RGPD
LOPDGDD
✓

Guía de uso y buenas prácticas de las redes sociales

Programa de cumplimiento activo de la normativa de protección de datos personales
CUMPLE
audidat
PROTECCIÓN DE DATOS

GUÍA DE USO Y BUENAS PRÁCTICAS DE LAS REDES SOCIALES

I. OBJETO DEL DOCUMENTO

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

En este sentido, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016) (RGPD), establece un marco sólido y coherente para la protección de datos en la Unión Europea, reforzando la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

En España, la protección de datos personales también es un derecho fundamental de las personas físicas consagrado en la Sentencia 292/2000, de 30 de noviembre de 2000, del Tribunal Constitucional (BOE núm. 4, 04-01-2001) (STC 292/2000).

A este respecto, cabe citar la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, 06-12-2018) (LOPDGDD), que tiene por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679.

Como consecuencia de lo anterior, la Dirección / Órgano de Gobierno de RECREATIVOS HERMANOS BLANCO S.L. ha asumido la máxima responsabilidad y compromiso con el establecimiento, implementación y mantenimiento de una Política de Protección de Datos en dicha entidad, garantizando la mejora continua con el objetivo de alcanzar la excelencia en relación con el cumplimiento del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018.

La Política de Protección de Datos de RECREATIVOS HERMANOS BLANCO S.L. descansa en el principio de «responsabilidad proactiva», según el cual el responsable del tratamiento es responsable del cumplimiento del marco normativo y jurisprudencial que gobierna dicha Política, y es capaz de demostrarlo ante las autoridades de control competentes.

En tal sentido, interesa subrayar que un uso inadecuado de las redes sociales puede conllevar importantes riesgos para los derechos y libertades de las personas físicas. En su consecuencia, el objeto del presente documento es establecer una «Guía de uso y buenas prácticas de las redes sociales», a fin de garantizar un correcto cumplimiento de la normativa de protección de datos personales en relación con la utilización de las redes sociales de la entidad por parte del personal autorizado de RECREATIVOS HERMANOS BLANCO S.L..

A tal fin, se han seguido las orientaciones y directrices recogidas en los siguientes documentos:

- «Buenas prácticas en Redes Sociales». CCN-CERT BP/08. Centro Criptológico Nacional (CCN). Agosto 2018.

- Guía de Seguridad de las TIC. CCN-STIC 821. Apéndice V: Normas de Creación y Uso de Contraseñas NP40. Centro Criptológico Nacional (CCN).
- Consideraciones a tener en cuenta al publicar en redes sociales. Oficina de Seguridad del Internauta (OSI) del Instituto Nacional de Ciberseguridad de España (INCIBE).
- Recomendaciones de la Agencia Española de Protección de Datos (AEPD).

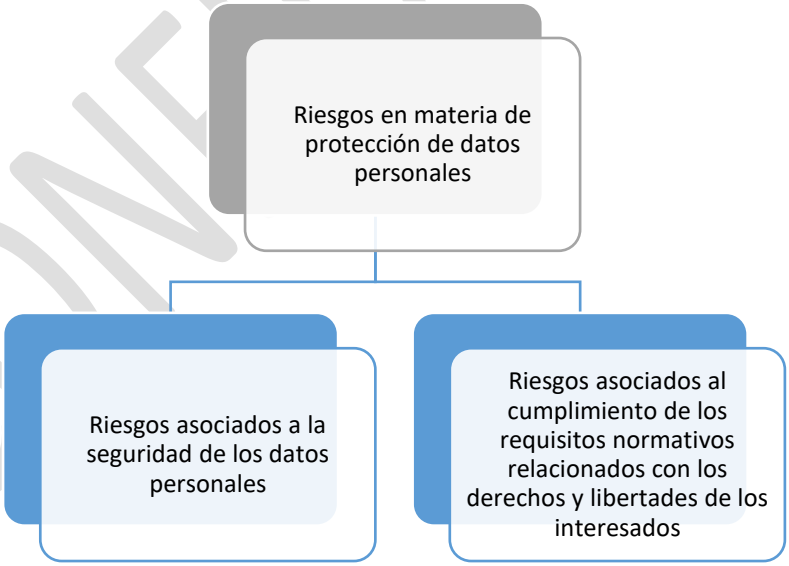
II. RIESGOS ASOCIADOS A LA SEGURIDAD Y A LA PRIVACIDAD EN LAS REDES SOCIALES

Para la Agencia Española de Protección de Datos, un «riesgo» se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas.

Así mismo, una «amenaza» es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos personales se realiza un tratamiento.

Como puede observarse, las amenazas y los riesgos asociados están directamente relacionados. En su consecuencia, la identificación de los riesgos comporta, en todo caso, considerar las amenazas que los pueden originar.

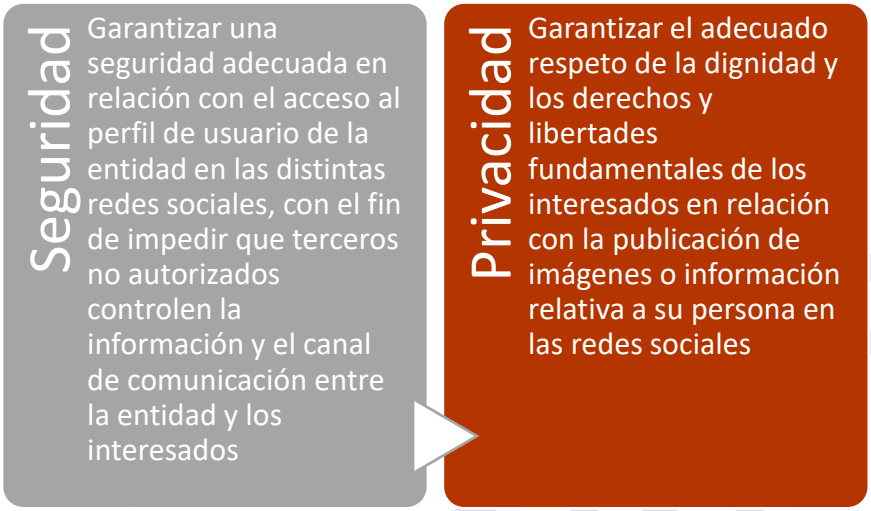
Desde la óptica de la protección de datos personales, los principales riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, se pueden categorizar en dos dimensiones básicas: a) riesgos asociados a la seguridad de los datos personales y b) riesgos asociados al cumplimiento de los requisitos normativos relacionados con los derechos y libertades de los interesados.



En el ámbito concreto de la utilización de las redes sociales por parte del responsable del tratamiento, podemos diferenciar dos categorías específicas de riesgos:

1. **Riesgos asociados a la seguridad en el acceso al perfil de usuario de la entidad:** Garantizar una seguridad adecuada en relación con el acceso al perfil de la entidad en las distintas redes sociales, con el fin de impedir que terceros no autorizados controlen la información y el canal de comunicación entre la entidad y los interesados.

2. **Riesgos asociados a la privacidad (principios de la protección de datos):** Garantizar el adecuado respeto de la dignidad y los derechos y libertades fundamentales de los interesados en relación con la publicación de imágenes o información relativa a su persona en las redes sociales.



III. SEGURIDAD

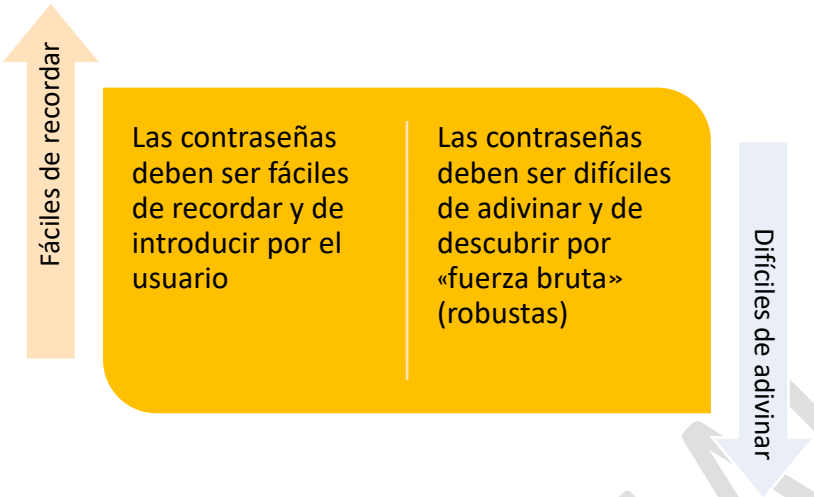
Las contraseñas son el mecanismo de autenticación más generalizado para el acceso al perfil de usuario en las redes sociales. En tal sentido, la aprobación, difusión y cumplimiento de una política de buenas prácticas en la creación, uso y cambio de contraseñas de acceso al perfil de nuestra entidad en las distintas redes sociales, es un aspecto trascendental para garantizar una seguridad y confidencialidad adecuadas y, en particular, para impedir que terceros no autorizados accedan a nuestro perfil y, por tanto, no solo controlen la información sino el propio canal de comunicación entre nuestra entidad y los interesados.

1. CREACIÓN DE LAS CONTRASEÑAS DE ACCESO AL PERFIL

Tal y como señala el Centro Criptológico Nacional, una de las causas principales de los accesos ilegítimos en redes sociales a datos personales e imágenes protegidas es la debilidad de las contraseñas elegidas por los usuarios para el acceso a las mismas.

De tal modo, para garantizar una seguridad adecuada de la información personal y de los contactos de nuestra entidad en las redes sociales, es necesario que las contraseñas que se utilicen como mecanismo de autenticación para el acceso a las mismas sean «robustas», esto es, difícilmente vulnerables.

En tal sentido, las contraseñas deben ser fáciles de recordar y de introducir por el usuario, y asimismo difíciles de adivinar y de descubrir por «fuerza bruta». El ataque de fuerza bruta es la forma de descubrir una contraseña probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.



En el ámbito de la ciberseguridad, la Agencia Española de Protección de Datos recomienda la utilización de sistemas de autenticación de doble factor para el acceso a la información. En este sentido, cabe señalar que algunas redes sociales tienen implantada la opción de verificación en dos pasos para el acceso de los usuarios a su perfil.

El uso de un segundo factor de autenticación consiste en una capa de seguridad «extra», de manera que, aparte del código o identificador de usuario y la contraseña, sea preciso un elemento adicional de comprobación para el acceso al perfil de usuario de la red social (por ejemplo, un código numérico de un solo uso enviado al usuario por SMS).

En su consecuencia, al margen de las directrices generales para la creación de contraseñas robustas que se expondrán a continuación, se recomienda la utilización de un segundo factor de autenticación para el acceso al perfil de usuario de las redes sociales, siempre que ello sea técnicamente posible.

a) Las contraseñas deben ser difíciles de adivinar y de descubrir por «fuerza bruta».

Para que las contraseñas sean suficientemente fuertes y difícilmente adivinables por terceros, con carácter general deberán seguirse las siguientes «Directrices generales para la creación de contraseñas robustas»:

(vid. página siguiente)

Directrices generales para la creación de contraseñas robustas

1. Deberán tener una longitud mínima de 8 caracteres.
2. Deberán combinar caracteres de distinto tipo: letras mayúsculas y minúsculas, números y signos de puntuación. En caso de dificultad del usuario para recordar una contraseña de estas características, podrá utilizarse una contraseña de tipo «passphrase»: una contraseña larga formada por una secuencia de palabras cuya deducción, automática o no, no sea simple.
3. No deberán coincidir con el código o identificador de usuario.
4. No deberán estar basadas en cadenas de caracteres que sean fácilmente asociables al usuario: nombre, apellidos, ciudad o fecha de nacimiento, número de DNI, nombres de familiares, matrícula del coche, etc., o combinaciones de las mismas (por ejemplo, nombre + año de nacimiento).
5. No deberán estar basadas en el uso de caracteres repetitivos (por ejemplo, «aaaaaaaa») o secuenciales (por ejemplo, «1234abcd»)
6. No deberán coincidir con palabras sencillas en cualquier idioma que puedan figurar en un diccionario (por ejemplo, «caracola»).
7. No deberán estar basadas en palabras formadas por caracteres próximos en el teclado (por ejemplo, «qwertyui»).
8. No deberán coincidir con frases famosas o refranes, estrofas de canciones o frases impactantes de películas o de obras de literatura.
9. La contraseña no deberá ser igual a ninguna de las últimas contraseñas usadas, ni estar formada por una concatenación de ellas (no reutilización).

b) Las contraseñas deben ser fáciles de recordar y de introducir por el usuario.

Como hemos señalado anteriormente, las contraseñas también deben ser fáciles de recordar por el usuario. En este sentido, un mecanismo útil para recordar una contraseña creada a partir de una combinación de caracteres de distinto tipo, son los llamados «acrósticos», que consisten en seleccionar un carácter de cada palabra de una frase fácilmente memorizable. Por ejemplo, la frase «Mi nombre es Mata Hari. Tengo 41 años.», puede generar la cadena de caracteres «MneMH.T41a.».

Si, no obstante, el usuario sigue teniendo dificultades para recordar su contraseña, existe la amenaza de que la apunte en un papel, pósit, o en cualquier otro lugar no seguro, comprometiendo la confidencialidad de la misma. En dicho caso concreto, se ha de implementar una solución de compromiso entre la robustez de la contraseña y la facilidad con la que el usuario puede recordarla, como utilizar una contraseña de tipo «passphrase»: una contraseña larga formada por una secuencia de palabras cuya deducción, automática o no, no sea simple (por ejemplo, «lapiceronubecoche»). Dicha secuencia de palabras también puede incluir los

espacios en blanco (por ejemplo, «lapicero nube coche»). Así mismo, pueden utilizarse frases cortas sin sentido (por ejemplo, «me voy de compras al río»).

2. USO DE LAS CONTRASEÑAS DE ACCESO AL PERFIL

Para preservar la confidencialidad de las contraseñas, con la finalidad de impedir el acceso o uso no autorizados del perfil de nuestra entidad en las redes sociales, los usuarios deberán cumplir las siguientes «Directrices generales de uso de contraseñas»:

Directrices generales de uso de contraseñas

1. El usuario deberá salvaguardar en todo momento el carácter confidencial, personal e intransferible de la contraseña. No deberá entregarla ni comunicarla a nadie. En caso de haber tenido necesidad de hacerlo por motivos de trabajo o mantenimiento, el usuario deberá proceder a cambiarla de forma inmediata.
2. El usuario no deberá apuntar su contraseña en un papel, pósit, o en cualquier otro lugar no seguro.
3. El usuario no deberá escribir su contraseña en correos electrónicos ni en formularios web cuyo origen no sea confiable.
4. El usuario no deberá utilizar la misma contraseña para el acceso a distintos servicios o recursos (por ejemplo, distintas redes sociales).
5. El usuario no deberá utilizar la misma contraseña para uso profesional y para uso personal o doméstico.
6. El usuario no deberá hacer uso de funcionalidades de recordatorio de contraseñas, ya que pueden facilitar el acceso a personas no autorizadas.
7. El usuario deberá proceder a cambiar la contraseña de forma inmediata si tiene indicios de que la confidencialidad de la misma ha podido verse comprometida.

3. CAMBIO DE CONTRASEÑAS DE ACCESO AL PERFIL

A pesar de lo robusta que sea una contraseña, la confidencialidad de la misma puede verse comprometida con el paso del tiempo. En su consecuencia, las contraseñas deben ser cambiadas periódicamente.

En este sentido, la contraseña de acceso al perfil de la entidad en cada red social deberá ser cambiada, como mínimo, cada doce meses (un año), y preferiblemente cada seis meses. Así mismo, en caso de que se tengan indicios de que la confidencialidad de la contraseña ha podido verse comprometida, esta deberá cambiarse inmediatamente.

IV. PRIVACIDAD (PRINCIPIOS DE LA PROTECCIÓN DE DATOS)

La segunda categoría de riesgos específicos en relación con la utilización de las redes sociales por parte del responsable del tratamiento, se refiere a los riesgos asociados a la privacidad, esto es, garantizar el adecuado respeto de la dignidad y los derechos y libertades fundamentales de los interesados en relación con la publicación de imágenes o información relativa a su persona en las redes sociales.

En este sentido, y dado que, como veremos, los menores son personas vulnerables que merecen una protección específica en las redes sociales, se establecerán, de un lado, unas directrices generales sobre la publicación de imágenes o información personal en redes sociales y, de otro lado, unas directrices específicas relativas a los menores de edad.

1. PUBLICACIÓN DE IMÁGENES O INFORMACIÓN PERSONAL EN REDES SOCIALES

Con la finalidad de garantizar el adecuado respeto de la dignidad y los derechos y libertades fundamentales de los interesados, los usuarios con acceso autorizado al perfil de la entidad en una o varias redes sociales deberán cumplir las siguientes «Directrices generales sobre la publicación de imágenes o información personal en redes sociales»:

(vid. página siguiente)

Directrices generales sobre la publicación de imágenes o información personal en redes sociales

1. La publicación de imágenes o información personal en las redes sociales requerirá el consentimiento previo del propio interesado. En tal sentido, habrá de informarse, utilizando un lenguaje claro y sencillo, sobre el tipo de imágenes o información que se pretende publicar, en qué redes sociales, con qué finalidad, quién podrá acceder a la información publicada, así como acerca de la posibilidad de ejercitar los derechos de acceso, rectificación, oposición y supresión.
2. El consentimiento del interesado no será necesario para la publicación en las redes sociales de imágenes de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público, salvo en el supuesto de que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza.
3. Así mismo, tampoco será necesario el consentimiento del interesado para la publicación de su imagen cuando esta aparezca como meramente accesoria en relación con la información gráfica sobre un suceso o acaecimiento público, esto es: la imagen es captada de manera accidental y secundaria en relación con el resto de la información gráfica en la que se inserta (menor tamaño, secundariedad de planos o carácter fugaz de la imagen del interesado, respecto al acontecimiento público que es el principal objeto de la fotografía o del vídeo). Si la imagen de la persona captada en el espacio en el que tiene lugar el evento público no aparece de manera meramente accesoria, deberá obtenerse el consentimiento del interesado.
4. Antes de publicar cualquier imagen o información personal en una red social, el usuario deberá reflexionar y hacer una evaluación del tipo de imagen o información, la pertinencia de su publicación y la finalidad de la misma. Cada vez más personas y empresas observan y analizan las redes sociales para adoptar un juicio sobre otras personas.
5. El usuario no deberá publicar en las redes sociales datos muy personales, cuyo conocimiento por parte de terceros no autorizados pueda implicar graves repercusiones en la vida cotidiana del interesado, tales como: documentos identificativos, números de teléfono, direcciones postales, localizaciones exactas, identificadores de vehículos, etc.
6. El usuario no deberá etiquetar por su nombre a otras personas que no tengan perfil en la red social sin solicitar previamente su consentimiento para hacerlo.
7. Deberá comprobarse periódicamente la configuración de privacidad tanto en el perfil de la entidad en la red social, como en los contenidos que se comparten.
8. Se deberá mantener en privado la lista de contactos y analizar en detenimiento las solicitudes de amistad de desconocidos.

2. PUBLICACIÓN DE IMÁGENES O INFORMACIÓN PERSONAL DE MENORES DE EDAD

De acuerdo con lo establecido en el Reglamento general de protección de datos, los menores son personas vulnerables que merecen una protección específica de sus datos personales. En este sentido, debe prestarse una especial atención en relación con la publicación de imágenes o información personal de menores de edad en las redes sociales, a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales. De tal modo, los usuarios deberán cumplir las siguientes «Directrices sobre la publicación de imágenes o información personal de menores de edad en redes sociales»:

Directrices sobre la publicación de imágenes o información personal de menores de edad en redes sociales

1. La publicación de imágenes o información personal de menores de edad en las redes sociales requerirá el consentimiento del propio interesado cuando este sea mayor de catorce años o, en caso de que sea menor de catorce años, el de los titulares de la patria potestad o tutela del menor.
2. En relación con la obtención del consentimiento, habrá de informarse previamente, utilizando un lenguaje claro y sencillo, sobre el tipo de imágenes o información que se pretende publicar, en qué redes sociales, con qué finalidad, quién podrá acceder a la información publicada, así como acerca de la posibilidad de ejercitar los derechos de acceso, rectificación, oposición y supresión.
3. Al margen del citado consentimiento, antes de publicar cualquier imagen o información personal relativa a un menor de edad en una red social, deberá hacerse una evaluación del tipo de imagen o información, la pertinencia de su publicación y la finalidad de la misma.
4. En el caso de las imágenes, habrá de prestarse una especial atención a aspectos como el entorno o la vestimenta del menor, a fin de preservar su dignidad y sus derechos fundamentales.
5. Cuando se publique la imagen de un menor, sin haber obtenido el consentimiento previo, como meramente accesoria en relación con la información gráfica sobre un suceso o acaecimiento público, deberán adoptarse las medidas técnicas adecuadas que no permitan en ningún caso la identificación del menor.

V. ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

Todos los usuarios con acceso autorizado al perfil de la entidad en una o varias redes sociales deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente «Guía de uso y buenas prácticas de las redes sociales», debiendo suscribir las normas y directrices recogidas en la misma a través del siguiente modelo de «Aceptación y compromiso de cumplimiento»:

ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO DE LA «GUÍA DE USO Y BUENAS PRÁCTICAS DE LAS REDES SOCIALES»

Mediante la cumplimentación de la presente declaración, el abajo firmante, como usuario con acceso autorizado al perfil de la entidad en una o varias redes sociales, dice haber leído y comprendido la «Guía de uso y buenas prácticas de las redes sociales» de la misma y se compromete, bajo su responsabilidad, a su cumplimiento.

En _____, a ____ de _____ de 20__

Denominación de la entidad:	
NIF de la entidad:	
Nombre y apellidos del usuario:	
DNI del usuario:	
Firma del usuario:	

Por la entidad:

D./ Dña. _____
DNI número: _____

VI. NORMATIVA APLICABLE

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016) (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, 06-12-2018) (LOPDGDD).