REDES SOCIALES | Facebook | Linkedin | Privacidad | Identidad digital

No se quede atrapado

Las redes sociales han ampliado nuestras posibilidades de comunicarnos. Pero también de meter la pata o de vernos envueltos en un mar de problemas.

En pocos años ha aumentado de forma exponencial el uso de las redes sociales en nuestro país. Mientras que en 2009 un 51 % de los internautas españoles era usuario de alguna, en 2012 la cifra se elevaba al 79 %.

Este rápido crecimiento está relacionado con la expansión de las nuevas tecnologías y con la generalización de smartphones, tabletas y dispositivos similares.

La mayoría de los internautas se decanta por Facebook (el 96 %). Le siguen YouTube, Twitter, Tuenti, Linkedin y Google+. También destaca la popularidad pujante de Pinterest, Instagram, Tumblr, Badoo o Flickr.

Evite riesgos configurando la privacidad

Muchos de los problemas que surgen en las redes sociales, aunque no todos, podrían evitarse con una buena configuración de las opciones de seguridad y privacidad. Desde el momento en el que decidimos crear nuestro perfil, debemos ser cautos y abstenernos de proporcionar ciertos datos, como nuestro teléfono o dirección, que otras personas pueden utilizar con fines ilícitos.

Tomando como ejemplo Facebook, cabe añadir que, junto con la adecuada configuración de la privacidad, es conveniente determinar las personas o listas de amigos que pueden acceder a nuestro perfil y contactar con nosotros. De lo contrario, nuestras fotografías y buena parte de la información de la cuenta serán accesibles para la mayoría de usuarios, aunque no nos conozcan de nada.

Asimismo, es posible configurar la herramienta de etiquetado de fotos para que el programa nos avise cada vez que alguien nos etiquete. En cualquier momento tenemos la opción de eliminar la etiqueta que nos identifica pero, si no hacemos nada para remediarlo, la fotografía seguirá online en el perfil de quien la subió y de aquellos que la hubieran compartido. Si no estamos conformes con esto, lo mejor es escribir a dicha persona y solicitarle que la retire. De no hacernos caso, podemos trasladar la solicitud a la propia red social (vea el recuadro de *Más información* en la página 17).

CONTROLE SU LISTA DE CONTACTOS PARA EVITAR QUE ALGUNOS COMENTARIOS O FOTOS AFECTEN A SU VIDA PROFESIONAL

CÓMO DESENREDAR LOS PROBLEMAS

Ante una situación problemática que no pueda solucionar directamente con el causante, no se quede de brazos cruzados. Le explicamos las opciones que tiene a su alcance, para que valore si le compensa emprender alguna.

Suplantan su identidad digital con el fin de molestarle, perjudicarle, menoscabar su nombre o su imagen, o divulgar información falsa sobre usted.

Se siente víctima de un posible delito: le están calumniando, han divulgado fotos o vídeos personales de carácter sexual, un menor de su entorno sufre ciberacoso...

Denuncie el problema en la propia red social a través del botón o formulario correspondiente. También puede realizar un requerimiento escrito al domicilio social de la red social.

¿Se soluciona el problema?

SÍ

NO

Fin del problema.

Traslade el caso a la Agencia Española de Protección de Datos. Si hay menores afectados, informe al Defensor del Menor autonómico.

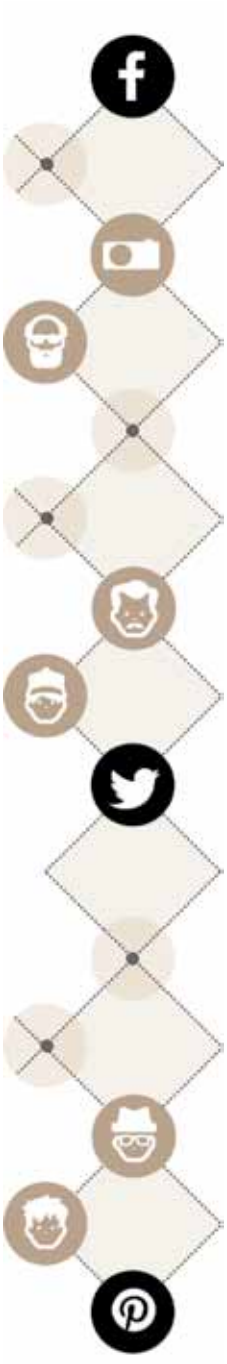
Puede instar un juicio por la vía civil, para proteger su derecho al honor, la intimidad y la propia imagen, dirigiéndose contra quien lo esté vulnerando, si ha podido identificarlo, o contra la red social por no atajar el problema.

Puede poner los hechos en conocimiento de la Fiscalía.

Denuncie los hechos ante la Policía Nacional (puede hacerlo a través de www.policia.es) o ante la Guardia Civil (en www.guardiacivil.es).

Puede instar un juicio por la vía penal, para perseguir delitos de injurias, calumnias, amenazas, acoso..., dirigiéndose contra el causante del perjuicio, si ha logrado identificarlo.

NO PERMITA QUE FOTOS QUE LE PERJUDIQUEN PERMANEZCAN COLGADAS



Es conveniente pensar en el contenido que compartimos y publicamos en las redes sociales. Una mala reputación digital, propiciada por indiscreciones, fotos, vídeos o comentarios inapropiados puede repercutir negativamente en nuestra vida en un momento determinado (por ejemplo, que nos rechacen en una entrevista de trabajo). Pero, además de los problemas derivados del uso inconsciente o inadecuado que pueda realizar uno mismo en las redes sociales, en ocasiones el usuario se ve inmerso en situaciones que son ajenas a sus acciones y a su voluntad.

¡Ese no soy yo!

Uno de los posibles quebraderos de cabeza es que un tercero se haga pasar por nosotros. Lo normal es que tal actuación sea realizada por personas próximas a nuestro entorno. Un ejemplo frecuente de suplantación de identidad se da entre parejas que rompen su relación. Con la intención de difamar o menoscabar la imagen de su ex, una de las partes accede ilegítimamente al perfil del otro (si conocía la contraseña) o crea uno falso.

La Agencia Española de Protección de Datos se ha pronunciado varias veces sobre este tipo de hechos. El 27 de julio de 2011 impuso una multa de 2.000 euros a una joven que suplantó a una supuesta amiga en la red Badoo, creando un perfil falso, con el fin de realizar comentarios inapropiados sobre sus preferencias sexuales *(R/01716/2011)*.

Lo más importante es usar el sentido común

LA MEJOR MANERA DE NO PERDER EL CONTROL SOBRE SUS DATOS ES QUE SOLO SUBA CONTENIDOS QUE NO LE IMPORTE QUE TRASCIENDAN

Otro ejemplo es la suplantación de la personalidad, mediante la creación de perfiles en Facebook y otras redes sociales por parte de la ex pareja de un usuario. La resolución, dictada el 22 de mayo de 2013, sancionó este comportamiento con 2.000 euros *(PS/00427/2012)*. Vea el gráfico de la página 16 para saber cómo actuar en caso de sufrir este u otro tipo de problemas.

Por otra parte, el 20 de junio de 2013, la Agencia Española de Protección de Datos abrió un procedimiento sancionador contra Google, como consecuencia de la modificación de su política de privacidad en marzo de 2012.

Los supuestos incumplimientos detectados son la falta de información adecuada sobre el uso de los datos que se recogen de los usuarios, la posibilidad que se arrogan de compartir la información entre diferentes servicios, el uso para fines desproporcionados de los datos que se les confían y su conservación por tiempo indefinido.

Ellas nos dan trabajo... y nos lo quitan

Las redes sociales son, cada vez más, un instrumento gracias al cual muchos usuarios consiguen un empleo. De hecho, hay redes específicas para este fin (Linkedin es la más conocida).

Pero igual que nos ayudan a ser contratados pueden ser motivo de despido. Una mala configuración de la privacidad, una lista de contactos indiscriminada que englobe a amigos, familiares, compañeros de trabajo e incluso al jefe, unidas a una actitud irresponsable, podrían suponer la pérdida del empleo. Es lo que le ocurrió a un trabajador con una supuesta baja por contractura cervical, que colgó en su perfil un extenso reportaje fotográfico de su visita a un parque de atracciones (*Tribunal Superior de Justicia de Andalucía, 22/03/2012*).

También puede darse el caso de ser despedido por hacer un uso excesivo de las redes sociales en horas de trabajo, desde el ordenador de la oficina.

¿Recomienda usar solo ciertas redes sociales?
Lo que debemos tener claro, antes de usar una red social, es para qué sirve y cómo puedo evitar que la información compartida pueda ser utilizada para perjudicarme en un futuro. La mayoría de las redes nos permiten restringir el acceso mediante las opciones de privacidad, pero muchos de los usuarios no las activan. Cuando alguien crea una cuenta en una red social ha de saber que está creando su huella digital, que es, ni más ni menos, un registro de su vida en diferentes momentos. Lo realmente importante no es en qué red social te inscribes sino utilizar el sentido común antes de publicar cualquier cosa.

¿Cuáles son los mayores riegos a la hora de utilizar las redes?
El hecho de publicar demasiados datos personales, información sobre tus relaciones y lo que haces en tu tiempo libre puede traer consecuencias desagradables. Deberíamos abstenernos de publicar datos personales como el número de teléfono o nuestra dirección. Si lo hacemos y además anunciamos que nos vamos de vacaciones, por ejemplo, podríamos ponérselo fácil a los ladrones. Además, también recomiendo evitar ordenadores de acceso público y, si se utilizan, no guardar las contraseñas y desconectarse debidamente.

Si abandonamos una red, ¿qué pasa con nuestros datos y fotos?
Habría que dirigirse a las condiciones de uso y política de privacidad. Por ejemplo, en Facebook podemos desactivar la cuenta o eliminarla. Cuando la desactivas, los datos no son borrados y aunque tu biografía ya no está disponible sigues saliendo en las listas de amigos. Al eliminar la cuenta, nuestros datos quedan almacenados en copias de seguridad durante un mes, pero no estarán disponibles para terceros, solo para las administraciones públicas, jueces y tribunales.

Omar Valle Moreno
Especialista en protección de datos (Gidat. Valencia)

MÁS INFORMACIÓN

En nuestra página web le explicamos, paso a paso, cómo mejorar las opciones de seguridad y privacidad de su cuenta de Facebook y le proporcionamos algunos consejos prácticos.

www.ocu.org/privacidad-redes-sociales

OCU ACONSEJA

Precaución y protección

- **Al crear una cuenta o perfil en una red social (o en cualquier página web, en general), la mayoría de usuarios marcan y aceptan tanto las condiciones de uso como la política de privacidad, sin mirararlas siquiera. Léalas tranquilamente para asegurarse de que está conforme con el uso y el tratamiento de sus datos.**
- **Establezca, de forma inicial, las opciones de privacidad de sus perfiles en las redes sociales. Además, si se producen cambios relacionados con la política de uso y privacidad, adapte la configuración.**
- **Nunca facilite sus claves y contraseñas a terceros.**
- **Es recomendable que mantenga distintos perfiles, teniendo en cuenta la red social y sus objetivos (uno profesional, uno personal, etc.).**
- **En la red no vale todo. Compórtese de una manera correcta, como lo haría en cualquier ámbito presencial.**
- **Enseñe a los menores a ser cautelosos y a practicar una navegación responsable. Use filtros para evitar peligros.**
- **Haga un uso moderado y responsable de las redes sociales en su trabajo. Si en su empresa se han establecido limitaciones de utilización, cúmplalas para evitar problemas.**