configuración de la privacidad**".



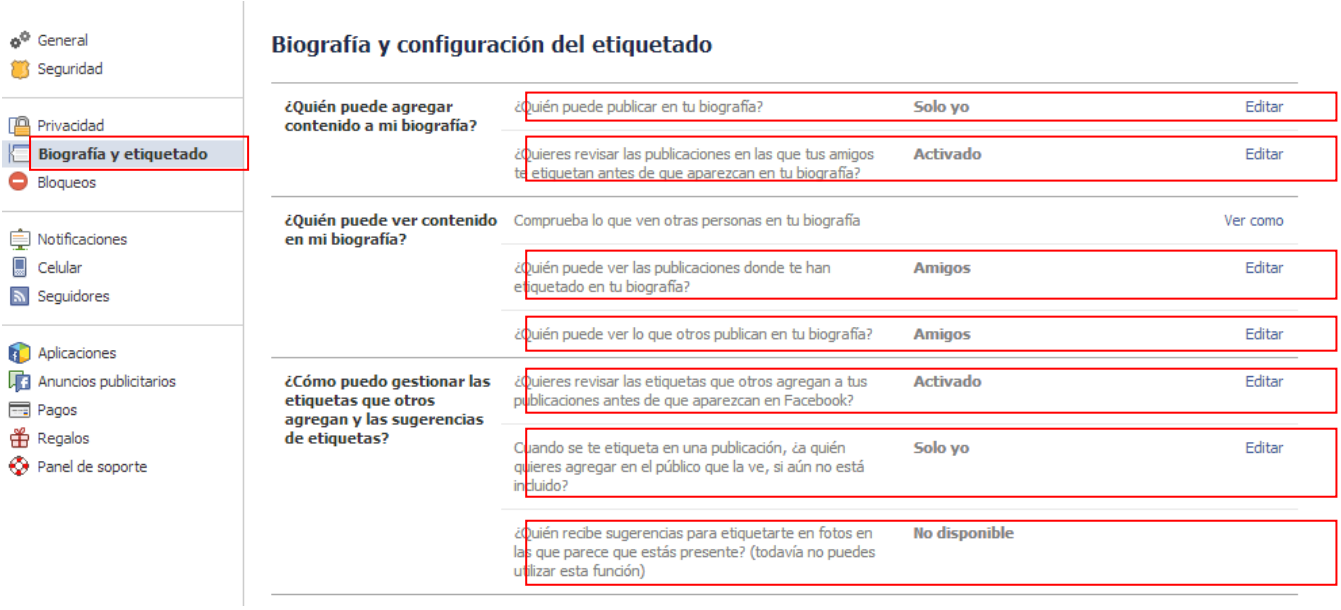
El usuario debe tener siempre muy claro que tipo de información quiere que cada usuario vea sobre él. Facebook nos permite modificar y configurar este aspecto a nuestro criterio. Para ello, se pulsa en el enlace "**Configuración de la privacidad**". En la ventana que aparece, Facebook muestra la configuración que se tiene actualmente. Si se desea modificarla, se proporciona un menú con distintas posibilidades de configuración, que son las siguientes:

Se debe establecer que sólo pueden ver nuestras publicaciones nuestros "amigos" al igual que buscarnos en Facebook por nuestro email y teléfono de registro, ya que no nos permite la opción de deshabilitarlo completamente.

Desmarcar la opción "Permitir que otros motores de búsqueda muestren el enlace de tu biografía" es vital para evitar la indexación no autorizada por parte de buscadores de Internet.

En la siguiente ventana "Seguridad" se activarán las opciones de Navegación segura (usar Facebook a través de una conexión segura siempre que sea posible) y notificaciones de inicio de sesión (informará cuando se acceda a la cuenta desde una computadora o dispositivo móvil que no se haya usado nunca).

También se pueden dar de alta los diferentes dispositivos (móvil) que se utilicen y poner contraseñas a las aplicaciones que se utilicen.



La siguiente ventana "**Biografía y configuración del etiquetado**" es fundamental a la hora de gestionar los contenidos que se publican sobre nosotros. Marcaremos que solo nosotros podemos publicar en nuestra biografía, activaremos la función de revisar las publicaciones en las que tus amigos te etiquetan antes de su publicación y la visibilidad de estas publicaciones en nuestro perfil.

Darte de baja en Facebook

Para darse de baja en Facebook se debe acceder al siguiente enlace https://www.facebook.com/help/delete_account y una vez registrado pulsar en "eliminar cuenta". Siguiendo ese enlace, uno podrá darse de baja para siempre. Teóricamente se elimina todo el contenido por completo de su Web y no podrá acceder nunca más, al menos con ese nombre de usuario.

Si por el contrario se quiere suspender temporalmente la cuenta y tener opción de recuperarla más adelante debe hacerse lo siguiente: Acceder a configuración de la cuenta, Seguridad y allí aparecerá "desactivar tu cuenta".

Seguidamente aparecerá una página donde se preguntará por qué nos damos de baja. Se elige uno de los motivos y se acepta.

Haciendo ésta operación no se está dando de baja uno completamente, ya que si se ingresa con el nombre de usuario y contraseña, que se había dado de baja, se reactiva la cuenta. Asimismo las fotos y demás material no desaparecen aunque no se vuelva a acceder.

5.2 Twitter

Antes de pasar a la configuración de la privacidad, en esta red social hay que tener en cuenta que la transcendencia del contenido de un tweet no queda especialmente limitada a un círculo específico, pues la difusión queda en manos de los distintos usuarios que conocen el asunto twitteado.

Por ello, a través de la opción de "retweet" el usuario originario de la noticia no conocerá con exactitud la relevancia que ha tenido el contenido del mismo. Sin embargo, en algunas ocasiones el contenido de un tweet puede manifestar expresiones que lesionan la dignidad de una persona, perjudican la estima o reputación de otra, o bien atribuye falsamente a una persona la comisión de un hecho considerado como delito.

Este tipo de tweets es llamado "Twibel", acrónimo de "Twitter libel", es decir, tweet difamatorio, cuya autoría está castiga penalmente. Igualmente, aquéllos que faciliten la difusión de un contenido ilícito, como puede ser la pornografía infantil, hechos descubiertos ilícitamente, etc… serán castigados como autores del delito que corresponda.

Publicar o retuitear un contenido no es un acto inocuo y sin importancia, puesto que es posible que se esté difundiendo una información calumniosa o injuriosa e incurriendo con ello en un delito. No se debe retuitear este tipo de información, puesto que se desconoce si es cierto o no, por lo que se puede incurrir en un delito de calumnias.

Así mismo, difundir este tipo de mensajes puede agravar el daño producido a la víctima al haber sido propagado a un mayor número de personas, siendo el número de "retuits" relevante a efectos de la cuantificación económica de la indemnización a percibir por el posible daño causado al honor.

Aquéllos usuarios que utilicen Twitter como soporte para cometer injurias o calumnias, o bien cometan un delito en el que la conducta castigada penalmente consista en la difusión, incurrirán en responsabilidad penal.[24] La reforma del Código Penal pretende penar a aquellas personas que difundan, sin autorización de la persona afectada, imágenes o fotografías, de tal modo que el delito no lo cometerá solo quien difunda por primera vez la grabación, también podría incurrir en él quien retuitee las mismas en redes sociales.

[24] Quirón. J. "El Tweet y su responsabilidad penal". Diciembre 2012

5.2.1 Configuración de la cuenta

Una vez accedemos a nuestro perfil y contraseña, para modificar nuestra configuración de seguridad deberemos ir a la barra que se encuentra en la parte superior de la página abrir el menú que aparece y seleccionar "configuración". A continuación aparecerá la siguiente página de configuración de la cuenta.

Cuenta

Cambia tu configuración de cuenta básica, idioma, privacidad de tweets y ubicación.

Nombre de usuario

El nombre de usuario no puede estar en blanco

https://twitter.com/

Correo electrónico

No puedes tener una dirección de correo electrónico en blanco.

El correo electrónico no será mostrado públicamente Aprender más.

Permitir que otros me encuentren por correo electrónico

Idioma

Español

¿Estás interesado en ayudar a traducir Twitter? Visita el Centro de Traducción.

Zona horaria

(GMT+01:00) Madrid

Ubicación del Tweet

Añade una ubicación a mis Tweets

Cuando publicas un Tweet con una ubicación, Twitter almacena esa ubicación. Puedes activar o desactivar esta opción en cada Tweet. Más

Borrar toda la información de ubicación

Esto borrará toda la información de ubicación de Tweets pasados. Esto puede tomar hasta 30 minutos.

Twittear multimedia

Mostrar multimedia que pueda contener material sensible.

Marca mi multimedia como material sensible.

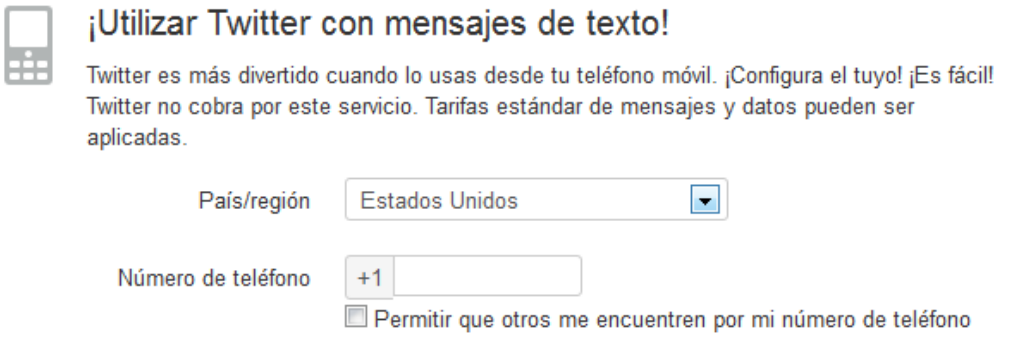
Si publicas imágenes o vídeos que puedan contener contenido sensible, por favor, marca esta casilla para que la gente esté advertida antes de verlo. Más información.

Privacidad de los Tweets

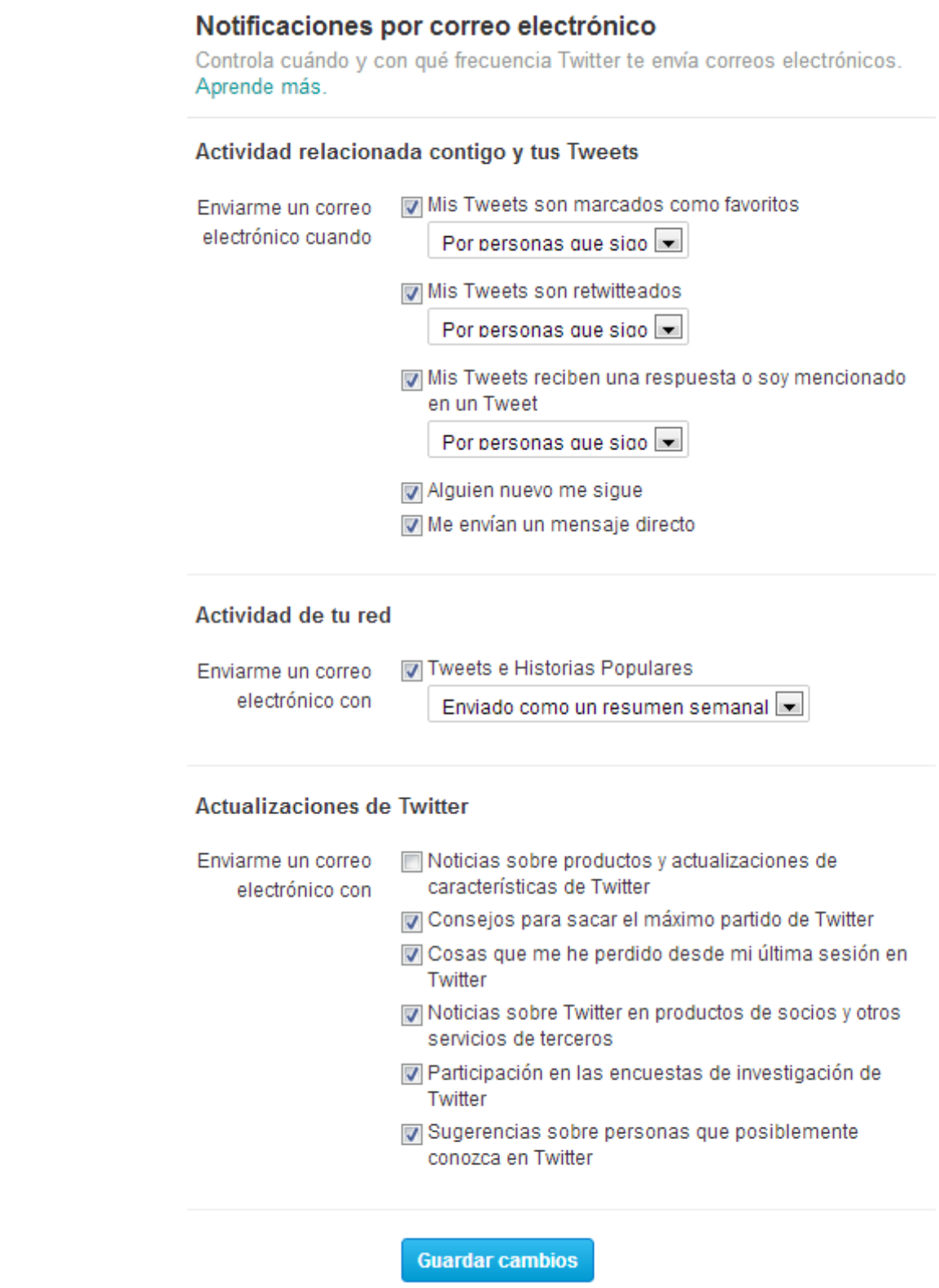
Proteger mis Tweets

Si eliges esta opción, solo los usuarios que apruebes podrán ver tus Tweets. Los Tweets que escribas en el futuro no estarán disponibles públicamente. Los Tweets escritos anteriormente podrían estar aún visibles públicamente en algunos sitios. Más información.

En la pestaña Móvil, **desmarcamos la casilla Permitir** que otros me encuentren por mi número de teléfono.



Twitter también da la opción de configurar las notificaciones que llegarán al correo electrónico. Esto se configurará según quiera el usuario.



Notificaciones por correo electrónico

Controla cuándo y con qué frecuencia Twitter te envía correos electrónicos. Aprende más.

Actividad relacionada contigo y tus Tweets

Enviarme un correo electrónico cuando

- [x] Mis Tweets son marcados como favoritos — Por personas que sigo
- [x] Mis Tweets son retwitteados — Por personas que sigo
- [x] Mis Tweets reciben una respuesta o soy mencionado en un Tweet — Por personas que sigo
- [x] Alguien nuevo me sigue
- [x] Me envían un mensaje directo

Actividad de tu red

Enviarme un correo electrónico con

- [x] Tweets e Historias Populares — Enviado como un resumen semanal

Actualizaciones de Twitter

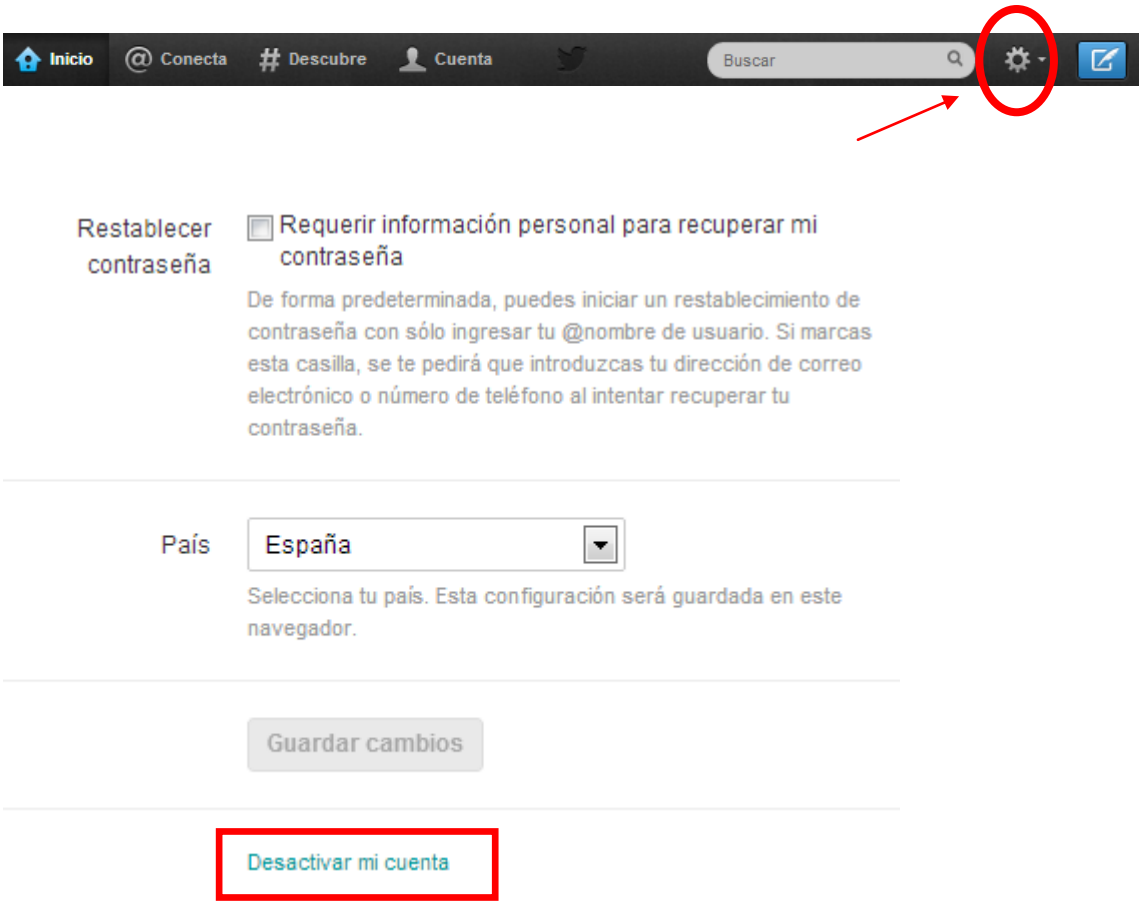
Enviarme un correo electrónico con

- [ ] Noticias sobre productos y actualizaciones de características de Twitter
- [x] Consejos para sacar el máximo partido de Twitter
- [x] Cosas que me he perdido desde mi última sesión en Twitter
- [x] Noticias sobre Twitter en productos de socios y otros servicios de terceros
- [x] Participación en las encuestas de investigación de Twitter
- [x] Sugerencias sobre personas que posiblemente conozca en Twitter

Guardar cambios

Dar de baja una cuenta en Twitter

Si ha tomado la firme decisión de dar de baja la cuenta en Twitter hay que hacer clic en su nombre de usuario, en la esquina superior derecha de la pantalla. Se desplegará un menú. Seleccionar la opción "configuración" y acceder a la ventana de "Preferencias"'. Se debe pulsar el botón "desactivar cuenta", en la parte baja de la pantalla.



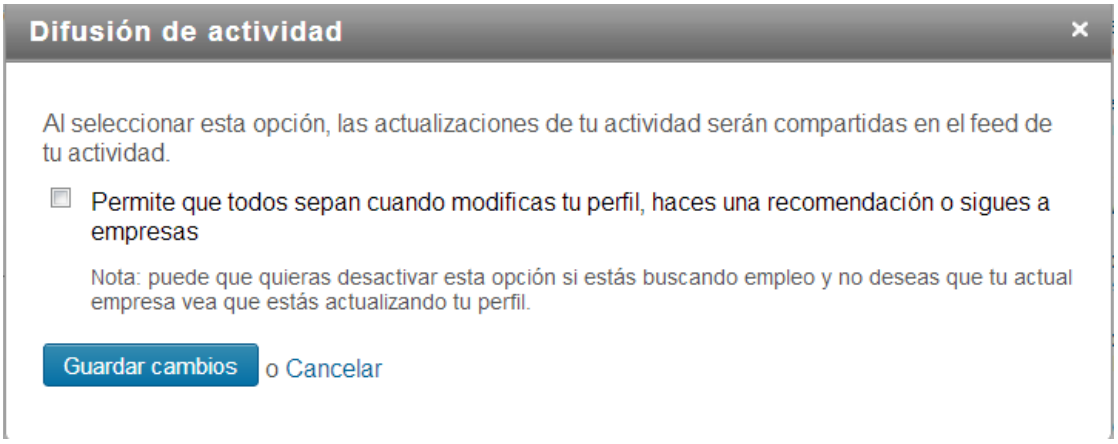
Una vez realizado este paso le aparecerá la siguiente ventana:

Cuando se haya hecho clic sobre "desactivar cuenta" surgirá una pequeña ventana pidiendo confirmación de la decisión. Se debe introducir la contraseña y pulsar sobre "Bien, borrar mi cuenta". Ya se habrá suprimido el perfil en Twitter.

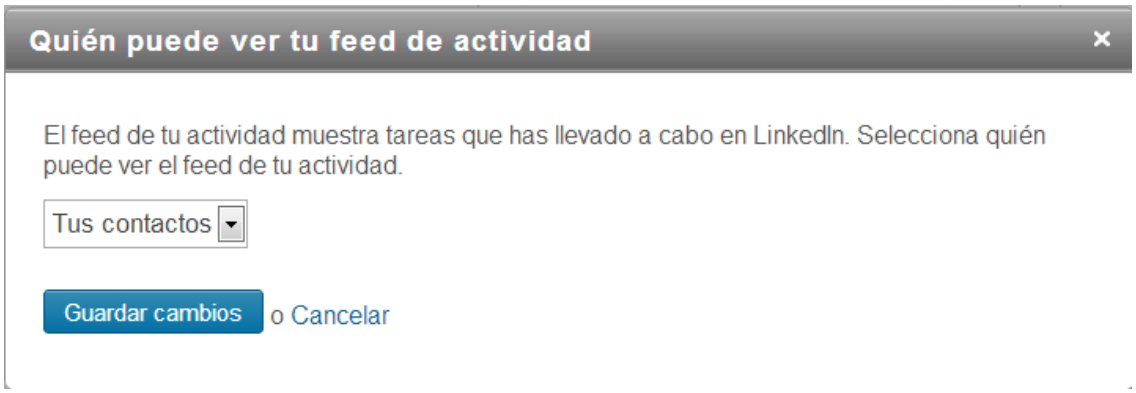
5.3 LinkedIn

A continuación se incorporan una serie de medidas que se pueden adoptar para mejorar la protección de la cuenta con respecto a la privacidad y seguridad.

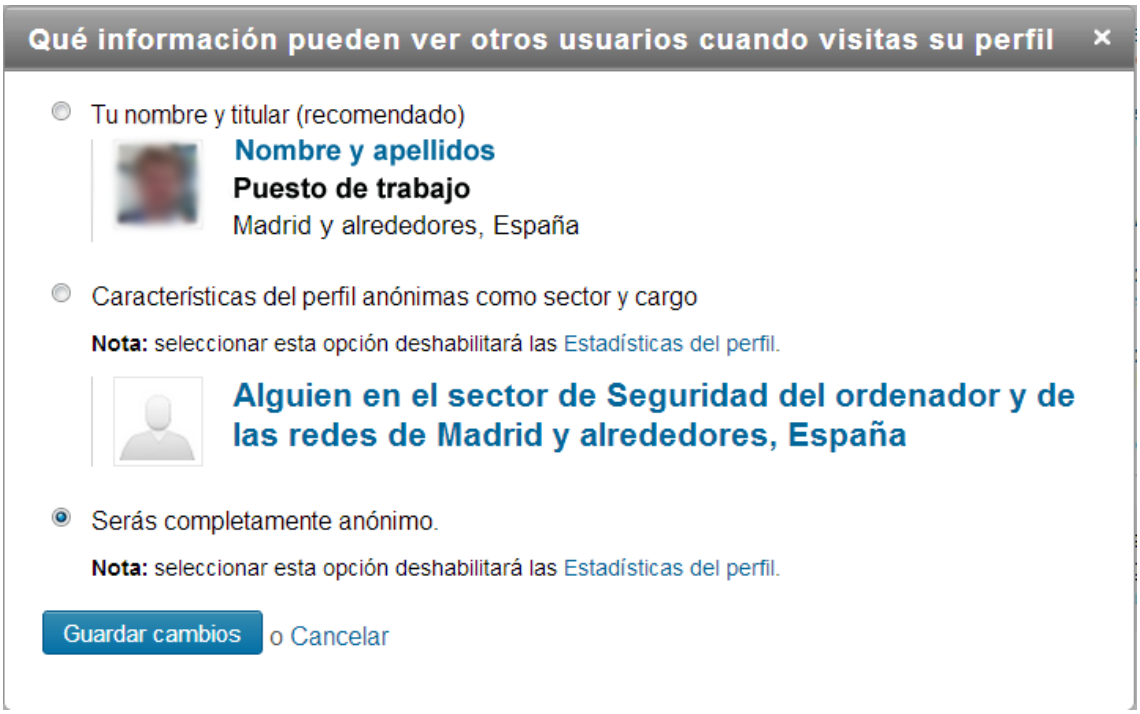
Para acceder a las siguientes opciones se debe hacer clic sobre el nombre del usuario en la parte superior derecha y luego en configuración. Allí se encuentran agrupadas en cuatro categorías los parámetros disponibles



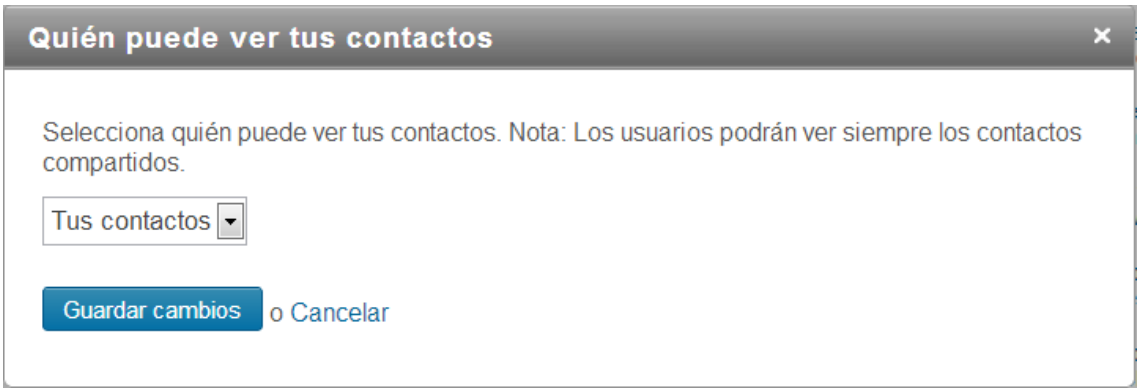
Es importante que la actividad del usuario solo pueda ser vista por sus contactos



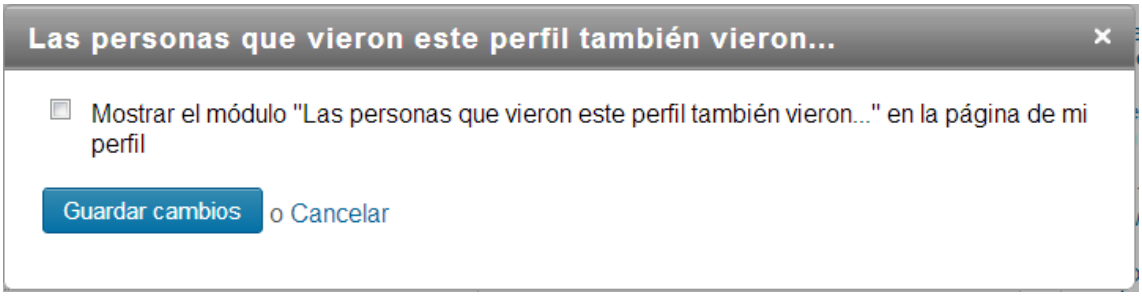
Además, es posible seleccionar que información será mostrada a los contactos cuando visiten el perfil. En base a las necesidades de cada persona, se puede seleccionar nombre y titular (predeterminado), información más genérica o el anonimato total.



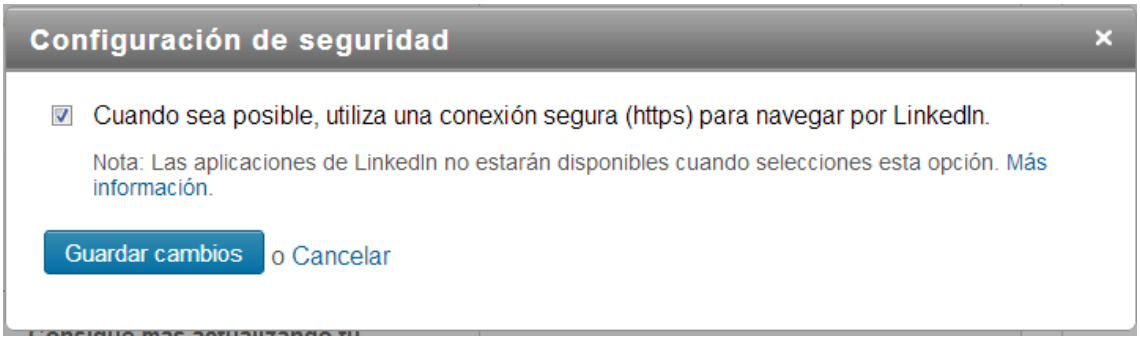
Por otro lado, es importante que los contactos del usuario sólo puedan ser vistos por aquellos que este considera como conocidos.



La selección de esta pestaña es opcional, pero se recomienda que no se marque para evitar que sean vistos contactos semejantes.



Al igual que lo que ocurre con otras redes sociales y servicios de correo electrónico, es posible y recomendable activar la opción de conexión segura (HTTPS), de este modo, la información transmitida entre el cliente y servidor es cifrada con el fin de evitar que un atacante pueda obtener fácilmente las credenciales de acceso u otra información. Es importante mencionar que esta opción afectará al funcionamiento de las aplicaciones de la red social.



Cerrar una cuenta en LinkedIn

Si cierra su cuenta de LinkedIn, no se podrá acceder a los contactos ni a la información que se haya añadido en la cuenta. También significa que nadie podrá ver el perfil en LinkedIn. La eliminación de un perfil público de motores de búsqueda como Yahoo! y Google puede llevar más tiempo y el proceso depende de los propios buscadores.

Se puede cerrar la cuenta de LinkedIn en la página de Configuración o seguir estos pasos.

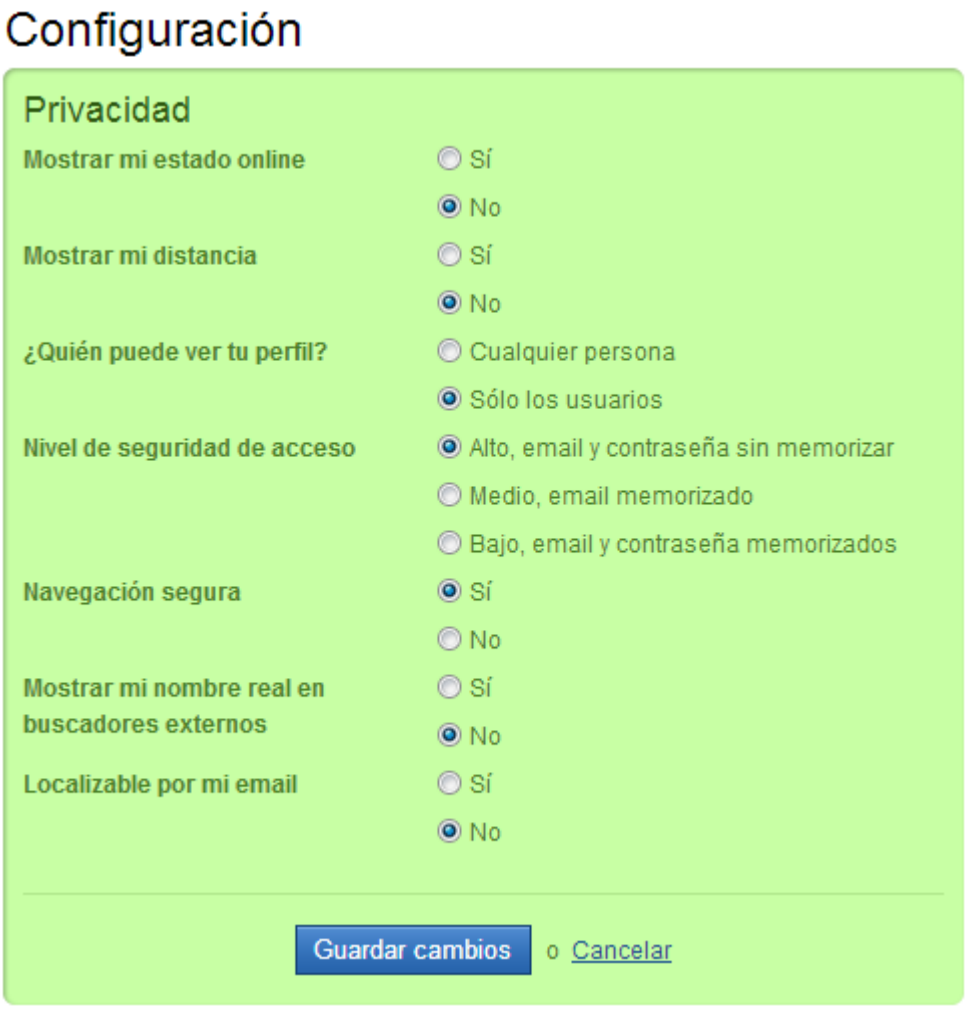
- Pasa el cursor por Configuración.
- Hacer clic en la pestaña Cuentas cerca de la parte inferior de la página y seleccionar "Cerrar tu cuenta".

5.4 Badoo

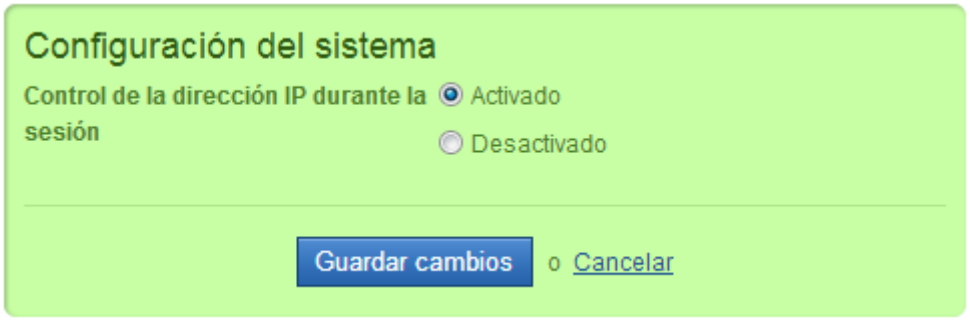
Se puede señalar que fue creada bajo el gran objetivo de acercar a personas para estrechar nuevos lazos de amistad, y por ende, a encontrar pareja. Referente a este gran objetivo, Badoo se ha vuelto una red social experta, brinda a sus usuarios todas las herramientas que permiten alcanzar ese objetivo.

Un sitio fácil de utilizar, de configurar y de navegar será sólo el principio de la oferta. También propondrá herramientas muy interesantes como subir videos, fotos o chatear. Además se incluye crear un perfil único para compartir con los demás usuarios, comentar el perfil de otras personas y agregarlos como amigos o simplemente visitarlos.

A continuación se muestra una configuración básica de seguridad para un perfil en Badoo.



El Control de IP de Badoo, consiste en que Badoo controla la IP desde donde uno se conecta, y si es una IP totalmente distinta a la utilizada por defecto, Badoo activará el modo seguro y no permitirá acceder a los datos personales ni a manipular el perfil de Badoo, así como no dejará que esta nueva IP modifique ni pueda utilizar esa cuenta.



5.5 Instagram

Instagram es una aplicación gratuita para compartir fotos con la que los usuarios pueden aplicar efectos fotográficos como filtros, marcos y colores retro y vintage y compartir las fotografías en diferentes redes sociales como Facebook, Twitter, Tumblr y Flickr. Una característica distintiva de la aplicación es que da una forma cuadrada y redondeada en las puntas a las fotografías en honor a la Kodak Instamatic y las cámaras Polaroid.

Es una aplicación solo disponible para dispositivos móviles y con la que hay que tener especial precaución a la hora de utilizarla. Se comenta este aspecto porque Instagram al poder vincularse a otras redes sociales permite subir el contenido "fotografía" directamente a estas plataformas por defecto.

Esto hace que gracias al atractivo y facilidad que tiene Instagram respecto a la edición de fotografías, muchos usuarios utilizan la aplicación para retocar sus imágenes y una vez hecho esto si no se evita (deseleccionando las pestañas correspondientes) se subirán a la plataforma de Instagram y a las redes vinculadas.

Casos recientes se han dado cuando el usuario al dejar su teléfono a uno de sus hijos y éste realizar una foto desde Instagram, se puede publicar una foto comprometida de su esposa o esposo en Twitter con las consecuencias sociales que esta publicación conlleva.

A continuación se muestra una configuración de seguridad para mantener todas las fotos que se realicen o retoquen con Instagram en privado.

Para acceder a las opciones se pulsa sobre el siguiente icono que aparece arriba en la parte derecha de la pantalla.

A continuación se accede al menú de opciones sobre la que se modificarán los puntos de configuración del "contenido compartido" y "las fotos son privadas". En configuración del contenido compartido no se vinculará ninguna cuenta.

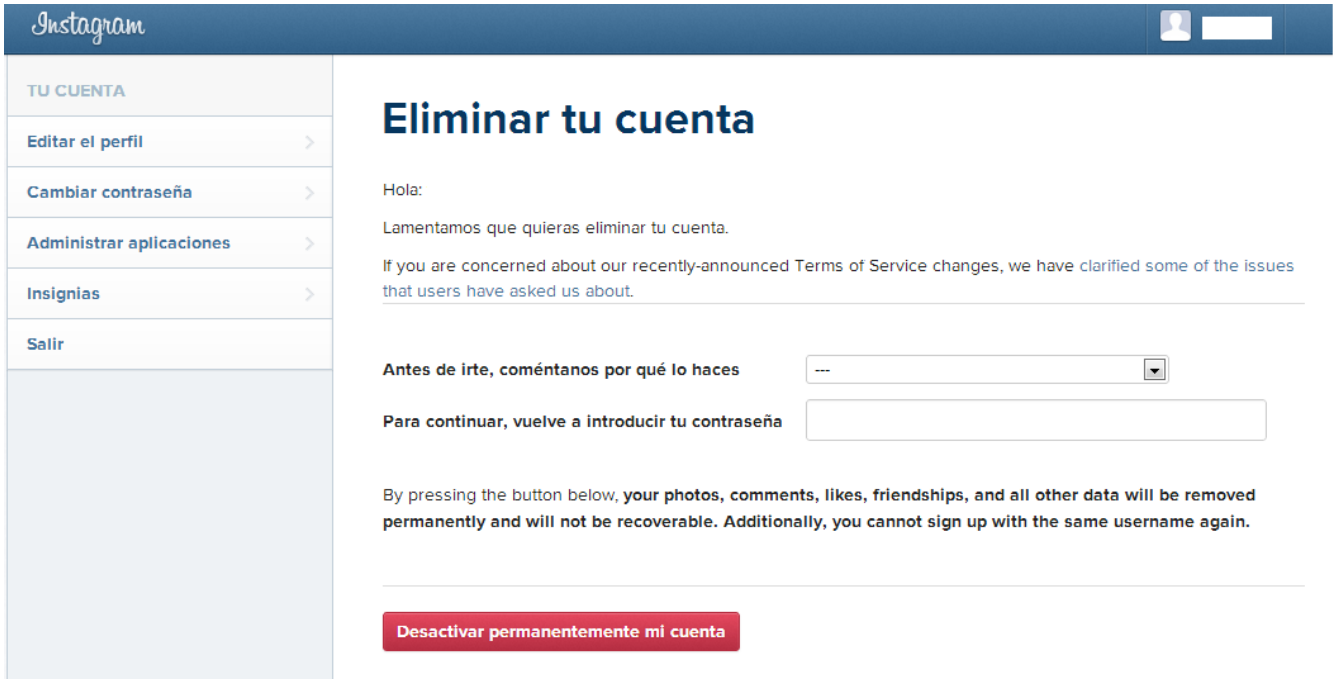
En "las fotos son privadas" al activarlo aparecerá la siguiente ventana, la cual una vez leído el contenido se cliqueará sobre SI, estoy seguro.

Así, se evitará que se vean las fotografías que se suban a la plataforma por gente que no se haya aceptado.

Eliminar una cuenta en Instagram

Para eliminar la cuenta se deberá acceder a la siguiente dirección: https://instagram.com/accounts/remove/ y seguir los pasos hasta pichar en desactivar permanentemente la cuenta.

Como se indica, las imágenes se borrarán y no se podrán recuperar.

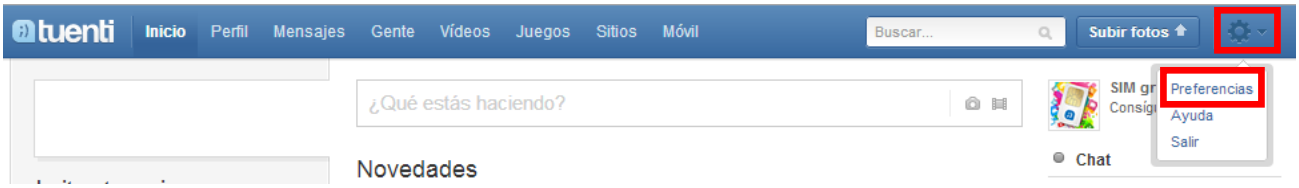


5.6 Tuenti

Tuenti es una red social privada española a la que sólo se accede por invitación. Para registrarte en Tuenti, debes ser invitado por algún usuario que ya pertenezca a la red. Como cualquier otra red social, permite compartir con amigos opiniones, intereses, gustos, fotos, noticias, etc.

Los servicios más destacados que ofrece Tuenti son: Amigos, comentarios y mensajes fotos, álbumes y etiquetas, chat y juegos.

Se puede acceder a las opciones de configuración de la cuenta pulsando en el menú "Mi cuenta", situado en la parte superior derecha de la pantalla, y, a continuación, seleccionando la opción "Preferencias".



La nueva pantalla contiene un menú en el lado izquierdo que te lleva a distintas configuraciones. Las más importantes son las que se encuentran en «Preferencias de mi cuenta», «Privacidad» y «Peticiones»

Es imprescindible configurar correctamente la información que se comparte con el resto de usuarios. En el apartado «Privacidad» se puede personalizar los niveles de privacidad de la cuenta.

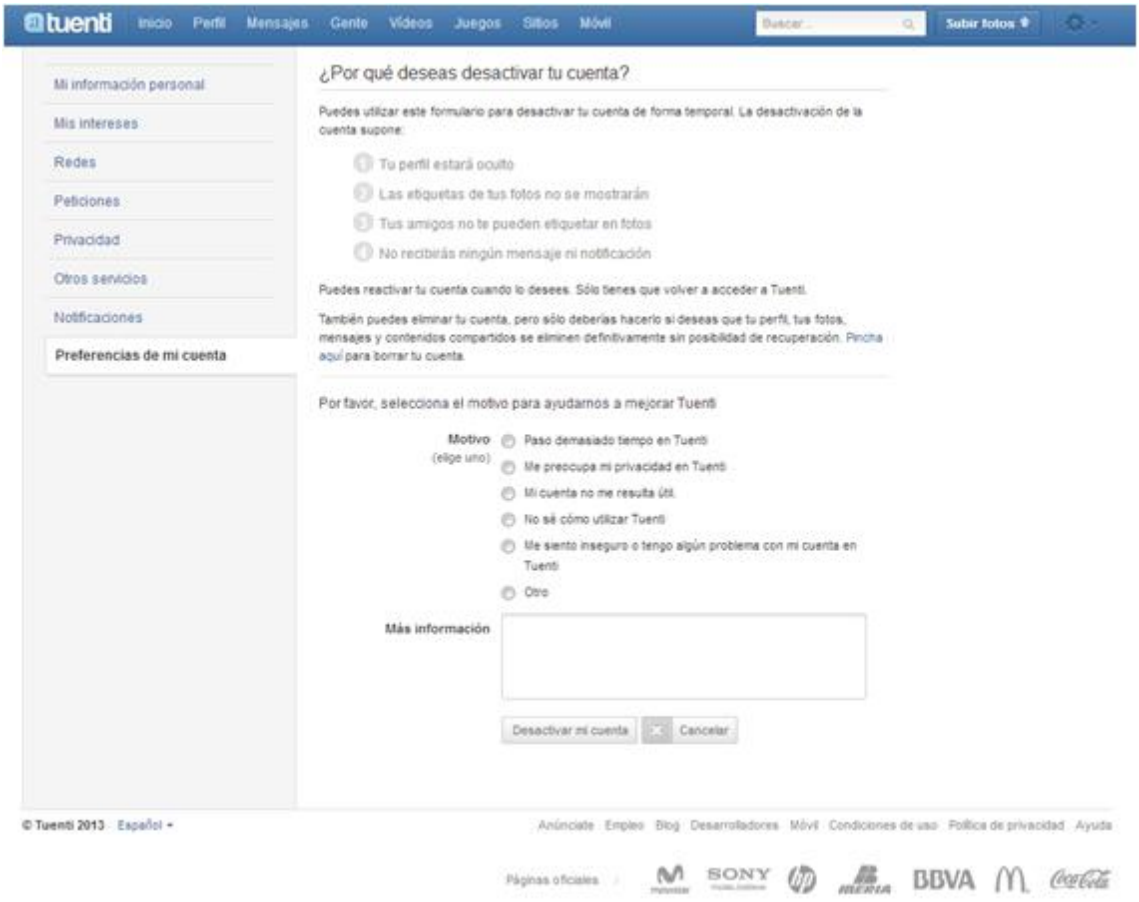
Desactivar la cuenta de TUENTI

Tuenti permite desactivar la cuenta temporalmente, lo cual supone:

1. Tu perfil está oculto.
2. Las etiquetas de tus amigos no se mostrarán.
3. Tus amigos no pueden etiquetarte en las fotos.
4. No recibirás ningún mensaje ni notificación.

Para **desactivar tu cuenta temporalmente** se debe acceder a la opción "Preferencias de mi cuenta" y al final de la pantalla se encontrará una sección llamada "Desactivar cuenta". Si haces clic en el botón, Tuenti redirige a una nueva ventana dónde preguntan los motivos por los que se desea dar de baja la cuenta temporalmente. Selecciona la opción que corresponda con cada caso y pulsar el botón "Desactivar mi cuenta".

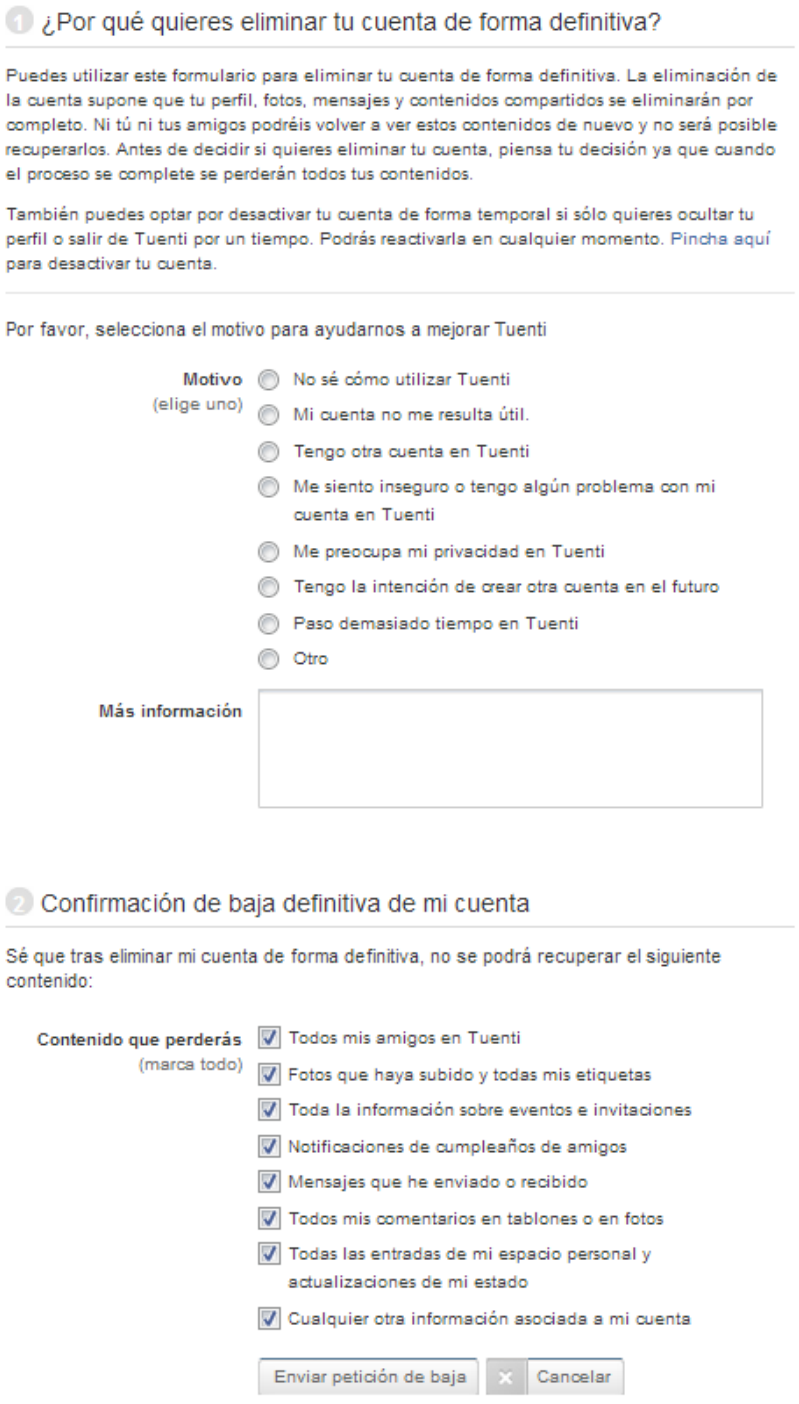
Para reactivar la cuenta simplemente se debe acceder de nuevo a Tuenti.



Por el contrario si prefiere **desactivar la cuenta definitivamente**, se debe acceder al enlace:

http://www.tuenti.com/#m=Settings&func=view_delete_account_page

y marcar las casillas que se indican a continuación y pinchar en "enviar petición de baja"



5.7 Youtube

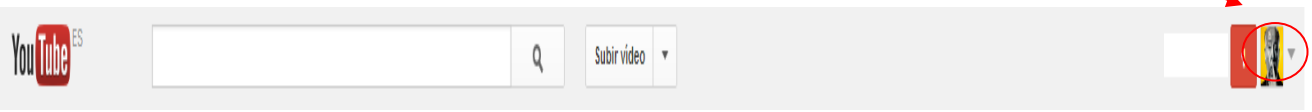
YouTube es un sitio Web en el cual los usuarios pueden subir y compartir vídeos.

Es muy popular gracias a la posibilidad de alojar vídeos personales de manera sencilla. Aloja una variedad de clips de películas, programas de televisión y vídeos musicales. A pesar de las reglas de YouTube contra subir vídeos con derechos de autor, este material existe en abundancia, así como contenidos amateur como videoblogs.

Los enlaces a vídeos de YouTube pueden ser también insertados en blogs y sitios electrónicos personales usando APIs o incrustando cierto código HTML.

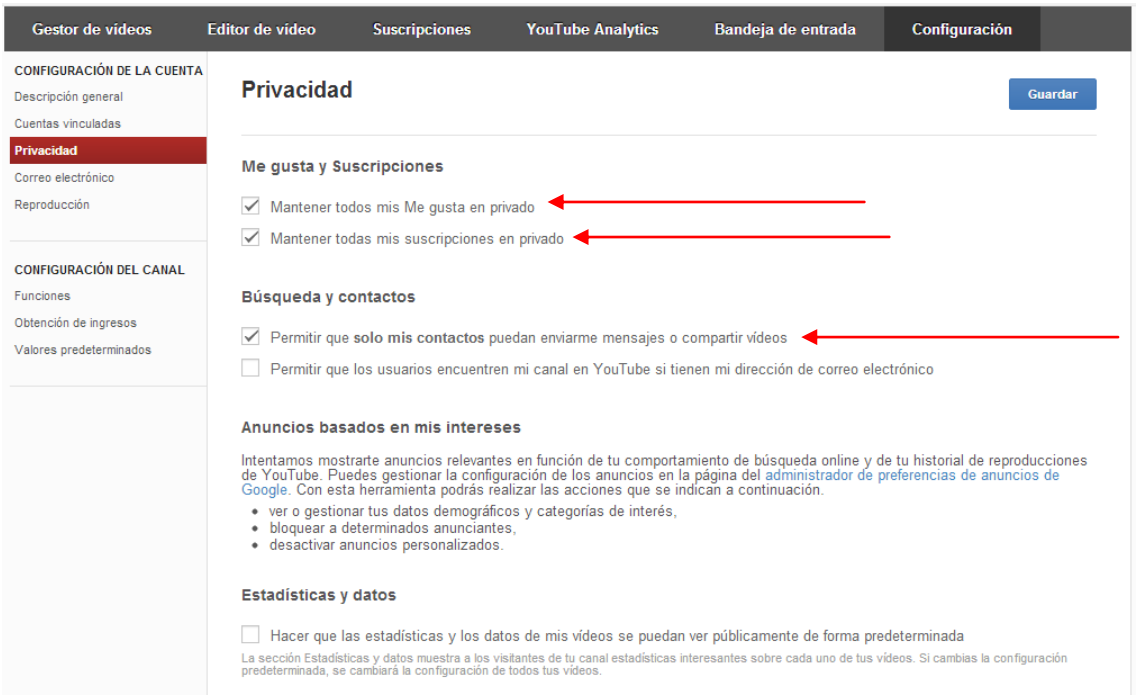
A continuación, se muestra la configuración de seguridad / privacidad básica para esta plataforma.

Para conectarnos a YouTube, ingresaremos con nuestra cuenta de Google. Para acceder a las opciones de privacidad deberemos pulsar sobre la pestaña que se encuentra a la derecha.



Posteriormente, se selecciona configurar Youtube

Seguidamente se accederá a la pestaña de "privacidad" en la que se marcarán las pestañas que se indican a continuación y se dejarán desmarcadas las demás.



Como se ha repetido constantemente durante el documento, se debe leer la política de privacidad de la plataforma. En el caso de Youtube, al pertenecer a Google se deberá configurar también desde la siguiente dirección:

https://www.google.com/settings/privacy

Para dar de baja una cuenta en Youtube es preciso darse de baja en Google, ya que comparten la misma cuenta para diferentes plataformas y servicios de esta compañía (Gmail, Google+, Picassa).

ANEXO D. NOTICIAS PUBLICADAS SOBRE SEGURIDAD EN REDES SOCIALES

Un fallo en Facebook pone al descubierto los números de teléfono de los usuarios

http://www.trecebits.com/2012/10/14/un-fallo-en-facebook-pone-al-descubierto-los-numeros-de-telefono-de-los-usuarios/

TreceBits - 14 /10/2012

Un fallo de seguridad en Facebook hace públicos los mensajes privados

http://www.diariovasco.com/v/20120925/al-dia-sociedad/fallo-seguridad-facebook-hace-20120925.html

Diario Vasco 25/09/2012

Hacker roba cuentas de Twitter de futbolistas

http://deportes.terra.com/futbol/internacional/hacker-roba-cuentas-de-twitter-de-futbolistas,a804dd227d079310VgnVCM4000009bcceb0aRCRD.html

Terra 29/08/2012

Un fallo de seguridad genera el caos en twitter

http://www.publico.es/337794/un-fallo-de-seguridad-genera-el-caos-en-twitter

Público 21/09/2010

LinkedIn investiga la filtración de 6,4 millones de contraseñas a una Web rusa

http://www.elmundo.es/elmundo/2012/06/06/navegante/1338999251.html

El Mundo 06/06/2012

Un fallo de seguridad hace públicas las conversaciones de WhatsApp

http://www.europapress.es/portaltic/movilidad/software/noticia-fallo-seguridad-hace-publicas-conversaciones-whatsapp-20120511163245.html

Europa Press 11/05/2012

Facebook pagará 7,5 millones de euros por vulnerar la privacidad de sus usuarios

http://www.20minutos.es/noticia/1595179/0/facebook/multa/privacidad-usuarios/

20 Minutos 21/09/2012

Paula Vázquez publica su número en Twitter y sufre "móvil-acoso"

http://www.europapress.es/portaltic/socialmedia/noticia-paula-vazquez-publica-numero-twitter-sufre-movilacoso-20121022173131.html

Europa Press 23/10/2012

Posible filtración de 6.5 millones de contraseñas de LinkedIn en Internet

http://tecnologia.elpais.com/tecnologia/2012/06/06/actualidad/1338996950_466073.html

El País 7/06/2012

Piratas informáticos aficionados se lanzan al robo "on line" de claves bancarias en las redes sociales

http://www.elperiodico.com/es/noticias/sociedad/piratas-aficionados-lanzan-robo-line-claves-bancarias-2195619

El Periódico 1/09/2012

Fallos de seguridad permiten el robo y venta de cuentas de Twitter

http://www.inteldig.com/2012/10/fallos-de-seguridad-permiten-el-robo-y-venta-de-cuentas-de-twitter/

IntelDig 1/10/2012

Dos policías de Cerdanyola del Vallès, suspendidos de empleo y sueldo por grabarse bailando mientras patrullaban y publicarlo en YouTube

http://www.huffingtonpost.es/2013/01/21/suspenden-seis-meses-a-lo_n_2521456.html

Huffingtonpost 3/10/2012

Santiago Cañizares revoluciona Twitter al publicar una foto de su mujer desnuda en la ducha

http://www.elmundo.es/elmundo/2012/07/07/valencia/1341685536.html

El Mundo 07/07/2012

Eduardo Casanova (Fidel en 'Aída') cuelga accidentalmente una imagen en twitter/Instagram practicando sexo con su novio

http://www.formulatv.com/noticias/27106/eduardo-casanova-fidel-aida-cuelga-accidentalmente-imagen-sexo-novio/

Formulatv 26/09/2012

ANEXO E. Referencias

[Ref – 1]	**ONTSI** Informe de resultados Observatorio de Redes Sociales Abril 2012
[Ref – 2]	**iRedes-Congreso Iberoamericano de Redes sociales** Diciembre de 2012 http://www.iredes.es/2012/03/iredes-presenta-la-segunda-version-del-mapa-de-las-redes-sociales/
[Ref – 3]	**Nielsen** State of the media: Social Media Report 2012 2012
[Ref – 4]	**Observatorio Tecnológico** Privacidad y seguridad en Redes Sociales Noviembre 2011 http://recursostic.educacion.es/
[Ref – 5]	**ESET** Guía de Seguridad en Redes Sociales 2012 http://www.eset-la.com/
[Ref – 6]	**Pantallas amigas** Grooming, acoso a menores en la Red http://www.pantallasamigas.net/
[Ref-7]	**Microsoft** Protección y privacidad en línea http://www.microsoft.com/
[Ref – 8]	**Department os State Bureau of diplomatic Security** Social Networking Cyber Security Awareness Briefing 2011
[Ref – 9]	**CCN-CERT** Informes de Amenazas STIC IA 06/12 2012 www.ccn-cert.cni.es
[Ref – 10]	**CCN-CERT** Informes de Amenazas STIC IA 17/12 2012
[Ref – 11]	**OSI** Protégete ante la suplantación de identidad en WhatsApp 2012
[Ref – 12]	**Guía de usos y estilo en las redes sociales de la Generalitat de Cataluña** Departamento de Presidencia de Generalitat Febrero de 2012 (quinta edición)

	http://www.gencat.cat/xarxessocials
[Ref – 13]	**Guía práctica para el uso de redes sociales en Ayuntamientos** Consejería de Fomento y Medio Ambiente de la Junta de Castilla y León
[Ref – 14]	**Guía de usos y estilos en las redes sociales del Gobierno Vasco** Junio de 2002 (segunda edición) *www.irekia.euskadi.net/assets/a_documents/1218/Gui%CC%81a_de_usos_y_estilo_en_las_Redes_Sociales_del_Gobierno_Vasco.pdf*
[Ref – 15]	**Mundo Twitter** 2011 José Luis Orihuela. Editorial Alienta
[Ref – 16]	**Las Redes Sociales en Internet** ONTSI 2011 http://www.ontsi.red.es/ontsi/sites/default/files/redes_sociales-documento_0.pdf
[Ref – 17]	**IAB Spain (International Advertaisement Bureau)** **Enero 2013** IV Estudio Anual de Redes Sociales