Amenazas 2.0 para la Biblioteca 2.0

Gonzalo Álvarez Marañón

Investigador del Departamento de Tratamiento de la Información y Codificación, Instituto de Física Aplicada, CSIC

> «La Biblioteca 1.0 llevaba la gente a la información, la Biblioteca 2.0 llevará la información a la gente.»
>
> —Ian Davis

Las redes sociales en línea constituyen una de las últimas modas de Internet, con un crecimiento espectacular en el número de usuarios: han pasado a ser los sitios más visitados, por delante incluso de grandes concentradores de información, como Google. Las redes sociales en línea están pasando a fagocitar la mayor parte del tiempo que los usuarios pasan conectados a Internet, ya sea desde dispositivos fijos o móviles.

Muchas organizaciones no saben qué estrategia adoptar antes este auge imparable: ignorar por completo las redes sociales, a riesgo de quedarse apeados del progreso digital, o abrazar las redes sociales e integrarlas en su planificación y actividad diaria. En el caso de las bibliotecas existe esa misma incertidumbre acerca de cómo afrontar el nuevo reto que supone su integración.

Por desgracia, junto con las innegables ventajas personales y corporativas del uso de las redes sociales, surgen como con cualquier aplicación web numerosas amenazas. De hecho, algunos riesgos se ven acentuados si cabe. No se puede dar la espalda al fenómeno de las redes sociales, pero tampoco se pueden integrar en el modelo de negocio sin conocer sus riesgos. En la medida en que el uso de las redes sociales está en pleno auge dentro y fuera de las organizaciones públicas y privadas, se están convirtiendo en un blanco favorito de cibercriminales, habiéndose convertido en el 2009 en uno de los vectores más significativos de filtración de datos y robo de identidad. El envío de spam y la distribución de malware a través de redes sociales están creciendo a ritmo espectacular. Pero no son las únicas amenazas. En esta ponencia se ofrece una clasificación de las más importantes derivadas de su uso en bibliotecas, junto con los ataques típicos para materializarlas.

La Biblioteca 2.0

No existe un consenso acerca de qué significa el término Biblioteca 2.0. A fin de cuentas, lo mismo sucede con la Web 2.0. Sin embargo, es fácil coincidir en que la Biblioteca 2.0 debe presentar al menos las siguientes características según El Documentalista Enredado:

1. Debe ser **abierta** para permitir el desarrollo y mejora de sus servicios y funcionamiento.
2. Debe ser **interactiva** de tal manera que sus usuarios puedan contribuir e interactuar con las herramientas disponibles en la Web 2.0.
3. Debe ser **convergente** para que las distintas herramientas de la Web 2.0 le permitan cumplir sus objetivos.

4. Debe ser **colaborativa** de tal forma que los usuarios y los bibliotecarios puedan comunicarse en el mismo nivel de autoridad.
5. Debe ser **participativa** puesto que la participación se halla en el cuadro central de la Web 2.0, si no es participativa la Biblioteca 2.0 no tiene sentido.

Para ello, la Biblioteca 2.0 deberá apoyarse en las correspondientes tecnologías Web 2.0:

- Mensajería instantánea
- Medios en streaming
- Blogs, microblogs, nanoblogs y Wikis
- Redes sociales generalistas, tipo Facebook o Tuenti
- RSS
- Etiquetado
- Mashups
- Y otras más, algunas ni siquiera inventadas todavía.

Partiendo de la hipótesis de que una Biblioteca 2.0 integra todas estas tecnologías en su oferta, ¿a qué riesgos se enfrenta?

La vida es riesgo

En la vida cotidiana continuamente nos enfrentamos a situaciones de peligro:

- Practicamos voluntariamente deportes de riesgo, en los que puede peligrar nuestra vida o nuestra integridad personal.
- En las carreteras, ponemos nuestra vida en juego cada vez que montamos en un vehículo, siendo a veces los causantes de los accidentes, otras siendo las víctimas de los errores de otros conductores.
- Incluso en el trabajo, dependiendo de la profesión desempeñada, es posible poner en riesgo la vida cada vez que se inicia la jornada.

¿Cómo es posible afrontar este riesgo continuo en nuestras vidas? Gestionándolo.

La gestión del riesgo es la disciplina que nos ayuda a sobrevivir. Aunque sea de manera inconsciente, en cada situación que pueda representar un riesgo potencial evaluamos cuál es el contexto, cuáles son nuestras expectativas y qué medidas de seguridad podemos aplicar. En función de la frecuencia con que se cumplen esas expectativas en ese contexto, se considera que las medidas de seguridad son adecuadas y que el riesgo está bajo control.

En definitiva, nos consideramos seguros cuando esperamos que nuestras expectativas se cumplan en una situación determinada. El cumplimiento repetido de nuestras expectativas refuerza nuestra sensación de seguridad.

Toda organización posee una serie de activos que debe proteger para la buena marcha de su actividad. De hecho, la seguridad suele definirse como «el resultado de alcanzar o superar continuamente los objetivos de la organización». La pérdida, robo, destrucción, disminución o daño de cualquiera de estos activos podría impedir que la organización alcance sus objetivos.

Entre los activos especialmente amenazados por las redes sociales en la Biblioteca 2.0 pueden señalarse los siguientes:

1. La información privada, que puede ser robada o utilizada en contra de su propietario para acosar, extorsionar o enviar publicidad hipercontextualizada.
2. La propiedad intelectual, que puede robarse o divulgarse sin pagar derechos, ocasionando pérdidas económicas.
3. La integridad física de empleados y de locales, que puede comprometerse por atacantes, criminales, acosadores y ladrones.
4. El acceso universal a la información, que puede verse amenazado en la medida en que la información migra a formatos digitales más difícilmente accesibles.
5. Los recursos computacionales y de red, que pueden consumirse con fines delictivos, originando pérdidas de servicio, degradación de la QoS y consecuencias legales derivadas de responsabilidad subsidiaria por daños a terceros.
6. La disponibilidad de la información en todo momento para quien la necesita.
7. La reputación de la biblioteca y del personal, que puede erosionarse o dañarse de forma irreparable.
8. La identidad digital de individuos de la biblioteca, que puede robarse o suplantarse.
9. Los activos financieros, que pueden malgastarse por una disminución en la productividad de los empleados.

En los siguientes apartados se revisarán cuáles son las amenazas o daños potenciales que pueden sufrir los activos anteriores como consecuencia del uso incontrolado de las redes sociales en la Biblioteca 2.0.

Privacidad: la biblioteca transparente

La propia naturaleza abierta, colaborativa y participativa de las nuevas aplicaciones Web 2.0 puede suponer una amenaza para la privacidad, en la medida en que el comportamiento de los usuarios de la Biblioteca 2.0 puede quedar expuesto a un número de usuarios mucho mayor del esperado. El uso de herramientas 2.0 deja por lo general un rastro que permite la **confección de perfiles personales**:

- En la Biblioteca 1.0 uno puede consultar libros y otros productos sin llegar a pedirlos en préstamo sin que quede registro alguno de ningún tipo. En la Biblioteca 2.0, en la medida en que las búsquedas dentro de las bases de datos de los catálogos sean públicas o puedan accederse de alguna manera, un atacante podrá averiguar cuáles son los intereses e inquietudes de los usuarios.
- En la Biblioteca 1.0 queda registrada la información de préstamos, a menudo en formato papel. Sin embargo, la Biblioteca 2.0 ofrece un catálogo mucho más amplio de productos y servicios. Como consecuencia, se puede saber qué tipo de información se consume: libros, música, archivos sonoros, comics, fotografías, vídeos, etc.; cuándo se consumen; e incluso desde dónde: lugar y tipo de dispositivo de acceso a Internet.
- En la Biblioteca 1.0 los usuarios comentan los productos que han consumido con otros usuarios o con los bibliotecarios, pero rara vez queda ningún registro. En cambio, en la Biblioteca 2.0 prácticamente todos los productos y servicios pueden comentarse, recomendarse y etiquetarse, lo que nuevamente deja un rastro de gustos y preferencias personales.

- En la Biblioteca 1.0 los usuarios raramente realizaban anotaciones, subrayados o marcas y en cualquier caso tras varios préstamos resultaba imposible atribuirlos a un usuario u otro. En la Biblioteca 2.0, que prima la colaboración y el acceso ubicuo, muchas de estas características quedarán unidas a los productos y servicios o podrán ser accedidos por un atacante.
- La información publicada por otros usuarios con referencias personales a otros usuarios resulta muy difícil de controlar: desde vídeos y fotografías, hasta comentarios y recomendaciones.

La Biblioteca 2.0 puede conducir a una biblioteca transparente, al estilo de los edificios de la distopía de Zamiatin, donde lo que hacen los usuarios en su interior queda a la vista de todos. Las redes sociales fomentan la transparencia absoluta. En la construcción de la Biblioteca 2.0 debe meditarse acerca del grado de transparencia necesario y especialmente y por encima de todo acerca de las herramientas de control de la propia privacidad por parte de los usuarios.

Propiedad intelectual: todo gratis

En la medida en que cada vez mayor cantidad de contenidos ofrecidos por las bibliotecas se digitalizan o se generan nativamente en formato digital, éstos se enfrentan a numerosas amenazas. La principal y más importante desde el punto de vista económico es la imposibilidad tecnológica de proteger los contenidos frente a copias ilícitas. Todo contenido digital se enfrenta al hecho de que puede ser y será copiado digitalmente. Un bit es un bit y como tal puede copiarse sin merma de calidad un número ilimitado de veces. No existe ni existirá ningún sistema de protección que impida la copia de estos productos. La distribución incontrolada de material protegido por derechos de autor ha conducido a muchos usuarios de Internet a considerar que todo lo que circula por Internet debe ser gratis. Esta concepción obligará a las bibliotecas e industrias asociadas a replantear sus modelos de negocio de una forma más acorde con las nuevas tecnologías. La Biblioteca 2.0 no despegará conservando estructuras comerciales que hoy han quedado obsoletas y chocan frontalmente con la forma de entender y vivir Internet por parte de las nuevas generaciones. Las redes sociales obviamente agravan este problema, ya que contribuyen a la difusión no autorizada del contenido protegido por derechos de autor.

Por otro lado, no hay que perder de vista que en la Biblioteca 2.0 el contenido no lo produce exclusivamente el proveedor tradicional: industria editorial, discográfica o filmográfica, etc. Los propios usuarios y bibliotecas serán además productores y consumidores de contenidos: lo que se conoce como la figura del *prosumidor*. Éste podrá generar y poner a disposición del público contenidos propios protegidos por las leyes de la propiedad intelectual: documentos escritos, archivos musicales, vídeos, software, etc., los cuales se enfrentan a su vez a varias amenazas.

En primer lugar, algunos usuarios descuidados o inconscientes podrían publicar con demasiada alegría contenidos protegidos por derechos de autor como parte integral de los suyos propios: fotografías, música, fragmentos de película, etc. Una vez distribuidos a través de las redes sociales, aunque posteriormente se retiren resultará imposible eliminar todas las copias fieles que han podido realizarse. Este tipo de generación de contenidos da origen a la cultura del *remix*, que abre de nuevo importantes interrogantes en cuanto al papel limitador de la creatividad del ejercicio a ultranza de los

derechos de autor clásicos. Nuevamente, la industria de contenidos necesita remodelar sus estructuras de negocio.

En segundo lugar, se sufre una pérdida de control sobre los contenidos publicados. En las licencias de uso de las plataformas sociales (que nadie lee detenidamente) se les ceden a menudo derechos draconianos de explotación de todo contenido digital publicado. Fue famoso el caso del grupo musical Artic Monkeys, el cual estuvo al borde de perder los derechos sobre sus propias canciones, al haberlas alojado en MySpace para darse a conocer en sus comienzos.

Por último, resulta muy complicado, si no imposible, eliminar o alterar información, fotos, vídeos, etc., colgados por terceros.

Nuevamente, el éxito de la Biblioteca 2.0 reside en la creación de herramientas de control de la privacidad y de los contenidos.

Integridad física: ahora estoy aquí, luego estoy allí

Las redes sociales pueden también comprometer indirectamente la seguridad física de sus usuarios. Por un lado, los usuarios a menudo revelan, voluntariamente o no, gran cantidad de información sobre su localización física en todo momento. Para saber dónde está, ha estado o estará una persona se puede acudir a numerosas fuentes de información.

Las fotografías publicadas pueden incorporar metainformación de geolocalización a partir de coordenadas GPS. También existen las técnicas de recuperación de imágenes basada en el contenido (Content Based Image Retrieval, CBIR), las cuales pueden reconocer en una fotografía el lugar donde ha sido tomada comparándola con grandes bases de datos de imágenes geográficas y de interiores en sitios públicos. Al margen de las fotografías, algunos usuarios actualizan continuamente su perfil con información sobre lo que están haciendo, incluyendo los lugares en los que se encuentran o a los que van, lo que facilita su localización actualizada.

El hecho de revelar alegremente la posición, a veces con todo lujo de detalle, junto con otra información como dirección del hogar o teléfono, agenda detallada con la planificación de actividades o el estado de conexión en línea continuamente actualizado, pueden facilitar el acoso, especialmente en colegios y universidades y otros centros de estudio similares. Algunas redes como Twitter tienden a enfatizar aún más la localización: los usuarios informan a cada momento de dónde están y qué están haciendo. Este acoso puede quedarse en el mundo online o puede trasladarse al mundo físico.

Marginación digital: no sabe/no contesta

Muchos de los servicios de la Biblioteca 2.0 estarán disponibles exclusivamente para aquellos usuarios poseedores de dispositivos conectados a Internet y con un aprendizaje adquirido en su manejo. En consecuencia, existen grandes colectivos que no podrán disfrutar de muchas de las ventajas de la Biblioteca 2.0:

- Las personas con discapacidades para quienes estas aplicaciones resulten inaccesibles o de muy difícil accesibilidad.

- Las personas «analfabetas digitales», para quienes se está ampliando drásticamente la brecha digital que las separa de las nuevas generaciones «conectadas».
- Las personas con escasos recursos económicos que no pueden permitirse ordenadores o dispositivos móviles conectados a Internet.

Resulta fundamental impulsar la creación de una Biblioteca 2.0 accesible, que cumpla con los estándares y legislación vigente en materia de accesibilidad. Todas las webs de las administraciones públicas españolas están obligadas a adoptar «las medidas necesarias para que la información disponible en sus respectivas páginas de Internet pueda ser accesible a personas con discapacidad y de edad avanzada». Además, aunque no se vieran obligados a ello por ley, los sitios pueden cumplir la norma UNE 139803:2004 «Aplicaciones informáticas para personas con discapacidad. Requisitos de accesibilidad para contenidos Web».

Deberá primarse asimismo la facilidad de uso en todo tipo de dispositivos, fijos y móviles.

Recursos computacionales y de red: al servicio del crimen organizado

Es de todos sabido que hoy en día la creación del malware ha quedado en manos de cibercriminales con el propósito de obtener beneficios económicos. ¿De qué manera puede ganarse dinero con el malware? Los ordenadores controlados por el hacker normalmente se integran dentro de botnets: grandes redes formadas por ordenadores personales comprometidos. Estas botnets pueden usarse con múltiples fines muy lucrativos: enviar mensajes de phishing para robar información financiera, enviar mensajes de spam anunciando productos y a menudo animando a la instalación de malware, cometer fraude en campañas publicitarias donde se cobra dinero por cada clic recibido en enlaces, realizar ataques distribuidos de denegación de servicio que interrumpen la operación de servidores en Internet, etc.

El spam y la distribución de malware están creciendo rápidamente en las redes sociales: explotan los recursos computacionales y de red de una organización (disco duro, tiempo de CPU y ancho de banda) para beneficio económico del ciberatacante. El hecho de que las redes sociales usan como soporte las tecnologías web, también las hace vulnerables a todos los ataques típicos en la Web 2.0, entre los que destacan los recientes gusanos de XSS, como Koobface o Mikeyy Mooney, y las aplicaciones o widgets maliciosas, como Secret Crush para Facebook.

Las bibliotecas han sido en los últimos años un lugar típico de acceso gratuito a Internet, poniendo ordenadores conectados a disposición de los usuarios. Es necesario extremar las precauciones en la detección de malware ejecutándose en los mismos, ya que hoy en día el objetivo no es la mera molestia, sino el robo de información financiera y personal de los usuarios. Y en la Biblioteca 2.0 es muy posible que exista mucha cantidad de ambas.

Disponibilidad: siempre y en todo momento

Cuando cada vez más bienes y servicios se adquieren o disfrutan a través de Internet, se produce una progresiva dependencia hacia la disponibilidad de los servicios de acceso. Por un lado, la migración de servicios hacia la nube facilita muchas labores de administrativas, como la gestión de copias de

seguridad, pero por otro va aumentando la dependencia. Las bibliotecas deberán buscar los mecanismos para asegurar que sus bienes y servicios se pueden ofrecer de forma ininterrumpida a cualquier hora del día o de la noche y en cualquier época del año.

A diferencia de la Biblioteca 1.0, con sus rígidos horarios de atención al público, la Biblioteca 2.0 debe abrir sus puertas ininterrumpidamente, lo que plantea nuevos retos más exigentes.

De hecho, muchos de sus contenidos ni siquiera serán descargados en los dispositivos de los usuarios, sino que serán visualizados en streaming, agravándose por tanto los problemas de demanda de ancho de banda y de disponibilidad cuando muchos usuarios los solicitan simultáneamente.

Reputación: me fío/no me fío

La reputación permite que los usuarios se formen expectativas sobre el comportamiento de una persona u organización basándose en el juicio de terceros, lo que reporta grandes beneficios económicos y sociales al poderse confiar en otros a los que no se conoce directamente. En los últimos tiempos, la reputación electrónica se está convirtiendo en un activo tan valioso como la reputación tradicional.

En aquellas redes sociales en las que la barrera de creación de nuevas identidades es prácticamente nula pueden crearse numerosas identidades ficticias en lo que se conoce como ataque de Sibila (una mujer que sufría desorden de personalidad múltiple), las cuales pueden utilizarse para orquestar campañas automatizadas de erosión de la reputación de un tercero.

Cualquier usuario puede publicar injurias y calumnias, con el agravante de que la publicación se realiza en sitios web públicos que pueden ser libremente indexados por los buscadores de Internet. La accesibilidad y visualización de estos contenidos aumenta así exponencialmente, agravándose el daño a los derechos de los usuarios.

De hecho, cuando el atacante es capaz de lanzar ataques de reputación contra un blanco, puede extorsionarle con el fin de obtener dinero o alguna otra ventaja a cambio de no realizar el ataque. Otra amenaza consiste en la colusión, cuando varios usuarios se alían para dañar la reputación de un tercero.

Las organizaciones con fuerte presencia en redes sociales también se enfrentan al riesgo del borreguismo o seguimiento de la masa a líderes o polarizadores de opinión: personas influyentes pueden hablar mal de un servicio o producto, condicionando negativamente a miles de seguidores.

Por otro lado, una falta de presencia en redes sociales o una presencia pobre, puede ser percibida por los usuarios habituales de las redes sociales de forma muy negativa. Este tipo de usuario hiperconectado no se acercará posiblemente a las bibliotecas que no sean 2.0 y aun entre éstas visitará más asiduamente aquellas que sean «más 2.0». La pasividad ante las redes sociales puede erosionar la reputación de las bibliotecas que no salten al vagón de la Biblioteca 2.0 frente a las que sí.

Identidad digital: en Internet nadie sabe que soy un perro

La Wikipedia define la identidad digital como la representación digital de un conjunto de afirmaciones realizadas por un sujeto digital sobre sí mismo o sobre otro sujeto digital.

Una amenaza terrible es la facilidad con que pueden crearse perfiles falsos sin ningún tipo de verificación. ¿Qué hace falta para crear un perfil en Facebook sobre un usuario? Nada, basta con una dirección de correo que puede obtenerse anónimamente en cualquier sitio. Se añade una foto del usuario, la cual podría seguramente obtenerse en Internet, y una dirección de correo de Gmail que incluya su nombre y apellido, y ya está listo un perfil capaz de suplantar a cualquier persona.

Otra forma de robar la identidad de un usuario consiste en acceder directamente a su cuenta, por ejemplo robándole sus credenciales a través de ataques de phishing. Como no podía ser de otra manera, también se están popularizando los ataques de phishing contra redes sociales como por ejemplo Facebook y Twitter. Además, estos ataques suelen estar muy contextualizados, lo que se conoce como *spear phishing*, ya que puede obtenerse gran cantidad de información sobre el usuario a partir de su perfil, lo que permite crear mensajes altamente personalizados en los que las víctimas confían ciegamente. Aunque con menor frecuencia, también se han producido casos en los que hackers pudieron hacerse con las bases de datos de usuarios y, por tanto, pudieron suplantar potencialmente a cualquier usuario.

En enero de 2009 las cuentas de Twitter de 33 celebridades, entre las que se encontraban Britney Spears o Barack Obama, tuvieron que ser suspendidas durante un tiempo tras haber sido secuestradas y comenzar a facilitar información falsa. Mientras la autenticación de los usuarios siga realizándose a través de un nombre de usuario y una contraseña, los ataques de suplantación de identidad serán una realidad difícil de combatir.

La Biblioteca 2.0 se enfrenta aquí al reto de conseguir formas de autenticación robustas, difíciles de suplantar, como por ejemplo el DNIe, pero que a la vez gocen de gran aceptación entre los usuarios, como las contraseñas. Un dilema difícil de resolver.

Activos financieros: un iPhone gratis

Las redes sociales se han convertido en vehículo predilecto de timos y fraudes. El spam se está extendiendo por las redes sociales, con el agravante de que la información publicada en los perfiles permite una hipercontextualización ausente en el correo masivo tradicional. Además, los mensajes pueden parecer proceder de contactos y amigos, lo que baja las defensas psicológicas de las víctimas. También es frecuente el envío de enlaces acortados, lo que impide conocer a priori a dónde se acude al hacer clic sobre ellos, y ser redirigido a sitios pornográficos o publicitarios, diseñados para vender algo. También se envían invitaciones de amigo procedentes de perfiles ficticios muy atractivos, que están luego atiborrados de enlaces a sitios publicitarios. También es frecuente enviar spam a los campos de comentarios con referencias a la empresa o producto o inundar con mensajes las redes de microblogging, como por ejemplo usando los temas de Twitter Trends, modelo adoptado del BlackHat SEO. Estos hiperenlaces conducen típicamente a sitios web de descarga de malware.

Por supuesto, también existen numerosos anuncios que ofrecen productos o servicios fraudulentos, por ejemplo explicando en la letra pequeña del contrato que los SMS recibidos se pagarán a un precio de 1,5 € la unidad.

Conclusión

Las redes sociales están aquí para quedarse. Traen consigo innumerables ventajas, pero también nuevos problemas y desafíos. Conocer las amenazas ayuda a saber a qué hay que enfrentarse. El análisis de riesgos no busca atemorizar con la exposición de los peligros, sino antes al contrario, ayudar a tomar decisiones razonadas basadas en el conocimiento preciso de estos peligros.

Se abre una nueva era para las bibliotecas: Biblioteca 2.0 sí, pero con seguridad.