GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 821

APÉNDICE VIII: NORMATIVA DE USO DE REDES SOCIALES NP70

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.02.23 09:34:54 +01'00'

FEBRERO 2018

ÍNDICE

1. OBJETIVO 1
2. ÁMBITO DE APLICACIÓN 1
3. VIGENCIA 1
4. REVISIÓN Y EVALUACIÓN 1
5. REFERENCIAS 2
6. NORMAS PREVIAS 2
7. JUSTIFICACIÓN 2
8. REDES SOCIALES: BENEFICIOS Y RIESGOS 3
9. NORMATIVA EN MATERIA DE USO DE REDES SOCIALES 5
10. AUTORIZACIÓN PREVIA 5
11. MEDIDAS COMPORTAMENTALES 6
12. USO DE MEDIOS SOCIALES CON FINES EXCLUSIVAMENTE PERSONALES 9
13. MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN 9
14. MEDIDAS DE ORDEN NORMATIVO 9
15. MEDIDAS DE SEGURIDAD TECNOLÓGICA 10
16. MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN 12
ANEXO A: MODELO DE FORMULARIO DE SOLICITUD PARA EL ALTA DE CUENTAS CORPORATIVAS 20
ANEXO B: PECULIARIDADES EN TORNO A LAS REDES SOCIALES MÁS USADAS 21
ANEXO C: REFERENCIAS Y DOCUMENTACIÓN USADA 25

1. OBJETIVO

1. El objetivo de la presente norma es presentar un **Normativa de Uso de Redes sociales**, para la <<ENTIDAD>>.

> La presente Normativa deberá ser complementada, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

2. Este documento se considera de uso interno de la <<ENTIDAD>> y, por tanto, no podrá ser divulgado salvo autorización del <<U/OC>>.

2. ÁMBITO DE APLICACIÓN

3. Esta normativa es de aplicación a todo el ámbito de actuación de la <<ENTIDAD>>, y sus contenidos se ubican bajo las directrices de carácter más general definidas en la Política de Seguridad de la Información de la <<ENTIDAD>>.

4. En este sentido, su alcance comprende toda la información utilizada para el desarrollo de las funciones y competencias atribuidas a la <<ENTIDAD>>, así como los sistemas de información que la gestionan, y s**erá de obligado cumplimiento para todo el personal propio o de terceras instituciones que preste sus servicios en la <<ENTIDAD>>**. Por tanto, su alcance incluye a todos los usuarios internos o de entidades externas a la <<ENTIDAD>> que requieran, en el marco de un acuerdo de colaboración o relación contractual, de acceso a los activos de información de la <<ENTIDAD>>.

3. VIGENCIA

5. La presente Norma ha sido aprobada por la <<U/OC>> de la <<ENTIDAD>>, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la <<ENTIDAD>> pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

6. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la <<ENTIDAD>>.

7. Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa.

4. REVISIÓN Y EVALUACIÓN

8. La gestión de esta Normativa corresponde a la <<U/OC>>, que es competente para:

   - Interpretar las dudas que puedan surgir en su aplicación.
   - Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.

- Verificar su efectividad.

9. Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), la <<U/OC>> revisará la presente Normativa, que se someterá, de haber modificaciones, a la aprobación de la <<U/OC>> de la <<ENTIDAD>>.

10. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

11. Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5. REFERENCIAS

12. *<<En este epígrafe se deben incluir aquellas referencias documentales que vengan a apoyar o completar esta Norma o que hubieren sido consideradas en su redacción.*

***Internas**:*

- ----
- ----
-

***Externas**:*

(Por ejemplo:

- *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*
- *UNE - ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la información.*
- *UNE - ISO/IEC 27001:2007 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.*
- *ISO/IEC 9001:2000 Sistemas de gestión de la calidad.*
- *Documentos y Guías CCN-STIC.*
- *Etc.>>*

6. NORMAS PREVIAS

13. El presente "Normativa de Uso de Redes Sociales" complementa, en sus aspectos específicos, a la "NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA <<ENTIDAD>>"1, por lo que tal normativa general será de aplicación en los aspectos no señalados en aquella.

7. JUSTIFICACIÓN

14. Con carácter general, los usuarios de la <<ENTIDAD>> dispondrán de acceso a Internet como herramienta de productividad y conocimiento, para el desempeño de su actividad profesional.

[1] Se recomienda que la entidad disponga de una Normativa General de Utilización de los Recursos y Sistemas de Información de la <<ENTIDAD>>, del tipo descrito en el documento CCN STIC – 821 - NG00.

15. Es necesario garantizar un uso adecuado de los recursos informáticos de acceso a Internet, por los siguientes motivos:

    - **Seguridad**: Debido al riesgo de infección por software dañino (virus, troyanos, etc.).
    - **Volumen del tráfico externo de datos**: Asegurando que el acceso a contenidos necesarios para la actividad profesional no se vea perjudicado por el tráfico generado por contenidos no vinculados con las competencias de la <<ENTIDAD>>.
    - **Volumen del tráfico interno de datos**: Como consecuencia de contenidos descargados de la Web y su posterior almacenamiento. Esta situación aconseja también regular el tipo de ficheros cuya descarga y almacenamiento está permitido.
    - **Ética**: Finalmente, es ineludible el compromiso que la <<ENTIDAD>> debe mantener con la sociedad, a la hora de vetar el acceso a contenidos que pudieran ser poco éticos, ofensivos o delictivos.

8. REDES SOCIALES: BENEFICIOS Y RIESGOS

16. El uso de las redes sociales, también en el marco del Sector Público, es especialmente significativo. Muchas organizaciones de las Administraciones Públicas y del Sector Público Institucional han decidido "hacerse presentes" en las redes sociales, en un intento más de acercar su actuación y competencias a los ciudadanos.

17. Por ello, no es raro ver perfiles públicos en redes sociales tales como Facebook, Twitter, Google+, Linkedin, Youtube, Flickr, Pinterest, Periscope, Instagram, Slideshare, etc.

18. La pretensión pública -siempre laudable- de compartir conocimientos, experiencias, información, etc., comporta no obstante ciertos riesgos que conviene conocer de antemano. Sólo siendo conscientes de su existencia podremos considerar la adopción de las medidas de mitigación del riesgo correspondientes y, en su consecuencia, decidir si, pese a todo, nos interesa "estar" en tal o cual red social.

19. Por la parte que ahora nos interesa en esta Guía, los riesgos más significativos en la utilización de las redes sociales devienen o están directamente relacionados con el cumplimento (incumplimiento, habría que decir) legal.

20. Efectivamente, la creación y el uso de perfiles "públicos" en las redes sociales obligan a las entidades públicas concernidas a la conformidad legal con distintas regulaciones, muy especialmente, las relativas a:

    - La **Protección de Datos de Carácter Personal**, regulada, además de en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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 ó RGPD), en la todavía vigente Ley Orgánica 15/1999, de Protección de Datos

de Carácter Personal y Real Decreto 1720, Reglamento de Desarrollo de la LOPD[2].

- Los **Derechos al Honor, la Intimidad y la Propia Imagen**, regulados en la Ley Orgánica 1/1982 de Protección Civil del derecho al honor, a la intimidad y a la propia imagen.
- La **Protección de los Derechos de Propiedad Intelectual**, regulados en el Real Decreto Legislativo 1/1996, Texto Refundido de la Ley de Propiedad Intelectual.
- La **Protección de los Derechos relativos a los Servicios de la Sociedad de la Información**, regulados en la Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico, y, por supuesto,
- La **Protección de la Información y los Servicios Prestados** por las entidades del Sector Público, regulada en el Real Decreto 3/2010, Esquema Nacional de Seguridad (ENS).

A la conformidad legal con esta última regulación se dirige el presente documento.

Pese a su variedad y a sus respectivas comunidades de usuarios (que se cuentan por millones, en todo el mundo), existen dos grandes tipos de redes sociales:

- Las **Personales**: donde el vínculo que une a sus usuarios se sustenta en las relaciones personales, (tales como F*acebook, Twitter, Google+, LinkedIn,* etc.) y
- Las basadas en **Contenidos**: en las que prevalece el contenido que cada usuario comparte con el resto, (tales como *YouTube, Slideshare, Instagram*, etc.)

La figura siguiente muestra una taxonomía de los medios sociales, atendiendo a su propia ontología y contenidos tratados.

MEDIOS SOCIALES				
REDES SOCIALES	**COMPARTIR**		**CREACIÓN DE CONTENIDOS**	**GEOLOCALIZACIÓN**
	MULTIMEDIA	**DOCUMENTOS**		
Twitter	*Youtube*	*Slideshare*	*Wikis*	*Foursquare*
Facebook	*Flickr*	*ISSUU*	*Blogs*	
Google +	*Instagram*		*Pinterest*	
Tuenti	*Picasa*		*Storify*	
Linkedin	*Vimeo*			
Xing				
Delicious				

[2] En tanto no entre en vigor la próxima Ley Orgánica de Protección de Datos, cuyo Anteproyecto se ha hecho público al tiempo de redactar este Apéndice.

21. **No es propósito del presente documento señalar cómo deben usarse las cuentas de titularidad pública de las redes sociales desde el punto de vista comunicacional, sino desde el punto de vista de la seguridad de la información, lo que, pese a todo y en algunos casos, nos obligará a tratar tangencialmente alguna cuestión de aquella naturaleza.**

9. NORMATIVA EN MATERIA DE USO DE REDES SOCIALES

22. Con el despliegue de las TIC y, en particular, con el desarrollo de Internet como herramienta de comunicación global, se han extendido igualmente las amenazas que pueden poner en peligro los sistemas de información de las organizaciones.

23. En este sentido, la medida de seguridad [mp.per.2] del ENS señala:

> **Deberes y obligaciones [mp.per.2].**
>
> 1. Se informará a cada persona que trabaje en el sistema, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.
>
> a) Se especificarán las medidas disciplinarias a que haya lugar.
>
> b) Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
>
> c) Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación.
>
> 2. En caso de personal contratado a través de un tercero:
>
> a) Se establecerán los deberes y obligaciones del personal.
>
> b) Se establecerán los deberes y obligaciones de cada parte.
>
> c) Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

24. Por tanto, para minimizar los riesgos derivados del uso de Internet, resulta necesario adoptar un conjunto mínimo de medidas de seguridad dirigidas a propiciar su correcto uso.

25. Los siguientes epígrafes recogen el conjunto de medidas que deben tenerse en cuenta cuando se use o se pretendan usar las Redes Sociales como herramienta de comunicación y difusión de las funciones competencialmente de la <<ENTIDAD>>.

10. AUTORIZACIÓN PREVIA

26. Con carácter general, y salvo las excepciones que pudieran autorizarse en la <<ENTIDAD>>, y que, en todo caso, deberán estar recogidas en la Política de Seguridad institucional,

> **Ninguna persona que preste sus servicios en la <<ENTIDAD>> podrá darse de alta en ninguna red social, en nombre o en representación de la**

<<ENTIDAD>>, salvo autorización expresa de la <<U/OC>> y con el conocimiento del Responsable de Seguridad.

Por tanto, salvo en el supuesto señalado, la presencia en las redes sociales de un empleado público de la <<ENTIDAD>> será siempre a título personal.

27. El Anexo A muestra un Modelo de Formulario de Solicitud para el Alta de Cuentas Corporativas.

11. MEDIDAS COMPORTAMENTALES

28. Una vez autorizado a darse de alta en una red social en representación de la <<ENTIDAD>>, el empleado público usuario de la red social de que se trate debe observar las siguientes normas de comportamiento:

C1	**Recordar en todo momento que las redes sociales constituyen un foro público. Por tanto, por el hecho de agregar cualquier dato, comentario o información, el usuario está asumiendo que éste puede ser visto por los restantes usuarios de tal social, por la <<ENTIDAD>> y, en general, por cualquier persona.**
C2	Si el usuario está usando el perfil de la red social en representación de la <<ENTIDAD>>, conviene mostrar abiertamente tal representación, a menos que existan circunstancias excepcionales que no lo aconsejen, tales como una amenaza potencial a la seguridad personal. En cualquier caso, nunca deben proporcionarse detalles personales tales como la dirección o los números de teléfono personales.
C3	Es siempre recomendable hablar en primera persona, tratando de aportar valor en los comentarios vertidos, facilitando informaciones y perspectivas contrastadas y que no se encuentren tipificadas como información clasificada o cuya revelación pudiera ocasionar un perjuicio a la <<ENTIDAD>> o, en general, a cualquier persona o entidad, pública o privada. El usuario debe recordar que será siempre responsable de sus aportaciones y de las eventuales consecuencias en su reputación y, por ende, en la de la <<ENTIDAD>> en el que presta sus servicios. En caso de dudas, lo mejor es abstenerse de hacer una contribución. En el orden jurídico, no olvidemos que el art. 53.3 del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público, señala que las actuaciones de los empleados públicos se ajustarán a los principios de lealtad y buena fe con la Administración en la que presten sus servicios, y con sus superiores, compañeros, subordinados y con los ciudadanos.
C4	Las redes sociales deben constituir un foro de intercambio de

	opiniones o para el debate constructivo, pero no es el ámbito apropiado para crear polémica, descalificar a otras personas o a terceros, ni para presentar quejas y reclamaciones que deben canalizarse a través de las vías específicas que la Administración Pública y la propia <<ENTIDAD>> tiene establecidas para esa finalidad.
C5	El usuario debe tratar con respeto a los otros usuarios, usando un lenguaje apropiado y correcto y actuando siempre como si estuviera en presencia de la(s) otra(s) persona(s).
C6	Salvo autorización, el usuario no debe publicar material publicitario ni comunicacional de la <<ENTIDAD>>, ni debe hacer uso de su perfil en la red social para lucrarse o hacer negocio, ni para comparar las funciones, competencias o, en general, desenvolvimiento de la <<ENTIDAD>> con otras entidades.
C7	Los contenidos publicados en las redes sociales pueden estar sujetos a Derechos de Propiedad Intelectual, por lo que la publicación de cualquier contenido requiere tener la certidumbre de que se encuentra libre de estas cargas[3].
C8	La contribución del usuario en la red social debe presentar datos reales, concretos y argumentación consistente. Se permiten citas o la reproducción de pequeños fragmentos de textos, libros u obras de terceros en general, siempre y cuando se indique la fuente y el nombre del autor. Si el usuario realiza una contribución propia (texto, fotografías, gráficos, videos o audios) debe saber que otorga a la <<ENTIDAD>> autorización para reproducirla en cualquier medio físico o virtual donde se indicará el nombre del empelado público como autor, todo ello sin perjuicio de que otros usuarios también podrían guardarlos o reproducirlos.
C9	El logotipo de la <<ENTIDAD>> y, en general, cualquier otro logotipo o distintivo gráfico de la <<ENTIDAD>> o de cualquier entidad del Sector Público constituyen marcas registradas. También son titularidad de la <<ENTIDAD>> los contenidos colgados en su portal o sede electrónica y, por tanto, la <<ENTIDAD>> se reserva todos los derechos de propiedad intelectual e industrial asociados a los mismos. El usuario debe comprometerse a respetarlos y a no utilizarlos sin la debida autorización, cualquiera que sea el medio.

[3] Es conveniente que los contenidos digitales generados por la entidad pública de que se trate dispongan de una licencia de uso. Una buena opción es utilizar las licencias de tipo Creative Commons (CC). Hay diferentes tipos de licencias, pero una de las más utilizadas por las AA.PP. la licencia Creative Commons Reconocimiento 3.0 (http://creativecommons.org/licenses/by/3.0/es/legalcode.es), que permite a los usuarios reutilizar (copiar, hacer obras derivadas, distribuir y comunicar) el contenido siempre que se reconozca al autor de la obra (la entidad pública) y no se haga uso comercial de la misma. (Ver epígrafe 16 de este documento.)

C10	La descarga de contenidos, su copia o impresión requerirá autorización de <<U/OC>>.
C11	En ningún caso deberá usarse la red social para el intercambio de credenciales o contraseñas, de cualquier sistema y para cualquier finalidad.
C12	La información contenida en el perfil de la red social no deberá considerarse nunca como información oficial en relación con las funciones y competencias de la <<ENTIDAD>>, en los términos que puedan estar reservados a las funciones de la sede electrónica de la <<ENTIDAD>>, según dispone el art. 38 de la Ley 40/2015.
C13	El perfil de la red social de que se trate puede contener manifestaciones sobre previsiones o estimaciones que incluyen comentarios sobre el desarrollo de las funciones de la <<ENTIDAD>> basadas en juicios actuales, pudiendo suceder que determinados riesgos, incertidumbres y otros factores relevantes, desconocidos o imprevisibles ocasionen que los resultados difieran materialmente de lo esperado. El usuario debe recordar que las declaraciones relativas a los resultados, funciones, competencias, etc., no pretenden dar a entender que el desempeño de la <<ENTIDAD>> será necesariamente el previsto. Nada en el perfil debe ser tomado como una previsión de resultados.
C14	La <<ENTIDAD>> velará en todo momento por preservar el buen uso del perfil y, por ello, la <<ENTIDAD>>, como administrador, se reserva el derecho a eliminar, sin derecho a réplica, cualquier aportación que: Considere ilegal, irrespetuosa, amenazante, infundada, calumniosa, inapropiada, ética o socialmente discriminatoria o laboralmente reprochable o que, de alguna forma, pueda ocasionar daños y perjuicios materiales o morales a la <<ENTIDAD>>, sus empleados, colaboradores o terceros. Incorpore datos de terceros sin su autorización. Contenga cualquier tipo de recomendación relativa a las funciones y competencias de la <<ENTIDAD>> privilegiada o material publicitario o de comunicación, personal o en beneficio de terceros, sean personas físicas o jurídicas. Sea redundante. No esté relacionada con la finalidad perseguida por la <<ENTIDAD>> al darse de alta en la red social de que se trate.

12. USO DE MEDIOS SOCIALES CON FINES EXCLUSIVAMENTE PERSONALES

29. En ocasiones, el uso personal o profesional de una red social pueden llegar a confundirse4. Por tanto, se debe ser consciente de las responsabilidades cuando se mezclan la vida personal y la laboral en estos medios.

30. Las personas que trabajan para la <<ENTIDAD>> deben usar su buen juicio y asumir la responsabilidad personal y profesional de los contenidos que publican a través de los medios sociales.

31. Es frecuente que se admita el uso de una cuenta personal para comentar sobre asuntos no relacionados con el trabajo, aunque no debiera permitirse, de manera general, que el uso de tales cuentas se lleve a cabo en horario laboral ni, por motivos de seguridad, usando los medios electrónicos de la <<ENTIDAD>>.

32. En cualquier caso, el uso de plataformas de redes sociales nunca debe interferir con las funciones principales, con la excepción de aquellos puestos de trabajo que incluyan entre sus tareas precisamente el uso de estas herramientas sociales.

33. Debemos recordar que el uso de una cuenta privada no exime de cumplir los códigos de buena conducta generalmente admitidos y los específicamente contemplados en la Política de Seguridad de la Información de la <<ENTIDAD>>.

34. Por todo ello, no deben publicarse opiniones personales a través de cuentas oficiales y tampoco promover las cuentas personales a través de cuentas oficiales.

35. No debe comentarse en redes sociales aquello que no se debe ser de dominio público, aunque exista una única persona a la que se desee dejar al margen. Las redes sociales pueden actuar de amplificador y comprometer a sus usuarios.

36. Aquellas personas que tienen responsabilidades de gobierno, en virtud de su posición, deben tener en cuenta si los comentarios personales que publican, incluso en lugares claramente personales, pueden ser mal interpretados como declaraciones realizadas por la <<ENTIDAD>>.

13. MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

37. En primer lugar, es preciso identificar claramente los canales oficiales de la <<ENTIDAD>> que ya pudieran existir y, en la medida de lo posible, diferenciar los canales verdaderos (mediante el uso de TL) e impulsar la vigilancia y el cierre de canales falsos.

14. MEDIDAS DE ORDEN NORMATIVO

38. Siempre resulta conveniente que la <<ENTIDAD>> disponga de una norma jurídica (bajo la forma pertinente: Resolución, Instrucción, Orden, …) que regule la creación y gestión de los canales digitales de la <<ENTIDAD>> (portales institucionales y

[4] Como sucede, por ejemplo, cuando un empleado público (directivo o no) mantiene una cuenta personal en una red social.

redes sociales, esencialmente), como vehículos estratégicos de comunicación, y otorgue consistencia jurídica a su modelo de gobernanza.

39. Dicha regulación deberá contener reglas precisas sobre la estructura de este nuevo modelo de gobernanza, que se concreta en dos ámbitos:

   – Dirección y el establecimiento de la estrategia digital de relación con los ciudadanos y profesionales, tareas que corresponderán a la <<U/OC>> competente (por ejemplo, un Comité de Estrategia Digital), que llevará a cabo una labor de asesoramiento, coordinación e impulso de las acciones en materia de comunicación digital.

   – Gestión diaria de los canales digitales, siendo frecuente que, para agilizar el mantenimiento y la actualización de los contenidos, se distribuyan las responsabilidades entre las diversas unidades sectoriales en función de sus respectivas competencias. Así, los responsables de los contenidos serán los encargados del mantenimiento y actualización de la información recogida en cada uno de los portales y perfiles de redes sociales y tendrán autonomía para designar una persona y asignarle que lleve a cabo esas tareas como *"Community Manager"* bajo su supervisión. Estas designaciones deberán comunicarse a la <<U/OC>> competente (Comité de Estrategia Digital, por ejemplo).

40. Por último, el apoyo técnico a los medios institucionales dependerá de las distintas unidades con competencias en materia de TIC, que ejercerán las funciones de apoyo técnico a la dirección y coordinación de los medios institucionales, en sus respectivos ámbitos materiales de competencia.

41. Todo esto se llevará a cabo bajo el principio de coordinación y ausencia de duplicidades, con el objetivo de que, como regla general, el contenido de medio institucional sea único y no reescrito en otro, con independencia de que se establezcan los enlaces necesarios.

42. En el epígrafe siguiente se contiene un Modelo de Política de Seguridad de Redes Sociales.

15. MEDIDAS DE SEGURIDAD TECNOLÓGICA

43. Las medidas de seguridad esenciales son las siguientes:

S1	**Las cuentas en redes sociales de la <<ENTIDAD>> se crearán desde correos electrónicos corporativos, delegándose la gestión de las mismas en las <<U/OC>> designadas para cada una de ellas.** **El Responsable de Seguridad de la <<ENTIDAD>> extenderá sus competencias a los perfiles de redes sociales que pudieran crearse.**
S2	La custodia de las contraseñas de los perfiles de las redes o de sus administradores que así lo requieran, estará centralizada y será responsabilidad de la <<U/OC>> de la entidad de que se trate.
S3	Cualquier instalación de aplicaciones de terceros que tenga algún tipo de permisos sobre cuentas de las redes sociales deberá ser

	previamente autorizada por el Responsable de Seguridad de la <<ENTIDAD>>, para verificar que esta aplicación no pone en riesgo ni los datos ni la seguridad de la cuenta.
S4	La modificación de cualquiera de las opciones de privacidad o publicación de comentarios deberá autorizarse previamente por la <<ENTIDAD>>, contando con la opinión del Responsable de Seguridad.
S5	Como norma general, las contraseñas de las plataformas de gestión deberán ser robustas. [Véase Guía CCN-STIC 821 – Apéndice V. Creación y uso de contraseñas].
S6	Siempre que sea posible, es conveniente mantener las cuentas desde una herramienta de gestión que pueda otorgar permisos diferentes de publicación y que su acceso no se realice a través de la propia contraseña de la red social de que se trate. El responsable de cada cuenta definirá quiénes son las personas que la gestionarán, velando y haciendo respetar la confidencialidad de las contraseñas de acceso.
S7	Siempre que sea posible, el acceso a las cuentas se realizará desde sistemas corporativos. En caso de necesitar publicar contenidos desde un dispositivo móvil, se hará desde una aplicación diferente a la que se utiliza de modo personal.

44. Se muestra seguidamente un listado con las redes sociales más usadas y los enlaces a las mismas que pueden usarse para configurar su uso seguro, así como un enlace a la página web de la AEPD sobre precauciones y comportamientos particulares en cada red.

FACEBOOK:

- Condiciones del servicio: https://www.facebook.com/legal/terms
- Política de privacidad: https://www.facebook.com/privacy/explanation
- Video explicativo: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/protegetuprivacidad/index_facebook-ides-idphp.php

TWITTER:

- Condiciones del servicio: https://twitter.com/tos?lang=es
- Política de privacidad: https://twitter.com/privacy?lang=es
- Video explicativo: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/protegetuprivacidad/index_twitter-ides-idphp.php

LINKEDIN:

- Condiciones de uso: https://www.linkedin.com/legal/user-agreement?_l=es_ES

- Política de privacidad: https://www.linkedin.com/legal/privacy-policy?_l=es_ES

GOOGLE+:

- Condiciones del servicio: https://www.google.com/intl/es-419/policies/terms/
- Política de privacidad: https://www.google.es/intl/es-419/policies/privacy/
- Video explicativo: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/protegetuprivacidad/index_google-ides-idphp.php

YOUTUBE:

- Condiciones del servicio: https://www.youtube.com/static?gl=ES&template=terms&hl=es
- Política de privacidad: https://www.youtube.com/yt/policyandsafety/es/
- Video explicativo: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/protegetuprivacidad/index_youtube-ides-idphp.php

INSTAGRAM:

- Condiciones del servicio: https://www.facebook.com/help/instagram/478745558852511
- Política de privacidad: https://www.facebook.com/help/instagram/155833707900388
- Video explicativo: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/protegetuprivacidad/index_instagram-ides-idphp.php

El Anexo B contiene información adicional sobre las redes sociales más usadas.

16. MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

45. Cada Política de Seguridad de Redes Sociales podrá variar en función de la <<ENTIDAD>> de que se trate (especialmente si forman parte de grupos diferenciados, tales como las entidades que pertenecen a las Administraciones Públicas de aquellas otras encuadradas en el Sector Público Institucional). Esta realidad podría hacer aconsejable, ocasionalmente, la presencia de elementos de política de seguridad diferentes.

46. Se presenta seguidamente un esquema básico que cada <<ENTIDAD>> puede adaptar para desarrollar su propia Política de Seguridad de Redes Sociales.

1. Introducción (De qué trata la Política). a) Gestión de la Política (Mecanismos de la <<ENTIDAD>> para cambiar y actualizar la Política).

b) Fecha de entrada en vigor.

c) Objetivos (Cuales son los objetivos perseguidos por la Política: fijación de pautas de comportamiento, determinación de responsabilidades, gestión de la reputación, etc.)

d) Propósito (Cual es el propósito del documento y quién debe aplicarlo).

e) Ámbito (Cual es la aplicabilidad de la Política a la tecnología, a los empleados, a los subcontratistas y a los *partners* de la <<ENTIDAD>>.

2. ¿Cómo se usan las Redes Sociales en la <<ENTIDAD>>?

a) Redes Sociales contempladas (Facebook, Flickr, LinkedIn, Twitter, YouTube, etc.)

b) Beneficios del uso de las redes sociales (comunicación, servicio a los administrados, desarrollo de nuevos servicios, respuesta de los usuarios, etc.)

c) Objetivos del Community Manager (¿Quién es el Community Manager de la <<ENTIDAD>?, ¿Cuáles son sus funciones y responsabilidades?)

d) Responsabilidades del Servicio TIC de la <<ENTIDAD>> (Definición de la Seguridad TIC, identificación de procesos para autenticar y autorizar en cada plataforma de red social, definición de responsabilidades de implementación, definición de responsabilidades de notificación, definición de responsabilidades de monitorización).

e) Responsabilidades del Servicio de Comunicación Institucional (Definición del papel de la Seguridad TIC como soporte al Servicio de Comunicación Institucional para desarrollar sus funciones de manera segura).

f) Responsabilidades del Servicio de Recursos Humanos (Definición del papel de la Seguridad TIC como soporte al Servicio de Recursos Humanos para desarrollar sus funciones de manera segura.)

g) Responsabilidades del Servicio/Asesoría Jurídico/a (Definición del papel de la Seguridad TIC como soporte al Servicio Jurídico para desarrollar sus funciones de manera segura.)

3. Políticas Generales para Redes Sociales.

a) Publicidad institucional.

b) Requisitos legales.

c) Gestión de la comunidad.

d) Confidencialidad (¿Qué información puede compartirse?)

e) Divulgaciones (Los empleados de la <<ENTIDAD>> y los terceros: ¿qué información puede revelar y cual no?)

f) Cuestiones legales (¿Es necesario aplicar alguna restricción en la red social de que se trate?)

g) Nivel de compromiso (¿Cuáles son las expectativas de compromiso con la

comunidad y qué recursos internos y externos deben usarse?)

h) Cómo gestionar los comentarios negativos.

i) Preguntas de la prensa (definición de responsabilidades en lo relativo a las relaciones con la prensa).

j) Empleados de terceras partes (Identificar procesos para la gestión de las relaciones con terceros).

k) Restricciones sobre el uso de marcas o, en general, derechos de propiedad intelectual (¿Cómo habrán de gestionarse las marcas o cualesquiera otros derechos sujetos a propiedad intelectual?)

4. Políticas de Seguridad TIC

a) Sobre la base de la que ya dispone en <<ENTIDAD>>, en función de lo exigido por el ENS.

b) Autenticación de acceso a las Redes Sociales - Contraseñas (Siga las recomendaciones del Apéndice V. Creación y uso de contraseñas de la Guía CCN-STIC 821).

c) Aplicaciones de redes sociales implementadas en la <<ENTIDAD>>

i. Inicio de sesión fallido

Reiterados errores en el inicio de sesión pueden indicar un intento de romper una contraseña y acceder de forma subrepticia a una cuenta de la red. Con el fin de protegerse contra la adivinación de la contraseña y los intentos por fuerza bruta, la <<ENTIDAD>> debe bloquear la cuenta de un usuario después de un número finito de inicios de sesión sin éxito.

ii. *Logging*

Las necesidades de *logging* varían dependiendo del tipo de sistema de red y del tipo de datos que contiene el sistema. Las siguientes secciones detallan los requisitos de la <<ENTIDAD>> para el *logging* y la revisión de registros.

1. Servidores de aplicaciones

Los registros de los servidores de aplicaciones son del máximo interés ya que estos servidores suelen permitir conexiones desde un gran número de fuentes internas y/o externas. Como mínimo, se registrarán los errores o fallos en el inicio de sesión.

2. Dispositivos de red

Los registros de dispositivos de red que protegen los servidores de aplicaciones son de interés ya que estos dispositivos controlan todo el tráfico de red y pueden tener un enorme impacto en la seguridad de la compañía. Como mínimo, se registrarán los errores o fallos en el inicio de sesión.

iii. Gestión de logs

1. Revisión de logs.

Las aplicaciones de gestión de logs pueden ayudar a resaltar eventos importantes, sin embargo, un miembro del equipo TIC de la <<ENTIDAD>> (Responsable de Seguridad) debe revisar los registros con la frecuencia que sea razonable.

2. Retención de logs

Los registros deben ser retenidos de acuerdo con la Política de Retención de la <<ENTIDAD>>.

iv. Detección de Intrusión / Prevención de Intrusión

La <<ENTIDAD>> precisará usar un IDS o IPS en servidores de aplicaciones críticas.

v. Pruebas de seguridad

Las auditorías de seguridad, incluyendo las pruebas de penetración, son una parte importante del mantenimiento de la seguridad de la red de la <<ENTIDAD>>, y deberán realizarse conforme a lo dispuesto en el ENS y en las Instrucciones Técnicas de Seguridad que lo desarrollan.

vi. Documentación de aplicaciones de redes sociales

La documentación proporcionada por las redes sociales, especialmente cuando trata de la seguridad de la información, es de suma importancia para una adecuada gestión de aplicaciones.

vii. Antivirus / Antimalware

viii. Todos los servidores de aplicaciones y sistemas de usuario final que se conectan a los servidores de aplicaciones deben tener el software antivirus/antimalware en ejecución.

ix. Política de uso de software

1. Las aplicaciones de software pueden ser fuente de riesgos de varias maneras y, por lo tanto, ciertos aspectos del uso del software deben ser cubiertos por esta Política.

2. Todo el software y las aplicaciones de redes sociales para usuarios finales que puedan descargarse en los ordenadores corporativos o en los dispositivos móviles deben ser aprobados por la <<U/OC>> competente.

x. Incidentes de seguridad

1. Ante la sospecha de un incidente de seguridad que pueda afectar a un dispositivo de red, deberá seguirse la Política de respuesta a incidentes de la <<ENTIDAD>>.

d) Aplicaciones hospedadas en terceros

i. Acuerdo de nivel de servicio

Es necesario revisar todos los acuerdos de nivel de servicio con sitios y

proveedores de aplicaciones.

ii. Actualizaciones

Se deben realizar todas actualizaciones que sean necesarias para solucionar problemas de seguridad.

iii. Pruebas

1. Los terceros deben aportar evidencias de las pruebas de seguridad realizadas o permitir a la <<ENTIDAD>> someter a los sistemas implicados a las adecuadas pruebas de seguridad.

2. Los terceros deben proporcionar pruebas de seguridad de la infraestructura usada, así como políticas que mantengan un entorno seguro para los datos de sus clientes.

e) Educación y entrenamiento

i. El Responsable de Seguridad de la <<ENTIDAD>> es responsable de proponer acciones de formación a los usuarios finales sobre los requisitos de seguridad para todos los recursos de hardware y software.

ii. El Servicio de Recursos Humanos es responsable de ejecutar los programas de formación propuestos.

iii. Realizar un programa anual de formación/concienciación para alertar a los usuarios de nuevos riesgos y de las medidas de seguridad que los mitigan.

5. ¿Qué se puede hacer con las redes sociales y qué no se puede hacer?

a) Con las redes sociales SE PUEDE…

Añadir valor, promover en la <<ENTIDAD>> una actitud positiva, formar e informar, responder a los usuarios, participar en conversaciones, ser un recurso de conocimiento, construir relaciones, conocer las restricciones sobre el contenido, entender los riesgos de los medios, comprobar todos los hechos, proporcionar divulgaciones, obtener retroalimentación, comprobar el riesgo normativo, comprender ramificaciones legales, asegurar las comunicaciones, proteger la información de los usuarios, entender los requisitos de privacidad, etc.

b) Con las redes sociales NO SE PUEDE…

Discutir información confidencial, compartir información privada de los usuarios, compartir comentarios despectivos, acceder a canales no seguros o no cifrados (si resulta de aplicación), discutir la actividad de los usuarios, publicar información interna, asociar la vida personal con las cuentas corporativas, desacreditar a otros, desacreditar a otras personas o instituciones, etc.

6. Política de "la Marca"

a. ¿Cuál es la política de "la marca" de la <<ENTIDAD>> y cuáles son las

directrices para discutir y promover “la marca”?
7. Política de uso de Twitter a) Identificar para qué se desea usar Twitter. b) Identificar objetivos (acceso, seguimiento de “la marca”, gestión de identidad, investigación, comunicaciones con los usuarios, cobertura de los medios de comunicación, etc.). c) Identificar quién puede crear y publicar tweets. d) Directrices respecto del contenido (Identificar requisitos de contenido tales como frecuencia, contexto, contenido, tono, uso del hashtag, seguidores, seguimiento, política de enlaces cortos, etc.) e) Re-tuiteo y seguimiento (Áreas principales: sector público, investigación, socios, noticias de la industria, estadísticas, otros contenidos relevantes). f) Gestión de cuentas de servicios específicos (Vincular cuentas a servicios, monitorizar cuentas específicas).
8. Política de uso de Facebook a) Identificar para qué pretende usarse Facebook. b) Identificar objetivos (monitorización de “la marca”, marketing, compromiso con la comunidad, desarrollo de alianzas, etc.). c) Identificar quién puede usar Facebook y publicar en las cuentas de la <<ENTIDAD>>. d) Directrices de contenido i. ¿Qué contenido es adecuado y está permitido? ii. Tipos de contenido y fuentes (tales como eventos, noticias, encuestas, fotos, etc.) iii. Tono del compromiso e interacción con la comunidad (personal, corporativo, amistoso, profesional) iv. Directrices generales desde una perspectiva de seguridad.
9. Política de blogs de la <<ENTIDAD>> a) Definir el propósito de los blogs corporativos. b) Objetivos c) Identificar quién es responsable de los blogs. d) Directrices de contenido: i. Definir qué contenido se permite en los blogs. ii. Identificar la política de vídeo para los blogs.
10. Política de Blogs personales a) Identificar cómo se permite a los empleados utilizar la información de la

<<ENTIDAD>> en blogs personales y en mensajes de redes sociales, y cuándo y dónde se puede acceder a los blogs personales. i. ¿Cuáles son las limitaciones? ii. ¿Qué IP corporativa se puede utilizar? iii. ¿Qué se puede decir de los servicios de la <<ENTIDAD>>? iv. Identificar políticas relevantes de Recursos Humanos que restrinjan la difusión de información de la <<ENTIDAD>> por parte de los empleados, en cualquier forma. v. ¿Qué tipo de información de la <<ENTIDAD>> u otra información puede publicarse? b) Proceso de aprobación c) Renuncia a responsabilidades (¿Qué renuncias deben usar los empleados?) d) Revelación o divulgación (¿Qué deben y no deben divulgar los empleados en sus blogs? e) Aprobaciones.
11. Política de Código de Conducta del Empleado a) Referencia al Manual de Referencia sobre el Código de Conducta (véase Guía CCN-STIC 821). b) No dañar la reputación de la <<ENTIDAD>>. c) Uso de comentarios inapropiados.

47. El contenido generado por la <<ENTIDAD>> puede crearse bajo distintas licencias, las más conocida son las *Creative Commons*[5]. Estas licencias permiten la copia, la distribución y la comunicación pública de la obra mientras se cite la autoría. Son las siguientes:

[5] Creative Commons España. Licencias. Véase: http://es.creativecommons.org/blog/licencias/

	**Reconocimiento (by):** Se permite cualquier explotación de la obra, incluyendo una finalidad comercial, así como la creación de obras derivadas, la distribución de las cuales también está permitida sin ninguna restricción.
	**Reconocimiento – NoComercial (by-nc):** Se permite la generación de obras derivadas siempre que no se haga un uso comercial. Tampoco se puede utilizar la obra original con finalidades comerciales.
	**Reconocimiento – NoComercial – CompartirIgual (by-nc-sa):** No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.
	**Reconocimiento – NoComercial – SinObraDerivada (by-nc-nd):** No se permite un uso comercial de la obra original ni la generación de obras derivadas.
	**Reconocimiento – CompartirIgual (by-sa):** Se permite el uso comercial de la obra y de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.
	**Reconocimiento – SinObraDerivada (by-nd):** Se permite el uso comercial de la obra pero no la generación de obras derivadas.

48. Plataformas como *Flickr, Youtube y Slideshare* incorporan las correspondientes funcionalidades para poder indicar qué licencia incorpora la imagen, el vídeo o la presentación en cuestión.

ANEXO A: MODELO DE FORMULARIO DE SOLICITUD PARA EL ALTA DE CUENTAS CORPORATIVAS

<table>
<tr><th colspan="4">Solicitud de Alta para Cuentas Corporativas</th></tr>
<tr><td>Solicitante:</td><td colspan="3"></td></tr>
<tr><td>Departamento / Servicio / Unidad:</td><td colspan="3"></td></tr>
<tr><td rowspan="3">Empleados públicos que gestionarán las cuentas (identificación y posición):</td><td>Apellidos y Nombre</td><td>Posición</td><td>Email / Tfno. corporativo</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Redes sociales para las que se solicita el alta:</td><td colspan="3"></td></tr>
<tr><td>Objetivos:</td><td colspan="3"></td></tr>
<tr><td>Contenidos:</td><td colspan="3"></td></tr>
<tr><td>Estrategia a desarrollar:</td><td colspan="3"></td></tr>
<tr><td>Destinatarios:</td><td colspan="3"></td></tr>
<tr><td>Observaciones:</td><td colspan="3"></td></tr>
<tr><td colspan="4">Fecha y firma:

Fdo: _____

El firmante manifiesta contar con la preceptiva autorización de la <<U/OC>> competente y se compromete a cumplir con la política de usos y estilos en redes sociales de la <<ENTIDAD>>.</td></tr>
</table>

ANEXO B: PECULIARIDADES EN TORNO A LAS REDES SOCIALES MÁS USADAS

TWITTER

Twitter es una plataforma de mensajería que permite a sus usuarios enviar pequeños mensajes de texto a través de navegadores web, software-cliente de escritorio y de dispositivos móviles. Las conversaciones se publican en Internet (aunque se pueden proteger las conversaciones de una cuenta para que sólo las puedan ver los seguidores de un usuario) y se construyen redes sociales a partir del seguimiento de los usuarios que interesen.

Se trata, por tanto, de una herramienta idónea para informar acerca de nuevos servicios, referenciar informaciones diversas (de agenda, emergencias, nuevas publicaciones, etc.) y para retransmitir eventos, pero también es una herramienta para dialogar y colaborar.

Integración

Las cuentas de *Twitter*, por su carácter público, se pueden asociar a otros espacios mediante pequeñas aplicaciones (widgets) que permiten integrar información externa en una página web. Estos widgets se pueden usar en:

- Espacios propios: blogs corporativos, webs de entidades públicas o webs especiales.
- Espacios propios externos: página de Facebook de la entidad pública de que se trate, páginas de Facebook de otros departamentos, etc., a través de una pestaña, un widget lateral o mediante la publicación automática.
- Espacios ajenos: posibilidad de integrar el widget para que cualquier persona lo pueda añadir a su página, blog, etc.

Verificación de la cuenta

Como quiera que puede ser difícil distinguir una cuenta oficial de una falsa, *Twitter* ofrece el servicio de cuenta verificada, que consiste en colocar un distintivo en aquellas cuentas cuya autenticidad se ha podido comprobar. Para poder disfrutar de este servicio hay que iniciar la sesión en Twitter y rellenar el formulario de verificación.

Antes de enviar el formulario, es importante publicar en la web oficial al menos un enlace a la cuenta de *Twitter*. De esta manera se facilita el proceso de verificación. Además, hay que tener en cuenta que cualquier cambio en el nombre de usuario, bio o información de la cuenta provocará la pérdida de la condición de cuenta verificada, por lo que será necesario volver a iniciar otro proceso de verificación.

Incidencias en la publicación

En la gestión de cuentas de *Twitter* puede suceder que estas aplicaciones dejen de funcionar puntualmente (por un error puntual de *Twitter*, por ejemplo). Puede suceder, asimismo, que la herramienta de gestión que se utilice para gestionar estas cuentas, (*Tweetdeck*, por ejemplo) sufra algún tipo de incidencia. Estas incidencias en el servicio no suelen durar mucho tiempo, pero pueden resultar críticas durante la cobertura o

retransmisión de un evento, por ejemplo. Para evitar que una incidencia de este tipo interfiera en la actividad normal de las cuentas, se proponen recursos alternativos para solucionarlo.

En caso de caída del servicio por mantenimiento: Clientes de movilidad: la mayoría de paradas de funcionamiento de las herramientas corresponden a mejoras en su interfaz web. Esto implica que no funciona la web, pero se puede acceder al servicio a través de terminales móviles previamente configurados.

Gestionar Twitter desde el dispositivo móvil

La gestión de las publicaciones se hará siempre desde la aplicación oficial de *Twitter*, disponible para todos los sistemas operativos móviles, aprovechando la opción multicuenta que ofrece la aplicación.

La <<ENTIDAD>> designará una unidad competente encargada de configurar el acceso en el dispositivo móvil.

FACEBOOK

Facebook es una de las redes sociales más conocidas en todo el mundo y con más usuarios activos, por lo que muchas entidades públicas han decidido hacerse presentes en esta red.

Se trata de una plataforma para comunicar y compartir, con usuarios conocidos, todo tipo de información, fotos, vídeos y enlaces, siendo los propios usuarios los que seleccionan aquellas comunidades que les interesen. Además, existe un conjunto de aplicaciones que complementan las funciones básicas de *Facebook* y que aportan un abanico nuevo de funciones, tanto profesionales como de ocio.

En *Facebook* se manejan los siguientes conceptos:

- Perfil: Tienen perfil las personas que, a título individual, se dan de alta en Facebook.
- Página: Las páginas están pensadas para instituciones, empresas o negocios, celebridades, etc. Las gestionan uno o varios administradores.
- Página oficial: Las páginas oficiales permiten que las instituciones, las empresas y otras entidades creen su espacio oficial dentro de Facebook, para poder comunicarse con sus seguidores.
- Grupo: Lo crea un usuario (creador) y las personas que se añaden pueden tener roles diferentes: administrador, vocal y miembro. Los grupos pueden ser públicos, privados o secretos, y sirven para formar una red en torno a un tema o a un interés específico.

Gestión de cuentas

Las páginas de *Facebook* de los diferentes departamentos de la <<ENTIDAD>> son páginas corporativas y las autoriza y configura la <<U/OC>> de la <<ENTIDAD>>. Los responsables de los departamentos deben contactar con la <<U/OC>> para obtener una cuenta de Facebook con el avatar correspondiente y las indicaciones en cuanto a la página y la imagen corporativa.

Facebook incorpora roles de **administrador de páginas**. La <<U/OC>>, que es el órgano encargado de abrir las páginas, ha de constar como administrador principal, mientras que los gestores de la página son los autores de contenido.

YOUTUBE

Las cuentas de *Youtube* de la <<ENTIDAD>> deben crearse desde correos electrónicos de la propia <<ENTIDAD>>. Para gestionarlos, se dejará una sesión abierta del perfil de *Youtube* correspondiente en una versión del navegador. Será necesario, sin embargo, prestar atención para no cerrar nunca la sesión cuando se salga del navegador y así evitar perder las claves de acceso.

No es recomendable vincular la cuenta de *YouTube* a la de *Facebook* o *Twitter*. Es preferible controlar manualmente la difusión de vídeos en otras redes sociales, de forma que el contenido relacionado con lo que se publica se adapte a cada red.

Contenidos e identificación de la <<ENTIDAD>>

La web de YouTube permite clasificar los vídeos en listas de reproducción y escoger una lista para que se reproduzca o seleccionar un vídeo para que aparezca como destacado en el apartado *Vídeos* y *listas de reproducción*.

A la hora de publicar un vídeo, es necesario ponerle un título y añadir una breve descripción. Además, conviene rellenar el campo *Etiquetas* con palabras clave que hagan referencia al vídeo en cuestión, para facilitar su búsqueda.

En el apartado *Escribe algo sobre ti* de la *Configuración del perfil* se especificará: Nombre del servicio, marca. Nombre del departamento. <<ENTIDAD>>.

Cuando sea posible, se replicarán estos contenidos en inglés.

Gestión

Aunque YouTube contiene funciones propias de las redes sociales para interactuar con los usuarios, como la mensajería instantánea y el sistema de comentarios, la <<ENTIDAD>> puede optar por concentrar esta función en el resto de herramientas presentadas y usar YouTube sólo como medio de difusión de vídeos.

En este sentido, con la misma idea de evitar la interacción con los usuarios a través de *Youtube* para concentrarse en las otras redes sociales, en cada uno de los vídeos que se publiquen se podrá marcar *No permitir comentarios*, *No permitir votaciones sobre comentarios*, *No permitir respuestas en vídeo* y *No permitir que se puntúe este vídeo*, salvo que la política comunicacional de la <<ENTIDAD>> señale otra cosa.

FLICKR

Flickr es un repositorio de imágenes. El límite de cargas es de 1 terabyte y se pueden subir fotos de hasta 200 MB, pudiendo escogerse el modo de visualización.

Los canales de *Flickr* de los diferentes departamentos de la <<ENTIDAD>> son corporativos y los autoriza y configura la <<U/OC>> de la <<ENTIDAD>>. Los responsables de los departamentos deberán contactar con la <<U/OC>> para obtener una cuenta con el avatar correspondiente y las indicaciones en cuanto al canal y a la imagen corporativa.

Para gestionar las cuentas de *Flickr* de la <<ENTIDAD>> se deja una sesión abierta del perfil correspondiente en una versión del navegador. Eso permite subir fotos y añadir el título, descripción, etiquetas y ordenarlas en álbumes que después serán visibles desde la web de Flickr.

Aunque caben otras opciones, dependiendo de la política comunicacional de la <<ENTIDAD>>, conviene configurar la cuenta de *Flickr* para que cumpla exclusivamente la función de repositorio de imágenes. Para ahorrar la publicación de comentarios que actúan como red social, hay que ir al apartado *Privacidad y permisos*, luego a *Opciones predeterminadas para las cargas nuevas* / *quien puede agregar notas, etiquetas y personas*, y seleccionar la opción *Solo tú.*

SLIDESHARE

Esta plataforma permite publicar presentaciones, documentos de texto y PDF.

Las cuentas de *Slideshare* de la <<ENTIDAD>> se crearán desde correos electrónicos de la <<ENTIDAD>>. Para gestionarlos se dejará una sesión abierta del perfil de *Slideshare* correspondiente en una versión del navegador. Esta aplicación permite acceder a los contenidos de *Slideshare* de la cuenta sin tener que acceder al sitio web de *Slideshare* y funciona de una manera muy parecida a la lógica de un cliente FTP. Permite subir presentaciones y añadir el título, la descripción y las etiquetas, que luego serán visibles desde la web de *Slideshare*.

Identificación de la <<ENTIDAD>>

En el apartado *About* de la *Información personal* se especificará: Nombre del servicio, marca. Nombre del departamento. <<ENTIDAD>>. Cuando sea posible, se replicará esta identificación en inglés.

Contenidos y Gestión

La difusión de los materiales publicados en *Slideshare* tiene lugar en otras redes sociales, como Twitter y Facebook, con el fin de llegar a un mayor número de usuarios. En el caso de *Slideshare* no se puede evitar que los usuarios hagan comentarios, pero suele ser aconsejable no promoverlos, salvo lo que disponga la política comunicacional de la <<ENTIDAD>>. La única parte de red de la aplicación que deberá usarse será la de suscripción.

Para que *Slideshare* cumpla exclusivamente la función de repositorio de presentaciones, hay que entrar a *Edit profile* / *Privacy settings* y seleccionar la opción *No one* de entre las cuatro opciones que aparecen.

Todos los materiales que se publiquen en *Slideshare*, ya sean presentaciones o documentos, deben estar en formato PDF. Habrá que definir los siguientes parámetros: título del documento, etiquetas, licencia CC correspondiente, formato de página continua, definición del fichero con el título del documento y visualización a página completa.

ANEXO C: REFERENCIAS Y DOCUMENTACIÓN USADA

- Guía CCN-STIC 821 Normas de Seguridad en el ENS. Normativa General y Apéndices I al VII.
- Junta de Castilla y León: Guía de Usos y Estilo en las redes sociales de la Junta de Castilla y León.
- Guía práctica para el uso de las redes sociales en los Ayuntamientos. Junta de Castilla y León.
- Social Media in Government. New Zealand Government Internal Affairs.
- Guía de redes sociales de la Generalitat de Cataluña.