

**Recepción:** 20 de marzo de 2015

**Aceptación:** 24 de marzo de 2015

**Publicación:** 26 de marzo de 2015

# USO RESPONSABLE DE LAS TIC POR UNIVERSITARIOS DE ESCUELAS TÉCNICAS

---

## RESPONSIBLE USE OF ICT BY STUDENTS OF TECHNICAL SCHOOLS IN THE UNIVERSITY

José Ramón Díaz Sáenz<sup>1</sup>

Hermenegildo Gil Gómez<sup>2</sup>

Raúl Fco. Oltra Badenes<sup>3</sup>

Juan Vicente Oltra Gutiérrez<sup>4</sup>

1. Ingeniero de Telecomunicación, por la Universidad Politécnica de Madrid. Doctorando en ITIO – UPV. España. E-Mail: [jrdiaz@iies.es](mailto:jrdiaz@iies.es)
2. Profesor Titular del Dpto. de Organización de Empresas en la Universidad Politécnica de Valencia. España. E-Mail: [hgil@ai2.upv.es](mailto:hgil@ai2.upv.es)
3. Profesor Asociado del Dpto. de Organización de Empresas en la Universidad Politécnica de Valencia. España. E-Mail: [rauloltra@doe.upv.es](mailto:rauloltra@doe.upv.es)
4. Profesor Titular del Dpto. de Organización de Empresas en la Universidad Politécnica de Valencia. España. E-Mail: [jvoltra@omp.upv.es](mailto:jvoltra@omp.upv.es)

## RESUMEN

Esta investigación muestra el nivel de seguridad que asumen los alumnos de Ingeniería de Telecomunicación y de Informática de la Universidad Politécnica de Valencia, como estudiantes con asignaturas técnicas sobre la utilización de sistemas digitales de comunicación, al utilizar recursos informáticos para navegar por internet.

Los resultados obtenidos muestran la importante brecha existente entre lo que han estudiado para poner en práctica en su vida diaria y como se comportan realmente.

## ABSTRACT

This research shows the level of security that take students of Telecommunications Engineering and Computer Science from the Polytechnic University of Valencia, as students with technical courses on the use of digital communication systems, using computer resources to internet browsing.

The results show the significant gap between what they have studied to implement in their daily lives and how they actually behave.

## PALABRAS CLAVE

TIC; Internet; Seguridad; Redes sociales; Aprendizaje

## KEYWORDS

ICT; Internet; Security; Social networking; Learning

## INTRODUCCIÓN

Miguel Angel Davara (2000) nos dice que *“todo el mundo navega por Internet aunque, irónicamente, puede decirse que, como mucho, flotan en la Red, porque para navegar hace falta rumbo y los incontrolados accesos a Internet son, si me apura, un flotar a la deriva”*. El problema puede surgir de la inseguridad que proporciona la duda y el desconocimiento debido a una falta de formación y adaptación de métodos y medios.

El Observatorio de la Seguridad de la Información, integrado en INTECO (2009), aconseja que se mantengan niveles educativos que favorezcan la implantación de medidas para garantizar una navegación más segura.

Entre las recomendaciones emanadas por la Agencia Española de Protección de Datos, encontramos directrices para los usuarios sobre contraseñas, mensajes de desconocidos, descargas no identificadas, actualización de antivirus, etc. (AEPD, 2009).

Con mucha frecuencia surgen problemas de seguridad como consecuencia del exceso de confianza al aportar información personal a las redes sociales (Urueña, 2011).

Aparecen riesgos al dejar rastros de nuestra actividad, tales como viajes, vacaciones, fotos, datos geoetiquetados, etc. que facilitan ser víctimas de delincuentes (ladrones, extorsionadores, acosadores...). INTECO (2010).

Incluso se expresan abiertamente opiniones políticas, tendencias sexuales o creencias religiosas.

Como etapa inicial para abordar un estudio sobre el riesgo asumido por usuarios en la navegación por redes sociales, donde se publica información accesible en función del perfil previo definido, decidimos averiguar si se ponían en práctica los conceptos básicos sobre seguridad (limitación de accesos, adopción de contraseñas, instalación de antivirus y firewalls, generación de copias de seguridad, etc.).

Basándonos en los resultados de una tesina del Máster CALSI (2009) sobre seguridad en la Web 2.0 observamos que los conocimientos, sensibilidad y actuación de los alumnos de primer curso de la Licenciatura de Comunicación Audiovisual eran muy preocupantes. Podía deberse a su reciente acceso a la Universidad, a una formación en el uso del PC mayoritariamente autodidacta o a que, procedentes de Humanidades, estaban menos familiarizados con las potencialidades y riesgos del uso de unas tecnologías sobre las que tenían poca formación y en las que no estaban muy seguros.

Decidimos profundizar un poco más en la situación real estudiando una población que no está alejada (Informática y Telecomunicación) de los estudios más relacionados con el tema que nos ocupa.

## OBJETIVOS

Vamos a investigar los posibles riesgos de seguridad informática que asumen los estudiantes de la Universidad Politécnica de Valencia más especializados en el tratamiento digital de datos cuando acceden a Internet, para comprobar el nivel de aplicación en la vida diaria de los conocimientos adquiridos sobre esta materia.

El comportamiento que los alumnos tienen en cuanto a medidas de seguridad a adoptar cuando utilizan ordenadores se fundamenta en estos aspectos:

1. Su ambiente sociocultural.
2. Su ambiente curricular e institucional de sus antecedentes escolares y formación.
3. Las motivaciones, intereses y sentimientos que le produce la navegación y uso de estas herramientas.

Esto surge de la psicología educativa constructivista (Risnes, 1999) que afirma que la manera en cómo los alumnos conciben el aprendizaje y cómo se ven a sí mismos con respecto a su capacidad de aprender, puede influir en sus resultados. Estudiado por Alonso Tapia (2004) a través de un cuestionario que mide las metas, valores-intereses y expectativas.

En relación con las Estrategias de aprendizaje, Beltrán (1993) señalaba que los resultados de dicho aprendizaje están muy vinculados con el uso de estrategias cognitivas que son las que convierten el material enseñado en material aprendido. A su vez, García y Pintrich (1994) indicaban que el uso de este tipo de estrategias, no su conocimiento, está relacionado e influenciado por la motivación del propio estudiante.

## ANTECEDENTES TEÓRICOS

Jacqueline Eccles y Allan Wigfield (2002) desarrollaron de un modelo sobre las componentes del valor asociado a una actividad en el que suponían que tanto las expectativas como los valores son creencias cognitivas relacionadas con las decisiones que los sujetos toman de forma consciente sobre sus logros y que pueden influir sobre su comportamiento. Se trata de un modelo racional de toma de decisiones sobre la motivación.

Raquel Salim (2004, 2006) se basó en esos indicadores al estudiar los enfoques y motivaciones de aprendizaje de estudiantes universitarios.

Cuestionarios que tenían en cuenta esas características fueron usados por Baca (2005) en el estudio de los factores que influyen en el estudio de las matemáticas, así como por Sánchez (2009).

José G. Clavel y Javier Balibrea (2010) indicaban la importancia del estímulo que supone la motivación para la educación, definiendo los denominados intangibles de la educación (factores no cuantificables, inherentes al estudiante) y su influencia en el rendimiento académico, así como la forma en que son medidos por PISA.

Los profesores Marwick, Murgia Díaz y Palfrey (2010) estudiaron el riesgo con el que los jóvenes se comunican a través de redes sociales y sus motivaciones.

Hoofnagle *et al.* (2010) investigaron el comportamiento sobre privacidad en Internet de los jóvenes americanos.

La motivación por el uso de redes sociales también fue estudiada por Gómez-Borja (2011).

Melissa de Zwart y David Lindsay (2011) abordaron la complejidad que supone el uso de redes sociales en la comunicación y los problemas de seguridad y de riesgos legales entre estudiantes.

Los profesores Shi-Woei Lin y Yu-Cheng Liu (2012), han relacionado parámetros medibles del nivel de uso de las redes sociales con parámetros emocionales.

Jiang, Z. *et al.* (2013) también han realizado investigaciones sobre privacidad en Redes Sociales, referenciando estudios en USA.

## METODOLOGÍA DE INVESTIGACIÓN

Utilizaremos la encuesta social como fuente de información.

El objetivo de la encuesta, que es del cuestionario, es conocer si los alumnos encuestados son conscientes del riesgo que corren cuando acceden a las redes sociales y si tienen la inquietud suficiente (actitud) para intentar evitarlos, para lo que necesitan la formación suficiente (aptitud), no solo de los riesgos de acceder a esas aplicaciones sino también de la propia navegación por Internet y del manejo de los recursos utilizados, y si ponen en práctica esa formación, actuando en consecuencia.

Se hacen preguntas para cubrir cada tema del tipo explicativo, abiertas y cerradas (dicotómicas o Likert), introductorias, de control, de relleno y variables actitudinales para las motivaciones, sentimientos e intereses que produce el aprendizaje de temas de seguridad informática.

Comprobamos la actuación referente a conceptos básicos sobre seguridad (limitación de accesos, adopción de contraseñas, instalación de antivirus y firewalls, generación de copias de seguridad, publicar información y/o sincerarse, etc.).

La población encuestada estaba formada por los alumnos de segundo curso de la Facultad de Informática (curso 2011-2012). Se escogió esa población por no ser la más formada (alumnos de últimos cursos de carrera) pero si ya con una base suficiente como para actuar de una forma coherente y segura.

La investigación “de campo” realizada (encuesta) la complementamos con una investigación más documental o hemerográfica (basada en artículos y estudios en revistas y periódicos especializados), que nos permite confiar en la elección del método que hemos considerado más adecuado.

Hicimos dos pilotos previos para asegurar la idoneidad de la redacción de las preguntas de la encuesta así como el entendimiento de las mismas, que nos sirvieron para modificar, simplificar, reagrupar y ordenar el cuestionario definitivo. Se incluyeron preguntas de control (sobre protección de acceso al PC) para asegurar coherencias.

La encuesta definitiva se hizo vía Internet obteniendo directamente una hoja Excel ya codificada para su proceso con SPSS.

Dimos como válidos 204 cuestionarios, eliminando algunos por falta de coherencia en las preguntas de checking, o por falta de respuesta generalizada en muchas variables, o por edad fuera de rango.

Para el análisis descriptivo utilizamos tablas de frecuencias, medidas de tendencia central, de variabilidad, representaciones gráficas, etc.

Para el relacional, tabulaciones cruzadas, medidas de asociación y Alfa de Cronbach para las correlaciones, para corroborar la fiabilidad de los indicadores.

Los resultados estadísticos obtenidos referentes a calidad, explicación de las varianzas e indicadores de correlación obtenidos son muy altos, lo que indica la coherencia de las respuestas y la idoneidad del planteamiento.

En el proceso de los datos con SPSS, nos apoyamos en la metodología teórica tratada con diversas aportaciones como las de Marcos Cupani (2008) o Miguel A. Ruiz (2010) para facilitar el estudio de casos en general o la de Corral-Verdugo (1995) aplicada a temas de conducta. Así como las directrices que, para evaluación educativa, reseña Torres Fernández (2010).

Los resultados obtenidos aconsejaron su comparación mediante nueva encuesta realizada en el curso siguiente (2012-2013) a los alumnos de 2º curso de Informática y a un grupo de alumnos de primer curso de la ETSI Telecomunicación. Obteniendo 133 respuestas válidas tras eliminar las demás por razones similares a las comentadas anteriormente. Utilizamos la misma metodología y obtuvimos unos resultados que confirmaban la coherencia con los ya obtenidos con los alumnos del curso anterior.

## RESULTADOS

El análisis de las muestras que conformaron los pilotos no eran significativas (<50 sujetos y con escasa proporción sujetos / variables) pero encontramos algunos detalles de frecuencias con resultados muy parecidos a los reflejados en la tesina del Máster CALSI referenciado anteriormente. Tales como que la mayoría mantiene fijas las contraseñas en los diferentes accesos y ninguno las cambiaba con una frecuencia por debajo de los seis meses, además de que muchos no hacen copias de seguridad y desconocen el riesgo de conectarse vía Wifi.

Hicimos dos encuestas en cursos consecutivos para verificar si podía haber algún tipo de problema, falta de oportunidad o enfoque en la encuesta. En las Tablas siguientes se pueden ver los resultados comparativos.

**Tabla 1:** Frecuencias de alumnos que realizan funciones sobre uso de contraseñas.

Contraseñas	Password única	Siempre fijas	Cambio anual	Grabación por navegador	Nombres sencillos	No protección acceso a PC	Seguros
2011-2012	36%	72%	22%	27%	8%	33%	4,5%
2012-2013	44%	68%	25%	23%	11%	29%	3,8%

**Tabla 2:** Frecuencias de alumnos que realizan funciones sobre uso de backups<sup>2</sup>

Copias de seguridad	Nunca hizo	Al cambiar PC	Anual	Semestral	En PC	Disco externo	Actualización automática
Curso 2011-2012	15%	33%	21%	18%	5%	57%	9%
Curso 2012-2013	15%	29%	15%	23%	3%	57%	16%

Un parámetro utilizado para conocer el porcentaje de alumnos que protegen su privacidad fue saber si se preocupan por la eliminación periódica de las cookies que se almacenan en el PC tras navegar por Internet. El resultado obtenido fue que el 38,6% del total de alumnos de los dos cursos no se preocupan por hacerlo (37,3% del curso 11-12, y 40,1% del 12-13).

1

- **Password única** implica una única contraseña para la mayoría de accesos
- **Siempre fijas** se refiere a no cambiarlas a lo largo del tiempo
- **En grabación por navegador** el propio sistema, de forma automática, las genera
- **Nombres sencillos** son contraseñas fáciles de adivinar
- **La no protección de acceso al PC** significa que es libre, sin contraseña para la sesión
- **Seguros** son los que utilizan nombres complejos, diferentes, y cambian con frecuencia

2

- **Nunca hizo** significa que no hacen copias de seguridad en ningún caso
- **Al cambiar de PC** es el porcentaje que hace copia en ese caso
- **En PC** indica el alojamiento en el que guardan las copias
- **Disco externo** es el alojamiento de las copias
- **Actualización automática** implica disponer de un sistema que se encarga de hacerlo



Vemos que los resultados obtenidos con los alumnos del curso 2011-2012 son de un orden de magnitud similar a los resultados obtenidos en el curso siguiente, lo que demuestra su coherencia.

**Tabla 3:** Correlación entre funciones de defensa que realizan los alumnos y Estadísticos básicos

	antivirus y firewall (*)	Archivos temp/histórico pgs. (**)	Significatividad	Explicación de varianza	Alfa de Cronbach	KMO
Curso 2011-2012	0,64	0,75	1%	85%	0,77	0,6
Curso 2012-2013	0,741	0,809	1%	89%	0,746	0,553

(\*) La correlación entre los que tienen activos antivirus y firewall, contribuyen a la autoprotección

(\*\*) La correlación entre los que eliminan archivos temporales y el histórico de páginas visitadas, conforman la idea de privacidad

**Tabla 4:** Frecuencias de los que realizan funciones sobre normas básicas de seguridad<sup>3</sup>

	Abren mails desconocidos	Despreocupación por vulnerabilidades	Info x amigos
Curso 2011-2012	24%	16%	26%
Curso 2012-2013	27%	12%	26%

**Tabla 5:** Frecuencias de alumnos que expresan contenidos a través de Redes Sociales<sup>4</sup>

Navegar x SNS	Info amistosa	Expresión libre	Aceptan sin leer conds.
Curso 2011-2012	45%	45%	62%
Curso 2012-2013	32%	47%	63%

3

- **Abren mails de desconocidos** para averiguar lo que pretenden
- **No tienen preocupaciones por vulnerabilidades** de seguridad
- **La información sobre vulnerabilidades** de seguridad se la cuentan **los amigos**

4

- **Información amistosa** es la personal (viajes, fotos, fiestas, composiciones propias....).
- **Expresarse libremente** implica manifestar opiniones políticas, religiosas, sexuales....
- **Aceptan sin leer condiciones** de registro, dando por suficientes las ofertadas por defecto.

## CONCLUSIONES

Los resultados de los alumnos encuestados del curso 2011-2012 fueron muy preocupantes al comprobar lo descuidados con la protección de sus accesos, datos y actividades que pueden ser los alumnos de Informática.

Ofrecen información suficiente como para que sea necesario revisar el proceso de aprendizaje y la necesidad de incrementar las precauciones para disminuir los riesgos de seguridad y privacidad.

Un tercio de los alumnos tiene una única contraseña para todos sus accesos y la misma proporción no tiene contraseña para iniciar la sesión de su PC, con riesgo para su privacidad.

Lo mismo ocurre con la protección de la disponibilidad de los datos. Es inadmisibles que una séptima parte de este tipo de estudiante no haya hecho nunca una copia de seguridad y una tercera parte lo haga solo cuando cambia de ordenador.

En la navegación por redes sociales no tienen la conciencia del escaparate en el que están y que un 45% hable libremente de sus intimidades personales, sexuales, políticas, religiosas es comprometer su futuro profesional, y puede que personal, sin ser conscientes de ello y pretendiendo ser profesionales tecnológicos.

Comparando con el estudio de la Universidad de Taiwán, teniendo en cuenta la distancia física, cultural, perfil de encuestados por edad y por selección, llegamos a converger en aspectos como la intensa correlación entre la frecuencia de navegación por redes sociales y la revelación de información (0,499 versus 0,437, en ambos casos con significatividad <1%).

También coincidimos en la afirmación de Shi-Woei Lin (2012) cuando dice: “nuestros resultados indican que la confianza puede efectivamente mitigar la preocupación de un usuario por su privacidad” pues encontramos una fuerte correlación entre los parámetros con los que nosotros hemos definido ambos conceptos (0,327, con significatividad <1%).

Jiang, Z. *et al.* (2013) ya indicaban que entre el 43 y el 51% de los encuestados dan información personal (domicilio, e-mail, creaciones personales, fotos, vídeos, asociaciones, opiniones) en las Redes Sociales. Marwick, Murgia Díaz y Palfrey (2010) referencian estudios en los que el 47% de jóvenes incluyen información de “comportamiento de riesgo” asociado a actividades sexuales, consumo de alcohol y drogas. Estas conclusiones obtenidas de investigaciones previas se corresponden con lo encontrado en nuestro estudio (45-47%).

Estos últimos investigadores referencian estudios de 2006 donde el 64% de jóvenes usuarios de Redes Sociales mantiene la configuración de privacidad que, por defecto, proporciona la plataforma, frente al 62-63% obtenido por nosotros para cada curso.

En nuestra investigación, un 38,6 % de los estudiantes no se preocupaba por eliminar cookies, coincidente con el 38% del estudio realizado por Hoofnagle y otros (2010).

Es recomendable crear un plan de formación específico sobre uso y riesgo de las herramientas informáticas más habituales de forma que se consiga concienciar al alumnado

en el sentido de que por mucho que se trabaje, si no se protege ese trabajo, puede perderse en su totalidad.

En esta línea tendría mucho sentido proponer una formación transversal sobre seguridad en una asignatura específica o coordinada entre varias asignaturas en los primeros cursos de carrera con muchos ejemplos prácticos de incidencias, abusos, experiencias, contratiempos, perjuicio, etc., de forma que facilite el interés de las medidas a adoptar para no perder información, arriesgar su privacidad, o poder ser víctimas de fraudes.

## REFERENCIAS BIBLIOGRÁFICAS

- AEPD (2009). *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Agencia Española de Protección de Datos <<http://www.inteco.es/file/vuiNP2GNuMinSjvyZnPW2w>><sup>5</sup>
- ALONSO TAPIA, J. (2005). *Motivaciones, expectativas y valores-intereses relacionados relacionados con el aprendizaje: el cuestionario MEVA*. Universidad Autónoma de Madrid. <<http://www.psicothema.com/psicothema.asp?id=3120>>
- BACA LOBERA, G. (2005). *La modelización con ecuaciones estructurales en la investigación operativa*. Producción Económica 2005, 2010, 17pp., UAX-Xochimilco. Méjico.
- BELTRÁN, J. (1993). *Procesos, estrategias y técnicas de aprendizaje*. Madrid: Síntesis.
- CALSI (2009). *Análisis de seguridad de la web 2.0, en alumnos de la UPV*. Trabajo Final de Máster de José Ramón Díaz Sáenz. Valencia. Universitat Politècnica. <<http://riunet.upv.es/handle/10251/14401>>
- CORRAL-VERDUGO, V. (1995). *Modelos de variables latentes para la investigación conductual*. Universidad de Sonora-Hermosillo
- CUPANI, M. (2008). “Análisis de Ecuaciones Estructurales: conceptos, etapas de desarrollo y un ejemplo de aplicación”, en *Revista Tesis Psicología*, 1, 164-176
- DAVARA, M.A. (2000). “El Humanismo Tecnológico”, en *Diario del Navegante* del 4 de marzo de 2000, página 1. Director del Instituto de Informática Jurídica de la Universidad de Comillas y asesor legal de la UE para TIs <[http://www.elmundo.es/navegante/2000/05/03/davara\\_humanismo.html](http://www.elmundo.es/navegante/2000/05/03/davara_humanismo.html)>.
- De ZWART, M. y LINDSAY, D. (2011). *Teenagers, Legal Risks and Social Networking Sites*. Monash University, en Victoria (Australia),
- ECCLES, J.; WIGFIELD, A.(2002). *Motivational beliefs, values, and goals*. University of Michigan.
- GARCÍA y PINTRICH (1994). *Regulating motivation and cognition in the classroom: The role of self-schemas and self-regulatory strategies*. Hillsdale, NJ England: Lawrence Erlbaum Associates, pp.127-154
- GARCÍA CLAVEL, J., y BALIBREA, J. (2010). *Motivación y rendimiento académico. Los intangibles de la educación*. Universidad de Murcia
- GÓMEZ-BORJA, M. A. (2011). *Redes sociales virtuales, ¿de qué depende su uso en España?* Universidad de Castilla-La Mancha.

<sup>5</sup> Todas las URLs que aparecen en la reseña bibliográfica han sido consultadas el 12-III-2015

- HOOFNAGLE, C. et al (2010). *How different are young adults from older Adults when it comes to information privacy attitudes & policies?*. Universidad de Berkeley.
- INTECO (2009), *Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles*. Instituto Nacional de Tecnologías de la Comunicación
- INTECO (2010). *Cuaderno de notas del Observatorio. Seguridad de la Información y Redes Sociales*. Instituto Nacional de Tecnologías de la Comunicación <[www.inteco.es/file/gt1clfwY4jEGEiZI7GiXgQ](http://www.inteco.es/file/gt1clfwY4jEGEiZI7GiXgQ)>
- JIANG, Z.; SUANG, C., CHOI, B. (2013). "Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions". *Information Systems Research*, volumen 24, nº 3 de septiembre 2013. Páginas 579-595. Dptº Sistemas de Información, de la Universidad Nacional de Singapur
- MARWICK, A., MURGÍA DÍAZ, D., PALFREY, J. (2010). *Youth, privacy and reputation*. Harvard University
- RISNES, A. (1999). "School Background, Motivational Belief and Achievement in Mathematics". *Proceedings of the Twenty First Annual Meeting Phychology of Mathematics Education*.
- RUIZ, M. A., PARDO, A., San MARTÍN, R. (2010). "Modelos de Ecuaciones Estructurales", en *Papeles del Psicólogo - Redalyc*
- SALIM, R. (2004). *Herramientas de evaluación de enfoques de aprendizaje en estudiantes unversitarios*. Universidad Nacional de Tucumán.
- SALIM, R. (2006), *Motivaciones, enfoques y estrategias de aprendizaje en estudiantes de Bioquímica de una universidad pública argentina*. Universidad Nacional de Tucumán.
- SÁNCHEZ GUEVARA, I. (2009). *Ecuaciones Estructurales en la Enseñanza-Aprendizaje de Matemáticas*. Dptº de Política y Cultura.Universidad Autónoma Metropolitana Xochimilco, de México
- SHI-WOEY LIN, YU-CHENG Liu (2012). "The effects of motivations, trust, and privacy concern in social networking", en *Service Business* 6:411-424. DOI 10.1007/s11628-012-0158-6. Departamento de Gestión Industrial de la Universidad Nacional de Ciencia y Tecnología, de Taiwán
- TORRES, P. (2010). "Modelos de Ecuaciones Estructurales". *El evaluador educativo*, nº 10, Año 1 – Junio <<http://www.cubaeduca.cu/medias/evaluador/junio2010-1.pdf> >
- URUEÑA, A. (2011). *Las redes sociales en internet*. Ontsi (Observatorio nacional de las telecomunicaciones y la Sociedad de la Información) <[http://www.ontsi.red.es/ontsi/sites/default/files/redes\\_sociales-documento\\_0.pdf](http://www.ontsi.red.es/ontsi/sites/default/files/redes_sociales-documento_0.pdf)>