Políticas de uso de servicios de participación ciudadana en el contexto de las Administraciones Públicas

CTIC
Centro Tecnológico

Políticas de uso de servicios de participación ciudadana en el contexto de las Administraciones Públicas

Créditos

Políticas de uso y servicios de participación ciudadana en el contexto de las Administraciones Públicas

1ª edición: diciembre 2009.

Promueve: Gobierno del Principado de Asturias (http://www.asturias.es) en el marco del Programa e-Asturias.

Edita: CTIC Centro Tecnológico (http://www.fundacionctic.org). Parque Científico y Tecnológico de Gijón. Edificio Centros Tecnológicos. C/ Ada Byron, 39. 33203 Gijón, Asturias, España.

En la presente publicación se ha utilizado expresamente un lenguaje no sexista con el triple objetivo de evitar la discriminación por cuestiones de género a través del lenguaje, de visibilizar y fomentar la presencia igualitaria de hombres y mujeres en el ámbito de las TIC y de familiarizar a las lectoras y a los lectores con un lenguaje incluyente. Todo ello contribuye a la promoción de una mayor igualdad de oportunidades entre hombres y mujeres.

Autores y autoras, en orden alfabético:

- Braña Gundin, Eloy (Principado de Asturias).
- García, Jesús (Fundación CTIC).
- Garriga, Marc (Ayuntamiento de Barcelona).
- Gisbert, Raquel (Ayuntamiento de Barcelona).
- Herrera, María del Carmen (Principado de Asturias).
- Pou, Dolors (Xperience Consulting).
- Ramos Gil de la Haza, Andrés (Bardají & Honrado Abogados).
- Rodríguez, José Luis (Principado de Asturias).
- Ruiz González, Miriam (Fundación CTIC).

Depósito Legal: AS-6650-2009

Índice de contenidos

Motivación

Motivación

Durante los últimos años hemos asistido al nacimiento de una nueva etapa de la web, ya que se ha pasado de un paradigma en el que la ciudadanía se limitaba a consumir pasivamente la información publicada, a otro basado en la interacción y las redes sociales y en el que la participación consiste en algo más que la simple recepción de contenidos.

La web participativa, conocida a menudo con el término Web 2.0, se refiere al uso de la inteligencia colectiva para desarrollar y proporcionar servicios interactivos, y en la que el control de los datos está en manos de las personas que los usan. De manera simplificada, se podría describir como los servicios que se apoyan en una base de datos y en los que se permite a usuarios y usuarias modificarla, tanto en su esencia (añadiendo, cambiando o borrando información, o asociando datos a la misma), como en la forma de presentar los contenidos.

El término Web 2.0 incluye una serie de tecnologías, aplicaciones y valores que pretenden explotar las ventajas de la conectividad que proporciona Internet para la creación de redes de personas y de contenidos. La web participativa se basa en valores como la firme creencia en que quienes usan los servicios pueden aportar activamente conocimiento (no solamente consumirlo), o el concepto de inteligencia colectiva. Sobre estas ideas surgen aplicaciones como los *blogs, wikis, podcasts, RSS feeds, tags* o etiquetas, redes sociales o sistemas colectivos de contenido multimedia que a estas alturas ya no son solamente una promesa, sino que han demostrado su valor con creces.

El futuro de la web no está simplemente en la integración de los datos en una aplicación centralizada, sino en compartirlos. Con el objetivo de potenciar el surgimiento de nuevos servicios de más valor añadido y de aprovechar al máximo la información disponible, permitiendo combinarla de todas las formas posibles para extraer de ella todo su valor, surgen asimismo tecnologías como AJAX, XML, API abiertos, web semántica, microformatos, etcétera, que constituyen un paso más en la creación de inteligencia colectiva en la red, y que permiten construir estructuras de información mayores que las que corresponden a la suma de los servicios por separado.

Se ha escrito ampliamente sobre la Web 2.0, que ha dejado de ser el futuro para convertirse en un presente que aprovecha la voluntad de colaboración de todo el mundo para generar, clasificar y elaborar la información de forma colectiva, obteniendo resultados muy superiores y con un esfuerzo y un coste mucho menor del que se tendría de otra manera.

En la actualidad, permitir que usuarios y usuarias interactúen con el propio portal o entre sí es lo más común y resulta prácticamente impensable mantener un portal cerrado, en el sentido de que sólo sea posible la comunicación unidireccional (desde el portal hacia quienes lo usan). El nuevo usuario o usuaria exige participar, aportar información, comunicarse con aquellas personas con quienes comparte aficiones, ideas o sentimientos. Esta información, además, resulta muy valiosa para la organización que gestiona el servicio si sabe aprovecharla.

Sin embargo, la adopción de este nuevo paradigma, como cualquier otro cambio, no viene exento de riesgos. A menudo, quienes se plantean abrir servicios participativos tienen dudas inconcretas sobre si realmente se puede confiar en quienes usan sus aplicaciones para cederles parte del control de la información, sobre si se usará el propio servicio en su contra, sobre los riesgos legales a los que puede tener que enfrentarse por culpa de la participación incívica de alguna persona o acerca de qué pondrá el periódico local en su portada sobre nuestra organización, si se equivoca.

Estos riesgos, aunque existentes, pueden ser magnificados involuntariamente si se perciben y afrontan de una forma intuitiva, subjetiva, desorganizada y asistemática. Es conveniente situarlos en una posición más realista para afrontarlos con mayores garantías de éxito, en el caso de que se consideren de una forma sistemática y lógica. Afortunadamente, disponemos en la actualidad de muchas herramientas y conocimiento acumulado para gestionar situaciones de riesgo en diversos aspectos de la vida (catástrofes naturales, seguridad laboral, aseguramiento del hogar, planificación de negocios, etcétera). Todo este conocimiento puede ser, por tanto, aplicado sin problemas a este nuevo campo que se abre delante nuestro.

Este documento describe la metodología de análisis de servicios web participativos desarrollada para el Gobierno del Principado de Asturias, dando cobertura a los principales riesgos a los que puede tener que enfrentarse una Administración Pública a la hora de establecer o gestionar servicios de este tipo, si bien también es aplicable a empresas u organizaciones de otro tipo que pretendan afrontar situaciones semejantes.

La web participativa o Web 2.0

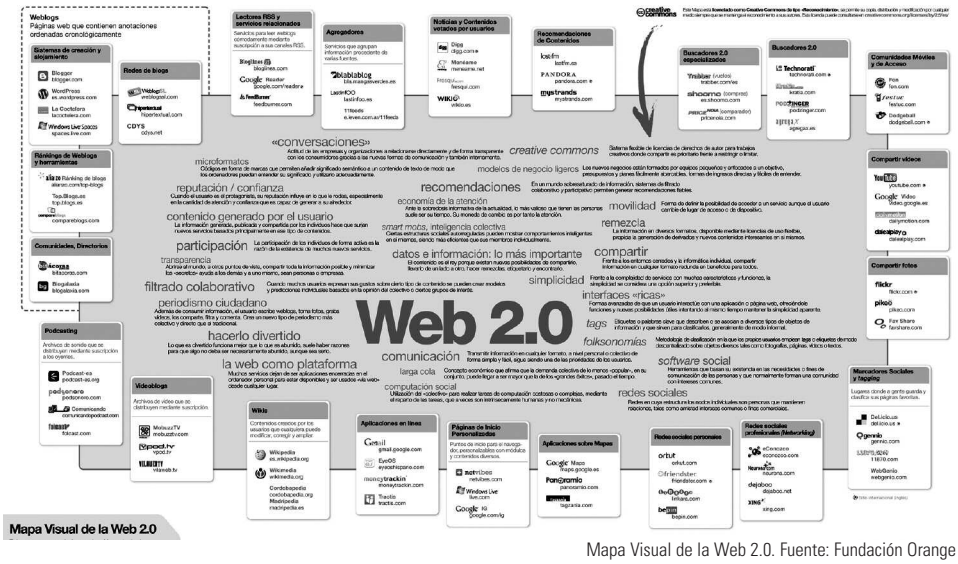
La web participativa o Web 2.0

El término Web 2.0, acuñado por Dale Dougherty en una tormenta de ideas, fue popularizado por Tim O`Reilly entre los años 2004 y 2005, haciendo referencia a una segunda generación o renacimiento de la tecnología web, que en ese momento comenzaba a estar basada en comunidades de personas y cuyo eje se define alrededor de una gama de servicios que fomentan la colaboración y el intercambio ágil de la información entre quienes usan estos sistemas.

Es difícil concretar con exactitud lo que implica la Web 2.0, definida inicialmente en base a ejemplos en lugar de hacerlo por comprensión, y que se sustenta sobre una infraestructura compleja y en constante evolución. Ésta incluye unos determinados protocolos universalizados de conexión entre las aplicaciones (de las que destaca indudablemente HTTP), la redifusión de la información, navegadores basados en estándares (HTML, CSS, XML o RDF), componentes multimedia también estándares, formales o de facto, y diferentes tipos de servicios. De cualquier forma, en el núcleo de la propia Web 2.0 encontramos, sin duda, el uso de los servicios como punto de intercambio de información entre usuarios y usuarias, al contrario que en el paradigma anterior en el que las webs estaban estructuradas según el concepto de consumo de contenidos o esquema productor-consumidor.

Tim O'Reilly y John Battelle resumieron los principios clave que caracterizan a las aplicaciones Web 2.0, situando a la web construida sobre las bases de datos como plataforma tecnológica, estableciendo los datos como el componente clave que aporta el valor añadido, señalando los efectos de red que surgen desde las arquitecturas participativas como el principal motor de funcionamiento, definiendo una estructura basada en pequeños componentes de negocio (elementos esenciales del sistema) capaces de combinar y redifundir la información, y asumiendo un estado de mejora continua ("beta perpetua"). De esta forma se pueden considerar ciertos puntos como los pilares sobre los que se sustenta la Web 2.0:

- **Desarrollo descentralizado o distribuido:** la información es generada y mantenida de una forma descentralizada y se tiende a que el contenido de los sitios sea gestionado colectivamente por diferentes personas, en lugar de basarse en un modelo editorial centralizado. Se confía en usuarios y usuarias para contribuir información y codesarrollar los servicios.
- **Modelos de programación ligeros:** es muy difícil añadir nueva funcionalidad a los sitios monolíticos debido a su poca flexibilidad, por lo que se intenta crearlos a partir de la integración de componentes más pequeños, sencillos, manejables y reusables, y que carecen de un fuerte acoplamiento entre ellos.



Mapa Visual de la Web 2.0. Fuente: Fundación Orange

- **Contenidos multipropósito:** la información puede ser utilizada y combinada para un propósito diferente al de su concepción inicial, para lo que se proveen mecanismos que permitan exportarlos e incorporarlos en otras aplicaciones, así como API abiertas para interaccionar con los servicios. Se favorece la combinación de la información disponible para obtener otra más elaborada.

- **Situación de "beta perpetua":** los sistemas se despliegan pronto, en lugar de esperar a que estén absolutamente terminados, y se realiza una mejora continua sobre ellos apoyándose en la retroalimentación por parte de usuarios y usuarias. Nunca se considera que un desarrollo está totalmente terminado.

- **Enriquecimiento de la experiencia de uso:** los sistemas incorporan componentes multimedia, tecnología AJAX, posibilidad de personalización de la información mostrada y su visualización, etcétera. Se busca hacer de la navegación una experiencia más parecida al uso de programas de escritorio.

La web participativa se caracteriza por la creación y el mantenimiento de los contenidos y de la información de una forma colectiva por parte de usuarios y usuarias, pudiendo éstos participar en cualquier aspecto posible de los servicios ofrecidos, entre los que destacan los siguientes:

- Generación de los contenidos.
- Clasificación de la información.
- Conversación sobre el contenido, añadiendo comentarios, referencias, calificaciones, etcétera.
- Gestión de la plataforma, al asumir quienes usan los servicios una parte del rol de gestión de la misma.

Si inicialmente la Web 1.0 consistía en un sistema unidireccional, dirigido desde quienes editaban la información hasta quienes se conectaban a ella para consumirla, con la Web 2.0 surgen sistemas en los que las personas se conectan a personas, colaborando y compartiendo la información y creando comunidades en este proceso. En el futuro veremos, seguramente, aplicaciones web conectándose a otras aplicaciones web para enriquecer la experiencia de las personas, yendo un paso más allá y haciendo realidad la Web 3.0, prometida por la web semántica.

Si la Web 2.0 tiene como principal protagonista al ser humano, la Web 3.0 está orientada hacia el predominio de sistemas procesadores de información que sean capaces de entender la lógica descriptiva, expresada en diversos lenguajes más elaborados de metadatos, de tal manera que sean capaces de entender de alguna forma el conocimiento almacenado, y procesar de forma eficiente la avalancha de información disponible.

Herramientas colaborativas en la web

Existen una serie de servicios y aplicaciones clave de la web participativa ampliamente conocidos, algunos de los cuales se han utilizado desde hace muchos años y están en la actualidad bastante asentados. Esta lista incluye, entre otros, componentes como *blogs, wikis*, sindicación de contenido a través de RSS o Atom, el uso del audio para comunicarse a través de *podcasting*, servicios de etiquetado, la compartición de recursos multimedia, el establecimiento de redes sociales, *microblogging*, etcétera. Estos servicios, que van adoptando constantemente nuevas formas y son combinados y ampliados con nuevas capacidades, están construidos sobre estándares abiertos soportados por Internet y por la web, dándoles habitualmente un uso creativo más allá de su concepción inicial, y se apoyan a menudo sobre otros servicios ya existentes.

Resulta inútil intentar realizar una lista exhaustiva de los servicios Web 2.0, ya que ésta estaría en constante evolución, siendo permanentemente ampliada gracias a la creatividad de la raza humana. Sin embargo, sí que es interesante familiarizarse con los principales servicios, ya que éstos constituyen las bases sobre las que está construida la actual Web 2.0.

Generación colectiva de información

Blogs o bitácoras

La palabra *blog* surge como versión simplificada de la yuxtaposición de las palabras inglesas *web* y *log*, que fueron inicialmente combinadas en una sola, *weblog* o bitácora de la web, y que acabó derivando en la expresión actual, *blog*. Un *blog* es, esencialmente, un sistema de publicación de contenidos, actualizado de forma periódica, en el que las entradas aparecen ordenadas cronológicamente y en el que los artículos más recientes se muestran en primer lugar, configurando una especie de diario personal en línea.

Como ocurre con otros servicios, alrededor del término *blog* ha surgido una nueva terminología que puede resultar algo críptica para quienes no están familiarizados con ella. En este sentido, el acto de escribir o publicar en un *blog* se conoce habitualmente como *blogging* o *bloguear* y una persona que escribe en un *blog* recibe el nombre de *blogger* o *bloguero*.

En un *blog* puede publicar artículos (o entradas) una sola persona o varias, y estos artículos pueden permitir comentarios por parte de quienes lo leen o no hacerlo. A veces, los artículos se marcan con etiquetas o *tags*, que consisten en una o dos palabras clave que describen el tema al que están referidas, o están estructurados en algún sistema predefinido de categorías, facilitando a los lectores la selección y seguimiento de los temas que les interesan.

Los enlaces hipertextuales son uno de los aspectos más importantes de los *blogs*, ya que permiten referenciar y recuperar la información relacionada contenida en otros *blogs*, y a menudo complementar la contenida en los artículos o encontrar las fuentes informativas en las que se basa. Para facilitar esto, los *blogs* incorporan un sistema llamado *permalink* o enlaces permanentes que garantizan que permanecerá inmodificable, permitiendo a terceras partes enlazar a los contenidos publicados con unas ciertas garantías de estabilidad.

Asimismo, los *blogs* incorporan a menudo enlaces inversos, llamados *trackback* o *pingback*, que permiten informar a los autores o autoras de otros *blogs* de que sus contenidos están siendo referenciados. Muchos *blogs* disponen además de un servicio de *blogroll* o lista de enlaces a otros *blogs* que, de alguna forma, se consideran útiles o interesantes. Por otra parte, es muy habitual en los *blogs* disponer de la posibilidad de sindicación de sus contenidos a través de mecanismos como RSS o Atom.

Puesto que se actualizan a menudo permiten a los visitantes responder a las entradas, los *blogs* funcionan frecuentemente como herramientas sociales. A veces es posible agregar fotografías o vídeos, lo que se conoce habitualmente como *fotoblogs* y *videoblogs*.

Los *blogs* son una de las herramientas más antiguas y sólidas establecidas en la web social y su concepto ha dado lugar a diversas variaciones, adaptadas a diferentes contextos, que a menudo reciben nombres especiales:

- *Microblog* o *nanoblog*: permite publicar mensajes exclusivamente textuales, con una longitud máxima de 140 caracteres, a través de SMS, mensajería instantánea, interfaces web o aplicaciones específicas. Ejemplos:
  Twitter, Jaiku o Pownce.
- *Fotoblog*: es un sistema de publicación de fotografías en un formato de *blog*. A diferencia de un álbum de fotos, en un *fotoblog* se publican unas pocas fotos diarias, generalmente una sola. Pueden incorporar

Página Principal de Twitter. Fuente: www.twitter.com

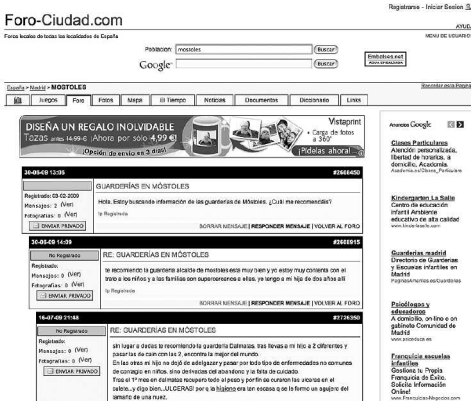
además comentarios, bien del autor o autora o a veces también de terceras personas, así como la fecha, información sobre la propia fotografía, características de la cámara usada o su geolocalización, así como enlaces a otros *fotoblogs*. Ejemplos: Fotolog o Flickr.

Página principal de Flickr. Fuente www.flickr.es

- *Videoblog* o *vlog:* es esencialmente una galería de clips de vídeo, ordenada cronológicamente, que es publicada por una o más personas. Para la visualización de los vídeos a través de la web se ha establecido como estándar de hecho el reproductor y el *codec* de vídeo del lenguaje Flash de Adobe, que permite su visualización inmediata, y los formatos MP4 o MOV para su descarga directa o a través de suscripciones vía RSS, aunque los nuevos estándares de HTML permiten incorporar estos elementos directamente.

Foros

Es esencialmente una aplicación web que da soporte a discusiones u opiniones en línea. Existen como complemento a un sitio web, para discutir o compartir información relevante según la temática del sitio de una forma libre e informal, con lo que se llega a formar una comunidad en torno a un interés común. No se permite modificar las aportaciones de otras y otros miembros, excepto en el caso de que se tengan ciertos permisos especiales (quienes moderan o administran).



Captura de pantalla de Foro-Ciudad.com. Fuente: www.foro-ciudad.com

Listas de correo

El correo electrónico o *e-mail* es uno de los mecanismos de comunicación electrónicos más antiguos que existen, anterior incluso a Internet, y cuyo objeto es el envío y la recepción de mensajes a través del uso de una serie de servidores intermedios que hacen de buzones, y en los que los mensajes son almacenados temporalmente hasta que son leídos por la persona destinataria.

Las listas de correo suponen un uso especial del correo electrónico, de tal forma que se puede distribuir la información de una forma masiva entre múltiples receptores en un único envío y de forma

simultánea. El funcionamiento habitual es que, al escribir a una dirección de correo determinada, el mismo correo es enviado masivamente a todas las personas inscritas en la lista.

Wikis

El término *wiki* proviene de la palabra hawaiana *wikiwiki*, que significa rápido o veloz. Consiste en una o varias páginas que pueden ser editadas fácilmente desde cualquier lugar a través de un sencillo interfaz web, que permite crear, modificar o borrar un mismo texto compartido. Habitualmente constituyen un sitio de construcción colectiva de la información por parte de múltiples voluntarios o voluntarias y su uso se extiende a la generación colaborativa de contenidos, al desarrollo de repositorios de recursos, como sistema generalista de compartición y almacenamiento de la información, a la transferencia de conocimiento dentro de una organización o, incluso, como herramienta comodín para muchas otras necesidades que no están cubiertas por una herramienta más específica.

Los *wikis*, a diferencia de los *blogs*, suelen conservar un historial de cambios que permite recuperar fácilmente cualquier estado anterior y permiten visualizar, de una forma sencilla, los cambios que se hayan efectuado, y relacionarlos con las personas que los hayan realizado. El contenido que muestra la página *wiki* editada se actualiza habitualmente sin una revisión previa, aunque siempre se provee la posibilidad de restaurar versiones anteriores o revertir los cambios realizados.

A veces, los *wikis* están asociados a una página de comentarios que permiten discutir los contenidos de las mismas, como ocurre en la Wikipedia, el ejemplo por excelencia de esta aplicación.

Página de inicio de Wikipedia. Fuente: es.wikipedia.org

Encuestas

Las encuestas son, tradicionalmente, conjuntos de preguntas normalizadas con los que se busca averiguar, con mayor o menor exactitud, qué es lo que piensa un grupo de personas sobre algún tema en concreto.

Las encuestas web, encuestas *online* o e-encuestas, son un recurso utilizado desde hace mucho tiempo para permitir una pequeña participación de quienes leen la información publicada en un portal. Dependiendo del objetivo buscado, éstas pueden estar compuestas de múltiples preguntas y requerir bastante tiempo y voluntad por parte de quienes las responden o, por el contrario, estar destinadas a averiguar qué opina la gente sobre un tema muy concreto a través de una única pregunta, o dos como mucho.

Habitualmente los resultados de este tipo de encuestas no son muy fiables debido a diversos motivos, como la posibilidad de que una persona vote más de una vez o el sesgo del colectivo que decide participar en la encuesta.

Comentarios

Mediante un formulario se permite a otros usuarios y usuarias de la web añadir comentarios a cada página o entrada, lo que puede generar un debate sobre sus contenidos, además de cualquier otra información.

A menudo, éste es uno de los recursos más valiosos y más usados para conseguir la participación de las personas en la web, y se puede incorporar casi a cualquier elemento, desde comentarios a los artículos o noticias que se publiquen, comentarios a las entradas de los blogs, a las fotografías, a los vídeos, comentarios adicionales a las páginas *wiki*, a las encuestas, etcétera. Probablemente no exista ningún componente desplegable en un portal web que no sea susceptible de permitir que se añadan comentarios.

Concursos

La creación de contenidos de algún tipo se ve impulsada por la generación de un concurso a su alrededor, en algunos casos con premios reales, virtuales o incluso a veces con el único premio de la mención pública de haber realizado la mejor obra. Es muy habitual ver concursos de fotografías, de logotipos, de *blogs*, de desarrollo de juegos, de relatos, entre otros. En todo caso, estos concursos se articulan entorno a la aportación de contenido por parte de usuarios y usuarias y, habitualmente, también la clasificación y puntuación de los mismos se hace de forma participativa.

Clasificación colectiva de contenidos

Si bien una de las facetas de la Web 2.0 es la generación participativa de información, no es la única en la que la inteligencia colectiva puede dar muy buenos resultados; en la clasificación de los contenidos es, asimismo, relevante.

Valoraciones

Consiste en el uso de un sistema de puntuación de las páginas web, a menudo mostrado visualmente con un número de estrellas, con una puntuación numérica de las mismas (*karma*), o mediante una representación textual de esa puntuación, que permite ordenar las páginas de mayor a menor importancia de acuerdo con los votos de los y las internautas que las visiten.

Éste es, probablemente, el recurso más usado para permitir retroalimentación de los contenidos por parte de quienes los leen, y es posible añadir este elemento a casi cualquier tipo de contenido publicable en un portal web.

Etiquetas o tags, folcsonomías y nubes de tags

Una etiqueta o *tag* es una palabra clave que se asigna a cualquier elemento para describirlo. Si bien se pueden asignar etiquetas pertenecientes a un conjunto cerrado previamente definido, a menudo se permite usar libremente cualquier etiqueta que se desee para categorizar colectivamente los contenidos de las páginas web, usando el vocabulario de la persona que realiza la clasificación.

El resultado de este etiquetado individual y libre, al ser realizado en gran cantidad, permite crear un tipo de clasificación que se conoce como *folcsonomía* (folc + taxo + nomía, *clasificación gestionada por el pueblo*, término acuñado por Thomas Vander Wall), y que facilita organizar la información sin jerarquías ni relaciones de dependencias.

Si bien las taxonomías, que son un sistema de clasificación jerárquica predefinida, proporcionan un sistema más estructurado y estricto de clasificación de la información, el desarrollo de éstas es mucho más complejo y ha de ser realizado de la mano de personas expertas. Las *folcsonomías* proporcionan un sistema colaborativo equivalente para la clasificación de la información que, aunque menos estructurado, se aprovecha de la inteligencia colectiva para realizarla de una forma más sencilla, utilizando la potencia de la Web participativa.

Sistemas de clasificación según la reputación

Son algoritmos de filtrado colaborativo en el que se intenta cualificar un conjunto de elementos en función de las opiniones que éstos tienen unos de otros. Son muy útiles en redes sociales grandes en las que hay usuarios y usuarias sin experiencia previa o en los que se publica contenidos generados por los usuarios y usuarias.

Intercambio de información

Exportación de información

Puesto que la tendencia actual es la generación de contenidos de valor añadido por agregación de los provenientes de diferentes fuentes, así como permitir que cada cual pueda consumirlos de la forma que le resulte más apropiada (incluyendo, por ejemplo, conceptos como usabilidad, accesibilidad o movilidad), se hace necesario poder exportar este conocimiento de tal forma que pueda ser usado por otros portales o por diferentes herramientas o aplicaciones de escritorio, así como la posible interacción desde éstas con nuestro portal. El objetivo ya no es forzar a usuarios o usuarias a acceder a la información a través de un canal determinado, quieran o no, sino facilitar el acceso a la misma para todo el mundo, de la forma que resulte más cómoda para cada cual.

Sindicación de contenidos

La sindicación de contenidos consiste en su exportación a través de protocolos como Atom o RSS (RDF Site Summary). El formato RSS es simplemente un formato de tipo XML dotado de una estructura idónea para presentar resúmenes de contenidos y se utiliza para poner a disposición de otras webs o aplicaciones, los contenidos más novedosos de un sitio web.

Publicación de información estructurada semánticamente

Consiste, esencialmente, en la publicación de la información en formatos RDF (Resource Description Framework), que permite el uso descentralizado de la misma y su combinación con otras fuentes. Es posible, asimismo, adoptar el uso de microformatos o de elementos RDFA (Resource Description Framework Attributes) embebidos en el código HTML para proveer información semántica que pueda ser procesada por otras aplicaciones, publicándola de una forma integral en la misma página web.

API abiertos

Los API, es decir, interfaces de programación de aplicaciones, representan el conjunto de llamadas a diversas funciones o procedimientos por parte de los programas de ordenador, mediante las cuales se ofrece acceso a ciertos servicios. Al permitir el acceso directo a los mismos a través de protocolos como SOAP, REST o JSON, se facilita la integración de la información publicada en otras páginas web o, incluso, la posibilidad de acceder a ésta a través de programas específicos que no tienen por qué ser navegadores web.

Integración de contenidos de terceras personas

De igual forma que resulta muy importante poder publicar la información en un formato que sea legible y utilizable por otras personas, también podemos hacer uso del contenido publicado desde

otros portales web para, combinándolo con la información que aportamos desde nuestros sistemas, dar un contenido con un valor añadido mucho mayor que lo que correspondería al publicar ésta en solitario.

Agregadores, planetas de blogs o metablogs

Un planeta de *blogs* agrupa en una misma página los *feeds* exportados por otras a través de RSS, Atom u otros derivados de XML/RDF, mostrando automáticamente los últimos artículos de una serie de *blogs* que comparten un interés común. En una sola página, presentada también habitualmente en formato de *blog*, se recogen las diferentes entradas ordenadas cronológicamente.

Mashups o aplicaciones web híbridas

Son sitios web o aplicaciones web que usan contenidos de terceros para crear uno nuevo completo. El contenido de un *mashup* normalmente proviene de sitios web de terceros a través de una interfaz pública o usando un API. Otros métodos que constituyen el origen de sus datos incluyen sindicadores web (RSS o Atom), extracción directa de la web mediante ingeniería inversa (*screen scraping),* etcétera.

Contenido multimedia: fotos, audio, vídeo, *flash,* etcétera

Una de las mayores áreas de crecimiento actual en la web se establece en aquellos servicios que facilitan almacenar y compartir contenidos multimedia de diferente tipo. En esta clase de servicios, habitualmente, los usuarios y usuarias no se limitan a consumir contenido, sino que contribuyen activamente en su producción. Este desarrollo se debe, en parte, a la evolución de la tecnología digital de imagen y sonido de alta calidad y de relativo bajo coste, como las cámaras fotográficas digitales, las grabadoras de vídeo o los teléfonos móviles.

Álbum fotográfico

Es un sistema de publicación de fotografías que permite exponerlas en la web de una forma semejante a los álbumes de fotos tradicionales, pudiendo incluir opciones como la edición de fotos (diferentes tamaños o disposiciones de las mismas). Algunos servicios, incluso, amplían la idea de un álbum de fotos permitiendo que una fotografía se convierta en parte de muchos álbumes, agregando comentarios y palabras claves a estas fotografías y utilizando dichas palabras como medio para crear nuevos álbumes de fotos.

Podcast

La palabra *podcast* proviene de la contracción de los términos *iPod* (reproductor MP3 de Apple) y *broadcast* (emisión); supone un paso más allá en los *blogs*, puesto que cambia a formato sonoro. Permite la creación de archivos de sonido (generalmente en formato MP3 o AAC y, en algunos casos, Ogg) y su distribución mediante un archivo Atom o RSS, al que se puede realizar una suscripción. La persona que accede al servicio puede escuchar, además, el archivo en el momento que quiera, una vez que lo haya descargado, generalmente en un reproductor portátil.

Video Podcast, vidcast o vodcast

Es una evolución del *podcast*, referida a la distribución de vídeo bajo demanda, en el que el RSS es usado como canal de televisión no lineal al que los usuarios y usuarias se pueden suscribir usando un ordenador, una televisión, un *media center* o un dispositivo móvil multimedia. Es posible distribuir los vídeos como archivos descargables, pero no siempre se hace así y a menudo solamente se permite su visualización en el momento, distribuyéndolos en forma de flujo o *stream*.

Página Principal de Videopodcasts tv
Fuente: www.videopodcasts.tv

Servicios basados en las relaciones entre personas

Chat o cibercharla

Se refiere a una comunicación escrita a través de Internet entre dos o más personas que se realiza instantáneamente. Hay numerosas variedades, que incluyen desde la posibilidad de hablar en comunicaciones privadas entre participantes, hasta que la comunicación se establezca en canales públicos.

Mensajería instantánea

El servicio más básico de conversaciones en tiempo real a través de la red es, probablemente, la mensajería instantánea. Existen numerosos ejemplos de redes que proveen este servicio, desde las asociadas a grandes empresas como MSN, Yahoo! o Google Talk, hasta las basadas en redes distribuidas, como Jabber, o a través de páginas web, como Facebook. En esencia, consiste en la posibilidad de que dos o más personas puedan estar conversando entre ellas mientras están conectadas a la red y que esta conversación se haga de una forma interactiva y en tiempo real. En muchos casos estas conversaciones se articulan alrededor de salas en las que conversan todas las personas que se conectan.

A veces este servicio de mensajería instantánea puede venir complementado con herramientas como pizarras compartidas, juegos multiusuario o cualquier servicio parecido que vaya más allá del simple texto.

Pagina inicial de Gajim.org. Fuente: www.gajim.org

Conferencias web

Las conferencias web consisten en reuniones virtuales a través de Internet cuyas personas participantes trabajan en distintas ubicaciones físicas. Cada una de ellas se sienta ante su ordenador, donde puede ver todo lo que, quien hace la presentación, va mostrando en su pantalla.

Audioconferencias y videoconferencias

Extendiendo el concepto inicial de mensajería instantánea, surgen los servicios de audioconferencia y videoconferencia. Una audioconferencia permite realizar un encuentro virtual a través de Internet en el que los y las participantes se comunican interactivamente mediante la transmisión y recepción de audio en tiempo real (VoIP). En el caso de las videoconferencias, la comunicación simultánea y bidireccional será tanto de audio como de vídeo, permitiendo mantener reuniones con grupos de personas situadas en lugares alejados entre sí.

Mundos virtuales

Los mundos virtuales consisten en la simulación de mundos o entornos en los que los usuarios y usuarias interaccionan con la máquina en entornos artificiales semejantes a la vida real, pudiendo a veces interactuar con otras personas usuarias estableciendo comunicaciones bidireccionales arbitrarias. Esto puede, a menudo, ser útil para realizar visitas a ciudades o museos remotos, o simplemente para proporcionar un entorno más acogedor para la celebración de reuniones virtuales.

Redes sociales

Una red social es una estructura que representa no solamente a las personas o los proyectos, sino también a las relaciones entre ellos, de tal forma que se puede usar esta información con diferentes fines.

El primer uso evidente de las redes sociales es el de mecanismo de clasificación y selección de la información publicada por otras personas y su participación en la red, de tal forma que el sistema puede priorizar aquella proveniente de personas o proyectos con quienes tengamos vínculos comunes, o deducir de la estructura de la red social cuáles son los contenidos más relevantes de una

forma automatizada. Este es el caso de servicios como Twitter, en el que toda la información es pública, pero la selección automatizada de la misma se hace en función de los enlaces que hayamos establecido con otras personas o proyectos (dicho en argot de Twitter a quién estemos siguiendo).

Las redes sociales permiten además, en los casos que se desea, proveer de un mecanismo de control que evite la diseminación indiscriminada de los datos de los usuarios y usuarias, permitiendo una cierta granularidad en su control a través de la configuración de dichos enlaces. Es el caso de redes como Tuenti o Facebook, en las que la seguridad de la información y la privacidad suponen un asunto primordial.

Además, tienen el beneficio añadido de que se produce una autocensura en el comportamiento de las personas basándose en que sus movimientos están siendo observados por personas de su círculo de amistades que han aceptado voluntariamente. Esto hace que muchos comportamientos habituales en foros públicos, como el *trolling* (insultos o provocaciones o simplemente la radicalización de las posiciones) sean mucho menos habituales en sistemas que disponen de este tipo de mecanismos de red social.

Por último, la propia estructura de red, creada por los usuarios y usuarias, tiene también un valor en sí misma ya que permite adaptar los contenidos y personalizar el acceso a la información. Este efecto es muy visible en redes como Facebook, que aprovecha el conocimiento de las relaciones entre los perfiles para promocionar otros elementos que potencialmente son interesantes para quienes lo usan; incluso la publicidad dirigida, como es el caso de Tuenti o Facebook.

Página principal de Facebook. Fuente: www.facebook.com

Intercambios económicos o comerciales entre participantes

Una de las novedades que conlleva Internet es el establecimiento de relaciones comerciales o de cualquier otro tipo de transacciones a través de mecanismos electrónicos. Existen diferentes modelos de comercio electrónico:

- Modelo B2C (*Business to Consumer*): hace referencia a las relaciones comerciales que se establecen entre una empresa y una persona usuaria o consumidora, con el fin de adquirir un producto o servicio.
- Modelo B2B (*Business to Business*): este modelo se fundamenta en el servicio que unas empresas dan a otras y, generalmente, es de mayorista a minorista o colectivo autónomo.
- Modelo C2C (*Consumer to Consumer*) o P2P (*Peer to Peer*): se refiere a las relaciones directas entre los usuarios y usuarias del portal, proporcionando éste un servicio de mero intercambio. Sin duda la empresa Ebay.com es un claro referente en este ámbito.
- Modelo C2B (*Business to Consumer*): se basa en una transacción de negocio originada por el usuario o usuaria final, que es quien fija las condiciones. En este sentido, existen páginas de personas que ofrecen sus casas como alquiler y las compañías de viajes pugnan por ellas. Un ejemplo de C2B es el portal Priceline.com.
- Modelo M2B (*Mobile to Business*): nace para los entornos de conectividad móviles que surgen de dispositivos como teléfonos o PDA y, en este caso, se usan los dispositivos móviles para conectar al usuario o usuaria con el servicio. Este mercado mueve a menudo productos como tonos, juegos, imágenes, música, vídeos, etcétera.
- Modelo A2B (*Administration to Business*), A2C (*Administration to Consumer*) y A2A *(Administration to Administration*): abarca las transacciones entre Administraciones Públicas u organizaciones gubernamentales y empresas, ciudadanía y otras administraciones, respectivamente.
- Modelo B2E (*Business to Employee*): hace referencia a las relaciones dentro de la red interna de la propia empresa u organización, que permite ofrecer productos o servicios a quienes trabajan o pertenecen a ella.

Si bien determinados modelos de comercio electrónico no son específicamente Web 2.0, sí que se muestra una tendencia, remarcada en varios de los modelos mencionados, a ciertos servicios de comercio en los que la participación de agentes externos a la organización que provee el servicio los hace entrar de lleno en esta categoría.

Posibles participantes

En el ámbito de la Administración electrónica, y de muchas organizaciones y empresas en general, se puede realizar una clasificación inicial de los perfiles de personas que usarán los servicios que puedan ofrecer.

Personal interno

En esta situación existe una relación contractual entre la persona y la organización, en principio, con una permanencia indefinida en la misma. El personal interno, por lo general, estará totalmente identificado en el uso que haga de los servicios puestos a su disposición; esta participación podrá estar regulada por las normas pactadas en el contrato establecido entre las partes y, además, se le dará una formación adecuada en el uso de dichos servicios, con lo que el riesgo de mal comportamiento será mucho menor que en otros casos y, por tanto, podrán ofrecerse mecanismos de participación más complejos.

Personal contratado

Al igual que en el caso anterior, existirá una relación contractual entre la persona y la organización, aunque la permanencia en ésta podrá ser temporal.

Personas externas

En este caso no existe relación contractual de ningún tipo con la persona que usa los servicios, aunque puede decirse que sí existe un vínculo entre ellas, bien sea una persona administrada por el organismo del que se trate, la clientela de la empresa, etcétera.

Personas ajenas

No existe relación de ningún tipo entre la persona y el organismo. Los usuarios y usuarias que se conectan podrían estar perfectamente en otro país u otro continente, o ser la primera vez que llegan a este servicio.

Personas anónimas

Se refiere al supuesto de que se trate de personas absolutamente sin identificar, de las que no se sabe nada.

Niveles de identificación

El nivel de identificación de una persona se refiere a qué se sabe de la identidad real de dicha persona. Un nivel de identificación más alto hará que se tenga una mayor certeza sobre quién es, mientras que un nivel de identificación menor implicará un mayor anonimato para la persona que usa el servicio.

Identificación total por métodos directos

El nivel más alto de identificación que se puede exigir a la hora de usar un servicio consiste en saber exactamente quién es la persona que está usando el sistema a través de su DNI, número de pasaporte o cualquier mecanismo similar. De esta forma se establece una relación uno a uno entre la identidad digital y la identidad de la persona.

Identificación total mediante métodos indirectos

Sin llegar a la identificación absoluta de quienes usan el sistema, se puede recurrir a mecanismos que, llegado el caso, puedan permitir la localización de la persona real que está detrás de la identidad digital (posiblemente a través de una orden judicial). Un mecanismo habitual para conseguirlo es la identificación a través de un número de teléfono, ya que debido a las actuales directivas comunitarias no se permite la existencia de números de teléfono de los que se desconozca la identidad de su titular.

En este caso, sin embargo, no existe ninguna garantía de que cada persona tenga una única identidad digital, puesto que podría tener dos números de teléfono diferentes, por ejemplo, y generar con ellos dos identidades digitales diferentes.

Identificación débil (seudónimo)

En este caso, lo único que se conoce de la persona es una dirección válida de correo electrónico, un identificador OpenID o un identificador de naturaleza semejante, lo que hace que a nivel efectivo pueda ser prácticamente imposible conseguir localizar a la persona real que hay detrás de ese identificador. Sin embargo, se puede establecer una conexión entre diferentes aportaciones de una misma persona, de tal forma que se sepa quien ha realizado dos aportaciones diferentes es la misma persona.

Como en el caso anterior, no se puede garantizar tampoco que una persona tenga una única identidad digital.

Participación anónima

Es el nivel más bajo de identificación posible. No hay nada que identifique a la persona que ha realizado la participación, excepto la IP y la hora en la que se realizó la conexión (sin que esto sea garantice nada, ya que esta persona ha podido, por ejemplo, usar un sistema anonimizador para que su IP real no sea revelada).

Obviamente, en este caso no es posible ni siquiera establecer una conexión entre aportaciones de la misma persona en momentos diferentes.

Nivel de autenticación

La autenticación o autentificación es el acto mediante el cual se puede confirmar que alguien es quien dice ser, habiéndose podido, en mayor o menor grado, verificar su identidad. Los métodos habituales de autenticación pueden estar basados en la existencia de algo que solamente es conocido, supuestamente, por esa persona (como un PIN o número de identificación personal o una contraseña); en algo que solamente esa persona posea (como una tarjeta de identidad, una clave privada de firma digital o un dispositivo hardware específico); o estar basados en una característica física o un acto involuntario de la persona (sistemas de verificación de voz, de escritura, de huellas, de patrones oculares, etcétera).

Autenticación mediante mecanismos biométricos

Dada la situación actual del estado del arte de estas tecnologías, como la carencia de dispositivos adecuados en los ordenadores personales domésticos, o la no necesidad de un grado tan fuerte de comprobación de la identidad, este tipo de autenticación simplemente no se usa en la actualidad para este tipo de servicios.

Conexión desde una red segura (intranet)

La autenticación se realiza permitiendo la conexión únicamente desde ciertos ordenadores, habitualmente pertenecientes a una intranet o a una red local totalmente identificada. No es habitual necesitar un grado de autenticación tan fuerte en los servicios participativos.

Autenticación fuerte (firma digital)

Se puede realizar una autenticación fuerte mediante algún mecanismo de firma digital, DNI electrónico, clave pública/clave privada, o similar. El uso de este tipo de autenticación suele provocar que haya una participación significativamente menor, por lo que no merece la pena exigirla si se quiere tener un servicio exitoso. Asimismo, evita que se pueda participar en el servicio desde ordenadores potencialmente inseguros, como los de los cibercafés.

Autenticación intermedia (datos de carácter privado)

La autenticación se puede realizar mediante la petición de datos que, con un cierto grado de probabilidad, solamente puedan estar en manos de la persona que pretende autenticar su identidad y que puedan ser comprobables por la organización que ofrece el servicio.

Autenticación débil (contraseña)

En este caso la autenticación se realiza mediante un identificador y una contraseña o un mecanismo de naturaleza similar.

Sin autentificar

Como indica el título del epígrafe, no se usa ningún tipo de autenticación.

Metodología de gestión de riesgos

Metodología de gestión de riesgos

Gestión de riesgos

No existe nada totalmente seguro. Cualquier actividad que realicemos, cualquier faceta de nuestra vida implica la posibilidad de que algo salga mal. Esto no deriva, evidentemente, en que no se realicen dichas actividades. Incluso el no hacer nada puede ocasionar problemas. Constantemente estamos tomando medidas para protegernos de estos posibles problemas y de los daños que pueden ocasionar. Antes de realizar o no una acción, calculamos más o menos lo que puede salir mal y actuamos en consecuencia, aceptando habitualmente los niveles bajos de riesgo y tratando de tomar medidas contra los niveles altos.

El término riesgo se refiere a las pérdidas esperadas a causa de una posible amenaza y su esencia radica en la posibilidad de sufrir un daño si se dan unas condiciones determinadas, obviamente no deseadas. Dependiendo del tipo de riesgo del que se trate, éste puede medirse según la pérdida económica que esperamos que se derive de él, el número de vidas perdidas o en función de la extensión del daño físico a una propiedad.

En el mundo físico, el daño ocasionado puede consistir en la pérdida de vidas humanas, la afectación de la salud, la pérdida de infraestructura, la inutilización de medios de producción, etcétera. En el caso de los procesos administrativos, el daño puede ser, por ejemplo, que no se cumplan las metas u objetivos, la afectación de los intereses económicos de la organización, la pérdida de credibilidad o la pérdida de clientela y ganancias.

Pese a la existencia inevitable de una serie de fenómenos que representan peligros o amenazas, el riesgo que originan depende también de las condiciones en las que se enfrentan dichos fenómenos, y no todos los peligros serán causantes de daño. La respuesta del proceso frente a los peligros se fundamenta en la eficacia de los controles que se aplican para evitar que dichas amenazas se concreten en daños reales.

El riesgo, pese a la incertidumbre intrínseca al mismo, se puede analizar y evaluar mediante técnicas estadísticas, lo que equivale a conocer más o menos el futuro. Para ello se puede calcular un cierto factor de riesgo, que será la característica que asociemos con la posibilidad de padecer un daño. Como se puede intuir de lo que hemos comentado, para el cálculo de este factor de riesgo se pueden tener en cuenta dos factores: la probabilidad de que ocurra un suceso que pueda causar un daño y la cuantificación de las pérdidas que se ocasionarían en el caso de que este daño se produjera. Podemos resumir todo esto en una sencilla ecuación:

$$\text{Riesgo} = \text{probabilidad} \times \text{daño}$$

Por tanto, para controlar los riesgos podemos tomar medidas en dos sentidos: por una parte, realizar actuaciones conducentes a una disminución de la probabilidad de que ocurra un suceso de este tipo y, por otra parte, tomar las medidas necesarias para que, si este suceso ocurre, el daño que ocasione sea el mínimo posible. En el primer caso estaríamos hablando de medidas proactivas o preventivas, mientras que en el segundo de medidas reactivas o correctivas.

Un ejemplo que permite visualizar más fácilmente la diferencia entre ellos es el siguiente: podemos fijarnos en lo que sería un trabajo en altura realizado sobre un andamio. Siempre existe, como es obvio, la posibilidad de que ocurra una caída, que podría ser muy grave. Para disminuir la probabilidad de que ocurra un accidente así, podemos optar por poner un andamio rodeado por una valla, con lo que la probabilidad será menor. Aun así, si se diera el caso, las consecuencias seguirían siendo muy graves. Además de la valla, podemos poner una red de protección u obligar al uso de un arnés. Estos elementos no modificarían la probabilidad de una caída, pero sí que harían que sus consecuencias, en caso de que ésta ocurra, fueran menores.

Para la gestión de los riesgos actuaremos, habitualmente, sobre los dos factores a la vez, disminuyendo la probabilidad mediante medidas preventivas y el daño mediante correctivas.

Proceso de gestión de riesgos

La gestión adecuada de los riesgos implica una serie de fases que abarquen la planificación, el desarrollo y la supervisión de los mecanismos de gestión, con vistas a que el sistema siga funcionando siempre correctamente, incluso cuando las condiciones cambien o sea progresivamente más eficiente:

- **Planificación:** se decide cómo se va a enfocar la administración o gestión de los riesgos y qué metodología se va a aplicar. Su principal resultado es el plan de administración de riesgos, en el que se documentan los procedimientos que se seguirán para evaluar y gestionar dichos riesgos.
- **Identificación de los peligros:** se trata de comprender qué eventos podrían potencialmente dañar o mejorar un proceso en particular. Aunque es importante identificar los riesgos potenciales lo antes posible, se debe repetir este proceso periódicamente para poder reaccionar a los cambios en el entorno.
- **Evaluación inicial de los riesgos:** implica evaluar la probabilidad de los peligros identificados y el impacto de los daños que podrían causar para determinar su magnitud y prioridad.
- **Planificación de las medidas a tomar:** una vez identificados y cuantificados los riesgos, se debe desarrollar una respuesta adecuada para afrontarlos. Se intentará, siempre que sea posible, eliminar los riesgos actuando sobre sus causas. En los casos en los que

no se pueda hacer esto, se deberá actuar en dos sentidos: por una parte, intentado disminuir la probabilidad de que se produzca un daño y, por otra, disminuir sus consecuencias en el caso de que se produzca.

- **Nueva evaluación de los riesgos:** una vez definidas las actuaciones que se van a tomar, se ha de realizar una nueva evaluación de riesgos en las nuevas circunstancias.
- **Control de los riesgos (ejecución de las medidas planificadas):** incluye la ejecución de los procesos de la gestión de riesgos que se han decidido incorporar para responder a eventos peligrosos.
- **Recopilación de datos:** durante el funcionamiento normal de los servicios se han de recopilar y almacenar datos que permitan revaluar e ir mejorando el sistema de gestión de los riesgos, así como planificar mejor dicha gestión en nuevos servicios.
- **Revisión del sistema de gestión de riesgos:** se ha de realizar una monitorización constante y periódica de los peligros detectados y de otros nuevos que puedan aparecer debido a los posibles cambios del entorno, de su frecuencia de ocurrencia y de su impacto sobre el sistema.

Cuantificación de la probabilidad y del daño

La probabilidad de que ocurra un riesgo, esté asociado al daño que sea, permanece como una cierta medida probabilística de sufrir un determinado daño frente a un peligro, bien en un margen de tiempo determinado o respecto a un número determinado de actuaciones. La conversión entre estas dos actuaciones, en cualquier caso, es bastante directa. El análisis de los daños asociados a un riesgo determinado puede ser muy subjetivo al mismo tiempo que complejo, ya que en muchos casos no será posible valorarlos numéricamente.

Puesto que el objetivo es el control de los riesgos, y no la determinación matemática, no tiene sentido invertir los numerosos recursos que serían necesarios para conseguir estos valores con precisión. Lo que tratamos de obtener es una lista de los riesgos y de las medidas que se deberían tomar para que éstos queden en unos valores asumibles. Evidentemente, un historial de datos estadísticos sobre el uso de los servicios nos pueden dar una referencia fundada sobre la que obtener datos más precisos, pero habitualmente a la hora de analizar un nuevo servicio, o de abrir un servicio a un sector de usuarios y usuarias nuevo, no se dispone de tanta precisión.

Cuantificación de la probabilidad:

- Probabilidad alta: el suceso peligroso se va a producir habitualmente.
- Probabilidad media: el suceso peligroso se va a producir de vez en cuando.
- Probabilidad baja: el suceso peligroso se producirá pocas veces.

- Probabilidad nula: es extremadamente improbable que se produzca el suceso peligroso.

Cuantificación del daño:

- Daño grave o suceso extremadamente dañino: si se produce el suceso, el daño ocasionado sería realmente muy importante.
- Daño serio o suceso dañino: el daño ocasionado sería considerable.
- Daño leve o suceso ligeramente dañino: el daño ocasionado no sería demasiado importante.
- Sin daño: no se produce ningún daño.

Si es necesario, se pueden crear más categorías para cualquiera de ellas, con lo que se aumentaría la granularidad a costa de incrementar la complejidad del proceso de estimación. En general, consideramos que con tres categorías para cada una es suficiente.

Riesgo en función de la vulnerabilidad y del daño

Por tanto, en función de la probabilidad de que ocurra el suceso dañino y las consecuencias que éste tenga, en el caso de ocurrir, podemos obtener directamente el riesgo asociado al mismo. Para ello, lo más sencillo es consultar la siguiente tabla:

Riesgo:	**Consecuencias (daño)**			
Probabilidad (peligro)		**Leve**	**Serio**	**Grave**
	Baja	Trivial	Tolerable	Moderado
	Media	Tolerable	Moderado	Importante
	Alta	Moderado	Importante	Intolerable

Valoración del riesgo

- **Trivial (T):** no se requiere acción específica.
- **Tolerable (TO):** no se necesita mejorar la acción preventiva. Se debe considerar, sin embargo, la posibilidad de introducir mejoras que no supongan una carga económica importante. Se requieren comprobaciones periódicas para asegurar que se mantiene la eficacia de las medidas de control.
- **Moderado (M):** se deben hacer esfuerzos para reducir el riesgo. Cuando está asociado con consecuencias importantes, será aconsejable una acción posterior para establecer, con más

precisión, la probabilidad de daño como base para determinar la necesidad de mejora de las medidas de control.

- **Importante (I):** no debe ponerse el servicio en funcionamiento hasta que se haya reducido el riesgo. Puede que se precisen recursos considerables para controlarlo. Si el riesgo corresponde a un servicio que ya esté en funcionamiento, debe priorizarse la resolución del problema respecto a los riesgos moderados.
- **Intolerable (IN):** se debe detener el funcionamiento del servicio hasta que se reduzca el riesgo. Si no es posible reducir el riesgo, incluso con recursos ilimitados, debe prohibirse el mismo.

Multidisciplinariedad del análisis de los riesgos

Una consideración global del riesgo debería incluir una gama completa de sus efectos, tanto los tangibles como los intangibles. A la hora de considerar los posibles daños ocasionados por un suceso hemos de tener en cuenta, por tanto, todas las posibles facetas de los mismos.

Para realizar un análisis lo más completo posible de los daños asociados a los riesgos que la mayoría de los servicios web participativos podría suponer para la organización, hemos tenido en cuenta cuatro aspectos principales de los mismos que consideramos más relevantes. En primer lugar, las actuaciones de los usuarios y usuarias de los servicios pueden dar lugar a responsabilidades legales, tanto penales como civiles. En segundo lugar, podría haber consecuencias económicas por diferentes motivos. En tercer lugar, podrían existir también hechos que tuvieran consecuencias mediáticas o de pérdida de prestigio para la institución y, por último, tenemos que afrontar el propio daño social que se podría causar sobre los servicios ofrecidos, como un uso inadecuado de los mismos que haga fracasar los objetivos que pretendemos alcanzar.

Aspectos legales

Nadie es ajeno, hoy en día, a las infinitas posibilidades que aporta Internet y al continuo flujo de información que supone. Internet es un mundo con pocas y muchas veces ineficaces barreras, con el consiguiente riesgo de menoscabo de todos los derechos implicados en el mundo en red. La ley, sin embargo, debe de aplicarse tanto en el mundo material como en el digital y deberá actuar, con más razón, ante aquellas actuaciones con mayor capacidad de difusión, por lo tanto, con mayor perjuicio para los implicados, como son las actividades que se llevan a cabo en Internet.

Hasta el momento actual, que podría denominarse primera época de Internet o Web 1.0, la mayor parte del flujo de información se realizaba en un solo sentido. Eran quienes creaban y proveían de servicios los que difundían la información. Con la denominada Web 2.0 se produce un auténtico intercambio de información entre todos los actores de la red. Permitir que los usuarios y usuarias interactúen con el portal o entre sí es hoy en día lo más común, y es prácticamente impensable

mantener un portal "cerrado", en el sentido de permitir una comunicación unidireccional, esto es, del portal hacia los usuarios y usuarias. El actual exige participar, aportar información y comunicarse con aquellos con quienes comparten aficiones, ideas o sentimientos. Es, por tanto, muy fácil que en estos flujos de comunicación se filtren datos no previstos en un principio, con lo que habrá que permanecer extremadamente atentos a todo aquello que se vaya desarrollando en la web.

Hay que cumplir la legislación vigente en todos sus aspectos, identificando de forma adecuada la organización que provee el servicio según indica la LSSI (Ley de Servicios de la Sociedad de la Información), cumpliendo con las obligaciones señaladas en la LOPD (Ley Orgánica de Protección de Datos) respecto a la gestión de datos personales de los usuarios y usuarias y los ficheros que los contienen, notificando los mismos ante el Registro General de la Agencia Española de Protección de Datos (AEPD) con anterioridad al uso de los mismos, informando siempre en la recogida de los datos, recabando el consentimiento explícito de la persona afectada, aclarando los usos y finalidades por los que se solicitan, y garantizando el cumplimiento de los deberes de secreto y seguridad establecidos por la ley.

El portal web deberá informar, en un sitio visible, fácilmente localizable y accesible a todas las personas que accedan al mismo, sean o no usuarias y usuarios registrados, de las condiciones legales que regulan su acceso a través de un documento habitualmente denominado Aviso Legal, en el que se detallan explícitamente los usos permitidos de la información contenida en el portal y las condiciones para la interacción con los servicios.

De igual forma, para cada servicio deberá informarse de las condiciones que regulan su uso, especificando los derechos y deberes de quienes acceden al mismo, así como las condiciones bajo las que se puede usar. A este documento, llamado habitualmente Condiciones de Uso, debe poder accederse antes de permitir a los usuarios y usuarias utilizar el servicio al que se refieren, y las condiciones señaladas han de ser explícitamente aceptadas antes de ser dados de alta.

Aspectos técnicos

La incorporación de tecnologías cada vez más avanzadas y complejas incrementa el riesgo de que éstas presenten problemas o que puedan ser usadas con propósitos equivocados. Derivados de las Tecnologías de la Información y la Comunicación han surgido nuevos desafíos a los que hay que enfrentarse para evitar que nuestro proyecto vaya a la deriva.

Abuso de los servicios a través de mecanismos automatizados

Una de las grandes lacras de la era Internet es el SPAM, o mensajes no solicitados (habitualmente de tipo publicitario) que, enviados en grandes cantidades, perjudican o molestan a quienes los reciben, puesto que no han dado su consentimiento. La ley intenta limitar en lo posible este fenómeno pero, en la práctica, no es capaz de contenerlo.

Además, existen ciertos programas o *scripts,* realizados por usuarias o usuarios maliciosos, que atacan servicios en Internet mediante el mecanismo de creación sistemática de cuentas en un servicio, o de intento de control de las ya existentes, con vistas a realizar SPAM, revender el servicio, realizar ataques de denegación de servicios (DoS), o simplemente fastidiar. Esto es muy habitual en el caso de *blogs* o foros en los que existe un *workflow* diferente para los comentarios anónimos que para los que no lo son, o en el caso de servicios que se pueden usar como plataforma para realizar SPAM en otros *sites*, como el caso de los servicios *webmail* o semejantes.

La mejor forma de limitar este tipo de ataques es mediante el uso de *captchas*. Éstos son utilizados para evitar que robots, también llamados *spambots,* puedan utilizar ciertos servicios. Consiste en obligar a quien quiera usar el servicio, a solucionar una prueba muy simple para un ser humano pero que suponga un gran desafío para un programa de ordenador. Hay que tener mucho cuidado a la hora de realizar dichas pruebas para evitar limitar de forma no deseada, el acceso al servicio de segmentos de la población que pudieran tener dificultades para solucionar dichos desafíos, como podrían ser las personas con necesidades especiales. De igual forma, han de ser lo suficientemente elaborados para evitar que un robot los pueda romper, inclusive mediante técnicas de OCR, fuerza bruta o bases de datos de respuestas prefabricadas.

Se produce el robo de datos personales cuando terceras personas obtienen ilegalmente la información personal de los usuarios y usuarias de nuestro sistema. El robo de listas de correo electrónico es un delito que puede llegar a ser muy lucrativo. Generalmente las listas generadas por cuenta propia, obtenidas por doble verificación o confirmación y con un patrón social definido, son las más apetecibles y, si el listado contiene además datos personales y refleja hábitos de compra de sus miembros, lo son aún más. Este tipo de delitos suele dejar escasas huellas, ser bastante anónimo y llevarse a cabo con bastante impunidad, ya que a menudo no es ni siquiera percibido.

Este riesgo puede materializarse por la acción de alguien con acceso a las bases de datos que pueda copiar las listas con impunidad, o por la intrusión de una persona ajena en el sistema que acceda a esas bases y pueda obtener una copia de la información almacenada en las mismas. A veces, también es posible recopilar los datos a través de un programa que los vaya recogiendo de las propias páginas publicadas, si es que los datos están abiertamente publicados en las mismas, aunque sea de forma dispersa.

La mejor forma de evitar los ataques por fuerza bruta es limitar el número de conexiones y el número de intentos consecutivos que se pueden insertar para realizar la operación, baneando o limitando temporalmente el acceso a la IP atacante, en el caso de que se detecte un intento de este tipo. El número de intentos límite deberá ser lo suficientemente grande para evitar que un ser humano pueda tener problemas por este motivo.

Sabotaje del sistema

Casi todos los navegadores tienen vulnerabilidades y éstas son habitualmente explotadas mediante el uso de programas malignos en Javascript, ActiveX u objetos embebidos que las pueden aprovechar para instalar un código maligno en la clientela. La mejor forma de prevenir este ataque es evitando que los usuarios y usuarias puedan utilizar las etiquetas HTML correspondientes a estos elementos enriquecidos, que en este contexto tampoco suelen aportar nada.

Muchos troyanos, virus, gusanos o *malware* en general se introducen en los ordenadores de los usuarios y usuarias a través de la ejecución directa de un programa proveniente de una fuente no fiable por parte de éstos, que o bien esté infectado o bien lleve intencionadamente una carga maligna.

Aunque un documento no ejecutable es pasivo y, por tanto, a priori no se le suponga la posibilidad de contener una carga maligna, a veces se usan documentos mal formados a propósito, de tal forma que con ello se puedan aprovechar para visualizarlas, vulnerabilidades de los programas que son habitualmente más usados. Esto ha ocurrido ya en el pasado con elementos multimedia como determinados formatos de imágenes, con elementos *flash* o *java* o con formatos documentales como PDF.

De la misma manera, algunos tipos de documentos pueden llevar también un programa ejecutable dentro de ellos en forma de macros, como los documentos de ofimática o las páginas web realizadas en HTML, o ser realmente un lenguaje de programación muy especializado que la ciudadanía, equivocadamente confunda con un documento pasivo (por ejemplo el lenguaje de impresión *postscript*). La única forma de prevenir este ataque es limitando, en la medida de lo posible, los documentos a aquellos que sean necesarios, comprobando, si se puede, que están bien formados y pasándolos a través de un programa de detección de *malware*, como un sistema antivirus.

Existen mecanismos como los marcos ocultos, la anulación del contenido de páginas o la generación de contenido gráfico o *popups* que engañan a los usuarios y usuarias del sistema que, mediante el uso de HTML, DHTML u otros códigos programables que pueden interpretar los navegadores de Internet de la clientela, permiten manipular la información visualizada en ellos y conseguir que los usuarios y usuarias se confíen y entreguen información confidencial a las personas atacantes sin quererlo, como contraseñas o números de tarjetas.

La mejor forma de prevenir este tipo de ataques es no permitir, a quienes aporten contenido, utilizar de ninguna forma lenguajes de *script* embebidos en la información web, ni marcos, ni DHTML, ni la generación de *popups*; y limitar el uso de imágenes y de los parámetros de los enlaces de tal forma que no sean peligrosos, salvo que sea estrictamente necesario no hacerlo.

Como medida de precaución, es conveniente no permitir tampoco la inserción de comandos *javascript* embebidos directamente en los enlaces (javascript:...), ni en respuestas a eventos dentro de

los comandos web (onClick, etcétera). Además, es recomendable, y así lo hacen muchos de los sistemas existentes, el uso de listas blancas de etiquetas permitidas y el filtrado de todas las demás, así como sus parámetros y los formatos de las URL indicadas en ellos.

Riesgos mediáticos

La publicación de contenido por parte de los usuarios y usuarias, tanto de forma directa (entrada en un *blog* o *wiki*, mensaje en una lista de distribución), como a través de otros sistemas de participación (ej.: comentarios), puede conllevar la propagación de informaciones no suficientemente contrastadas y/o rumores que otros usuarios o usuarias pueden leer y aceptar como válidos, al estar bajo el paraguas de un portal oficial, con lo que hay que tener especial cuidado en delimitar claramente quién aporta cada contenido.

Además, el hecho de que usuarios u usuarias pertenecientes al ámbito oficial publiquen contenido en *blogs* o *wikis,* también supone riesgos como que, en un ejercicio de transparencia o por error, se filtren o revelen de forma pública a la ciudadanía informaciones confidenciales o de riesgo.

Una de las características de la Web 2.0 es la apertura de parte del contenido y/o aplicaciones para que la web se extienda más allá de los límites de un portal, por ejemplo, mediante la creación de *mashups* por parte de personas usuarias en otros sistemas. Esto puede derivar en la utilización de dicha información para propósitos no acordes con el fin inicial.

Aspectos sociales de la web participativa

La web participativa, al estar centrada en la colaboración de los usuarios y usuarias, ha de prestar una atención especial a las dinámicas que se establecen en el uso del servicio, así como a las interacciones que surjan entre diferentes personas, con el objetivo de obtener el mejor resultado posible. Asimismo, se puede plantear la incorporación de la figura de un animador o animadora que fomente el uso adecuado y productivo de los recursos y la participación en el servicio.

Será necesario disponer de mecanismos adecuados de resolución de conflictos, que indudablemente los habrá, con el objetivo de evitar los posibles problemas que surgen ineludiblemente de toda interacción humana. En este sentido, habrá que impulsar el uso educado de los recursos que conduzca a un enriquecimiento de la comunidad y la obtención de la mejor relación señal/ruido posible. Se deben fomentar los comportamientos asertivos, poner los medios para minimizar o eliminar la participación negativa o destructiva, promover los mecanismos adecuados de motivación que conduzcan a la participación activa y señalar con claridad las temáticas tratadas en cada sección para evitar un rumbo a la deriva en la generación del conocimiento colectivo.

Es necesario prestar especial atención a que se den las condiciones que permitan participar a todas las personas en los servicios ofrecidos, independientemente de su condición física o psíquica. En este sentido se habrá de considerar seriamente la accesibilidad, no sólo en el desarrollo del siste-

ma, sino en su propio diseño. Todas las personas deben poder hacer uso del servicio, independientemente de las necesidades especiales que puedan tener, y no han de estar excluidas del mismo por su dificultad para comunicarse con él. La restricción de la participación de ciertos ciudadanos y ciudadanas a un servicio de la Administración Pública por el simple hecho de padecer un tipo de discapacidad o tener ciertas limitaciones físicas o mentales podría incluso derivar en un problema legal de discriminación.

Aunque la página web sea accesible, se pueden llegar a producir incumplimientos de accesibilidad en los sistemas de publicación personal, ya que los conocimientos de edición de contenidos de usuarios y usuarias son muy dispares. Hay que proveer los medios para intentar evitar que esta parte del contenido que generan no sea accesible.

La utilización de este tipo de herramientas puede llegar a producir la exclusión de determinados grupos de población que no están habituados a ellas. El hecho de utilizar sólo ciertas aplicaciones tipo Web 2.0 para determinados procesos o no hacer la labor pedagógica o didáctica para que sean usables, accesibles y compresibles puede alejar a muchas personas, lo que conduce a una participación sesgada o restringida a un sector de la población. Para evitar esto se deben estudiar las necesidades reales, pensar en el público final y adecuar la herramienta a sus conocimientos (y no al revés), tener presentes siempre las normas de usabilidad y accesibilidad a la hora de ponerlos en marcha, introducir siempre secciones de ayuda, FAQ e incluso tutoriales para usuarios y usuarias con conocimientos más básicos de Internet, etcétera.

En esta misma línea, se debe indicar que en los espacios de participación directa y en aquellos que gestionan la relevancia de los y las participantes mediante sistema tipo karma, se puede llegar a producir la creación de un grupo de élite dominante que, de forma indirecta, acabe por convertir el producto en algo exclusivo e impedir la escalada e implicación de otros usuarios en él. Este tipo de comportamiento no suele ser deseado.

La participación activa de usuarios y usuarias conlleva que viertan contenidos en listas de mensajes, foros, *wikis* o comentarios o perfiles propios. En muchas ocasiones, estas personas no son conscientes del nivel de exposición pública de ciertos contenidos privados (claves, información personal, etcétera) que pueden publicar o intercambiar. Este tipo de riesgo se agudiza y se convierte en uno social cuando determinados usuarios o usuarias publican o exponen datos de terceras personas.

Gestión de datos de carácter personal

El derecho fundamental a la protección de datos de carácter personal se deriva del artículo 18.4 de la Constitución Española, que dispone que la ley limitará el uso de la información para garantizar el honor y la intimidad personal y familiar de la ciudadanía y el pleno ejercicio de sus derechos. El citado precepto ha venido a desarrollarse a través de la Ley Orgánica 15/1999, de 13 de diciembre,

de Protección de Datos de Carácter Personal (LOPD). Esta ley recoge las obligaciones que las personas responsables de los ficheros y de los tratamientos deberán observar para garantizar el derecho a la protección de datos. Esta norma se ha desarrollado recientemente en virtud del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.

La Agencia Española de Protección de Datos (AGPD), en su reglamento de medidas de seguridad RD 994, hace referencia a tres niveles diferentes de seguridad, definidos en función del contenido de los ficheros en los que se almacenan los datos:

- Nivel Básico: se refiere a ficheros con datos de carácter personal, de consumo, etcétera.
- Nivel Medio: además de los tipos de datos incluidos en el nivel básico, incorpora otros de tipo administrativo, penal o financiero.
- Nivel Alto: incluye, además de datos de nivel básico o medio, otros datos referidos a la ideología, religión, creencias, origen racial, salud o vida sexual de las personas.

Antes de abordar el contenido de este apartado, centrado en las cuestiones que plantea el fenómeno Web 2.0 en relación con la protección de datos, es necesario aclarar una serie de conceptos respecto a la protección de datos:

- Datos de carácter personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. A continuación se dan algunos ejemplos de datos de carácter personal: nombre y apellidos, *e-mail*, número de teléfono, DNI, IP, huella digital, fotografía, etcétera.
- Fichero: todo conjunto organizado de datos de carácter personal que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. El fichero de titularidad pública tendrá como responsable a los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos.
- Responsable del fichero o del tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.
- Persona encargada del tratamiento: persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta de la persona responsable del tratamiento o del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Se entiende por tratamiento de datos cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supre-

sión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Por tanto, en primer lugar será necesario definir los ficheros en relación con el portal web y con posterioridad identificar a la persona responsable de los mismos así como a la encargada del tratamiento.

Aunque el artículo 6.1 de la LOPD establece, como norma general, la necesidad de contar con el consentimiento inequívoco de la persona afectada para proceder al tratamiento de sus datos; esta regla general admite una serie de excepciones. Entre éstas se encuentra la recogida de sus datos "para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias". Si entre las competencias atribuidas al organismo está, por ejemplo, la gestión de campañas o el envío de información a la ciudadanía, no requeriría solicitar este consentimiento.

Obligaciones de la persona responsable del fichero

A continuación se analizan las principales obligaciones que deberá cumplir la persona responsable del fichero y que se contienen tanto en la LOPD como en su Reglamento de Desarrollo.

- **Notificar los ficheros ante el Registro General de la Agencia Española de Protección de Datos (AEPD)** con anterioridad al uso de los ficheros, lo cual implica el compromiso por parte de la persona responsable de que el fichero cumple con todas las exigencias legales. Es importante resaltar que la creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse mediante disposición general publicada en el BOE o diario oficial correspondiente, en virtud del artículo 20.1 de la LOPD. Una vez inscrito el fichero, es necesario elaborar, conforme a las prescripciones legales, un documento de seguridad para el mismo.
- **Información en la recogida de datos:** de conformidad con lo establecido por el artículo 5 de la LOPD, las personas a las que se soliciten datos personales a través de Internet deberán ser previamente informadas de modo expreso, preciso e inequívoco:
    - de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios y destinatarias de la información;
    - del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas;
    - de las consecuencias de la obtención de los datos o de la negativa a suministrarlos;
    - de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición;
    - de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

En todas y cada una de las páginas web desde las que se recaben datos de carácter personal se incluirá claramente visible la información a la que hace referencia el artículo 5 de la LOPD, que el usuario o usuaria deberá poder obtener con facilidad y de forma directa y permanente. Podrá optarse por incorporar en todas esas páginas un texto o un botón adecuadamente etiquetado que, al ser seleccionado mediante un click, permita obtener la citada información. No obstante, se considera más adecuada una opción según la cual la lectura de dicha información se presente como ineludible (y no optativa) dentro del flujo de acciones que deba ejecutar el usuario o usuaria para expresar la aceptación definitiva de la transmisión de sus datos a la entidad que los está recabando.

En particular, se especificará claramente:

- El nombre o denominación social y el domicilio de la persona responsable del fichero al que se incorporarán los datos personales solicitados.
- El código de inscripción asignado por el Registro General de Protección de Datos.
- La dirección ante la cual pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición, en el caso de que sea distinta del domicilio especificado, así como el procedimiento que deberán seguir los usuarios y usuarias, ya sea electrónico, postal, telefónico o cualquier otro que se considere válido. En el caso de que los datos personales vayan a ser inicialmente incorporados a los ficheros de distintos responsables, se referirá toda la información anterior a cada uno de ellos.

- **Consentimiento de la persona afectada:** de acuerdo con lo que dispone el artículo 6.1 de la LOPD, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco de la persona afectada, salvo que la ley disponga otra cosa o sean de aplicación las excepciones previstas en el apartado 2 del mismo artículo. Cuando un usuario o usuaria facilita voluntariamente sus datos de carácter personal a través de Internet, se entenderá que consiente en el tratamiento de los mismos en los términos en los que ha sido convenientemente informado en el momento de la recogida. Asimismo, ha de tenerse en cuenta que siempre que la ley no lo impida y el afectado o afectada haya revocado su consentimiento para el tratamiento de sus datos de carácter personal, la persona responsable del fichero habilitará los medios oportunos para excluir del tratamiento dichos datos.
- **Usos y finalidades:** tal y como dispone el artículo 4.1 de la LOPD, los datos de carácter personal sólo se podrán recoger para su tratamiento cuando sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquella que ha justificado su recogida. Para recabar este consentimiento en Internet, se considerará válido un procedimiento en el que el usuario o usuaria tenga una participación activa, de tal forma que, a través de la web, pueda manifestar su voluntad en uno u otro sentido.

Si, aparte de los datos personales que se faciliten voluntariamente a través de Internet, se utilizan procedimientos automáticos invisibles de recogida de datos relativos a una persona identificada o identificable (cookies, datos de navegación, información proporcionada por los navegadores, entre otros), se informará claramente de esta circunstancia a dicha persona, antes de comenzar la recogida de datos. Así mismo, se deberá informar al afectado o afectada del nombre de dominio del servidor que transmite o activa los procedimientos automáticos de recogida, de la finalidad de los mismos, de su plazo de validez, de si es necesaria o no la aceptación de dichos procedimientos para visitar el sito web y de la opción de que dispone todo usuario y usuaria de oponerse a esta modalidad de tratamiento, además de las consecuencias de desactivar la ejecución de dichos procedimientos, cuando dicha opción esté disponible.

- **Cancelación de datos:** según prevé el artículo 4.5 de la LOPD, los datos de carácter personal serán cancelados a propia iniciativa de la persona responsable del fichero cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados. Igualmente serán cancelados cuando así lo solicite el interesado o interesada.

- **Acceso a los datos por cuenta de terceras personas:** de conformidad con lo dispuesto en el artículo 12.1 de la LOPD, la realización de tratamientos por cuenta de terceras personas deberá estar regulada en un contrato en el que conste por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que quien tenga que realizar el tratamiento únicamente utilizará los datos conforme a las instrucciones del o la responsable del mismo, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el citado contrato se estipularán, asimismo, las medidas de seguridad a las que se refiere el artículo 9 de la LOPD que la persona encargada del tratamiento está obligada a implementar. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos a quien sea responsable del tratamiento, al igual que cualquier soporte o documentos en los que conste algún dato de carácter personal objeto del tratamiento.

- **Comunicación de datos:** según dispone el artículo 11.1 de la LOPD, los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a una tercera persona para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento de la persona interesada. A este respecto se tendrán en cuenta, sin embargo, las excepciones previstas en el apartado 2 del citado artículo. Cuando los datos personales recabados a través de Internet vayan a ser comunicados a otras compañías (incluso cuando éstas pertenezcan al mismo grupo empresarial) deberá informarse al usuario o usuaria, de tal forma que pueda conocer explícitamente las finalidades determinadas a las que se destinarán los datos. La información podrá referirse genéricamente a un sector de actividad económica (por ejemplo, servicios financieros), sin que puedan admitirse

finalidades indeterminadas o no comprensibles para dicha persona (por ejemplo, actividad comercial, actividad publicitaria, empresas del grupo...). Los usuarios y usuarias serán convenientemente informados en los casos en los que sus datos vayan a ser comunicados. En tales casos, se especificará claramente qué datos serán comunicados, así como la identidad y dirección de los cesionarios.

- **Movimiento internacional de datos:** de conformidad con lo establecido por el artículo 33 de la LOPD, no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la LOPD, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del director de la Agencia de Protección de Datos. A este respecto, se tendrán en cuenta las excepciones previstas en el artículo 34 de la LOPD.
- **Garantizar el cumplimiento de los deberes de secreto y seguridad:** de acuerdo con lo establecido por el artículo 9 y 10 de la LOPD, la persona responsable del fichero y, en su caso, quien realiza algún tratamiento sobre la información deberán guardar secreto profesional sobre los datos y adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones determinadas en el Real Decreto de desarrollo de la LOPD. Cuando las usuarias y usuarios registrados en una web tengan acceso online a los datos de que dispone quien sea responsable del fichero respecto a su persona, deberán establecerse procedimientos de identificación, autenticación y control de accesos, de acuerdo con lo establecido en el citado Real Decreto.
- **Cumplir, cuando proceda, con lo dispuesto en la legislación sectorial que resultare de aplicación.**

Derechos de las personas titulares de los datos

Al mismo tiempo que las personas que tratan datos de carácter personal tienen obligaciones, los y las titulares de los datos ostentan una serie de derechos en relación con dicho tratamiento. Los de mayor calado se detallan a continuación:

- Cuando se recaben sus datos tendrán derecho, en virtud del artículo 5 de la LOPD, a recibir información sobre:

  La existencia del fichero o tratamiento de datos, la finalidad de la recogida y los destinatarios de la información.

- El carácter optativo u obligatorio de las preguntas.
- Las consecuencias sobre la obtención de los datos, así como la negativa a suministrarlos.
- La posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.
- La identidad y dirección de la persona responsable del tratamiento o su representante.

Durante el tratamiento de sus datos, los y las titulares podrán ejercer los derechos de acceso, rectificación, cancelación y oposición (ARCO). En este punto es de especial importancia observar las obligaciones de la persona responsable y encargada de la información que aparecen en el Reglamento de desarrollo de la LOPD:

- **Derecho de acceso**: el artículo 15 de la LOPD establece que la persona afectada pueda recabar información de sus datos de carácter personal sometidos a tratamiento, el origen de los mismos y las cesiones o comunicaciones realizadas o que se prevean realizar. El acceso podrá consistir en la mera consulta de los ficheros por medio de la visualización o en la indicación de los datos objeto de tratamiento por escrito.
- **Derechos de rectificación y cancelación:** en virtud del artículo 16 de la LOPD, la persona interesada pueda instar a la responsable del fichero, a cumplir la obligación de mantener la exactitud de los datos, rectificando o cancelando los datos de carácter personal cuando resulten incompletos o inexactos, o bien sean inadecuados o excesivos para la finalidad de la recogida o cuyo tratamiento no se ajuste a la ley.
- **Derecho de oposición:** el artículo 6.4 y 30.4 de la LOPD dispone que cuando no sea necesario prestar consentimiento para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, cualquier persona podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, quien sea responsable del fichero deberá excluir del tratamiento los datos relativos a dicha persona.

Riesgos en la web participativa

Riesgos en la web participativa

R01: Atentados contra la intimidad personal, el honor o la imagen de las personas

El derecho al honor es un derecho de enorme envergadura en nuestro ordenamiento jurídico que, como tal, debe protegerse con el máximo cuidado. La Constitución Española, en su artículo 18.1, consagra el derecho al honor, a la intimidad personal y familiar y a la propia imagen como derechos fundamentales. Este derecho ha sido desarrollado con posterioridad por la Ley 1/1982, de la Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen. El Código Penal, por su parte, consagra el Título X a los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y el Título XI, a los delitos contra el honor.

Este derecho puede ser vulnerado, fundamentalmente, a través de injurias y/o difamaciones. El elemento diferenciador entre lo que entra en la esfera de la libertad de expresión y lo que supone una ofensa al derecho al honor es la exactitud o veracidad de los hechos expresados. Así se expresa la multitudinaria jurisprudencia existente en materia de derecho al honor y a la intimidad de las personas. Gran parte de dicha jurisprudencia está determinada por conflictos entre personajes públicos y medios de comunicación, ya que en estos casos es más difícil definir la esfera personal, al entenderse que las personas famosas tienen un aspecto público que implica una menor protección de su derecho a la intimidad.

Asimismo, conviene recordar que el Tribunal Constitucional ha reconocido ya de manera expresa la titularidad del derecho al honor por parte de personas jurídicas, partiendo para ello de un concepto de honor en sentido objetivo, entendido como buena reputación, por lo que habrá que cuidar que los usuarios y usuarias del servicio web no denigren el buen nombre de una persona jurídica.

En Internet, como hemos dicho, la difusión de un insulto o una calumnia tiene una escala potencialmente mundial, por lo que será fácil demostrar el perjuicio moral que pueda sufrir cualquier persona por culpa de un insulto o injuria. La calumnia, que supone la inexactitud de lo expresado, es muy recurrente en el ámbito periodístico, en el que a diario los y las profesionales se ven obligados a describir determinados comportamientos y a exponerlos ante la opinión pública.

Según la jurisprudencia, la exactitud de lo expresado no siempre será el elemento esencial para calificar la conducta. En ocasiones, puede expresarse un hecho que resulte no ser veraz, que además pueda ser perjudicial para el honor de la persona a la que se refiere y, sin embargo, gozar de una cierta protección por haber sido objeto de una investigación suficiente y tener apariencia de veracidad, por la fiabilidad de las fuentes, por ejemplo. Otras veces, en cambio, un hecho veraz expresado por una tercera persona puede constituir un delito contra el honor, al estar la informa-

ción desvelada protegida por el derecho a la intimidad. Ciertas informaciones, en efecto, pertenecen a la esfera privada y no pueden ser divulgadas a pesar de la veracidad de las mismas.

Se trata, por lo tanto, de unos derechos muy sensibles al estar absolutamente relacionados con la personalidad de las personas y que, por otra parte, se encuentran a menudo en conflicto con otros derechos igualmente importantes en el ordenamiento jurídico, como puede ser el derecho a la libertad de expresión, libertad de prensa o el derecho a la información.

Respecto a los ataques a la intimidad de las personas, legalmente pueden tener una doble vertiente: penal y civil.

El Código Penal considera un delito el descubrimiento de secretos o la vulneración de la intimidad de otra persona cuando se realice sin su consentimiento y se haga apoderándose de correos electrónicos, de cualquier otro documento o cuando se utilicen artificios técnicos que intercepten una transmisión o que realicen una grabación inconsentida. Es poco probable que la persona responsable de una plataforma sea considerada responsable subsidiaria por las vulneraciones a la intimidad que pueda realizar un usuario o usuaria de su servicio, sobre todo cuando se han tomado las medidas de seguridad oportunas para mantener la información proporcionada por terceras personas en un ámbito privado, facilitando recursos que impidan el acceso desautorizado a dicha información.

Desde un punto de vista civil, se considera una intromisión ilegítima a la intimidad de una persona:

- La utilización de cualquier medio para el conocimiento de la vida íntima de las personas.
- Su grabación, registro o reproducción.
- La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre.
- La revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.
- La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.
- La captación, reproducción o publicación por cualquier mecanismo audiovisual de la imagen de una persona salvo que ésta tenga una proyección pública.
- La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios o comerciales.
- La imputación de hechos o la manifestación de juicios de valor que lesionen la dignidad de otra persona, su fama o su propia estima.

Los elementos multimedia, como fotografías o vídeos, pueden contener también elementos que, dependiendo de multitud de factores, pudieran ser considerados una infracción a los derechos fundamentales de la persona. En determinados casos, una fotografía o un vídeo puede mostrar la imagen de una persona que no ha otorgado su autorización para que su rostro o apariencia fuesen divulgados, o ni siquiera para que dicha grabación fuera realizada, y su publicación en Internet puede atentar contra su honor y su intimidad personal.

Es importante recordar que los derechos de una persona integran tanto la apariencia de la misma (su imagen) como su voz u otros elementos que, sin ser propiamente visuales, conforman la personalidad de un individuo. Por este motivo, es importante tener presente que cualquier explotación de la imagen o la voz de una persona deberá realizarse con el consentimiento de su titular.

Además, se podría vulnerar la intimidad de las personas publicando imágenes, vídeo o audio de una conversación mantenida en un entorno privado o que pudieran atentar contra el honor de terceras personas. Asimismo, en cualquier medio se podrían realizar manifestaciones que pudiesen resultar injuriosas o difamantes, o que pudieran atentar contra la imagen de un individuo al utilizar su voz para la explotación comercial de un producto o servicio, y hacerlo todo ello sin la autorización del titular.

Hay que destacar que, mientras que está permitida la difusión de imágenes de personas con cargo público o notorio durante un acto público o en lugar abierto al público (la ley 1/1982 lo permite), para publicar la imagen de una persona que no tenga dicha proyección pública se necesita la autorización de la misma, se haga dicha publicación con o sin ánimo de lucro.

La responsabilidad del portal, cuando la fotografía es colgada por un usuario o usuaria, es relativamente limitada siempre y cuando las fotografías se publiquen en un espacio reservado a la comunicación y no sea usada con posterioridad por el portal a modo de ilustración o promoción del mismo, si bien deberá demostrarse una vigilancia y control razonables.

R02: Revelación y divulgación de secretos o datos confidenciales

El descubrimiento es el acto mediante el cual una persona se apodera de unos datos secretos ajenos, mientras que la revelación es aquel que supone la difusión o cesión de esa información. El descubrimiento y revelación de secretos está previsto en el artículo 197 del Código Penal.

Es importante diferenciar entre aquellos secretos de naturaleza personal, como su afinidad religiosa, inclinación sexual, etcétera, y los que, en cambio, tienen una naturaleza puramente comercial. En este segundo caso, estaríamos ante dos figuras que también deben ser diferenciadas: por una parte, el descubrimiento y revelación de aquellos secretos que el código penal describe como "datos reservados de personas jurídicas" (art. 200) y, por otra, los que describe como "secretos de empresa" (art. 278).

Finalmente, son objeto de protección específica los secretos industriales, que junto con el llamado *know how,* forman parte del conjunto de derechos a los que la propiedad industrial concede una normativa particular y que pueden ser protegidos también por vía de la competencia desleal. En este caso, la protección se otorga según criterios objetivos marcados por la ley, mientras que aquellos secretos a los que nos referíamos con anterioridad lo eran porque así los consideraba la persona de la que procedían.

Los riesgos de que el portal y sus diferentes servicios puedan ser usados como plataforma a través de la cual los usuarios y usuarias revelen secretos en sus distintas aceptaciones legales son, cuanto menos, mínimos. Ahora bien, no puede descartarse por completo que ello ocurra en aquellos espacios en los que se permita que los usuarios y usuarias conversen entre sí, ya sea de forma simultánea (*chat*) o de forma consecutiva (foros, *blogs*, correos).

R03: Contenidos ilegales o apología ilegal de delitos

La apología de un delito o crimen consiste en el elogio, solidaridad pública o glorificación de un hecho criminal, o de su autor o autora a causa de este hecho. El artículo 18 del Código Penal define la apología como la exposición, ante una concurrencia de personas o por cualquier medio de difusión, de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor o autora.

La apología sólo será delictiva como forma de provocación y si, por su naturaleza y circunstancias, constituye una incitación directa a cometer un delito. El Código Penal castiga la apología de una serie de delitos determinados: homicidio y asesinato, lesiones, detenciones ilegales y secuestros, exhibicionismo y provocación sexual, robo, extorsión, estafa o apropiación indebida, receptación y otras conductas afines, cultivo y tráfico de drogas, rebelión militar, delitos contra la Corona, asociación ilícita, sedición, atentados, terrorismo y genocidio. Sólo puede ser castigada, como forma de provocación, la apología de aquellos delitos para los que el código lo prevé.

Asimismo, no es constitutiva de delito la apología realizada en privado o la simple expresión de alegría explícita hacia un delito o hacia quien lo ha cometido.

R04: Contenidos no deseados o apología de actividades no deseadas

Pese a que sólo puede ser castigada como forma de provocación la apología de aquellos delitos para los que el código lo prevé, no es deseable que ocurra en el caso de otras actividades ilegales y reprobables, como la apología de la pornografía infantil, de los trastornos alimenticios como anorexia o bulimia, etcétera. Aunque algunas de estas actuaciones puedan no tener consecuencias penales, sí que van a poder tenerlas negativas de diferente naturaleza, tanto para el propio servicio como para la organización, en cuanto al prestigio y la participación, entre otras.

R05: Cruces de ataques o insultos

Las discusiones en Internet tienden a alargarse eternamente, repitiéndose los mismos argumentos una y otra vez, a menudo con la radicalización de las posturas de las personas participantes, así como el intercambio de insultos y ataques personales entre las mismas. Todo este ciclo es contraproducente y lo único que sirve es para generar malestar en el resto de participantes que, poco a poco, van dejando de leer los argumentos y, si la situación se repite habitualmente, pueden abandonar el servicio.

R06: Amenazas

Las amenazas constituyen un delito, tal y como se establece en los artículos 169 a 171 del Código Penal. Existen distintos tipos de amenaza: las que se dirigen a una persona, a su familia o a una persona estrechamente relacionada con ella, amenazando con causar un mal que constituya un delito; las que van dirigidas a colectivos concretos, grupos de personas o habitantes de una población y en las que además concurra el hecho de que dicha amenaza pueda razonablemente ser cumplida; y aquellas cuyo cumplimiento no suponga un delito, dependiendo de qué fines se persigan o de qué condiciones se impongan, como la revelación de un secreto, de un delito cometido por la persona amenazada, o las amenazas que, siendo leves, vayan dirigidas a una especialmente vulnerable del entorno de la amenazada.

Los delitos de amenazas no son demasiado comunes en Internet, al menos en su esfera pública (es decir, en aquellos espacios accesibles por el público). Además, estas amenazas, cuando aparecen, suelen corresponder más a formas violentas de expresión que a auténticas amenazas potencialmente materializables. En cualquier caso, el peligro es lo suficientemente serio como para ser tomado muy en cuenta y es necesario llevar a cabo una vigilancia especial para evitar que se den estos comportamientos.

Al igual que ocurre con las injurias, insultos, difamaciones y demás atentados contra el honor de las personas, las amenazas tienen, en los espacios de interactuación de los usuarios y usuarias, su más probable escaparate y, al igual que ellos, también pueden afectar tanto a los usuarios y usuarias como al portal y a la gente que representa.

A continuación se detallan algunos riesgos que se derivan de estas amenazas:

- Que se haga responsable a quien presta el servicio de las amenazas que se viertan en su portal web.
- Que el portal acabe usándose como "campo de batalla" en el que los usuarios y usuarias se profieran amenazas, o que una amenaza, en un momento determinado, pueda dañar la imagen del portal, reduciendo su uso y el número de usuarios y usuarias.

- También existe el riesgo, aunque a nuestro entender sea muy reducido, de que las amenazas se hagan en nombre de alguna banda terrorista o cuyo trasfondo sea político, y que pueda entenderse que deban ser tenidas en cuenta por suponer un riesgo posible.

R07: Acoso psicológico continuado

El acoso es una situación a través de la que una persona o un grupo de personas ejercen una violencia psicológica continuada y de forma sistemática sobre otra persona, con el objetivo de destruir su autoestima, su reputación o sus redes de comunicación mediante un trato vejatorio y descalificador. La víctima, por tanto, es objeto de acoso y ataques sistemáticos de forma continuada, de modo directo o indirecto, por parte de una o más personas.

Se suele usar el término ciberacoso para referirse al uso de los mecanismos provistos por las Tecnologías de la Información y la Comunicación, en todas sus diferentes variantes, para acosar a una persona o a un grupo. Este tipo de actuaciones pueden constituir un delito informático, además de ser absolutamente reprobable.

El ciberacoso es voluntario, busca infringir un daño de forma recurrente y repetitiva y no tiene un propósito legítimo de realizar ninguna actividad de comunicación. Éste puede producirse de muchas formas, desde actitudes pasivo-agresivas a la agresividad explícita más violenta. A menudo, puede incluir amenazas, connotaciones sexuales, etiquetas peyorativas o descalificativas de la persona, discurso del odio, etcétera.

Este tipo de acoso se puede producir basándose en diferentes estrategias: la descalificación y desacreditación constante de la víctima, el rechazo de la comunicación directa con ella, su aislamiento social, burlarse de sus puntos débiles, de sus ideas, convicciones o gustos, ridiculizarla en público, hacer alusiones desagradables o poner en tela de juicio su capacidad de juicio y decisión, entre otras.

La persona que realiza el acoso actúa habitualmente con una forma de violencia indirecta, criticando, faltando al respeto, extendiendo rumores, etcétera, con la única pretensión de anular a la otra persona. En la víctima, a la propia confusión por la situación, se suma un sentimiento de culpa que, en el caso de personas con tendencia a culpabilizarse, puede llegar a extremos perjudiciales. Las personas del entorno, que ignoran la situación o colaboran con ella, más o menos intencionadamente, no hacen más que agravar la situación de abuso.

R08: Acoso sexual

La Unión Europea define el acoso relacionado con el sexo de una persona como "la situación en la que se produce un comportamiento no deseado relacionado con el sexo de una persona con el propósito o efecto de atentar contra su dignidad y de crear un entorno intimidatorio, hostil, degradante, humillante u ofensivo", por parte de una persona que sabe o debe saber que es una conducta ofensiva y no deseada por la víctima.

Aunque en un espacio digital no se puede realizar un acoso sexual de carácter físico, sí que pueden aparecer este tipo de situaciones respecto a conductas verbales o no verbales de naturaleza sexual, bien a través de insinuaciones sexuales molestas, proposiciones, flirteos ofensivos, comentarios o insinuaciones obscenas, o mediante la exhibición de fotos sexualmente sugestivas o pornográficas, materiales escritos, etcétera.

R11: Uso de la plataforma para la promoción empresarial o personal

A menudo, nos podemos encontrar con que algunos servicios diseñados para que un tipo de usuarios o usuarias participen, son utilizados por otras personas para su promoción empresarial o personal. Este tipo de actitudes pueden variar entre quien aprovecha cualquier tema de conversación para anunciar, de una forma lo más casual posible, que tiene una empresa de asesoría a la que puedes acudir, hasta quienes se ocultan tras apodos anónimos para anunciar lo increíblemente bueno que es el hotel que regentan.

En la medida de lo posible se han de poner los medios para disuadir o evitar este tipo de comportamientos, ya que pueden devaluar el servicio que se quiere dar y la información que se pretende recopilar, y transformarse en una página no deseada de anuncios por palabras.

R12: Publicidad negativa o participaciones destructivas o negativas

La publicidad negativa consiste esencialmente en destacar una serie de elementos, ciertos o no, que desacreditan o afectan negativamente a los rivales. Con el auge de las redes sociales y de los mecanismos publicitarios de carácter viral, han llegado también las hordas de intervenciones interesadas que, camufladas bajo opiniones independientes o no, buscan esencialmente desacreditar a otras personas o entidades, con el objetivo de reforzar su posición. Este tipo de comportamiento, difícil de separar a menudo de las intervenciones críticas legítimas, pueden ocasionar que un servicio no funcione adecuadamente o no se obtengan de él los resultados deseados, sino que se transforme en campo de batalla encubierto de diferentes intereses comerciales, políticos o de cualquier otra índole.

Por otra parte, y aún sin llegar al extremo de que haya intereses inconfesables detrás de los comentarios, las participaciones de carácter negativo, críticas destructivas y, en general, todo aquello que conduzca a resaltar lo negativo, redunda generalmente en un peor resultado que lo que se fundamenta en destacar los aspectos positivos, con lo que se deberá intentar, dentro de lo posible, fomentar las participaciones de este último tipo. En algunos casos, la propia existencia de críticas negativas puede hacer fracasar el servicio entero, sobre todo cuando, de forma directa o indirecta, hay intereses económicos, comerciales o políticos en juego, con lo que se debe analizar y controlar cuidadosamente este factor, con la delicadeza necesaria para no caer en una censura que evite la aparición de puntos de vista alternativos.

R13: Asuntos irrelevantes o ajenos a la temática de la lista *(off-topic)*

El término *off-topic* se refiere a todas aquellas contribuciones que, de alguna manera, no guardan relación con la discusión que dio origen al tema. Salvo que se trate de espacios especialmente habilitados para ello, en los que simplemente se promueve el hablar por hablar, es conveniente que los comentarios sobre temas ajenos al propio hilo de conversación estén acotados, ya que si se producen en una cantidad relevante pueden conseguir apagar la conversación sobre el tema que realmente se está pretendiendo tratar, disminuye mucho la relación señal/ruido de la información y, a menudo, consigue hacer enfadar a las personas que sí quieren tratar de la temática propuesta en ese apartado del servicio que corresponda.

Otra cosa que ocurre a veces en los servicios colaborativos es que alguna persona realiza una exposición excesiva de elementos que corresponden a su privacidad, en una maniobra de exhibicionismo que es contraproducente tanto para el servicio en sí como para la persona que lo realiza. La publicación de datos excesivamente personales en un servicio público de gran alcance social como es un portal web, aunque sea realizada por esa misma persona y, por tanto, sea legal, puede tener consecuencias personales muy negativas para la persona que las realiza, ya que pueden repercutir a su vez sobre el propio servicio o sobre la organización.

R14: Baja calidad de las aportaciones

Para que un servicio sea bien valorado por los usuarios y usuarias y, por tanto, les apetezca seguir entrando y participando, hay que conseguir que la información que éste les aporte sea, al menos, suficiente para compensar el esfuerzo que están haciendo individualmente para aportar su granito de arena. Si la calidad media de los comentarios es muy baja y hace falta rebuscar y leer mucho antes de encontrar información interesante, la mayor parte de la gente se aburrirá y abandonará el servicio, provocando con ello un mayor decremento de la relación señal/ruido del servicio que lo puede llegar a hacer inservible y contraproducente.

Dentro de esta categoría se incluyen también aquellos debates interminables entre las partes que participan en una discusión, que repiten constantemente una y otra vez los mismos argumentos sin aportar nada nuevo, intentando vencer por agotamiento y que aburren al resto de lectores y lectoras de una forma irremediable.

R15: Propagación de rumores e información falsa

Internet es un medio en el cual la información se difunde muy rápidamente, tanto la verdadera como la falsa. A priori, es muy difícil diferenciar entre ambas y la única forma más o menos fiable de hacerlo es indicando fuentes que corroboren la información que damos, en forma de enlaces. Cuanto más fiables sean las fuentes de las que bebemos, más lo será la información para los lectores y lectoras. A veces, es fácil intuir qué noticias pueden ser falsas por la alerta que intentan sembrar, por lo escandalosas que son o por su ausencia de eco en la web. Es importante no limitar el impacto de la difusión de estas noticias ya que haciéndolo, estaremos reforzándolas con el valor de credibilidad del servicio que estamos ofreciendo.

R16: Pérdida de confianza en el servicio

La confianza de los usuarios y usuarias en un servicio tiene una inercia que depende de su trayectoria. La credibilidad y prestigio del mismo es un valor importante que, a su vez, hará que vengan un tipo diferente de nuevas personas al mismo, así como el tipo de aportaciones que hagan. Gran parte de este prestigio vendrá dado por las expectativas que quienes participan tengan del mismo.

R17: Pérdida de credibilidad de la institución

Un servicio colaborativo en un portal web de una institución está respaldado de alguna forma por el nombre de la institución que le da cobertura. La actuación de dicha institución respecto a la gestión del servicio, así como de las cosas que se permiten y las que no, transmitirá a su vez una imagen sobre dicho organismo. La forma de comportarse de la institución respecto al uso abusivo que se pueda hacer del servicio por parte de personas externas que lo usen debe ser, por tanto, consistente con la imagen que se quiere transmitir y con la credibilidad que se pretende conseguir. Dejar impunes y consentir cierto tipo de actuaciones podrá dar una imagen de pasividad o de tolerancia con cosas con las que no se debería tener y, por otro lado, una mano excesivamente dura con críticas constructivas transmitiría una imagen de organismo censurador e intolerante que tampoco es deseada.

R18: Participación forzada de terceras personas

Se puede dar el caso de que unas personas usen el servicio para realizar una acción que afecte a otras de una forma no deseada. Esta situación se da, por ejemplo, en servicios como enviar artículos por correo a otras personas.

En este sentido, es importante tomar en consideración una resolución dictada por la Agencia Española de Protección de Datos (AEPD) en la que se impone una sanción pecuniaria a quien es titular de un portal web por remitir a una persona un correo electrónico no solicitado, sin haber obtenido previamente su consentimiento. Lo novedoso del supuesto es que no fue el portal el que remitió la comunicación, sino la persona haciendo uso de la aplicación "enviar a alguien" o *share this*.

R21: Vulneración del derecho a la protección de datos de carácter personal

El derecho fundamental a la protección de datos de carácter personal se deriva del artículo 18.4 de la Constitución Española, que dispone que la ley limitará el uso de la información para garantizar el honor y la intimidad personal y familiar de la ciudadanía y el pleno ejercicio de sus derechos. La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) desarrolla el derecho a la protección de datos de carácter personal derivado del artículo 18.4 de la Constitución Española, recogiendo las obligaciones que las personas responsables de los ficheros y las encargadas de los tratamientos deberán observar para garantizar el derecho a la protección de datos. Esta norma se ha desarrollado recientemente en virtud del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Se entiende por dato personal cualquier información de cualquier tipo concerniente a personas físicas identificadas o identificables. Algunos ejemplos de datos de carácter personal son nombre y apellidos, *e-mail*, número de teléfono, DNI, IP, huella digital, fotografía, etcétera. Cualquier fichero o conjunto organizado de datos de carácter personal que permita el acceso a dichos datos está regulado por este reglamento, por lo que debe tener unas personas responsables tanto de su finalidad, contenido y uso, como de su tratamiento y ha de ser notificado ante el Registro General de la Agencia Española de Protección de Datos (AEPD) con anterioridad a su uso.

Desde el punto de vista de la Agencia Española de Protección de Datos (AEPD), la voz de una persona puede considerarse por sí sola como un dato de carácter personal. Por ello, su registro y tratamiento requieren la autorización del afectado. Además, habrá tratamiento de datos cuando se realicen operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

De esta manera, hay que tener en cuenta que la AEPD puede requerir la regularización de ficheros en los que se incluyan *podcasts*, al considerar este tratamiento dentro de las exigencias de la LOPD.

Respecto a sus datos personales, las personas tienen una serie de derechos:

- Han de ser previamente informadas de modo expreso, preciso e inequívoco respecto a la gestión que se realizará de sus datos personales de acuerdo con el artículo 5 de la LOPD.
- Es necesario su consentimiento.
- Los datos sólo se podrán obtener cuando sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados.
- El acceso a los datos por parte de terceras personas ha de estar regulado y no podrán ser comunicados a otras indiscriminadamente.
- Se ha de garantizar el cumplimiento de los deberes de secreto y seguridad y los derechos de acceso, rectificación, cancelación y oposición (ARCO).

Desde el punto de vista de la AEPD, la imagen se considera un dato de carácter personal por lo que, puesto que el artículo 6 de la LOPD dispone que el tratamiento de los datos de carácter personal "requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra", para que su tratamiento resulte conforme con el principio de consentimiento, deberá concurrir alguno de los supuestos previstos en el citado artículo.

Hay que tener, asimismo, cuidado con los datos que inesperadamente puedan introducir usuarias y usuarios sobre sí mismos y del carácter que puedan tener, ya que podrían contaminar nuestros ficheros y hacer que tengan un nivel de protección diferente del que deberían tener. Por ejemplo, si una persona nos dice en su perfil que tiene algún problema médico, el archivo será de diferente sensibilidad, de acuerdo con la LOPD, que si no incluye este tipo de datos.

El artículo 45 de la LOPD sanciona los incumplimientos de la normativa, cuya cuantía se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que la AEPD considere relevante.

La cuantía variará, asimismo, dependiendo del tipo de infracción cometida:

- Las infracciones leves (artículo 44.2 LOPD) serán sancionadas con multa de 601,01 a 60.101,21 euros.
- Las infracciones graves (artículo 44.3 LOPD) serán sancionadas con multa de 60.101,21 a 300.506,05 euros.
- Las infracciones muy graves (artículo 44.4 LOPD) serán sancionadas con multa de 300.506,05 a 601.012,10 euros.

R22: Vulneración de derechos de propiedad intelectual de terceras personas

La Ley de Propiedad Intelectual (LPI) protege las obras literarias, artísticas o científicas siempre y cuando sean originales y creativas, no siendo necesario inscribir dichas obras en ningún registro para que el ordenamiento jurídico otorgue protección al autor o autora. Por este motivo, estarán protegidos por la LPI, entre otras, las novelas, ensayos, esculturas, obras pictóricas, guiones, fotografías, obras audiovisuales y, en general, cualquiera que cumpla unos estándares mínimos de creatividad y originalidad. Es lo que se denomina derechos de autoría.

Además de estos derechos, se encuentran los derechos conexos, por los que la LPI otorga protección a las personas titulares de grabaciones audiovisuales, a productores de fonogramas, a artistas intérpretes o ejecutantes, a bases de datos y a meras fotografías sin matices de creatividad y originalidad.

La LPI otorga quienes sean titulares de los derechos de estas obras la capacidad exclusiva de explotarlas, así como de otorgar licencias a cualquier tercera persona; por este motivo, y a priori, cualquier explotación de una obra protegida deberá requerir la correspondiente autorización del o la titular de sus derechos. Sin embargo, la LPI establece ciertos límites a estos derechos exclusivos por lo que se permitirá, a determinadas personas y en determinadas circunstancias, explotar obras protegidas. Los principales límites son la copia privada, las citas y reseñas, trabajos sobre temas de la actualidad, obras situadas de forma permanente en la vía pública o la parodia:

- Trabajos sobre temas de actualidad: posibilidad de reproducir trabajos y artículos sobre temas de actualidad, siempre y cuando el o la titular de derechos originario no hubiese hecho una reserva de derechos de manera expresa. En cualquier caso, se deberá citar al autor o autora original, a quien se le deberá remunerar según acuerden las partes.
- Informaciones de actualidad y obras situadas en vías públicas: cualquier obra que puede ser vista u oída con ocasión de un acontecimiento (celebración de un acto, mitin, concierto, etcétera), o que estuviese de forma permanente en la vía pública, podrá ser reproducida, distribuida o comunicada públicamente.
- Parodia: está permitida la parodia de una obra siempre y cuando tenga por objeto parodiar a la propia obra y no a un hecho o persona ajena a ella (por ejemplo, utilizar un cuadro para ridiculizar a un político), y que no implique riesgo de confusión con la misma ni se provoque un daño a la obra original o a su autor o autora. Un ejemplo de parodia son las obras audiovisuales como *Scary movie*, que ridiculizan o parodian a otras obras audiovisuales.

Uno de los principales límites a los derechos de autoría es el establecido en el artículo 32.1 de la LPI, que considera lícita la reproducción de fragmentos de otra obra cuando ésta se haya divulgado ya y su inclusión se haga para citar o para hacer un análisis o juicio crítico, o cuando esta utilización tenga fines docentes o de investigación y se indique la autoría y la fuente de origen de la cita.

No obstante, aunque socialmente se suele afirmar que es lícito citar una obra siempre y cuando se nombre el autor o autora y la fuente de procedencia, la ley y los tribunales exigen que esta cita se realice con fines docentes y de investigación, lo que deja fuera todo aquello que no cumpla estos requisitos, como puede ser citar un fragmento de la obra de un autor o autora en un *blog* o en un *podcast* que no tenga fines docentes o de investigación.

Consecuentemente, y para el caso de un sitio basado en servicios de la Web 2.0, si éste no tiene fines docentes o de investigación no podrá citar obras de terceras personas sin su autorización expresa.

Las fotografías son contempladas en la Ley de Propiedad Intelectual como obras merecedoras de la protección por dos vías: como obras creativas y originales y, si adolecen de estas características, simplemente como fotografías. La diferencia entre uno y otro tipo radica básicamente en la duración de la protección (25 años para la mera fotografía y los 70 para la obra fotográfica original y creativa, tras la muerte del autor o autora) y en la existencia o no del derecho moral, ya que el resto de derechos (impedir la publicación de una fotografía, distribuirla, etcétera) son análogos para uno u otro caso.

En cualquier caso, la publicación de una fotografía sin la autorización pertinente de su autor, autora o titular de derechos constituye una infracción al derecho de la propiedad intelectual por suponer una comunicación pública no consentida. La propiedad intelectual requiere que se respete la autoría de las obras, por lo que, además de contar con la debida autorización, quien cuelgue una fotografía ajena deberá asimismo citar a su autor o autora.

Dentro de las posibles infracciones que se pueden cometer a través de un servicio de *podcasting*, la propiedad intelectual es quizá la más importante. Hay que recordar que cualquier explotación de una obra o prestación de una propiedad de una tercera persona requiere la expresa autorización de ésta. Por lo tanto, para poder incluir obras musicales en un *podcast* se deberá contar con el consentimiento de los y las titulares de los derechos sobre tales fonogramas, lo cual se puede conseguir a través de las entidades de gestión de derechos operantes en España o por medio de las conocidas licencias libres o *copyleft*, que permiten la utilización de las obras que las contienen bajo determinados requisitos.

Dentro de una obra musical puede haber múltiples titulares de derechos de propiedad intelectual: el autor o autora de la obra musical, cuyos derechos gestiona la Sociedad General de Autores y Editores (SGAE); el o la artista intérprete o ejecutante de la obra, es decir, cantantes y músicos, cuyos derechos gestiona Artistas Intérpretes y Ejecutantes, Sociedad de Gestión (AIE); y quien produce el fonograma, generalmente una casa discográfica, cuyos derechos gestiona la Asociación de Gestión de Derechos Intelectuales (AGEDI).

De esta forma, si un o una *podcaster* desea poner obras musicales gestionadas por estas entidades en un *podcast* deberá recabar su previo consentimiento para la modalidad de explotación

específica de *podcasts*. En la fecha en la que se redacta el presente documento, ninguna de las entidades de gestión operativas en España tiene licencias específicas para *podcasts*, por lo que habría que negociar en su caso con cada una de ellas para que autorizasen tal explotación.

En este sentido, durante los últimos años han proliferado las denominadas licencias libres (por ejemplo, Creative Commons o Colorluris) que, incorporadas a determinadas obras musicales, permiten su utilización en *podcasts*. Así, existen multitud de sitios web donde los usuarios y usuarias pueden subir sus canciones para que otras personas las utilicen, entre ellos en *podcast*; ejemplos de estos sitios son Jamendo, Magnatune y Podsafe Music Network.

Lo mismo es aplicable para la utilización de cualquier obra protegida en un *podcast*, ya sea la lectura de un fragmento de una obra literaria, o la publicación de segmentos de una película, para lo que en todo caso se deberá contar con la autorización del o la titular de derechos (siempre y cuando la obra no haya caído en el dominio público).

R23: Suplantación de la personalidad

La suplantación de identidad es aquella por la que un usuario o usuaria se comunica con varias personas en un espacio público o con una sola en una conversación privada, usando la identidad de otra persona, se ésta real o inventada a tal efecto.

El Código Penal prevé lo que llama Usurpación del Estado Civil en su artículo 401. Esta usurpación de identidad es distinta a la suplantación en sentido amplio, ya que en el tipo previsto por el Código Penal se exige, además, que la sustitución de la persona se lleve a cabo para uso "de sus derechos y acciones", por lo que "no es bastante para la existencia de tal delito arrogarse una personalidad ajena asumiendo el nombre de otro".

La suplantación de identidad, en sentido amplio, es una figura muy habitual en Internet y en especial en las florecientes redes sociales. Puede darse de distintas maneras:

- Usando datos personales ajenos a la hora de registrarse en el portal web.
- Usando un *nickname* o alias, que de nuevo puede ser inventado o no referirse a nadie en particular, o usando un nombre que se identifique claramente con una persona conocida (por ejemplo, quien usara Rafael Nadal como *nickname*).
- Publicando como avatares propios fotos de otra persona.

La suplantación de identidad alcanzará más entidad cuanta más información se le solicite al usuario o usuaria como condición previa al registro. Por otra parte, será más fácil detectar este tipo de infracciones cuantos más datos se tengan de quien se registró. Para un registro de identificación media, rara vez se pedirá al usuario o usuaria que facilite datos personales que vayan más allá de nombre y apellido, sexo, edad y correo electrónico, y siempre y cuando el portal no se dedique

directamente a la venta electrónica, en cuyo caso se pedirían además, datos de contacto y bancarios. Por lo tanto, el grado de identificación que se le pide a una persona para registrarse, y consiguientemente el alcance de una eventual suplantación de la identidad, dependerá de los servicios que se quieran ofrecer a través de la web.

Todos los servicios de la Web 2.0 permiten, de forma sencilla, una suplantación de identidad. En líneas generales, para hacer uso de estos servicios no se exige el establecimiento fiable de una identidad de la persona emisora y receptora, ni se utilizan mecanismos que garanticen la confidencialidad de las comunicaciones. Por ello, el riesgo de suplantación de identidad y/o violación del secreto de las comunicaciones es elevado.

Las consecuencias que dicha suplantación pueda conllevar son, sin embargo, relativamente reducidas. Por una parte, la detección de estos comportamientos puede resultar muy complicada quienes administren el portal, puesto que no disponen de herramientas que permitan cotejar los datos aportados por una persona al registrarse y, por otra, el uso de la identidad falsa que pueda hacer el usuario o usuaria se antoja, asimismo, escaso de consecuencias legales.

Sin embargo, puede ocurrir que el dueño de la identidad suplantada denuncie el hecho mediante notificación a los administradores, lo que supondría un deber de investigación por parte del portal. Si el resultado de tales averiguaciones arrojase que efectivamente el comportamiento denunciado es real, deberán tomarse las medidas oportunas, según el grado de gravedad, contra el infractor.

Si bien estos comportamientos son probables e incluso habituales, es difícil que los mismos alcancen un nivel de importancia tal que deba suponer una vigilancia y control más allá del meramente razonable. Por este motivo, quien presta el servicio deberá poner los medios necesarios para identificar y bloquear cualquier suplantación de la personalidad, estableciendo una política interna en la que se le requiera, al usuario o usuaria que realiza la infracción, a que se identifique y, si se comprueba que no tiene un interés legítimo sobre el *nickname* utilizado, se proceda a la cancelación de la cuenta.

En cambio, los casos de usurpación del estado civil en su aceptación penal son menos probables, a nuestro entender, puesto que en principio el portal no ofrece servicios cuya identificación otorgue derechos que puedan ser objeto de usurpación, pese a lo cual el riesgo siempre existe y exige un mínimo de vigilancia.

R24: Vulneración del derecho de protección de los y las menores

El artículo 13.1 del Reglamento de Desarrollo de la LOPD dice que, como regla general, podrá procederse al tratamiento de los datos de las personas mayores de 14 años con su consentimiento, salvo en aquellos casos en los que la ley exija para su prestación la asistencia de los y las titulares de la patria potestad o tutela. En el caso de los y las menores de 14 años se requerirá el con-

sentimiento de padres, madres o quienes ejerzan su tutela. Esto quiere decir que sólo los y las mayores de 14 años podrán facilitar sus datos de carácter personal. Si se estableciese un servicio dirigido a menores de esta edad, se deberá articular un canal por el cual sus progenitores deberán prestar el consentimiento, debiéndose acreditar adecuadamente como tales.

Asimismo, los y las menores de edad no tienen personalidad jurídica suficiente para realizar transacciones comerciales, con lo que se habrá de prestar una especial atención a que no se presten servicios a este colectivo que pudieran implicar la realización de actos que el ordenamiento jurídico no permite.

La Ley 1/1982, de la Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen establece en su artículo 3 que las personas menores de edad deberán prestar su consentimiento cuando se realice una explotación de su imagen, siempre y cuando sus condiciones de madurez así lo permitan. En caso contrario, el consentimiento deberá otorgarlo su representante legal, quien deberá notificar dicha explotación con carácter previo al Ministerio Fiscal, quien tendrá ocho días para manifestarse. Publicar una fotografía o vídeo con la cara de un o una menor en Internet supone, para esta ley, una explotación de su imagen, lo cual deberá llevar aparejado la consiguiente autorización de sus representantes legales y la notificación al Ministerio Fiscal (adviértase que simplemente hay que notificar, no solicitar autorización a dicho órgano).

R25: Estafa

La estafa es un delito contra la propiedad o el patrimonio basado en el engaño. El artículo 248 del Código Penal considera que cometen estafa las personas que:

- Con ánimo de lucro, utilizan el engaño para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
- Con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de terceras personas.
- Fabriquen, introduzcan, posean o faciliten programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo.

Al igual que ocurre con algunas de las conductas analizadas, las estafas tienen en los espacios de interactuación de las personas, su más probable escaparate y pueden afectar tanto a los usuarios y usuarias como al portal y a la gente que representa. El riesgo para quien presta el servicio pudiera ser que se le haga responsable de las estafas que se lleven a cabo en su portal web, aunque ello es poco probable. En el caso de que éste tuviese conocimiento de que a través del portal web se están produciendo estafas, deberá denunciar de forma inmediata ante la autoridad competente. Puede darse el caso de estafas a través de *blogs*, en los comentarios o incluso a través del chat, en cuyo caso se deberá actuar tal y como se expone en el presente capítulo.

R26: Engaño o *phishing*

El término *phishing* se usa para referirse a un tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta. Para ello, se suele hacer pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Consiste en usar la mentira o conseguir fraudulentamente la confianza de otra persona con el objetivo de que ésta nos dé sus datos personales, algo que no haría voluntariamente de no mediar el engaño. Dependiendo de la naturaleza de los datos y de la finalidad con la que éstos son obtenidos, pueden ser usados maliciosamente por quien ha realizado dicho fraude para obtener algún tipo de beneficio o causar algún tipo de perjuicio. Esto puede indirectamente causar daño también a la institución, dependiendo de las circunstancias.

A nivel técnico, existen mecanismos como los marcos ocultos, la anulación del contenido de páginas o la generación de contenido gráfico o *popups,* que engañan a los usuarios y usuarias del sistema que, mediante el uso de HTML, DHTML u otros códigos programables que pueden interpretar los navegadores de Internet de la clientela, permiten manipular la información visualizada en ellos y conseguir que los usuarios y usuarias se confíen y entreguen sin querer información confidencial a las personas atacantes, como contraseñas o números de tarjetas.

Para prevenir este tipo de ataques no se permitirá, a quienes aporten contenido, utilizar lenguajes de *script* embebidos en la información web, ni marcos, ni DHTML, ni la generación de *popups*, y se limitará el uso de imágenes y de parámetros de los enlaces de tal forma que no sean peligrosos.

Como medida de precaución, no se permitirá tampoco la inserción de comandos *javascript* embebidos directamente en los enlaces (*javascript:...*), ni en respuestas a eventos dentro de los comandos web (ej. onClick). Por otro lado, se usarán listas blancas de etiquetas permitidas, se filtrarán todas las demás y se hará de igual forma con los parámetros de las etiquetas permitidas y con los formatos de las URL indicadas en ellos.

R31: SPAM o mensajes masivos no solicitados

El artículo 21.1 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico que regula la materia de las comunicaciones comerciales (LSSI) dispone que *queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. El anexo de la ley define comunicación comercial como toda forma de comunicación dirigida a la promoción, directa o*

indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

Esta regla sólo se verá exceptuada en el supuesto contemplado en el artículo 21.2, por el que *lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente. El precepto concluye indicando que, en todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.*

El SPAM puede definirse, por tanto, como aquellos mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades, que perjudican de alguna o varias maneras a quien los recibe. La vía más habitual de *spamming* o envío de SPAM es la basada en el correo electrónico, aunque también afecta de forma importante a otras tecnologías de Internet como grupos de noticias, *usenet,* motores de búsqueda, *wikis*, foros, *blogs*, e incluso a través de *popups* y de todo tipo de imágenes y textos en la web.

La mejor forma de prevenir el SPAM es mediante el uso de programas de filtrado automático de los mismos, así como del uso de *captchas* (acrónimo de *Completely automated public turing test to tell computers and humans apart* o prueba pública y automática para diferenciar a máquinas y humanos).

R32: Sabotaje: *malware,* virus, troyanos, *spyware*...

Los principales programas maliciosos son los virus, gusanos y otro tipo de *malware*, diseñados para insertar troyanos (programas que, de forma silenciosa, permiten el control del sistema por parte de terceras personas con la finalidad de utilizar sus recursos en su propio beneficio) o *spyware* (programas cuyo objetivo es la obtención de información personal del usuario o usuaria o del sistema, sin su consentimiento), en sistemas de información. Muchas veces son causantes de daños irreparables y de la recogida de información confidencial en sistemas informáticos.

Legalmente, con carácter general, habrá que aplicar las reglas de la responsabilidad extracontractual, cuyo fundamento normativo se encuentra en el artículo 1902 del Código Civil, o bien puede derivarse de una responsabilidad penal (263-267 CP).

La forma más habitual de distribución de código malicioso es a través de archivos adjuntos a los correos electrónicos. Por ello, una manera de reducir el riesgo será impidiendo que los usuarios y usuarias puedan adjuntar documentos a los mensajes que envían, restringiendo el tipo de archivos

que puedan adjuntar o comprobar si incluyen código malicioso a través de, por ejemplo, un programa antivirus.

Si un organismo no pone los medios adecuados para evitar un daño, podría tener que responder por ese perjuicio, además de ser considerado negligente. Este tipo de medidas técnicas permite demostrar la diligencia en la prestación de servicios.

Otra forma de ejecutar un código malicioso en la clientela es a través de vulnerabilidades en los lenguajes de *script* incorporados en las páginas web, por ejemplo *javascript*. Casi todos los navegadores tienen vulnerabilidades y éstas son habitualmente explotadas mediante el uso de programas malignos en Javascript, ActiveX u objetos embebidos que las pueden aprovechar para instalar un código maligno en la clientela. La mejor forma de prevenir este ataque es evitando que las personas puedan usar las etiquetas HTML correspondientes a estos elementos enriquecidos, que en este contexto no aportan nada.

Muchos troyanos, virus, gusanos o *malware* en general se introducen en los ordenadores de los usuarios y usuarias a través de la ejecución directa de un programa proveniente de una fuente no fiable que, o bien esté infectado o lleve intencionadamente una carga maligna. La única forma realmente fiable de evitar este problema es advirtiendo a las personas que visiten la página de este hecho y/o evitando que se pueda enlazar directamente programas ejecutables.

Por último, hay que tener en cuenta que algunos archivos aparentemente inofensivos, como pudieran ser imágenes, documentos de textos, etcétera, que en principio no tienen contenido ejecutable, pueden estar estructurados a propósito de tal forma que aprovechen vulnerabilidades en los programas que los visualizan para ejecutar programas maliciosos.

Aunque un documento no ejecutable es pasivo y, por tanto, a priori no se le suponga la posibilidad de contener una carga maligna, a veces se usan documentos mal formados a propósito, de tal forma que con ello se puedan aprovechar vulnerabilidades de los programas que son más habitualmente usados para visualizarlos. Esto ha ocurrido ya en el pasado con elementos multimedia como determinados formatos de imágenes, con elementos *flash* o *java* o con formatos documentales como PDF. De igual forma, algunos tipos de documentos pueden llevar también un programa ejecutable dentro de ellos en forma de macros, por ejemplo, los documentos de ofimática o las páginas web realizadas en HTML, o ser realmente un lenguaje de programación muy especializado que los usuarios y usuarias equivocadamente confundan con un documento pasivo (como el lenguaje de impresión *postscript*). La única forma de prevenir este ataque es limitando en lo posible los documentos a aquellos que sean necesarios, comprobando si es posible que están bien formados, y pasándolos a través de un programa de detección de *malware*.

R33: Suscripción masiva

A menudo, ciertos programas o *scripts* atacan servicios en Internet mediante el mecanismo de la creación sistemática de cuentas en un servicio, o de intento de control de las ya existentes con vistas a enviar SPAM, revender el servicio, realizar ataques de denegación de servicios (DoS) o simplemente fastidiar. Esto es muy habitual en el caso de *blogs* o foros, en los que existe un *workflow* diferente para los comentarios anónimos que para los que no lo son. Sucede en el caso de servicios que se pueden usar como plataforma para realizar SPAM en otros *sites*, como el caso de los servicios *webmail* o semejantes.

La mejor forma de limitar este tipo de ataques es mediante el uso de *captchas*. Éstos son utilizados para evitar que robots, también llamados *spambots*, puedan utilizar ciertos servicios. Consiste en obligar a quien quiera usar el servicio, a solucionar una prueba muy simple para un ser humano, pero que suponga un gran desafío para un programa de ordenador. Hay que tener mucho cuidado a la hora de realizar dichas pruebas para evitar limitar de forma no deseada el acceso al servicio a segmentos de la poblaciópn que pudieran tener dificultades para solucionar dichos desafíos, como las personas con necesidades especiales. De la misma manera, han de ser lo suficientemente elaborados para evitar que un robot los pueda romper, incluso mediante técnicas de OCR (Reconocimiento Óptico de Caracteres), "fuerza bruta" (probar todas las combinaciones posibles) o bases de datos de respuestas prefabricadas ("diccionarios").

Para evitar los ataques por "fuerza bruta", la mejor forma es limitar el número de conexiones y el número de intentos consecutivos que se pueden realizar para solucionar la operación, *baneando* o limitando temporalmente el acceso a la IP atacante, en el caso de que se detecte un intento de este tipo. El número de intentos limitante deberá ser lo suficientemente grande para evitar que una persona pueda tener problemas por este motivo.

R34: Robo masivo de datos personales

Se produce el robo de datos personales cuando terceras personas obtienen ilegalmente la información personal de los usuarios y usuarias de nuestro sistema. El robo de listas de correo electrónico es un delito que puede llegar a ser muy lucrativo. Por lo general, las listas generadas por cuenta propia, obtenidas por doble verificación o confirmación y con un patrón social definido son las más apetecibles y, si el listado contiene además datos personales y refleja hábitos de compra de sus miembros, lo es aún más. Este tipo de delitos suele dejar escasas huellas, ser bastante anónimo y llevarse a cabo con bastante impunidad ya que, a menudo, no es ni siquiera percibido.

Este riesgo puede materializarse por la acción de alguien con acceso a las bases de datos que pueda copiar las listas con impunidad, o por la intrusión de una persona ajena en el sistema que acceda a las bases de datos y pueda obtener una copia de la información almacenada en las mismas. A veces, es posible recopilar los datos a través de un programa que los vaya recogiendo de

las páginas publicadas, si es que los datos están abiertamente publicados en las mismas, aunque sea de forma dispersa.

R35: Problemas de accesibilidad

Se entiende por accesibilidad al hecho de que todas las personas puedan hacer uso del servicio, independientemente de las necesidades especiales que puedan tener, y no estén excluidas del mismo por su dificultad para comunicarse con él. Este término engloba muchos tipos de discapacidades, incluyendo problemas visuales, auditivos, físicos, cognitivos, neurológicos y del habla, así como personas que, por ejemplo, han visto mermadas sus habilidades a consecuencia de la edad.

Estas personas tienen también derecho a acceder a los servicios. Es muy importante que éstos sean accesibles para poder proporcionar un acceso equitativo y con igualdad de oportunidades para todas las personas.

Por otra parte, la organización no puede permitirse el lujo de dejar fuera a estas personas si lo que pretende es obtener, recopilar y clasificar la información de la forma más óptima y objetiva. En última instancia, la organización es la principal beneficiaria de los servicios web colaborativos, en los que los usuarios y usuarias están realizando un esfuerzo en beneficio de la misma. Si dejamos fuera a un segmento de la población, el resultado estará sesgado y, por tanto, tendrá menos valor que si se hubiera podido obtener desde una participación más plural.

R41: Baja participación

En la mayoría de servicios colaborativos, el número de aportaciones es directamente proporcional al tamaño del servicio, de tal forma que, por ejemplo, una *wikipedia* que ya tenga una gran cantidad de contenidos atraerá a más usuarios y usuarias y, por tanto, crecerá más deprisa que una de menor tamaño. De igual forma, cualquier tipo de red social tendrá un crecimiento y un valor mayores según sea su propio tamaño.

R42: Uso masivo del servicio ("morir de éxito")

Puede ocurrir que un servicio tenga una afluencia y un éxito tan importantes que haga que, por diferentes motivos, el servicio no resulte utilizable para quienes acceden a él, e incluso que no pueda ser siquiera accesible, bien por el exceso de información, por dificultades técnicas, etcétera.

Se deberá tener en cuenta, por tanto, las posibilidades de expansión del servicio tanto en el aspecto técnico como en el humano, en el caso de que pueda ser previsible que ocurra. A veces, sucede que un servicio inicialmente planteado para un colectivo restringido, se difunda más allá de su ámbito inicial y empieza a atraer a mucha más gente de la esperada, ocasionando habitualmente

problemas técnicos debido al menor dimensionamiento inicial de las infraestructuras (ancho de banda, espacio de almacenamiento, exposición de la información, etcétera). Por otra parte, mecanismos participativos que están pensados para uso de un grupo limitado de personas pueden no ser escalables a grupos mayores sin ser modificados.

R43: Participación sesgada o restringida a un sector de la población

Como se ha mencionado, es importante dar cabida en el servicio a todos los segmentos de la población si se quiere tener una participación plural, respetando, por una parte, los derechos de todas las personas a participar y, por otra, haciendo que la organización disponga de una información más general y completa. Se habrá de evitar en lo posible que exista un sesgo importante de participación por cuestiones de género, edad, cultura, ideología, etcétera, así como de la ya mencionada eliminación de las barreras que limiten el acceso a todas las personas, independientemente de las necesidades especiales que puedan tener. Todo esto deberá ser contemplado, evidentemente, considerando que existen más barreras tecnológicas y sociales sobre las que la organización puede no tener control, pero siempre deberá actuar con el objetivo de disminuir las limitaciones y exclusiones que puedan ser dependientes del servicio.

R44: Aparición de grupos de poder

Hay que tener en cuenta el riesgo de que pueden aparecer grupos de poder o élites dentro de los servicios, que se aprovechen de las posibilidades que ofrece la herramienta para excluir a otros usuarios o usuarias del servicio.

R51: Uso inapropiado de la información en servicios ajenos

Dependiendo de la licencia bajo la que publiquemos nuestra información, y si dejamos a terceras personas citarla y reproducirla, puede ocurrir que ésta aparezca en entornos no deseados o asociada a otras informaciones o contextos que puedan implicar una degradación del prestigio de la institución.

Medidas para el control de riesgos en la web participativa

Medidas para el control de riesgos en la web participativa

Medidas proactivas o preventivas de gestión de las vulnerabilidades

Aviso Legal y condiciones de uso de los servicios

Se debe disponer de un texto de Aviso Legal en el que se expliquen las reglas de acceso, uso y, en general, la relación entre la organización proveedora del portal y los servicios y quienes hacen uso de los mismos. Se ha de incluir la prohibición expresa de conductas que puedan atentar contra el honor, la intimidad y la imagen de las personas, así como de conductas que puedan infringir los derechos de propiedad intelectual de terceras personas. De igual forma se deberá advertir sobre la prohibición de conductas que puedan suponer una divulgación no autorizada de cualquier tipo de datos personales de otras personas, así como de secretos protegidos por la ley.

Se incluirá, además, la prohibición expresa absoluta de que los usuarios y usuarias puedan usar los servicios para el envío de comunicaciones comerciales no solicitadas por las personas destinatarias (SPAM).

En el Aviso Legal, se advertirá de la adopción de respuestas contundentes ante los comportamientos no permitidos, que podrán ir desde la retirada de comentarios o contenidos que se consideren inapropiados o impedir acceder al servicio a usuarios o usuarias que no respeten las normas previstas en él, hasta una posible denuncia ante las autoridades competentes llegado el caso.

De igual forma se avisará de que el uso de perfiles falsos o suplantación de la personalidad, así como el uso ilegítimo de apodos o *nicks*, o de marcas registradas sobre las cuales no se posean los derechos, podría conducir a la cancelación de la cuenta de usuario o usuaria.

El Aviso Legal deberá contener la exención de responsabilidad a favor de quien presta el servicio ante las opiniones que las usuarias o usuarios puedan verter en él.

Aviso sobre la protección de datos personales

Siempre que se recaben datos de los usuarios y usuarias que se consideren personales (incluyendo elementos como nombre y apellidos, *e-mail*, número de teléfono, DNI, IP, huella digital, fotografía, voz, etcétera), habrá que notificarlo a la persona afectada a través de un texto legal como el siguiente: "Según lo dispuesto en la L. O. 15/1999 de Protección de Datos de Carácter Personal, _____ (Organismo) le informa de que los datos de carácter personal facilitados serán

incorporados a un fichero automatizado de su titularidad, y su finalidad será la gestión de las usuarias y usuarios registrados para la utilización de los servicios ofrecidos en _____ (página web). Usted puede ejercitar su derecho a acceder, rectificar, cancelar u oponerse a la información personal registrada, en (el correo electrónico _____@_____ / la dirección postal _____)".

Si se van a almacenar *cookies*, se deberá informar al usuario o usuaria. Es interesante notar que no solamente usan *cookies* las páginas web convencionales, sino que tecnologías como *Flash* también pueden estar haciendo uso de ellas. En cualquier caso, se deberá informar a quien use los servicios de la web, de que el sistema está almacenando información en su ordenador en forma de *cookies*. Esto puede ser importante especialmente en el caso de que se esté accediendo a los servicios ofrecidos desde ordenadores de uso colectivo.

Información a los usuarios y usuarias de los servicios

Es importante informar adecuadamente a los usuarios y usuarias, a través de recomendaciones prácticas, notas o códigos de conducta, sobre el uso adecuado de los servicios con el objetivo de prevenir posibles problemas:

- Al crear un apodo o *nick*, éste no debería contener información personal de ninguna clase.
- Son importantes las medidas que se deben adoptar en lo referido a contraseñas, pudiendo recomendarse el uso de *nicks* "fuertes" (habitualmente se aconseja que contengan un número mínimo de caracteres, dígitos, mayúsculas y minúsculas).
- Es recomendable que, en ordenadores compartidos o no seguros, se evite el uso de las herramientas de "guardar contraseña" que, en ocasiones, se ofrece al usuario o usuaria para evitar tener que introducirla de nuevo en cada conexión.
- Si se está utilizando un ordenador público, no se deberá seleccionar el inicio de sesión automático. Con ello se evita que otras personas puedan acceder al servicio usando ese mismo ordenador suplantando la identidad del anterior usuario o usuaria.
- Al introducir contenido, ya sea a través de entradas en los *blogs*, comentarios, *wikis*, *chats*, etcétera, el usuario o usuaria nunca deberá facilitar información personal confidencial.
- Advertir a las personas que visiten la página de que no existe ningún control sobre los contenidos enlazados en portales o servidores ajenos a la organización.

Formación al personal de la organización

Se debe proporcionar la formación adecuada a las personas de la organización o a aquellas que colaboren con ella, respecto al uso y gestión de los servicios en los que participen o que estén encargadas de administrar. Se puede incluir una guía de publicación en *blogs* o *wikis* y unas recomendaciones sobre la edición y revisión posterior de los contenidos.

Colaboración con entidades de derecho de autoría

Si se considera conveniente, se pueden recabar cuantas autorizaciones sean necesarias de titulares de derechos o de entidades de gestión de derechos de propiedad intelectual (SGAE, AIE, entre otras), para la explotación autorizada de música, obras literarias o cualquier otra creación protegida por la LPI.

Gestión adecuada de los datos personales

Se debe cumplir escrupulosamente con lo establecido en la normativa sobre protección de datos.

Limitación de la participación de menores

Consideramos conveniente desarrollar una política propia interna y externa en la que se asegure un entorno seguro para los y las menores, y donde haya una especial sensibilidad por parte de quien presta el servicio por crear un entorno seguro y propicio en el que puedan relacionarse.

Moderación

Se puede exigir la aprobación previa de las aportaciones de usuarios y usuarias por parte de las personas que administran el servicio antes de que sean efectivamente integradas dentro del sistema, con o sin la posible edición previa de lo que se vaya a publicar, con lo que se consigue evitar el peligro en sus primeras etapas, antes de su publicación.

La moderación, en todo caso, también tiene unos serios inconvenientes:

- Requiere intervención humana y, por tanto, tiene un mayor coste.
- No es fácilmente escalable. Según se incrementa el número de elementos que hay que moderar, han de aumentarse proporcionalmente los recursos humanos involucrados.
- Existe un retraso considerable entre el envío de la información y su publicación.

Filtrado automático

Se puede disponer de sistemas automatizados de filtrado de los contenidos que no se consideren apropiados para ser publicados o transmitidos. El filtrado automático es una de las herramientas más potentes para evitar el SPAM y la transmisión de *malware* o programas informáticos maliciosos.

Asimismo, suele ser conveniente asegurarse de que los correos salientes no incorporan archivos adjuntos que puedan suponer un peligro para quienes los reciben. Esto garantizará, por ejemplo, que los virus y gusanos no sean importados automáticamente a otros sistemas. Lo más conveniente-

te, en este caso, es limitar en lo posible los documentos a aquellos que sean necesarios, comprobando, si es posible, que están bien formados y pasándolos a través de un programa de detección de *malware*.

Identificación

Si los y las participantes están lo suficientemente identificados como para sentir que son responsables de lo que escriben, y que en caso de que causen problemas tendrán que afrontar las consecuencias, generalmente disminuye la incidencia de los problemas. Además, en el caso de problemas legales, se podrán aportar datos de la persona responsable a las autoridades competentes.

Como puntos negativos de la exigencia de un alto grado de identificación para el uso de los servicios, hay que resaltar que hace más engorrosa la participación y puede producir una sensación sobre quienes los usan de estar siendo vigilados, y de que su participación pudiera tener consecuencias no deseadas (efecto *Gran Hermano*).

Limitación del acceso a los contenidos

Se puede acotar el impacto de la publicación de contenidos inadecuados a través del establecimiento de una limitación (temporal o indefinida) del acceso a los mismos a un subconjunto de personas.

En algunos casos, debido a la naturaleza del servicio, es conveniente establecer una política diferente de acceso a la información en función del perfil de la persona. De esta forma, puede existir información que solamente esté accesible para la administración del sistema y para el propietario o propietaria de la misma; puede haber información que solamente se comparta con un entorno definido de personas relacionadas con ella; que solamente se exponga para quienes tienen asignado un rol específico dentro de la aplicación; o la limitación puede ser totalmente arbitraria y aleatoria con vistas a limitar el número de personas que acceden a ella.

El objetivo de esta limitación de acceso puede tener su origen en diferentes causas, dependiendo de la naturaleza de la información. Es posible haber datos personales que solamente se desee difundir de una forma limitada, como es el caso de algunas redes sociales. Es posible que exista información sensible que solamente se quiera distribuir a un conjunto determinado de la población, es posible que se haya llegado a un acuerdo con las entidades de gestión de derechos para limitar el acceso a la misma, o cualquier otra causa.

Asimismo, se puede implementar un sistema de automoderación basado en una limitación inicial de la exposición de la información a cierto grupo de control, en función de cuya respuesta se decidirá si se realiza o no la apertura de la misma al resto de usuarios y usuarias del servicio.

Participación directa en el servicio

Las comunidades pueden estar dirigidas desde dentro usando técnicas habituales de la animación sociocultural. Esto permite marcar la dirección de la forma en la que se produce la participación de la comunidad, maximizar su efectividad, aumentar la confianza de usuarios y usuarias respecto a la comunidad, producir un aumento en las aportaciones, además de suavizar y mitigar los efectos de acontecimientos peligrosos que puedan ocurrir, a través de la movilización de la comunidad para contrarrestarlos.

Definición de planes de contingencia

Es aconsejable tener planificada la posible respuesta ante acontecimientos que, aunque sea con una probabilidad muy pequeña, sea previsible que puedan ocurrir, si el efecto de éstos se atenúa con una intervención rápida y bien planificada.

Planificación de la puesta en marcha

Se refiere al comportamiento de las personas al entrar en contacto con una nueva comunidad; a menudo se define en función de la propia dinámica que observen en dicha comunidad, de tal forma que, esa misma persona, se puede comportar de forma muy diferente en distintos contextos. En este sentido, es muy importante gestionar adecuadamente la puesta en marcha del servicio y la evolución de la comunidad que surja de él, en muchos casos incluso limitando artificialmente el tamaño de la misma e interactuando con ella para dirigirla hacia el comportamiento que estimemos más adecuado, de tal forma que, llegado un momento crítico, la comunidad tenga una cierta inercia y de alguna forma se autoregule con una intervención mínima.

Medidas reactivas o correctivas de gestión de las vulnerabilidades

Vigilancia

Quien presta el servicio debe vigilar el portal y sus contenidos, así como estar atento a las posibles alertas que terceras personas pudieran realizarle en relación con el mismo. Asimismo, respecto al uso de la información publicada, se sugiere llevar un control y/o seguimiento de la explotación de los contenidos por parte de otros portales externos, para certificar su adecuación a los criterios de la organización.

Aviso de problemas por parte de la comunidad

Se debe establecer un procedimiento sencillo y eficaz por el cual cualquier persona pueda notificar, a quienes administran los servicios, cualquier tipo de problema que pueda haber.

En lo que respecta a posibles ataques contra la intimidad o el honor de las personas, se deberá implementar algún sistema de notificación voluntaria a través de correo electrónico, *chat*, teléfono u otro medio de comunicación directa y eficaz.

En lo relativo a la propiedad intelectual, debe existir algún canal para que, quien ostente la titularidad de los derechos, pueda notificar a la persona responsable del sitio web que uno de sus usuarios o usuarias está vulnerando sus derechos y se ponga fin a dicha explotación no consentida. Para solucionar esto podría servir una cuenta de correo electrónico.

Se deberá crear una cuenta de correo electrónico específica para recibir notificaciones de los usuarios y usuarias en relación con sus datos personales, del tipo *lopd@xxx.xx*. La misma deberá comprobarse a diario y, en el supuesto de que éstos ejerciten sus derechos ARCO (acceso, rectificación, cancelación y oposición), se cumplirá con lo que establece el Reglamento de desarrollo de la LOPD al respecto (Título III) y, muy especialmente, en lo relativo a los plazos de contestación.

Para conocer intentos de estafas puede resultar de utilidad para quien presta el servicio facilitar a los usuarios y usuarias herramientas mediante las cuales denuncien comportamientos inadecuados de otras personas, y así permitir a quien presta el servicio tomar la decisión de comunicarlo ante las autoridades competentes.

Además, este tipo de mecanismos, hacen partícipe y responsable a la comunidad de cuidar de sí misma, con lo que aumenta su sensación de formar parte del sistema.

Retirada de contenidos

Si fuera necesario, quien presta el servicio deberá proceder a la retirada de los contenidos que no sean apropiados para el sitio web, sin perjuicio de que se deban tomar otra serie de decisiones más drásticas, como el bloqueo de usuarios o usuarias o la denuncia ante las autoridades competentes, en los supuestos más graves.

Modificación de lo publicado

Si las aportaciones son susceptibles de causar problemas, pueden ser editadas o eliminadas, total o parcialmente, incluso tras su publicación.

Cancelación de la cuenta

Se podrá impedir el acceso al servicio a usuarios o usuarias que no respeten las normas de uso previstas para el servicio, en el supuesto de que ocasionen situaciones de riesgo con su comportamiento.

De igual forma, en caso de una situación comprobada de suplantación de la personalidad o de que el usuario o usuaria no tiene un interés legítimo sobre el apodo o *nick* utilizado, se puede proceder a la cancelación de la cuenta.

Denuncias

En determinados casos, dependiendo de la legislación vigente, quien presta el servicio deberá proceder a la denuncia de la situación ante las autoridades competentes.

En caso de amenazas que tengan un contenido personal o las que se hagan en nombre de una banda terrorista o con trasfondo político, el portal tendrá la obligación legal, en la medida en que haya tenido conocimiento de ello, de denunciar dichos actos inapropiados ante las autoridades competentes. La valoración de estos comportamientos es muy delicada y dependerá siempre de la subjetividad de quien esté al cargo de estas comprobaciones, por lo que debe imponerse el sentido común.

También hay que denunciar ante la AEPD cualquier acceso no autorizado a ficheros de los que la persona que presta el servicio sea responsable o encargada del tratamiento.

En el caso de que quien presta el servicio tuviese conocimiento de que a través del portal web se están produciendo estafas, deberá denunciar de forma inmediata ante la autoridad competente cualquier indicio o notificación que reciba.

Moderación colectiva por parte de la comunidad

Los usuarios y usuarias, mediante su valoración de la información aportada por otros y otras miembros de la comunidad, pueden influir sobre su visibilidad o, incluso, sobre su eliminación.

Al igual que sucede con los mecanismos de clasificación de contenidos basados en la valoración de los usuarios y usuarias, se corre el riesgo de que este tipo de herramientas puedan convertirse en un arma más, con lo que han de ser supervisadas y controladas.

Evaluación periódica de las medidas

Recogida de datos

Independientemente de las obligaciones legales de almacenamiento de *logs* y de información de los usuarios y usuarias, que evidentemente habrá que cumplir también, se deberán recoger y almacenar los datos sobre la utilización del servicio que se consideren apropiados, para poder analizar y mejorar los sistemas de control y gestión del sistema en las subsiguientes revisiones periódicas de la evaluación de riesgos del servicio.

Evaluación de servicios web colaborativos

Evaluación de servicios web colaborativos

Servicio: Enviar a alguien la referencia de un artículo de la Web

Definición

Esta opción, muy habitual en páginas que incorporan artículos o noticias, consiste en permitir que el sistema envíe el contenido de la misma a través de correo electrónico a alguna persona a quien pueda resultar de interés.

Tradicionalmente se suele incluir la opción de enviar por SPAM el artículo a terceras personas, pero ciertas resoluciones recientes de la AEPD sancionando a quienes proveen del servicio, hacen que sea necesario replantearse este método y sustituirlo por el envío del artículo a la misma persona que lo solicita, para que sea ésta quien lo reenvíe mediante su propio correo electrónico.

Clasificación

No existen diferencias esenciales en la implementación de este tipo de servicios.

Riesgos

En este tipo de servicio no aparece ningún riesgo significativo que no se incluya en la lista general de riesgos.

Consecuencias

No existen consecuencias específicas asociadas a los riesgos que no se mencionen en el documento general.

Recogida de datos

Será interesante almacenar estadísticas de uso de este servicio que permitan evaluar tanto la extensión de su uso como los registros que queden de posibles intentos de abuso del mismo. Estos datos estadísticos incluirán, como mínimo, el número de veces que se ha usado este servicio desde cada página en que esté disponible y el número de solicitudes que ha habido de envío de un *e-mail* a cada dirección de correo concreta, sin revelar, si se quiere, dicha dirección mediante el uso

de algún algoritmo de *hash* (MD5, SHA...), en el caso de desear eliminar del archivo cualquier resto de datos personales. Estos datos se almacenarán por unidad de tiempo, preferentemente por el día, para poder realizar un análisis temporal de los mismos si es preciso.

Actuaciones

A02: Uso de un captcha *semántico para acceder al servicio*

A la hora de darse de alta, baja o interaccionar de cualquier forma con el sistema de control de las listas, el usuario o usuaria deberá responder a una pregunta sencilla que sea complicada de resolver por una máquina, para asegurarse de que está siendo operado realmente por una persona. Esta pregunta se realizará en texto simple, sin recurrir a imágenes o sonidos, para no limitar la accesibilidad del servicio. Debido a esto, las preguntas tendrán que estar fundamentadas en una base de datos de conocimiento lo suficientemente extensa como para evitar que una máquina automatizada las pueda acertar con una probabilidad importante, y debe ser periódicamente renovada y/o extendida.

A03: Limitación del uso del servicio por parte de menores de 14 años

Para evitar tener que abordar todos los procedimientos necesarios para permitir la participación de menores de 14 años en el servicio, se ha optado por limitar su uso a personas mayores de 14 años. Para eso, a la hora de inscribirse, los usuarios y usuarias deberán confirmar mediante una casilla de confirmación que habrá de ser rellenada online por el usuario o usuaria, que inicialmente no estará marcada por defecto.

A04: Información de las condiciones de uso del servicio

Se informará a los usuarios y usuarias de las condiciones de uso del servicio. Antes de poder acceder a éste deben confirmar que las han leído, entendido, cumplen con los requisitos exigidos y se comprometen a respetar las normas y las condiciones allí descritas.

El texto de las condiciones de uso será algo semejante a éste: "Puedes enviarte esta noticia por correo electrónico si así lo deseas. Para ello has de introducir tu dirección de correo electrónico, a la que será enviada la información solicitada. En ningún caso está permitido introducir direcciones de correo de otras personas, respetando, de esta forma, la interpretación que realiza la Agencia Española de Protección de Datos de la legislación española. Si conoces a alguien a quien le pudiera interesar recibir esta noticia, tienes que introducir tu dirección de correo, recibir el artículo en tu buzón y reenviarlo manualmente a las personas a quienes consideres oportuno. No está permitido el uso de este servicio de una forma diferente a la descrita. En caso de abuso, la administración del mismo se reserva el derecho de tomar las medidas que se estimen adecuadas".

A05: Información respecto al tratamiento de los datos personales

A continuación se reproduce el texto sobre protección de datos que deberá ponerse en cada página en la que se recaben datos de usuarios o usuarias:

El texto sobre el tratamiento de los datos personales será similar al que sigue: "Según lo dispuesto en la L.O. 15/1999 de Protección de Datos de Carácter Personal, _____ (Organismo) le informa de que los datos de carácter personal facilitados serán incorporados a un fichero automatizado de su titularidad, y su finalidad será la gestión de las usuarias y usuarios registrados para la utilización de los servicios ofrecidos en _____ (página web). Usted puede ejercitar su derecho a acceder, rectificar, cancelar u oponerse a la información personal registrada en (el correo electrónico _____@_____ / la dirección postal _____)".

Son datos de carácter personal, entre otros, el nombre y apellidos de una persona, su dirección, DNI e IP.

A06: Definición restrictiva del uso del servicio

Teniendo en consideración la resolución dictada por la AEPD en la que se impone una sanción económica a la persona titular de un portal web por remitir a un o una particular un correo electrónico no solicitado, sin haber obtenido previamente el consentimiento del mismo como persona destinataria de la comunicación, al haber hecho una tercera persona uso de una aplicación del tipo "enviar a alguien" o *share this*, se ha decidido preventivamente sustituir este tipo de servicio por otro de funcionalidad equivalente en el que el envío del artículo se realiza a la misma persona que lo solicita, para que sea ésta quien lo reenvíe, si así lo desea, mediante su correo electrónico.

A21: Limitaciones técnicas para evitar el abuso del servicio

Este tipo de servicio no requiere un uso exagerado de recursos del sistema, especialmente respecto al número de *e-mails* que pueden ser requeridos desde una sola IP, y es posible establecer de forma genérica, una cota máxima de uso de los mismos, por unidad de tiempo. Esta cota deberá delimitarse de tal forma que permita el uso normal del sistema, incluso en el caso de que una misma IP pueda ser usada por diferentes personas, pero que impida el envío de cantidades desproporcionadas de correos electrónicos.

A31: Eliminación de campos CC y múltiples destinatarios y destinatarias

No se enviarán correos electrónicos con múltiples destinatarios o destinatarias ni con otros nombres aparte de cada receptor individual en sus cabeceras, para evitar difundir sin permiso información personal de terceras personas.

A32: Ocultación de datos de usuarios y usuarias

No se dispondrá de ningún servicio abierto a personas ajenas a la administración del servicio que permita ver quién ha solicitado el uso de este servicio, ni sus nombres ni sus direcciones de correo.

A42: Notificación privada por parte de un usuario o usuaria

Se deberá disponer de una dirección de correo de emergencia a la cual puedan acudir los usuarios y usuarias del sistema para realizar notificaciones privadas de cualquier problema que puedan tener.

A51: Publicitar, anunciar e incitar a que la gente se apunte al servicio

Se habrá de situar un enlace o etiqueta visible en las páginas en las que se ofrezca este servicio, mostrando con claridad para qué sirve.

Evaluación

Datos de carácter personal

Riesgos:

- R21: Vulneración del derecho a la protección de datos de carácter personal.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Grave	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A05	Información del tratamiento de los datos personales	=	⬇
A31	Eliminación de campos CC y múltiples destinatarios o destinatarias	⬇	=

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Suplantación de la personalidad

Riesgos:

- R23: Suplantación de la personalidad.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Baja	Dañino	Tolerable

Ref.	*Actuación*	*Prob.*	*Daño*
A04	Información de las condiciones de uso del servicio	=	⬇
A42	Notificación privada por parte de un usuario o usuaria	=	⬇

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Suscripción al servicio

Riesgos:

- R18: Participación forzada de terceras personas.
- R33: Suscripción masiva.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Moderado	Tolerable

Ref.	*Actuación*	*Prob.*	*Daño*
A02	Uso de un *captcha* semántico para acceder al servicio	⬇ ⬇	=
A21	Limitaciones técnicas para evitar el abuso del servicio	⬇	⬇
A04	Información de las condiciones de uso del servicio	=	⬇
A06	Definición restrictiva del uso del servicio	=	⬇

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Robo de datos de usuarios y usuarias del sistema

Riesgos:

- R34: Robo masivo de datos personales.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Dañino	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A04	Información de las condiciones de uso del servicio	=	⬇
A31	Eliminación de campos CC y múltiples destinatarios o destinatarias	⬇ ⬇	=
A32	Ocultación de datos de usuarios y usuarias	⬇	=

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Baja participación

Riesgos:

- R41: Baja participación.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Leve	Tolerable

Ref.	*Actuación*	*Prob.*	*Daño*
A51	Publicitar y anunciar el servicio	⬇	=

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Alta participación

Riesgos:

- R42: Uso masivo del servicio ("morir de exito").

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Baja	Leve	Trivial

Ref.	*Actuación*	*Prob.*	*Daño*
A21	Limitaciones técnicas para evitar el abuso del servicio	⬇	⬇

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Servicio: Listas de correo

Las listas de correo electrónico son un uso especial del correo electrónico que permite la distribución masiva de información entre múltiples usuarios y usuarias de Internet a la vez. En una lista de correo se escribe un correo a la dirección de la lista y le llega masivamente a todas las personas inscritas en ella. Dependiendo de cómo esté configurada, el receptor podrá o no tener la posibilidad de reenviar el correo.

El objetivo de una lista de distribución es hacer llegar mensajes a varios usuarios o usuarias de una vez, en lugar de enviar un mensaje individual. Las listas de distribución son útiles para compartir información en un servicio u organización, o para organizar grupos de trabajo cuyas personas que lo componen deban estar permanentemente informadas del desarrollo de una tarea.

Definición

Las listas de correo son un mecanismo de intercambio de información entre las personas pertenecientes a un grupo de trabajo sobre cualquier tema de interés común. Las listas de correo tienen como principal característica que no obliga a los usuarios y usuarias a buscar información, sino que ésta les llega, y pueden usar cualquier programa o sistema de gestión de correo electrónico para leerla y gestionarla. Uno de los principales puntos fuertes de éstas es que permiten leer, buscar y responder a las consultas incluso cuando no hay disponible una conexión a la red, y permiten tener almacenado en el ordenador una pequeña base de conocimiento sobre el tema.

La principal desventaja de las listas de correo sobre los foros es que, a usuarios y usuarias ocasionales, les puede parecer demasiado engorroso. Las listas de correo recogen y aglutinan a la gente con más interés en el tema y de forma más permanente que quienes pasan casualmente por ahí. Un foro es más proclive a visitas casuales, pero menos generador de grupos de personas que sean verdaderamente asiduas al mismo (típicamente 2 ó 3, casi independientemente de la cantidad de personas que lo usen). La lista de correo, en principio, puede asustar un poco más al usuario o usuaria casual y sólo reunirá a quienes tengan verdadero interés en el tema.

Sin embargo, esta barrera puede atenuarse con la disponibilidad *online* de los mensajes enviados a través de la lista, así como de la existencia de servicios como *gmane* que hacen de pasarela entre listas de correo y foros.

En cuanto a la administración del sistema, el principal problema de las listas de correo deriva de que, una vez enviado un correo electrónico, resulta imposible retirarlo.

Clasificación

Dependiendo de la política de suscripción (quién puede suscribirse)

- **Abierta:** una lista es abierta cuando cualquier persona puede suscribirse/desuscribirse por sí mismo.
- **Cerrada:** solamente puede suscribir a alguien quien ostente las funciones de administración de la lista.

Dependiendo de la política de distribución (qué se hace con los mensajes que lleguen a la lista)

- **Pública:** cualquier persona tiene permiso para mandar mensajes a la lista (lista de debate pública).
- **Semipública:** un grupo de usuarios o usuarias de la lista tiene permiso para enviar mensajes a la lista (lista de debate semipública).
- **Privada:** medio unidireccional de información y al que solamente pueden escribir determinadas personas encargadas de la publicación de dicho boletín (boletín electrónico).

Dependiendo de la forma de suscribirse

- **Manual:** quienes usen el servicio han tenido que suscribirse voluntariamente a él.
- **Automática:** la suscripción/desuscripción se hace automáticamente, cada cierto tiempo y según un criterio determinado.

Riesgos

En este tipo de servicio no aparece ningún riesgo significativo que no se incluya en la lista general de riesgos.

Consecuencias

No existen consecuencias específicas asociadas a los riesgos que no se mencionen en el documento general.

Recogida de datos

Se almacenarán datos estadísticos del envío de mensajes a la lista por cada una de las direcciones de correo que hayan realizado el envío y unidad de tiempo (preferentemente el día). Asimismo, se almacenará la información relativa a la aceptación o rechazo de los mensajes por parte de la moderación. Si se desea, éstos podrán conservar el anonimato para evitar los problemas asociados con el tratamiento de datos personales, sustituyendo las direcciones de correo por el resultado de la ejecución de algún algoritmo de *hash* sobre las mismas (MD5, SHA...).

Actuaciones

A01: Identificación previa de participantes

Las personas que escriban en la lista de correo deberán estar dadas de alta en una base de datos de suscriptores o suscriptoras. La inscripción en dicha lista es libre, pero deberá confirmarse que la persona que se está inscribiendo posee realmente control sobre la dirección de correo electrónico que indica como suya. Para ello, todas las interacciones con el sistema de gestión del servicio, que se realizarán a través de página web, deberán de ser confirmadas a través del aseguramiento de la recepción de un correo electrónico enviado a la misma, bien acudiendo a una URL temporal indicada en dicho correo o respondiendo al mismo.

La dirección de correo será el único dato personal que se almacene sobre los usuarios y usuarias de este sistema. Además, no es necesario utilizar una contraseña.

A02: *Uso de un* captcha *semántico para acceder al servicio*

A la hora de darse de alta, baja o interaccionar de cualquier forma con el sistema de control de las listas, el usuario o usuaria debe responder a una pregunta sencilla que sea complicada de resolver por una máquina, para asegurarse de que está siendo operado realmente por una persona. Esta pregunta se realizará en texto simple, sin recurrir a imágenes o sonidos, para no limitar la accesibilidad del servicio. Debido a esto, las preguntas estarán extraídas en una base de datos de conocimiento lo suficientemente extensa como para evitar que una máquina automatizada las pueda acertar con una probabilidad importante, y debe ser periódicamente renovada y/o extendida.

A03: Limitación del uso del servicio por parte de menores de 14 años

Para evitar tener que abordar todos los procedimientos necesarios para permitir la participación de menores de 14 años en el servicio, se ha optado por limitar su uso a personas mayores de 14 años. Para eso, a la hora de inscribirse, los usuarios y usuarias deberán confirmar mediante una casilla de confirmación que habrá de ser rellenada online, que inicialmente no estará marcada por defecto.

A04: Información de las condiciones de uso del servicio

Se informará a usuarios y usuarias de las condiciones de uso del servicio. Antes de poder acceder a éste deben confirmar que las han leído, entendido, cumplen con los requisitos exigidos y se comprometen a respetar las normas y las condiciones allí descritas. Hay que redactar un texto, por tanto, que debe ser accesible a todas las personas susceptibles de utilizar los servicios (sin necesidad de que se den de alta previamente en ellos), en el que se definan las condiciones de uso, tanto en términos de quiénes pueden usar el servicio, cuáles son los objetivos del mismo y qué actitudes y comportamientos son aceptables o rechazables.

A05: Información a usuarios y usuarias respecto al tratamiento de sus datos personales

A continuación, se detalla un texto sobre protección de datos que deberá ponerse en cada página en la que se recaben datos de usuarios o usuarias:

El texto sobre el tratamiento de los datos personales será parecido a éste: "Según lo dispuesto en la L.O. 15/1999 de Protección de Datos de Carácter Personal, _____ (Organismo) le informa de que los datos de carácter personal facilitados serán incorporados a un fichero automatizado de su titularidad, y su finalidad será la gestión de las usuarias y usuarios registrados para la utilización de los servicios ofrecidos en _____ (página web). Usted puede ejercitar su derecho a acceder, rectificar, cancelar u oponerse a la información personal registrada en (el correo electrónico _____@_____ / la dirección postal _____)".

Son datos de carácter personal, entre otros, el nombre y apellidos de una persona, su dirección, DNI, *e-mail* e IP.

A11: Moderación basada en listas de clasificación de los usuarios y usuarias ("Listas de colores")

Aunque una moderación absoluta podría ser un mecanismo bastante fiable para no dejar pasar contenidos no deseados, es una opción demasiado costosa en relación con los recursos humanos necesarios para realizar la tarea, así como en lo relativo al retraso constante en la aprobación de los mismos, que puede ser bastante inconveniente y desmotivador para usuarios y usuarias en algunos servicios, y totalmente inaceptable en otros.

Para conseguir la mayor parte de los beneficios de la moderación, pero atenuando en lo posible los problemas que presenta, se adoptará una moderación parcial, que no afectará a las personas que lleven utilizando un cierto tiempo el servicio sin haber planteado problemas de ningún tipo. Esto será decidido tanto en función del tiempo que lleven dados de alta como de la participación real que hayan tenido en el servicio, de tal forma que los usuarios y usuarias más habituales, que son

quienes presumiblemente harán la mayor parte de las colaboraciones, aunque están exentos de la moderación una vez que el servicio lleve un cierto tiempo en funcionamiento.

Por tanto, se plantea la creación de varias listas en las que ubicar a estas personas:

- Una lista negra, común a todos los servicios, con la gente que ha sido expulsada e inhabilitada para usarlos.
- Una lista verde, por cada servicio, con la gente que no ha causado problemas, habiendo participado ya un tiempo suficiente como para valorarlo.
- Una lista amarilla, por cada servicio, con las personas que aún no han participado lo suficiente en ese servicio como para poder evaluarlas.
- Una lista roja, por cada servicio, con las personas cuyos comentarios han tenido que ser censurados alguna vez en dicho servicio o han demostrado ser problemáticas, sin llegar al extremo de que se les prohíba el uso.

Se establecerá un flujo de personas entre unas listas y otras en función del tiempo que lleven dados o dadas de alta, de la cantidad de veces que hayan participado en ese servicio y de los problemas que hayan causado. El paso de unas a otras será realizado automáticamente teniendo en cuenta los datos de los que se dispone, incluso los intentos de participación excluidos por la moderación, y podrá ser configurado para cada servicio en función de sus características particulares.

A la hora de realizar la moderación, los mensajes provenientes de personas en la lista verde pasarán directamente, asumiéndose un cierto riesgo, pero muy controlado. Las personas en la lista amarilla serán moderadas de forma prioritaria respecto a las de la lista roja. Quienes estén en la lista negra no podrán participar.

Se habrá de redactar, por tanto, un texto que permita unificar los criterios con respecto a qué tipo de mensajes se permitirán y cuáles no, basados tanto en el contenido como en la forma de los mismos. Este texto debe ser un documento vivo, que evolucione según se vayan definiendo las actuaciones en los casos más dudosos. Se habrá de definir también qué respuesta se dará a los tipos de situaciones que allí se planteen, que pueden variar desde una notificación a la persona responsable, la prohibición del uso de dicho servicio en el futuro a la persona causante de la situación, la notificación a las autoridades competentes o incluso la realización de las actuaciones legales que se estimen oportunas.

A12: Filtrado automático según el contenido del mensaje

Será conveniente evaluar la posibilidad de incorporar un mecanismo de filtrado automático de los mensajes que cumplan ciertas condiciones.

En su forma más primitiva, este filtrado se podrá realizar en función de la existencia dentro de los mismos de ciertas expresiones no válidas, como insultos, contenido sexual o violento, publicidad,

enlaces no deseados, etcétera. Esta lista deberá ser fácilmente actualizable por la administración del sistema para adecuarse a las necesidades dinámicas del entorno.

Si es posible, sería conveniente que este filtrado obedeciera a un análisis semántico del texto.

A13: Filtrado automático según el contenido de los adjuntos

Dependiendo de las necesidades de cada servicio se habilitará la posibilidad de permitir o no adjuntos a los mensajes y los tipos permitidos. Éstos deberán pasar por un filtro automatizado que compruebe que no contienen ningún *malware* escondido. Asimismo, se limitará su tamaño máximo.

En el caso de que el adjunto se rechace, bien por el tipo de fichero que es, o porque contiene algo potencialmente peligroso, se denegará el mensaje entero y se notificará a su emisor o emisora. En el supuesto de que contenga *malware* se podrán tomar las medidas que se consideren adecuadas (comenzando por la notificación a la persona en el caso de que se considere que ha sido infectada por un virus, hasta la posibilidad de notificarlo a las autoridades competentes).

A21: Prohibición de mensajes en formato HTML

Para evitar problemas de usabilidad y accesibilidad, así como eliminar los riesgos de que alguien pueda introducir un código malicioso en el texto enviado, y dado que los mensajes en HTML no son universalmente compatibles con todos los y las clientes de correo, que consumen bastante más ancho de banda, y que habitualmente no aportan mucha más información que el mensaje, no se permitirá el envío de mensajes formateados en HTML. En el caso de recibirse, éste se rechazará, indicándole por correo los motivos.

A22: Restricción de los tipos de adjunto que se pueden enviar

Se deberán limitar los tipos de adjunto permitidos a los tipos de archivos que se consideren seguros, implementando, si es necesario, una lista blanca y rechazando los tipos de archivo que no estén en ella. No se permitirán archivos ejecutables ni aquellos que tengan una mayor probabilidad de contener virus o *malware*, incluso aunque vayan dentro de archivos comprimidos. Es habitual que, por ejemplo, en listas de desarrollo, sí se deba permitir al menos el envío de parches de código en forma de texto.

A23: Filtro anti-SPAM automatizado

Se habrá de disponer de un sistema automático que permita el filtrado de los *e-mails* masivos no solicitados.

A31: Eliminación de campos CC y múltiples destinatarios y destinatarias

No se enviarán correos electrónicos con múltiples destinatarios y destinatarias ni con otros nombres aparte de cada receptor o receptora individual en sus cabeceras, para evitar difundir sin permiso información personal de terceras personas.

A32: Ocultación de datos de usuarias y usuarios

No se dispondrá de ningún servicio abierto a personas ajenas a la administración del servicio que permita ver quién está suscrito o suscrita al uso de este servicio, ni sus nombres ni sus direcciones de correo, salvo en el caso de que estas personas hayan aceptado voluntariamente aparecer en este tipo de listado.

A41: Avisos por parte de la comunidad

Se deberá desarrollar un mecanismo sencillo de denuncia de las páginas o mensajes con contenidos inapropiados o que incumplan las condiciones de uso del servicio, de tal forma que los usuarios y usuarias puedan dar aviso de aquellos contenidos que consideran que no deberían estar.

A42: Notificación privada por parte de un usuario o usuaria

Se deberá disponer de una dirección de correo de emergencia a la cual puedan acudir los usuarios y usuarias del sistema para realizar notificaciones privadas de cualquier problema que puedan tener.

A43: Eliminación de mensajes indeseados

Aunque no hay forma de retirar un mensaje de correo electrónico que ya haya sido enviado, sí que deberá disponerse de la opción de eliminar estos mensajes de los archivos disponibles a través de servicios web.

A44: Notificación a las autoridades

Se debe disponer de un protocolo de comunicación con las autoridades competentes en el caso de que sea necesario notificarles una actuación ilegal, así como de una persona dentro de la organización responsable de hacerlo.

A45: Eliminación del acceso al servicio a un usuario o usuaria

Deberá disponerse de un mecanismo para eliminar y bloquear el acceso al servicio a personas que, por algún motivo, no se les quiera permitir más el acceso.

A51: Publicitar, anunciar e incitar a que la gente se apunte al servicio

Se deberá informar de la existencia de la lista de correo en el portal web al que pertenezca, así como del tipo de lista del que se trate, el objetivo de su existencia y a quién está destinada.

A52: Dinamización, activación y motivación desde dentro de la propia comunidad

Esta categoría incluye todas las actuaciones que se pueden llevar a cabo por las personas encargadas de gestionar el servicio para dinamizarlo, activarlo y motivar a las personas, mediante la participación activa en el mismo. Asimismo, es importante la aportación de contenidos interesantes por parte de la institución cuando éstos escaseen.

La fase de puesta en marcha del servicio es importante, ya que casi todas las personas se van a ajustar a las dinámicas sociales que perciban en la comunidad de usuarios y usuarias al conectar con éste. Es importante, por tanto, poner los recursos necesarios para garantizar el establecimiento de una dinámica social adecuada al poner en marcha el servicio.

Evaluación

Contenidos ilegales aportados por terceras personas

Riesgos:

- R01: Ataques a la intimidad personal, al honor y a la propia imagen de las personas.
- R02: Revelación y divulgación de secretos.
- R03: Apología ilegal de delitos.
- R06: Amenazas.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Grave	Intolerable

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A04	Información de las condiciones de uso del servicio	=	↓
A11	Moderación	↓	=
A12	Filtrado automático según el contenido del mensaje	↓	↓
A41	Avisos por parte de la comunidad	=	↓
A42	Notificación privada por parte de un usuario o usuaria	=	↓
A43	Eliminación del mensaje	=	↓
A44	Notificación a las autoridades	=	↓

Prob. Final	*Daño Final*	*Riesgo Final*
Media	Leve	Tolerable

Contenidos inapropiados enviados por terceras personas

Riesgos:

- R04: Apología no ilegal de actividades no deseadas.
- R05: Cruces de ataques o insultos.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Dañino	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A04	Información de las condiciones de uso del servicio	=	↓
A11	Moderación	↓	=
A12	Filtrado automático según el contenido del mensaje	↓	=
A41	Avisos por parte de la comunidad	=	↓
A42	Notificación privada por parte de un usuario o usuaria	=	↓
A43	Eliminación del mensaje	=	↓

Prob. Final	*Daño Final*	*Riesgo Final*
Media	Leve	Tolerable

Relación señal/ruido en los contenidos enviados por terceras personas

Riesgos:

- R11: Uso de la plataforma para la promoción empresarial o personal.
- R12: Publicidad negativa.
- R13: Asuntos irrelevantes o ajenos a la temática de la lista (*off-topic*).
- R14: Baja calidad de las aportaciones.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Dañino	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A11	Moderación	↓	=
A41	Avisos por parte de la comunidad	=	↓
A42	Notificación privada por parte de un usuario o usuaria	=	↓
A43	Eliminación del mensaje	=	↓
A52	Dinamización, activación y motivación de la comunidad	↓	=

Prob. Final	*Daño Final*	*Riesgo Final*
Media	Leve	Tolerable

Ataques personalizados contra usuarios o usuarias

Riesgos:

- R07: Acoso continuado.
- R08: Acoso sexual.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Baja	Grave	Moderado

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	⬇	=
A04	Información de las condiciones de uso del servicio	=	⬇
A11	Moderación	⬇	=
A41	Avisos por parte de la comunidad	=	⬇
A42	Notificación privada por parte de un usuario o usuaria	=	⬇
A43	Eliminación del mensaje	=	⬇
A44	Notificación a las autoridades	=	⬇
A45	Eliminación del acceso al servicio a un usuario o usuaria	⬇	⬇

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Datos de carácter personal

Riesgos:

- R21: Vulneración del derecho a la protección de datos de carácter personal.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Grave	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	⬆	⬇
A05	Información de las condiciones de los datos personales	=	⬇
A11	Moderación	⬇	=
A31	Eliminación de campos CC y múltiples destinatarios y destinatarias	⬇	=
A41	Avisos por parte de la comunidad	=	⬇
A42	Notificación privada por parte de un usuario o usuaria	=	⬇
A43	Eliminación del mensaje	=	⬇
A45	Eliminación del acceso al servicio a un usuario o usuaria	⬇	⬇

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Propiedad intelectual

Riesgos:

- R22: Vulneración de derechos de propiedad intelectual de terceros.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Grave	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A04	Información de las condiciones de uso del servicio	=	↓
A11	Moderación	↓	=
A22	Restricción de los tipos de documentos adjuntos	↓	=
A41	Avisos por parte de la comunidad	=	↓
A42	Notificación privada por parte de un usuario o usuaria	=	↓
A43	Eliminación del mensaje	=	↓
A45	Eliminación del acceso al servicio a un usuario o usuaria	↓	↓

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Suplantación de la personalidad

Riesgos:

- R23: Suplantación de la personalidad.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Baja	Dañino	Tolerable

Ref.	*Actuación*	*Prob.*	*Daño*
A04	Información de las condiciones de uso del servicio	=	↓
A42	Notificación privada por parte de un usuario o usuaria	=	↓
A43	Eliminación del mensaje	=	↓
A45	Eliminación del acceso al servicio a un usuario o usuaria	↓	↓

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Menores

Riesgos:

- R24: Vulneración del derecho de protección de menores.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Grave	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A03	Exclusión del uso del servicio a menores de 14 años	⬇	=
A04	Información de las condiciones de uso del servicio	=	⬇
A11	Moderación	⬇	=
A41	Avisos por parte de la comunidad	=	⬇
A42	Notificación privada por parte de un usuario o usuaria	=	⬇
A43	Eliminación del mensaje	=	⬇
A44	Notificación a las autoridades	=	⬇

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

SPAM

Riesgos:

- R31: SPAM o mensajes masivos no solicitados.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Leve	Moderado

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A11	Moderación	↓	=
A02	Uso de un *captcha* semántico para acceder al servicio	↓	=
A23	Filtro anti-SPAM automatizado	↓ ↓	=
A41	Avisos por parte de la comunidad	=	↓
A42	Eliminación del mensaje	=	↓

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Malware

Riesgos:

- R32: Sabotaje: *malware*, virus, troyanos, *spyware,* etcétera.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Grave	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A11	Moderación	↓	=
A12	Filtrado automático según el contenido del mensaje	↓	=
A13	Filtrado automático según el contenido de los adjuntos	↓	=
A21	Prohibición de mensajes en formato HTML	↓	=
A22	Restricción de los tipos de documentos adjuntos	↓	=
A41	Avisos por parte de la comunidad	=	↓
A42	Notificación privada por parte de un usuario o usuaria	=	↓
A43	Eliminación del mensaje	=	↓
A44	Notificación a las autoridades	=	↓

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Suscripción al servicio

Riesgos:

- R33: Suscripción masiva.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Leve	Tolerable

Ref.	*Actuación*	*Prob.*	*Daño*
A02	Uso de un *captcha* semántico para acceder al servicio	↓ ↓	=
A04	Información de las condiciones de uso del servicio	=	↓

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Robo de datos de usuarios y usuarias del sistema

Riesgos:

- R34: Robo masivo de datos personales.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Dañino	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A04	Información de las condiciones de uso del servicio	=	↓
A31	Eliminación de campos CC y múltiples destinatarios y destinatarias	↓ ↓	=
A32	Ocultación de datos de usuarios y usuarias	↓	=

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Accesibilidad

Riesgos:

- R35: Incumplimiento de la accesibilidad.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Leve	Moderado

Ref.	*Actuación*	*Prob.*	*Daño*
A21	Prohibición de mensajes en formato HTML	↓ ↓	=

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Baja participación

Riesgos:

- R41: Baja participación.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Leve	Moderado

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↑	=
A11	Moderación	↑	=
A51	Publicitar, anunciar e incitar al uso del servicio	↓	=
A22	Dinamización, activación y motivación de la comunidad	↓	=

Prob. Final	*Daño Final*	*Riesgo Final*
Media	Leve	Tolerable

Alta participación

Riesgos:

- R42: Uso masivo del servicio ("morir de exito").

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Baja	Dañino	Tolerable

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	⬇	=

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Dañino	Tolerable

Forma de participación

Riesgos:

- R43: Participación sesgada o restringida a un sector de la población.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Leve	Moderado

Ref.	*Actuación*	*Prob.*	*Daño*
A51	Publicitar, anunciar e incitar al uso del servicio	⬇	=
A52	Dinamización, activación y motivación de la comunidad	⬇	=

Prob. Final	*Daño Final*	*Riesgo Final*
Media	Leve	Tolerable.

Servicio: *Blog* con fotografías

Definición

Un *blog* es un servicio de publicación de artículos en el cual éstos son mostrados cronológicamente, apareciendo en primer lugar las entradas más recientes. En una misma entrada de *blog* se pueden combinar diferentes recursos, en el caso del servicio analizado, se permite integrar texto e imágenes.

En el *blog* analizado no se permiten comentarios de otras personas a los artículos publicados.

Clasificación

Dependiendo de quién pueda publicar artículos

- **Individual:** cualquier persona tiene permiso para mandar mensajes a la lista (Lista de debate pública).
- **Colectivo:** un grupo de usuarios o usuarias de la lista tiene permiso para enviar mensajes a la lista (Lista de debate semipública).

Dependiendo de quién pueda acceder a los artículos publicados

- **Público:** cualquier persona puede acceder al contenido de los artículos, sin necesidad de autenticarse.
- **Semipúblico:** existen ciertos artículos de acceso público y abierto, y otros a los cuales solamente pueden acceder algunas personas, tras haberse autenticado en el sistema.
- **Privado:** solamente pueden leer los artículos algunas personas.

Riesgos

No aparece ningún riesgo significativo que no se incluya en la lista general de riesgos.

Consecuencias

En este tipo de servicio no existen consecuencias específicas asociadas a los riesgos que no se mencionen en el documento general.

Recogida de datos

Se recogerán, al menos, los datos correspondientes a los resultados de la moderación de los artículos, así como las estadísticas respecto al acceso al número de veces que han sido leídos, preferentemente por cada día, para poder realizar un análisis en el tiempo de los mismos. Si es necesario mantener anónimos los datos, se usará un *hash* en lugar del identificador del *blog*.

Actuaciones

A01: Identificación previa de participantes

Las personas que publiquen en el servicio deberán estar dadas de alta en una base de datos de suscriptores. La inscripción en dicha lista es libre, pero deberá confirmarse que la persona que se está inscribiendo posee realmente control sobre la dirección de correo electrónico que indica como suya. Para ello, el alta en el uso del servicio, que se podrá realizar a través de página web, deberá de ser confirmada a través del aseguramiento de la recepción de un correo electrónico enviado a la misma, bien acudiendo a una URL temporal indicada en dicho correo, bien respondiendo al mismo.

La autenticación posterior en las interacciones con el servicio se realizará basándose en dicha dirección de correo electrónico y en una contraseña aportada por el usuario o usuaria del sistema en el momento de la creación de la cuenta y que, además, podrá ser cambiada con posterioridad en cualquier momento.

A02: Uso de un captcha semántico para acceder al servicio

A la hora de darse de alta, baja o interaccionar de cualquier forma con el sistema, el usuario o usuaria habrá de responder a una pregunta sencilla que sea complicada de resolver por una máquina, para asegurarse de que está siendo operado realmente por una persona. Esta pregunta se realizará en texto simple, sin recurrir a imágenes o sonidos, para no limitar la accesibilidad del servicio. Por este motivo, las preguntas deberán estar basadas en una base de datos de conocimiento lo suficientemente extensa como para evitar que una máquina automatizada las pueda acertar con una probabilidad importante, y que debería ser periódicamente renovada y/o extendida.

A03: Limitación del uso del servicio por parte de menores de 14 años

Para evitar tener que abordar todos los procedimientos necesarios para permitir la participación de menores de 14 años en el servicio, se ha optado por limitar el uso de éste a personas mayores de 14 años. Por tanto, a la hora de inscribirse, los usuarios y usuarias deberán confirmar mediante una casilla de confirmación que deberá ser cumplimentada *online* por el usuario o la usuaria, que inicialmente no estará marcada por defecto.

A04: Definición e información de las condiciones de uso del servicio

Se han de definir unas condiciones de uso claras que limiten aquellas actuaciones de usuarios y usuarias que no sean permisibles, e informar públicamente sobre ellas. Antes de poder acceder deben confirmar que las han leído, entendido, que cumplen con los requisitos exigidos y se comprometen a respetar las normas y las condiciones descritas.

Se habrá de redactar un texto, por tanto, que ha de estar accesible para todas las personas susceptibles de acceder a los servicios (sin necesidad de que se den de alta previamente en ellos), en el que se definan las condiciones de uso del mismo, tanto en términos de quiénes pueden usar el servicio, cuáles son los objetivos del mismo y qué actitudes y comportamientos son aceptables o rechazables.

A05: Definición e información sobre el licenciamiento de la información

Se han de definir con claridad las condiciones de reutilización de la información publicada en los *blogs* por parte de terceras personas que quieran hacer uso de ella, por ejemplo mediante la integración de la misma en otros portales, a través de su exportación en formatos RSS o *Atom*. También se deberá informar sobre la misma a todas aquellas personas que contribuyan información al servicio en las condiciones de uso, de tal forma que quede muy claro que consienten en permitir dicho uso de la misma por parte del portal al estar haciendo uso del servicio.

A06: Información a usuarios y usuarias respecto al tratamiento de sus datos personales

A continuación se reproduce un texto sobre protección de datos que deberá ponerse en cada página en la que se recaben datos de usuarios o usuarias:

El texto sobre el tratamiento de los datos personales será algo como el que sigue: "Según lo dispuesto en la L.O. 15/1999 de Protección de Datos de Carácter Personal, _____ (Organismo) le informa de que los datos de carácter personal facilitados serán incorporados a un fichero automatizado de su titularidad, y su finalidad será la gestión de los usuarios y las usuarias registrados para la utilización de los servicios ofrecidos en _____ (página web). Usted puede ejercitar su derecho a acceder, rectificar, cancelar u oponerse a la información personal registrada en (el correo electrónico _____@_____ / la dirección postal _____)".

Son datos de carácter personal, entre otros, el nombre y apellidos de una persona, su dirección, DNI, *e-mail* e IP.

A07: Información al público general sobre la administración del servicio

Para evitar que terceras personas puedan abusar de la confianza de las personas usuarias del portal e intentar usar técnicas de ingeniería social, haciéndose pasar por personas administradoras del portal para obtener información sensible o para forzar a otras personas a realizar algún acto no deseado, deberá establecerse e informar con claridad al darse de alta en los servicios, sobre cuáles serán las vías de posible contacto y los medios de interacción válidos entre la administración del portal y las usuarias y usuarios finales.

A08: Confirmación de que el usuario o usuaria controla el medio de contacto

En aquellos servicios en los que se use como mecanismo de identificación de la persona un sistema que permita establecer un contacto, se habrá de confirmar que la usuaria o usuario posee el control de éste mediante el requisito de recepción de un mensaje de respuesta como confirmación. En el caso de cuentas de correo electrónico, éste podrá consistir en un enlace URL enviado por correo a esa dirección, que deberá ser pulsado para activar la cuenta o el servicio, o en su defecto, el envío de una respuesta por correo. En el caso de identificadores basados en números telefónicos, se enviará a los mismos un código a través de un mensaje SMS que habrá de insertar en el servicio como confirmación de su recepción.

A11: Moderación asistida por parte de la comunidad

Para conseguir algunos de los beneficios de la moderación, pero sin la necesidad de un importante esfuerzo humano y dedicación permanente, así como minimizar el retraso entre la publicación de una entrada y su aparición efectiva en la página, se ha optado por un sistema mediante el cual la entrada se visualiza para las usuarias y usuarios registrados de forma inmediata, pero se mantiene en cuarentena respecto a los usuarios y las usuarias anónimos e indexación en buscadores durante un tiempo prudencial. Durante este tiempo, si hay una cierta afluencia de personas registradas en el portal y hay algún problema con la entrada, éstos pueden pulsar el enlace correspondiente a la notificación de un abuso. En el caso de que haya un número mínimo de abusos señalados, la entrada se retirará cautelarmente hasta que sea revisada por un moderador o moderadora, que tomará la decisión definitiva de qué hacer con dicha entrada.

A12: Filtrado automático según el contenido del mensaje

Será conveniente evaluar la posibilidad de incorporar un mecanismo de filtrado automático de los mensajes que cumplan ciertas condiciones para disminuir la carga de la moderación, rechazándose de forma automática los mensajes que incumplan ciertos criterios.

En su forma más primitiva, este filtrado se podrá realizar en función de la existencia dentro de los mismos de ciertas expresiones no válidas, como insultos, contenido sexual o violento, publicidad, enlaces no deseados, etcétera. Esta lista deberá ser fácilmente actualizable por la administración del sistema para adecuarse a las necesidades dinámicas del entorno.

En caso de ser posible, sería conveniente que este filtrado obedeciera a un análisis semántico del texto.

A23: Filtro anti-SPAM automatizado

Se habrá de disponer de un sistema automático que permita el filtrado de los envíos masivos no solicitados.

A24: Interfaz GUI para introducir el texto de los mensajes

En lugar de introducirse los mensajes directamente en HTML o en algún lenguaje específico de marcado, se ofrecerá la posibilidad de un interfaz WYSIWYG *(what you see is what you get)* en el que se muestre cómo se va a visualizar ese mensaje al mismo tiempo que se va componiendo éste.

A25: Filtrado de las etiquetas HTML no aceptables

Se dispondrá de una lista blanca de etiquetas HTML aceptables. Cualquier etiqueta que no esté en la lista será filtrada. Esto garantiza tanto la accesibilidad del resultado como el hecho de que no se estén usando etiquetas concretas de forma inapropiada.

A32: Ocultación de datos de usuarios y usuarias

No se revelará más información personal sobre quien escribe los artículos que la que la persona haya aceptado mostrar. La identificación se hará en función de un nick o apodo que la persona haya elegido y no se mostrará ni su nombre verdadero, ni su dirección de correo, ni ningún otro dato de carácter personal, salvo que la persona lo haya decidido así y haya dado su permiso explícito para mostrarlo.

A33: Limitación del tamaño de las fotos que se pueden subir

Se pondrá un límite razonable al tamaño máximo en Mb que pueden ocupar las fotografías que se deseen publicar.

A34: Reescalado y ajuste automático de la imagen a un formato adecuado

Aunque las fotografías se podrán aceptar en múltiples formatos y con diferentes tamaños, el sistema procederá a su adaptación a un formato estándar y un tamaño razonable antes de su almacenamiento en el mismo, de tal forma que cuando se muestre a otras personas se haga en las condiciones adecuadas.

A35: Filtrado automático de los metadatos contenidos en las cabeceras

Algunos formatos de imágenes, como el JPEG, incluyen en sus cabeceras metadatos que pueden contener información que no se desea comunicar públicamente, entre ellos datos personales, información sobre la cámara usada, información sobre geolocalización de la toma de la fotografía, o la versión en miniatura de la misma y que, en general, puede incluir información que no deseemos publicar. Es conveniente, por tanto, filtrar los metadatos no deseados que éstas incluyan antes de publicarlas. Esta operación no implica una pérdida de calidad en las fotografías.

A41: Avisos por parte de la comunidad

Se deberá desarrollar un mecanismo sencillo de denuncia de las páginas o mensajes con contenidos inapropiados o que incumplan las condiciones de uso del servicio, de tal forma que los usuarios y las usuarias puedan dar aviso de aquellos contenidos que consideran que no deberían aparecer.

A42: Notificación privada por parte de un usuario o usuaria

Se deberá disponer de una dirección de correo de emergencia a la cual puedan acudir los usuarios y las usuarias del sistema para realizar notificaciones privadas de cualquier problema que puedan tener.

A43: Eliminación del mensaje

En el caso de que sea necesario, se deberá disponer de un mecanismo de eliminación de los artículos publicados que sean problemáticos.

A44: Notificación a las autoridades

Se habrá de disponer de un protocolo de comunicación con las autoridades en el caso de que sea necesario notificarles una actuación ilegal, así como de una persona dentro de la organización responsable de hacerlo.

A45: Eliminación del acceso al servicio a un usuario o usuaria

Deberá disponerse de un mecanismo para eliminar y bloquear el acceso al servicio a personas que, por algún motivo, no se les quiera permitir más el acceso al mismo.

A51: Publicitar, anunciar e incitar a que la gente se apunte al servicio

Se deberá informar de la existencia del servicio en el portal web al que pertenezca, así como de su objetivo y a quién está destinado.

A52: Dinamización, activación y motivación desde dentro de la propia comunidad

Esta categoría incluye todas las actuaciones que se pueden llevar a cabo por las personas encargadas de gestionar el servicio para dinamizarlo, activarlo y motivar a los participantes, mediante la participación activa en el mismo. Asimismo, es importante la aportación de contenidos interesantes por parte de la institución cuando éstos escaseen.

El pase de puesta en marcha del servicio es importante, ya que casi todas las personas se van a ajustar a las dinámicas sociales que perciban en la comunidad de usuarios y usuarias al conectar con éste. Es importante, por tanto, poner los recursos necesarios para garantizar el establecimiento de una dinámica social adecuada al poner en marcha el servicio.

Evaluación

Contenidos ilegales aportados por terceras personas

Riesgos:

- R01: Ataques a la intimidad personal, al honor y a la propia imagen de las personas.
- R02: Revelación y divulgación de secretos.
- R03: Apología ilegal de delitos.
- R06: Amenazas.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Grave	Intolerable

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A04	Información de las condiciones de uso del servicio	=	↓
A11	Moderación	↓	=
A12	Filtrado automático según el contenido del mensaje	↓	↓
A41	Avisos por parte de la comunidad	=	↓
A42	Notificación privada por parte de un usuario o usuaria	=	↓
A43	Eliminación del mensaje	=	↓
A44	Notificación a las autoridades	=	↓

Prob. Final	*Daño Final*	*Riesgo Final*
Media	Leve	Tolerable

Contenidos inapropiados enviados por terceros

Riesgos:

- R04: Apología no ilegal de actividades no deseadas.
- R05: Cruces de ataques o insultos.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Dañino	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	⬇	=
A04	Información de las condiciones de uso del servicio	=	⬇
A11	Moderación	⬇	=
A12	Filtrado automático según el contenido del mensaje	⬇	⬇
A41	Avisos por parte de la comunidad	=	⬇
A42	Notificación privada por parte de un usuario o usuaria	=	⬇
A43	Eliminación del mensaje	=	⬇

Prob. Final	*Daño Final*	*Riesgo Final*
Media	Leve	Tolerable

Estafas

Riesgos:

- R25: Estafa.
- R26: Engaño o *Phishing*.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Grave	Intolerable

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A04	Información de las condiciones de uso del servicio	=	↓
A07	Información pública sobre la administración del servicio	↓	=
A11	Moderación	↓	=
A12	Filtrado automático según el contenido del mensaje	↓	=
A41	Avisos por parte de la comunidad	=	↓
A42	Notificación privada por parte de un usuario o usuaria	=	↓
A43	Eliminación del mensaje	=	↓
A44	Notificación a las autoridades	=	↓
A45	Eliminación del acceso al servicio a un usuario o usuaria	↓	=

Prob. Final	*Daño Final*	*Riesgo Final*
Media	Leve	Tolerable

Relación señal/ruido en los contenidos enviados por terceros

Riesgos:

- R11: Uso de la plataforma para la promoción empresarial o personal.
- R12: Publicidad negativa.
- R13: Asuntos irrelevantes o ajenos a la temática de la lista *(off-topic)*.
- R14: Baja calidad de las aportaciones.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Dañino	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A11	Moderación	↓	=
A41	Avisos por parte de la comunidad	=	↓
A42	Notificación privada por parte de un usuario o usuaria	=	↓
A43	Eliminación del mensaje	=	↓
A52	Dinamización, activación y motivación de la comunidad	↓	=

Prob. Final	*Daño Final*	*Riesgo Final*
Media	Leve	Tolerable

Ataques personalizados contra usuarios o usuarias

Riesgos:

- R07: Acoso continuado.
- R08: Acoso sexual.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Baja	Grave	Moderado

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A04	Información de las condiciones de uso del servicio	=	↓
A11	Moderación	↓	=
A41	Avisos por parte de la comunidad	=	↓
A42	Notificación privada por parte de un usuario o usuaria	=	↓
A43	Eliminación del mensaje	=	↓
A44	Notificación a las autoridades	=	↓
A45	Eliminación del acceso al servicio a un usuario o usuaria	↓	↓

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Datos de carácter personal

Riesgos:

- R21: Vulneración del derecho a la protección de datos de carácter personal.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Grave	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↑	↓
A06	Información sobre el tratamiento de datos personales	=	↓
A11	Moderación	↓	=
A35	Filtrado automático de los metadatos de las cabeceras	↓	=
A41	Avisos por parte de la comunidad	=	↓
A42	Notificación privada por parte de un usuario o usuaria	=	↓
A43	Eliminación del mensaje	=	↓
A45	Eliminación del acceso al servicio a un usuario o usuaria	↓	↓

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Propiedad intelectual

Riesgos:

- R22: Vulneración de derechos de propiedad intelectual de terceras personas.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Grave	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A04	Información de las condiciones de uso del servicio	=	↓
A11	Moderación	↓	=
A12	Filtrado automático según el contenido del mensaje	↓	=
A41	Avisos por parte de la comunidad	=	↓
A42	Notificación privada por parte de un usuario o usuaria	=	↓
A43	Eliminación del mensaje	=	↓
A45	Eliminación del acceso al servicio a un usuario o usuaria	↓	↓

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Suplantación de la personalidad

Riesgos:

- R23: Suplantación de la personalidad.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Baja	Dañino	Tolerable

Ref.	*Actuación*	*Prob.*	*Daño*
A04	Información de las condiciones de uso del servicio	=	⬇
A08	Respuesta que confirme la posesión del medio de contacto	⬇	=
A42	Notificación privada por parte de un usuario o usuaria	=	⬇
A43	Eliminación del mensaje	=	⬇
A45	Eliminación del acceso al servicio a un usuario o usuaria	⬇	⬇

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Menores

Riesgos:

- R24: Vulneración del derecho de protección de menores.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Grave	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A03	Exclusión del uso del servicio a menores de 14 años	⬇	=
A04	Información de las condiciones de uso del servicio	=	⬇
A11	Moderación	⬇	=
A41	Avisos por parte de la comunidad	=	⬇
A42	Notificación privada por parte de un usuario o usuaria	=	⬇
A43	Eliminación del mensaje	=	⬇
A44	Notificación a las autoridades	=	⬇
A45	Eliminación del acceso al servicio a un usuario o usuaria	⬇	=

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

SPAM

Riesgos:

- R31: SPAM o mensajes masivos no solicitados.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Leve	Moderado

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	↓	=
A11	Moderación	↓	=
A02	Uso de un *captcha* semántico para acceder al servicio	↓	=
A23	Filtro anti-SPAM automatizado	↓ ↓	=
A41	Avisos por parte de la comunidad	=	↓
A42	Eliminación del mensaje	=	↓

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Malware

Riesgos:

- R32: Sabotaje: *malware*, virus, troyanos, *spyware*, etcétera.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Grave	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	⬇	=
A11	Seudomoderación por parte de la comunidad	⬇	=
A12	Filtrado automático según el contenido del mensaje	⬇	=
A35	Filtrado automático de los metadatos de las cabeceras	⬇	=
A41	Avisos por parte de la comunidad	=	⬇
A42	Notificación privada por parte de un usuario o usuaria	=	⬇
A43	Eliminación del mensaje	=	⬇
A44	Notificación a las autoridades	=	⬇
A45	Eliminación del acceso al servicio a un usuario o usuaria	⬇	=

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Suscripción al servicio

Riesgos:

- R33: Suscripción masiva.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Media	Leve	Tolerable

Ref.	*Actuación*	*Prob.*	*Daño*
A02	Uso de un *captcha* semántico para acceder al servicio	⬇ ⬇	=
A04	Información de las condiciones de uso del servicio	=	⬇
A45	Eliminación del acceso al servicio a un usuario o usuaria	⬇	=

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Tribial

Robo de datos de usuarios y usuarias del sistema

Riesgos:

- R34: Robo masivo de datos personales.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Dañino	Importante

Ref.	*Actuación*	*Prob.*	*Daño*
A04	Información de las condiciones de uso del servicio	=	⬇
A32	Ocultación de datos de usuarios y usuarias	⬇	=

Prob. Final	*Daño Final*	*Riesgo Final*
Media	Leve	Tolerable

Accesibilidad

Riesgos:

- R35: Incumplimiento accesibilidad.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Leve	Moderado

Ref.	*Actuación*	*Prob.*	*Daño*
A21	Limitación de las etiquetas HTML que se pueden usar	⬇	=
A24	Interfaz GUI para introducir el texto de los mensajes	⬇	=
A25	Filtrado de las etiquetas HTML no aceptables	⬇	=
A41	Avisos por parte de la comunidad	=	⬇

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Leve	Trivial

Baja participación

Riesgos:

- R41: Baja participación.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Leve	Moderado

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	⬆	=
A11	Seudomoderación por parte de la comunidad	⬆	=
A51	Publicitar, anunciar e incitar al uso del servicio	⬇	=
A52	Dinamización, activación y motivación de la comunidad	⬇	=

Prob. Final	*Daño Final*	*Riesgo Final*
Media	Leve	Tolerable

Alta participación

Riesgos:

- R42: Uso masivo del servicio ("morir de exito").

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Baja	Dañino	Tolerable

Ref.	*Actuación*	*Prob.*	*Daño*
A01	Identificación previa de participantes	⬇	=
A33	Limitación del tamaño de las fotos que se pueden subir	=	⬇
A34	Reescalado y ajuste automático de la imagen	=	⬇

Prob. Final	*Daño Final*	*Riesgo Final*
Baja	Dañino	Tolerable

Forma de participación

Riesgos:

- R43: Participación sesgada o restringida a un sector de la población.

Prob. Inicial	*Daño Inicial*	*Riesgo Inicial*
Alta	Leve	Moderado

Ref.	*Actuación*	*Prob.*	*Daño*
A34	Reescalado y ajuste automático de la imagen	↓	=
A51	Publicitar, anunciar e incitar al uso del servicio	↓	=
A52	Dinamización, activación y motivación de la comunidad	↓	=

Prob. Final	*Daño Final*	*Riesgo Final*
Media	Leve	Tolerable

Gobierno del Principado de Asturias

CTIC Centro Tecnológico