PLAN DE PREVENCIÓN
DEL CIBERACOSO
Y PROMOCIÓN DE LA
NAVEGACIÓN SEGURA
EN CENTROS
ESCOLARES

Manual del buen uso de los medios informáticos.

Junta de
Castilla y León

Miembros del Equipo Interdisciplinar:

Fernando Sánchez-Pascuala Neira (Coordinador)
Viceconsejería de Educación Escolar

Teresa Barroso Botrán
Secretaría General

Jaime Álvarez Rodríguez
D.G. de Planificación, Ordenación e Inspección Educativa

José Luis Martín Sanz
Secretaría General

Antonio Pérez Cano
D.G. de Infraestructuras, Equipamiento y Servicios

Javier Fernández Sáez
D.G. de Calidad, Innovación y Formación del Profesorado

José Ignacio Recio Rivas
D.G. de Planificación, Ordenación e Inspección Educativa

Colaboradores externos:
Francisco Javier Gómez González
Cristina Durlan
Departamento de Sociología y Trabajo Social. Universidad de Valladolid

Apoyo y asistencia: Oficina Técnica Viceconsejería de Educación Escolar

Diseño y creación: Soldegato Laboratorio de Ideas S.L.L.

ÍNDICE

I. Introducción

I. INTRODUCCIÓN

El gran pensador liberal Ortega y Gasset aseguraba que no vivimos con la tecnología, sino que vivimos en ella. Este diagnóstico temprano, formulado a principios del siglo XX, se hace cada vez más real un siglo después, en un momento en que los ámbitos de aplicación y los impactos de la tecnología abarcan prácticamente todo el espectro de la vida social.

Según el informe anual sobre el desarrollo de la sociedad de la información en España1, realizado por la Fundación Orange, en el año 2007, más de 10,5 millones de hogares disponen de un ordenador personal, lo que representa casi un 60,4% del total de los hogares españoles.

Esta integración entre actividades humanas y tecnología también se ha producido en el ámbito de la educación, llegando a un punto en la cual hablar de Tecnologías de la Información y Comunicación (TIC) y de procesos educativos empieza a ser, cada vez más, hablar de una misma cosa, puesto que los sistemas educativos forman usando las TICs y, a su vez, forman para el uso de las TICs.

Consecuentemente, los sistemas educativos no sólo están obligados a adaptarse a los cambios tecnológicos, sino que tienen un enorme protagonismo en la generación de estos cambios y en la apropiación social de las tecnologías producidas.

Esta dinámica de integración de la tecnología en el entramado social y económico debe entenderse como un proceso secuencial, caracterizado por fenómenos muy diferenciados en cada una de las fases de desarrollo. Habitualmente, en los primeros momentos de implantación de una innovación, la cultura, las actitudes y los valores de uso no están todavía bien configurados, de manera que son frecuentes los riesgos de adicción y de dependencia, la posibilidad de indefensión o desregulación ante determinados riesgos que la tecnología genera, las actitudes de rechazo o la inflación de expectativas.

No obstante, esta política preventiva no debe caer en la tentación de la tecnofobia, en el pesimismo sobre la tecnología o la exageración de los riesgos. La idea de posponer, limitar o reducir el uso de la tecnología entre los jóvenes no es el escenario que debe orientar la actuación. El riesgo de la tecnofobia es grave, porque supone cerrarse al progreso y, además, porque es una actitud que no está justificada, se basa en estereotipos y, con frecuencia, es consecuencia de la brecha tecnológica que se establece entre las generaciones y que separa claramente a docentes y alumnos.

---

[1] Fundación Orange (2008): *E-España 2008. Informe anual sobre el desarrollo de la sociedad de la información en España.*

Frente a esta tecnofobia, se propone la tecnofilia constructiva, basada en un optimismo razonable sobre las aportaciones de las Nuevas Tecnologías y en una gestión responsable de sus posibles riesgos. Esta actitud se concreta en una educación para el uso autónomo de la tecnología, en una investigación sobre el potencial de los artefactos para el desarrollo de una educación personalizada y para el uso de todas las posibilidades que tiene la tecnología en el desarrollo profesional, ciudadano y personal de los alumnos.

Hoy en día, estos niños y jóvenes, están utilizando la tecnología de muchas formas, enriqueciendo así sus conocimientos con la variedad de instrumentos que se ofertan en la red. Con la aparición de las tecnologías Web 2.0 (tecnologías web que fomentan la colaboración on-line y el intercambio entre los usuarios), los jóvenes ya no son sujetos pasivos en el intercambio de la información virtual, sino que se transforman en creadores de contenidos digitales, utilizando así los instrumentos de software social. En su exploración de estas Nuevas Tecnologías, no solamente desarrollan sus competencias digitales, pero también desarrollan una multitud de competencias "más soft" –la creatividad, la comunicación y la capacidad de cooperar, entre otras -, competencias que serán muy demandadas en los futuros empleos.

El informe realizado por el Observatorio de las Telecomunicaciones y de la Sociedad de la Información[2], relativo a la infancia y la adolescencia en la sociedad de la información, determina una relación muy positiva entre los menores de 18 años y las Nuevas Tecnologías. En comparación con la relación que tienen los adultos con estas tecnologías, los menores de 18 años se ven más animados a probar los nuevos avances, se sienten más identificados con las tecnologías, a las que no consideran una barrera para la comunicación, y no les frena su posible complejidad de uso. Además, las consideran una herramienta útil en su desarrollo personal, ven más clara su utilidad que los adultos y muestran más interés por las mismas, aunque las consideren caras.

Otro estudio, elaborado por INTECO[3], concluye que el primer contacto con Nuevas Tecnologías, y más concretamente con Internet, se produce entre los 10 y 11 años. Este dato reivindica la tan utilizada y conocida expresión "nativos digitales", que fue acuñada por Marc Prensky en un ensayo titulado *La muerte del mando y del control*, y que describe a los estudiantes, menores de 30 años, que han crecido con la tecnología y que desarrollan una habilidad innata en el lenguaje y en el entorno digital. Para esta nueva generación, las Nuevas Tecnologías representan una parte central y clave en sus vidas, ya que dependen de

[2] Observatorio de las Telecomunicaciones y de la Sociedad de la Información (2005): *"Información y Adolescencia en la Sociedad de la Información".* Red.es.

[3] INTECO (2009): *Estudio sobre los hábitos seguros en el uso de las NUEVAS TECNOLOGÍAS por niños y adolescentes y e-confianza de sus padres*. Observatorio de la Seguridad de la Información.

ellas para realizar muchas actividades cotidianas como estudiar, relacionarse, comprar, informarse o divertirse.

Sin embargo, y a pesar de la aparente familiaridad de los jóvenes con esta nueva tecnología y de la sensación de control o inocuidad que experimentan, la red se desarrolla cualitativa y cuantitativamente en direcciones no siempre deseables, y a una velocidad que hace difícil el establecimiento de medidas mitigadoras de los posibles impactos perjudiciales sobre el crecimiento emocional y personal de los adolescentes. El informe INTECO, antes mencionado, determina también que 84,5% de los menores de 18 años son capaces de dar una respuesta, en cuanto a las medidas que toman, ante la incidencia de un riesgo de las Nuevas Tecnologías. El 15,5% restante ofrece respuestas como cerrar la conexión o salirse de la web o chat, negarse a hacer lo que le piden y pedir ayuda a los padres (sólo un 1,1% de los niños declara esta opción).

En cuanto a los padres, ellos siguen principalmente medidas de tipo físico o técnico (entendiendo por medidas físicas aquellas que implican una actuación sobre el equipo). En mucha menor medida, los padres mencionan medidas educativas y coercitivas. Las medidas educativas engloban aquéllas que implican el diálogo, la advertencia o la formulación de recomendaciones. Las medidas coercitivas implican el establecimiento de algún tipo de limitación o control (horario, supervisión…). Por último, sólo un 0,3% de los padres inicia acciones de denuncia ante las autoridades oportunas. Un 3% no hace nada, y más de un 16% no es capaz de dar una respuesta.

Sin duda, estas Nuevas Tecnologías conllevan nuevos riesgos, pero muchos autores están de acuerdo en que esta nueva generación también es capaz de auto regularse si está bien informada sobre los distintos niveles de riesgo. Las escuelas tienen el deber de enseñar a los niños y a los jóvenes a permanecer seguros cuando navegan en Internet, ya sea dentro del centro educativo o fuera.

Si los centros educativos empiezan a utilizar cada vez más estas Nuevas Tecnologías, reconociendo que sus beneficios educativos y sociales son mucho mayores que los peligros que engendran, la flexibilidad de su currículo se aumentará cada vez más.

II. Fundamentación

II. FUNDAMENTACIÓN

La comunicación entre ordenadores se ha configurado como una realidad joven, pero de profundo calado en una sociedad del conocimiento. Su rápida evolución transformó pronto las redes informáticas originales, de carácter militar, en redes universitarias para el intercambio de información científica. Desde estos usos instrumentales, y gracias a lo que pudo haberse concebido originariamente como un pequeño salto cualitativo hacia la adquisición de una dimensión social, se ha producido una expansión vertiginosa de esta red de ordenadores interconectados, alcanzando carácter internacional y un uso generalizado en los diferentes grupos de edad, aunque con un protagonismo especial de los más jóvenes, cuya alfabetización en estas tecnologías se ha realizado desde edades muy tempranas.

Las Nuevas Tecnologías de la Información y la Comunicación representan para los centros y procesos educativos, tanto una gran oportunidad de aprendizaje e innovación, como un grave riesgo de fomento del desarrollo de comportamientos disfuncionales y problemas de convivencia. Esta ambivalencia, característica de los desarrollos tecnológicos, anima a la necesidad de fomentar pautas de manejo y relación con la tecnología que potencien sus dimensiones positivas y atenúen o eliminen sus dimensiones negativas.

De esta manera, para dar respuesta a los impactos de la aparición de foros, programas de redes sociales y páginas web que pueden incrementar el riesgo de agresión o vejación al alumnado e incentivar el ciberacoso, la Consejería de Educación de la Junta de Castilla y León ha considerado de gran importancia la puesta en marcha de medidas especificas orientadas a fomentar el uso y manejo apropiado tanto de los artículos electrónicos de uso habitual en el alumnado (teléfonos móviles, reproductores MP3, consolas portátiles, etc.), como de los equipos informáticos de los centros educativos y los servicios de Internet.

En enero de 2009, el Procurado del Común de la Comunidad de Castilla y León ha emitido un escrito dirigido a la Consejería de Fomento, la Consejería de Familia e Igualdad de Oportunidades y la Consejería de Educación, referido a la protección de los menores de esta Comunidad frente a la aparición de foros y páginas web que puedan constituir formas de agresión o vejación entre alumnos e incentivar el ciberacoso, animando a la puesta en marcha de acciones concretas que garanticen la protección de los menores de esta Comunidad.

La extensión del ciberacoso y el carácter horizontal de este fenómeno ha hecho necesaria la aplicación de medidas que cuenten con la implicación de los diferentes órganos directivos de la Administración Educativa y la planificación conjunta de estrategias de coordinación e implementación en los centros educativos y de actuaciones tendentes a la reducción del acoso escolar mediante las tecnologías de la información y la comunicación. En este sentido, en la Comunidad de Castilla y León, durante el mes de octubre de 2008, se constituyó un Grupo de Trabajo Interdisciplinar, integrado por distintas unidades de la Consejería de

Educación, con el principal objetivo de diseñar y proponer actuaciones que den respuesta a esta problemática. La creación de este Grupo Interdisciplinar representa, por otro lado, la respuesta que ofrece la Viceconsejería de Educación Escolar a la Resolución del Procurador del Común sobre la protección de los menores de edad en Internet.

Este Grupo de Trabajo, cuya coordinación se ha realizado desde la Viceconsejería de Educación Escolar, ha elaborado, a través de varias reuniones desarrolladas durante los meses de noviembre - diciembre 2008 y enero – marzo 2009, una serie de estrategias clave para la prevención del ciberacoso y la promoción de la navegación segura en los centros escolares.

Los principales objetivos de estas estrategias se configuran en torno a las siguientes acciones:

a) Fomentar el uso seguro de los medios informáticos en los centros educativos, promoviendo hábitos y modelos de manejo que eliminen los impactos negativos de su uso y garanticen el bienestar de los usuarios y su optimización como recursos de aprendizaje.

b) Promover hábitos de prevención y procedimientos que garanticen la seguridad de los miembros de la comunidad educativa y eliminen situaciones de ciberacoso o acceso a contenidos inapropiados y potencialmente peligrosos.

c) Incrementar la dotación de recursos e información para gestionar los procedimientos de seguridad informática.

Para la consecución de los anteriores objetivos, se ha planteado un modelo de intervención que se fundamenta en los siguientes principios metodológicos:

1. Carácter interdisciplinar. La participación de representantes de diferentes planteamientos técnicos y disciplinares es la base tanto de las actuaciones, como de los grupos de trabajo constituidos para el diseño y desarrollo de las medidas.
2. Carácter transversal basado en la cooperación interinstitucional.

Así mismo, la metodología utilizada para la elaboración de los distintos materiales ha asumido como propios los siguientes principios metodológicos:

Incremento de la periodicidad del análisis del entorno, debido a la velocidad de los cambios sociales y tecnológicos.

Elaboración de diagnóstico de las dimensiones normativas, técnicas, educativas, sociales y psicológicas de los problemas.

Comparación de la situación de Castilla y León con su entorno de referencia, evaluando las actuaciones más avanzadas en prevención y fomento de la seguridad en Castilla y León.

Definición clara de comportamientos no deseados y contenidos no recomendados por su carácter explícitamente pornográfico, xenófobo, misógino, violento, o susceptible de causar un efecto negativo en el desarrollo personal o social del alumnado o afectar a la convivencia en el centro.

Determinar y fomentar la asunción de responsabilidades de prevención mediante la asignación de medios y recursos para el cumplimiento de los objetivos.

Elaboración de protocolos que muestren el papel activo de la Consejería de Educación en este campo, definiendo claramente las responsabilidades de los agentes implicados en la comisión de un posible delito de ciberacoso.

En este sentido, este Grupo Interdisciplinar ha propuesto, para una mayor operativización de las estrategias elaboradas, la publicación del presente manual, como una firme apuesta de la Consejería de Educación por una educación equitativa y adecuada a la nueva sociedad del conocimiento.

III. Antecedentes

III. ANTECEDENTES

La Junta de Castilla y León siempre ha expresado su gran interés en el fomento y la integración de las Tecnologías de la Información y Comunicación en varios foros y a través de varios manifiestos, no sólo por su extraordinario impacto en la educación, sino por su carácter transversal y por la incidencia que tiene en la práctica totalidad de la vida social.

Es evidente que estas Nuevas Tecnologías tienen un gran impacto en la economía, en los aspectos laborales, sociales y culturales. Desde esta óptica, desde la Junta de Castilla y León se ha realizado un gran esfuerzo para la promoción de la sociedad de la información y el conocimiento como objetivo prioritario de la estrategia de situar a esta región entre las más avanzadas y competitivas de Europa.

A continuación, y a modo de esquemas, se presentan algunas de las iniciativas desarrolladas en Castilla y León relacionadas con este tema.

ESTRATEGIA REGIONAL PARA LA SOCIEDAD DIGITAL DEL CONOCIMIENTO DE CASTILLA Y LEÓN PARA EL PERIODO 2007-2013

El Consejo de Gobierno del día 10 de mayo de 2007 aprobó la nueva Estrategia Regional para la Sociedad Digital del Conocimiento de Castilla y León para el periodo 2007-2013.

Hasta ahora, la planificación estratégica de la Junta de Castilla y León en materia de Sociedad de la Información ha estado contenida en la Estrategia Regional de Sociedad de la información 2003-2006 y el Plan Director de Infraestructuras y Servicios de Telecomunicaciones 2004-2006.

Los programas de la Estrategia se dirigen a todos Ciudadanos (especialmente a los de mayor riesgo de exclusión digital); Empresas (especialmente Pymes y micropymes) y Administraciones, así como al medio rural y a las ciudades. Se enumeran muy someramente las líneas estratégicas:

PLAN DIRECTOR DE TELECOMUNICACIONES: *Garantizar infraestructuras y servicios de telecomunicación asequibles y de calidad, haciendo hincapié en aquellos vinculados con el acceso a la información y el conocimiento, y garantizando el acceso igualitario en los territorios con menor capacidad de demanda. Las iniciativas incluidas son: Infraestructuras y Servicios de Telecomunicaciones Avanzadas, Telecomunicaciones avanzadas en la Administración y Red Regional de Cibercentros.*

CIUDADANO DIGITAL. *Promover el desarrollo de actuaciones de formación, educación y sensibilización dirigidas a la sociedad castellana y leonesa en su conjunto, con el objetivo de facilitar su incorporación y acceso a las oportunidades de futuro que ofrece esta nueva sociedad. Las iniciativas incluidas son: Inici@te, Inclusión Digital y Hogar Digital: Conéct@te.*

ENTORNO EMPRESARIAL DIGITAL. *Impulsar el crecimiento y la capacidad de innovación del tejido empresarial de la región generando un entorno empresarial dinámico a través de la promoción del uso generalizado de las Nuevas Tecnologías por parte de las empresas, la incentivación del desarrollo del negocio electrónico y la potenciación del sector Nuevas Tecnologías regional.*

MUNICIPIOS DIGITALES DE CASTILLA Y LEÓN. *Incluye medidas de impulso de la Sociedad de la información en los municipios de la región así como de Administración Electrónica e Interoperabilidad. A*

través de su incorporación mediante convenios, se creará la Red de Municipios Digitales de Castilla y León en las principales ciudades y también en las Diputaciones.

E-ADMINISTRACIÓN. Explotar al máximo las posibilidades de la Administración Electrónica para prestar unos servicios públicos más eficaces y de mejor calidad.

SERVICIOS PÚBLICOS PARA LA SOCIEDAD DIGITAL DEL CONOCIMIENTO. Modernizar los servicios públicos como la educación, la sanidad, el transporte, etc. Mediante un mayor uso de las herramientas de la Sociedad Digital del Conocimiento, en términos de mejora de la calidad, agilidad, eficiencia y satisfacción de los usuarios.

CONTENIDOS Y SERVICIOS DIGITALES. Impulso de la oferta y puesta en línea de contenidos y servicios de alto valor añadido, capaces de generar el interés necesario para impulsar la componente de demanda y, en definitiva, favorecer la participación activa en la Sociedad Digital del Conocimiento y el disfrute de sus ventajas por parte de los destinatarios finales..

IMPULSO DEL SECTOR AUDIOVISUAL. Adopción de iniciativas encaminadas a favorecer el progreso en Castilla y León de la Televisión y la Radio Digital Terrestre.

RED DE CENTROS PILOTO DE LA JUNTA DE CASTILLA Y LEÓN

Durante el curso 2005-2006, se constituyó la Red de centros piloto de la Junta de Castilla y León en materia de innovación pedagógica y metodológica con Tecnologías de la Información y la Comunicación. Mediante la elaboración de un proyecto pedagógico de aplicación de las Nuevas Tecnologías a la labor docente, se ha dotado del equipamiento necesario para el desarrollo del proyecto, y una propuesta de formación requerida por el profesorado para la aplicación de dichas tecnologías al aula.

La dotación tecnológica para el desarrollo de esta Red de centros piloto ha sido aportada por la Dirección General de Infraestructuras y Equipamiento, mientras que la formación se ha organizado a través de los Centros de Formación e Innovación Educativa a cuyo ámbito pertenece cada uno de los centros, en forma de Proyecto de Formación en Centros.

PROYECTO AMERA

Las siglas del proyecto responden al proyecto de Actualización Metodológica y Evaluación del uso de la Red en el Aula. El objetivo es potenciar la formación e investigación metodológica en el uso de las Nuevas Tecnologías, mediante el análisis de contenidos y elaboración de estrategias de intervención en el aula, la puesta en práctica del Proyecto en la acción de aula y la evaluación de los procesos llevados a efecto.

PROGRAMA "INTERNET EN EL AULA"

Resultado del convenio bilateral firmado el 3 de marzo de 2003 entre la Entidad Pública Empresarial Red.es y la Comunidad de Castilla y León, este programa dota a los centros educativos de toda la infraestructura considerada básica para la introducción efectiva de las Nuevas Tecnologías e Internet en el entorno educativo. Asimismo, se fomenta la formación de los docentes y la creación de contenidos multimedia de calidad.

PROGRAMA INICI@TE

El Programa Iníci@te, gestionado por la Consejería de Fomento de la Junta de Castilla y León, ofrece a todos los ciudadanos, a través de la Red de Cibercentros de Castilla y León y aulas cedidas por los ayuntamientos que colaboran en el programa, formación presencial y formación on-line con apoyo remoto.

El Programa Iníci@te dispone de una amplia temática sobre formación en Nuevas Tecnologías y uso inteligente de Internet para todos los ciudadanos, pero especialmente para los que tienen mayor riesgo de exclusión digital y necesitan un apoyo para facilitar su incorporación a la Sociedad Digital del Conocimiento. Se imparten cursos básicos de introducción a Internet, herramientas de comunicación a través de la red, usos principales de Internet como Administración Electrónica, Comercio Electrónico, etc.

Los Cibercentros son Centros Públicos de Acceso a Internet dotados de varios ordenadores donde cualquier persona puede disponer de acceso gratuito a Internet de Banda Ancha además de correo electrónico, videoconferencia, fotografía digital y en general, disfrutar de todos los contenidos y servicios de la Sociedad Digital y del Conocimiento. La Red de Cibercentros de Castilla y León dispone de alrededor de 700 Cibercentros a través de los cuales, el Programa de Formación Iníci@te ofrece a todos los ciudadanos formación presencial con profesores especializados y formación on-line con la supervisión de tutores, en materias relacionadas con las Nuevas Tecnologías.

PROGRAMA APRENDE

A través de este Programa de la Consejería de Fomento, en colaboración con la Consejería de Educación de la Junta de Castilla y León, los centros educativos se convierten en el punto de encuentro de jornadas TIC (Tecnologías de la Información y la Comunicación). Alumnos y padres interesados en el uso inteligente de las tecnologías pueden realizar talleres formativos e informativos que permitan seguir avanzando en la Sociedad del Conocimiento, de manera segura e inteligente.

En el marco de este Programa, se ha editado y publicado la Guía sobre el Uso Inteligente de las Nuevas Tecnologías, que pretende ser una ayuda para padres y educadores, en el ámbito de las Nuevas Tecnologías, que, día a día, están cambiando la manera en que vivimos, nos relacionamos y aprendemos. Con ella, se busca educarlos, orientarlos y dotarles de los recursos necesarios para que sepan cómo reaccionar y qué medidas tomar ante las situaciones de riesgo.

PROYECTO INTERNET SIN RIESGOS

El proyecto **Internet sin Riesgos** *nace con el objetivo de sensibilizar a los niños sobre los riesgos de Internet y transmitirles buenas prácticas de uso, además de sensibilizar e informar a los padres y educadores para que sepan proteger a los menores.*

Internet sin Riesgos, proyecto llevado a cabo por CEDETEL, va dirigido a niños de entre 7 y 12 años, a sus familiares (principalmente sus padres), a educadores y a monitores y dinamizadores de cibercentros, centros cívicos y asociaciones.

En el portal web del proyecto "Internet sin Riesgos", se puede encontrar información dirigida a los más pequeños (episodios de dibujos animados, actividades interactivas en forma de desafíos, glosario de términos más utilizados en la Red) e información dirigida a padres y educadores (contenidos didácticos con información básica sobre Internet y consejos para fomentar un uso seguro de las Nuevas Tecnologías, información sobre organizaciones naciones e internacionales que trabajan en defensa de los menores y que promueven iniciativas dirigidas a los más pequeños, calendario de eventos, etc.):

Internet sin Riesgos se ha realizado con la colaboración de TRALALERE y con el apoyo del Ministerio de Industria, Turismo y Comercio dentro del Plan Avanza y de la Consejería de Fomento de la Junta de Castilla y León. Más información sobre este proyecto en: www.internetsinriesgos.es

IV. Presentación del material

IV. PRESENTACIÓN DEL MATERIAL

En la estructura del material cuya base es el Manual para la Prevención del Ciberacoso y la Promoción de la Navegación Segura en los Centros Escolares, se distinguen dos partes fundamentales:

a) Una parte informativa, constituida por el *Manual del buen uso de los medios informáticos.*

b) Una parte operativa, constituida por tres guías distintas, dirigidas a diferentes colectivos de la comunidad educativa, respectivamente a los alumnos, las familias y los centros escolares y el profesorado.

En este sentido, la parte principal, el *Manual del buen uso de los medios informáticos* representa una guía general e introductoria, cuyo contenido materializa los tres objetivos principales establecidos por el Grupo Interdisciplinar:

a) Fomento del uso seguro de los medios informáticos en los centros educativos (*Dimensión social*)

b) Promoción de hábitos de prevención y procedimientos (*Dimensión jurídica*)

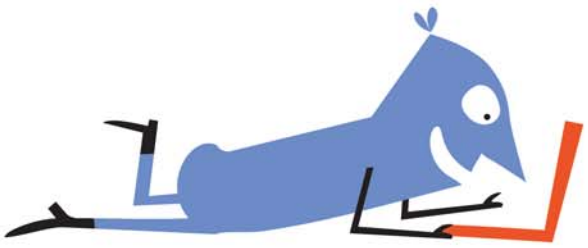
c) Gestión de los procedimientos de seguridad informática (*Dimensión técnica*)

El *Manual del buen uso de los medios informáticos* está estructurado en seis capítulos principales. El primer capítulo, *Introducción,* ofrece una perspectiva general sobre el impacto, tanto positivo como negativo, de las Tecnologías de la Comunicación y la Información, especialmente en el ámbito educativo. El segundo capítulo, *Antecedentes,* presenta, de manera esquemática, las principales iniciativas en materia de TICs promovidas por la Junta de Castilla y León.

La dimensión jurídica está representada por el capítulo cinco, *La protección legal de los menores frente al ciberacoso,* y tiene como objetivo principal ofrecer un recordatorio de la normativa existente en materia de protección legal de los menores frente a los riesgos e impactos negativos de las TICs.

El capítulo seis, *El fomento de un buen uso de los medios informáticos,* representa tanto la dimensión social como la dimensión técnica del manual. Este capítulo aporta, básicamente, información sobre las acciones de gestión de la seguridad informática, pero también ofrece unas orientaciones de carácter general sobre los códigos cívicos para el buen uso de los medios informáticos en los centros escolares.

La parte final del Manual constituye información complementaria y anexos, a través de la que se ofrece un glosario de los términos informáticos más utilizado, pero también un listado de páginas web de interés.



V. La protección legal de los menores frente al ciberacoso

V. LA PROTECCIÓN LEGAL DE LOS MENORES FRENTE AL CIBERACOSO

La incesante expansión de las conexiones a Internet está haciendo accesible la red a un mercado cada vez más amplio, variado, y menos restringido, por condicionantes socioeconómicos o culturales. Los tiempos en que el privilegio de la información "on-line" se reservaba al mundo científico o empresarial se quedan atrás; hoy en día, por poco más de lo que cuesta un café, incluso las personas sin ordenador personal, pueden acceder a Internet y navegar libremente en la red.

La plena alfabetización tecnológica, tan recomendable en la sociedad actual e imprescindible en la venidera, parece entonces un hito fácilmente alcanzable, una realidad que llegará a materializarse por sí misma sin necesidad de esfuerzo u orientación.

Sin embargo, esta mayor disponibilidad del acceso a Internet, y la fabulosa capacidad de movimiento virtual que nos proporciona, trae aparejada un delicado equilibrio entre la libertad de información y expresión y la adecuación a la legalidad de la información recibida o proporcionada según su propia naturaleza o el destinatario de ésta.

Es sabido que la evolución de la normativa relacionada con las Nuevas Tecnologías a menudo no es capaz de dar alcance a la potencialidad de los nuevos servicios proporcionados por la red. Y al amparo de la magnitud de este potencial y de la vastedad inabarcable de información presente en Internet, han surgido contenidos en la red que caen en el más flagrante de los delitos sin necesidad de nuevas leyes: vulneración de los derechos de la propiedad intelectual, pornografía infantil, menosprecio a la dignidad personal, exaltación de la violencia, apología de conductas contrarias a la salud pública, etc.

Por ello, es necesario saber "qué puede pasar si…". Ser consciente de las responsabilidades que cada uno de nosotros tenemos respecto al uso de Internet y actuar correctamente ante este tipo de situaciones se convierte entonces en el mejor antivirus para la protección de nuestros derechos.

A. Fundamentación y objetivos del capítulo

El uso de los equipos informáticos en los centros escolares y de la capacitación del profesorado en esta materia ha constituido una mejora en el ejercicio de la docencia, aplicable a la práctica totalidad de las materias. Sin embargo, las sesiones lectivas que se desarrollan utilizando aplicaciones informáticas presentan nuevos riesgos y nuevas situaciones que deben contar con su regulación específica y con procedimientos específicos que garanticen las buenas prácticas de uso de la tecnología.

Los objetivos que se pretenden alcanzar con la elaboración de este recordatorio son:

a) Orientar a los centros sobre la repercusión del acceso a páginas web con contenidos inapropiados (carácter explícitamente pornográfico, xenófobo, misógino, violento, etc.) que son susceptibles de causar un efecto negativo en el desarrollo personal o social del alumnado o afectar a la convivencia del centro.

b) Identificación del marco normativo en el ámbito de la educación en Castilla y León.

c) Propuestas de inclusión de orientaciones a los centros para ser recogidas en sus planes de convivencia y reglamentos de régimen interior.

d) Intervención en el marco del programa de asistencia jurídica.

B. La normativa existente y su utilización para la prevención del acoso escolar mediante las Nuevas Tecnologías

Como ya se ha dicho en más de una ocasión, Internet es una de las mayores evidencias del progreso social, económico y político de nuestros tiempos, haciendo accesible la información y la comunicación a nivel global para cualquier persona que se conecta al World Wide Web. Y, sin embargo, también puede ser utilizado para perpetrar acciones delictivas que atacan a valores jurídicos protegidos, como son la libertad, la intimidad personal y familiar, la propia imagen, la dignidad humana, etc.

En lo que se refiere a los menores, en los últimos años, esta gran herramienta educativa ha demostrado ser un arma de doble filo, ya que engendra muchos peligros para los más vulnerables. Según la Agencia de Calidad de Internet (IQUA)[4], estos peligros se podrían clasificar de la siguiente manera:

a) Personales. Aquellos riesgos que consisten en la existencia de distintos acosadores que utilizan los foros, los chats y los programas de mensajería instantánea tipo Messenger y Skype para lograr captar a sus víctimas, menores de edad, fáciles de engañar y mucho más accesibles que cualquier otra persona.

b) De contenido. Estos peligros se refieren al acceso, voluntario o involuntario, a contenidos como imágenes, vídeos o textos violentos, de carácter sexual, racista, xenófobo o sectario, no apto para todos los públicos.

c) De adicción. Este riesgo se refiere al comportamiento que pueden adquirir los niños, igual que los adultos, de dependencia del uso de Internet, también llamado “desorden de adicción a Internet”.

[4] Agencia de Calidad de Internet (IQUA): www.iqua.es

Por otro lado, según afirma la ONG Protégeles, en los últimos años, la aparición de una nueva práctica conocida como ciberacoso o cyberbulling, ha supuesto la manifestación de una nueva forma de acoso escolar. El ciberacoso[5] se puede definir como una agresión psicológica, sostenida y repetida en el tiempo, perpetrada por uno o varios individuos contra otros, utilizando para ello las Nuevas Tecnologías. Actualmente, el ciberacoso es una forma de humillación en los colegios entre los adolescentes por la que son víctimas de agresiones realizadas a través de la red. Un método habitual para llevar a la práctica este medio de violencia suele ser el acceso a páginas web para realizar insultos, mensajes intimidatorios, difusión de rumores crueles, fotos trucadas o amenazas (bajo el amparo de un seudónimo) entre compañeros de un mismo colegio o de varios centros educativos.

El ciberacoso es una nueva forma de acoso escolar, y se refiere a diferentes tipos de acoso (racista, homofóbico, o acoso relacionado con discapacidades, etc.). La diferencia es que el acoso se realiza a través de las Nuevas Tecnologías. El ciberacoso incluye una variedad muy amplia de comportamientos inapropiados, incluyendo el abuso, las amenazas, los insultos, e igual que el acoso escolar, está dirigido a dañar el bienestar de la persona acosada.

Entre las principales características del ciberacoso, se podría citar:

a) Para considerar una actuación como ciberacoso, se debe tener en cuenta si la agresión es repetida. Un episodio aislado de envío de mensajes inapropiados o incluso desagradables, aun cuando sea reprobable, no puede ser considerado como tal.

b) La difusión de información a través de Internet es inmediata y el alcance de la posible agresión es difícilmente cuantificable. Una vez realizado, a veces no es posible detener su propagación, ni aun para el agresor que la inició.

c) Como norma casi general, cualquier episodio de ciberacoso es la transposición de situaciones de acoso en la vida real e incluso de acoso escolar. Además, también es habitual que se produzca en una situación de poder del acosador respecto de la víctima.

Como apuntamos anteriormente, el ciberacoso se realiza mediante la utilización de cualquier medio tecnológico, especialmente aquellos que favorecen la relación entre usuarios. Los más habituales, por su proliferación entre los colectivos a que nos referimos son:

a) El teléfono móvil. Envíos de sms, grabación de secuencias de vídeo, etc.

[5] http://www.internetsinacoso.com/ciber-bullying.php

b) Internet. La actual facilidad de acceso y el anonimato que se cree que proporciona, hacen de este medio el más utilizado.

c) Por otro lado, actualmente las redes sociales como Youtube posibilitan la difusión global de actuaciones que antes se "limitaban" a enviarse de móvil a móvil mediante mensajes o conexiones a través de bluetooth o infrarrojos.

El ciberacoso se puede manifestar en distintas formas, algunas de ellas más difícil de detectar o menos asociadas con las formas habituales de acoso:

a) *Amenazas e intimidación*, que se puede realizar a través del teléfono móvil, el correo electrónico, los comentarios en la red, las redes sociales, etc.

b) *Acoso o acecho*. Los mensajes repetidos, prolongados e indeseados, ya sean explícitamente ofensivos o no, representan una forma de acoso. El acoso online puede provocar daños psicológicos serios y miedo, la navegación online transformándose así en una fuente de malestar. Estas formas de acoso online incluyen: los mensajes de textos o la mensajería instantánea con contenido indeseado, la utilización de los foros públicos para realizar comentarios difamatorios o despectivos; la utilización del spyware; el envío de virus informáticos, etc.

c) *La denigración o la difamación*. El ciberacoso incluye también la publicación de mensajes difamatorios sobre un individuo y, generalmente, se refieren a insultos. Los alumnos pueden utilizar sus teléfonos móviles o correos electrónicos para enviar mensajes sexistas, homofóbicas o racistas, por ejemplo, o pueden utilizar otro tipo de diferencias –una discapacidad física o mental, el origen cultural o religioso, la posición socio-económica, etc.

d) *La exclusión y el rechazo*. La exclusión online puede ser más difícil de detectar que en la vida real. Las redes sociales, como Facebook, Tuenti, etc. ofrecen una plataforma para que los jóvenes establezcan relaciones de amistad y de comunicación con otros miembros de la red. Estas redes pueden representar una importante extensión del espacio y la actividad social de los jóvenes. Sin embargo, a través de estas plataformas, los alumnos pueden crear grupos cerrados para protegerse de contactos indeseados. En este marco, pueden aparecer situaciones de exclusión y/o rechazo de uno de sus miembros, situaciones que pueden tener importantes consecuencias emocionales.

e) *El robo de identidad, el acceso no autorizado y suplantación de identidad.* El pirateo significa, habitualmente, que otra persona tiene acceso a la cuenta de otro usuario de la red, a través de la decodificación del nombre de usuario y la contraseña. Este tipo de acciones se pueden utilizar como forma de ciberacoso, utilizando y copiando la información personal de un usuario, incluyendo correos o imágenes para acosarlos e humillarlos. Esto puede incluir la publicación de información

privada en sitios públicos, la impresión y difusión de información personal, etc. Estas formas de ciberacoso también pueden referirse a las situaciones de eliminación de información personal de un usuario o las situaciones de suplantación de identidad.

f) *La difusión de información personal o privada e imágenes en sitios públicos.*

g) *La manipulación*. La manipulación es una forma de ciberacoso muy poco considerada por su dificultad a la hora de detección. Desgraciadamente, existen muchos casos de ciberacoso manipulativo. Los ejemplos incluyen la presión ejercida sobre un usuario para revelar información personal o para concertar una cita. Otras formas pueden implicar el hacer a un usuario hablar o comportarse de forma provocativa. La manipulación también es utilizada por los adultos que tienen un interés sexual en los niños e intentan convencerles con el objetivo de conocerles en persona.

En este sentido, es evidente que el ciberacoso tiene efectos emocionales devastadores en sus víctimas, socavando su bienestar e invadiendo espacios muy necesarios para el menor como son su descanso o su tiempo de estudio.

Con motivo de la celebración del Día Europeo de Internet Seguro (10 de febrero de 2009), el presidente de la ONG Protégeles indicó que el 20% de las denuncias atendidas por esta ONG, durante el año 2008, eran relativas a situaciones de ciberacoso, fenómeno que, en el año 2006, apenas alcanzaba el 1%. En cuanto a las consecuencias de esta forma de acoso, son sobre todo emocionales, aunque en un 13% de las situaciones se derivan consecuencias físicas y disminución del rendimiento escolar, un 6% provoca aislamiento social y el 3% genera absentismo escolar.

Por ello, la importancia de las herramientas de protección, tanto legal como civil, es fundamental. La configuración de unas leyes que regulen la materia y penalicen las conductas perjudiciales es esencial, pero no suficiente. Todo ello se debe complementar con una importante labor educativa por parte de las familias y los docentes que, a través de su experiencia, deben fomentar un buen uso de estos medios.

La necesidad de conocer y saber utilizar Internet es una condición primordial en la sociedad actual, por lo que la protección, en todos sus términos, no debe privar a los menores de esta herramienta, imprescindible en su vida laboral. La prohibición y el control no representan el camino hacia una navegación segura y responsable de los menores. Es importante enseñarles a utilizar esta herramienta con criterio, haciendo un buen uso de los muchos beneficios que aporta, pero también es necesario darles a conocer la manera de afrontar determinadas situaciones.

Por ello, la protección legal representa el paso inicial fundamental para asegurar unos hábitos adecuados de uso de Internet.

En este sentido, en la segunda reunión celebrada por el Grupo Multidisciplinar, se ha propuesto la elaboración de un guía de uso y procedimiento para la prevención del acoso escolar mediante las Nuevas Tecnologías, que recoja tanto las normas de uso como el procedimiento sancionador.

Atendiendo a este objetivo, a continuación se presentan los principales hitos en materia de legislación con respecto al uso delictivo e ilegal de las Nuevas Tecnologías.

A. La normativa de marco general

A nivel internacional:

A.1. La Resolución de 27 de febrero de 1996 del Consejo de Telecomunicaciones de la Unión Europea para impedir la difusión de contenidos ilícitos de Internet, especialmente la pornografía infantil, que propone medidas para intensificar la colaboración entre los estados miembros, independientemente de que cada uno de ellos aplique la legislación que exista en su país sobre la materia.

A.2. El *Libro Verde sobre la protección de los menores y de la dignidad humana en los servicios audiovisuales y de información (1996)* de la Unión Europea tiene por objeto profundizar el debate sobre las condiciones necesarias para la creación de un marco coherente para la protección de los menores y de la dignidad humana en los servicios audiovisuales y de información.

En su Capítulo I, plantea la necesidad de diferenciar entre los contenidos que son ilícitos, que están sujetos a sanciones penales (como la pornografía infantil) y por tanto no deben tener cabida en la Red, y el hecho de que los menores puedan acceder a páginas pornográficas que no son ilegales para adultos (lo que debe tratar de evitarse aún cuando no se han eliminando las mismas).

El capítulo II precisa que las disposiciones aplicables a nivel nacional y europeo se inscriben en el marco de los derechos fundamentales que figuran en el Convenio Europeo de los Derechos Humanos. En artículo 10 del referido Convenio, que proclama la libertad de expresión, establece que la misma puede verse limitada para evitar la prevención de delitos.

De la misma manera, la libre prestación de servicios, que constituye una de las cuatro libertades que garantiza el Tratado de la Unión Europea, puede verse restringida por razones primordiales de interés público, como la protección de los menores y de la dignidad humana.

Se plantean también diferentes posibilidades para reforzar la cooperación entre las diferentes administraciones nacionales: intercambio de informaciones, análisis comparado de sus legislaciones, cooperación en los marcos de la justicia y de los asuntos interiores.

Por las características de Internet no cabe duda que aplicar soluciones globales es difícil, pero no debe abandonarse el empeño por buscar las que sean más compatibles para los Estados Miembros.

A.3. La Recomendación 98/560/CE del Consejo de la Unión Europea es el primer instrumento jurídico elaborado para la protección de los menores antes los contenidos perjudiciales o ilegales de Internet. Esta Recomendación se ideó a raíz del Libro Verde de 1996 sobre la protección de los menores y de la dignidad humana en los servicios audiovisuales y de información, que fue el inicio de un debate a escala europea sobre la dimensión ética de la sociedad de la información y sobre la forma en que el interés general puede protegerse en los nuevos servicios.

A.4. La Recomendación 2006/952/CE, que completa la Recomendación 98/560/CE, invita a dar un paso más hacia la instauración de una cooperación eficaz entre los Estados miembros, la industria y las demás partes interesadas en materia de protección de los menores y de la dignidad humana en los sectores de la radiodifusión y de los servicios de Internet.

A nivel estatal:

A.5. La Constitución Española regula la protección de los menores en diferentes artículos. Así, el artículo 20.4 limita la libertad de expresión, de información y de cátedra, *"... en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia*".

Por su parte, el artículo 39.4 del mismo texto determina que "*Los niños gozarán de la protección prevista en los acuerdos internacionales que velan por sus derechos*".

A.6. La Ley Orgánica /2006, de 3 de mayo, de Educación, establece el marco de los derechos y deberes en materia de educación. Tres son los principios que presiden esta Ley, el primero la exigencia de proporcionar una educación de calidad a todos los ciudadanos, al mismo tiempo garantizar una igualdad efectiva de oportunidades, el segundo la necesidad de que todos los componentes de la comunidad educativa colaboren para conseguir ese objetivo. El tercer principio consiste en un compromiso decidido con los objetivos educativos planteados por la Unión Europea para los próximos años, dirigidos hacia una cierta convergencia de los sistemas de educación y formación.

A.7. La Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, impone la obligación a toda persona o autoridad de comunicar a la autoridad o sus agentes las situaciones de riesgo que puedan afectar a un menor sin perjuicio de prestarle el auxilio inmediato que precise. Esta Ley aborda una reforma en profundidad de las tradicionales instituciones de protección del menor reguladas en el Código Civil, pretende construir un amplio marco jurídico de protección que vincula a todos los Poderes Públicos, a las instituciones específicamente relacionadas con los menores, a los padres y familiares y a los ciudadanos en general. En

esta Ley, también se manifiesta la preocupación por agilizar y clarificar los trámites de los procedimientos administrativos y judiciales que afectan al menor, con la finalidad de que éste no quede indefenso o desprotegido en ningún momento.

A.8. La Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores, se presenta el principio de que la responsabilidad penal de los menores tiene, frente a la de los adultos, un carácter primordial de intervención educativa. Esta Ley desarrolla la exigencia de una verdadera responsabilidad jurídica a los menores infractores, y se aplica para exigir la responsabilidad de las personas mayores de catorce años y menores de dieciocho por la comisión de hechos tipificados como delitos o faltas en el Código Penal o las leyes penales especiales.

A.9. La Ley Orgánica 1/2004, de 28 de diciembre, de medidas de protección integral contra la violencia de género. Establece el marco del fomento de la convivencia y abarca tanto los aspectos preventivos, educativos, sociales, asistenciales y de atención posterior a las víctimas, como la normativa civil que incide en el ámbito familiar o de convivencia. El ámbito educativo forma una parte importante de esta Ley, ya que expone que desde la Educación Infantil, en la que se contribuirá a desarrollar en la infancia el aprendizaje en la resolución pacífica de conflictos, hasta en la enseñanza de los adultos pasando por la Educación Primaria, Secundaria y el Bachillerato y la Formación Profesional, se trabajará para conocer, valorar y respetar la igualdad de oportunidades de hombres y mujeres.

A.10. La Instrucción de la Fiscalía General del Estado, 10/2005, de 6 de octubre, sobre el tratamiento del acoso escolar desde el sistema de justicia juvenil, establece unas líneas de actuación respecto al acoso escolar, partiendo del hecho de que negar o relativizar el problema es el error más grave en el que se puede incurrir. En este sentido, se determina el modo de actuación de los fiscales ante este problema, así como la comunicación entre los diferentes órganos administrativos implicados, también las pautas generales de la tipificación penal del acoso escolar, medidas cautelares y los distintos delitos en los que se incurre en el acoso escolar o de otro tipo como puede ser el laboral.

A.11. La Ley 14/2002 de 25 de julio de promoción, atención y protección a la infancia en Castilla y León. Esta Ley impone a la Administración de la Comunidad Autónoma de Castilla y León el fomento de la elaboración de códigos deontológicos para la protección de los menores y la implantación y uso de sistemas que impidan o dificulten que éstos tengan la posibilidad de acceder, por medio de las telecomunicaciones y la telemática, a servicios que puedan ser ilícitos o nocivos para su correcto desarrollo físico o psíquico.

B. La normativa específica de convivencia escolar

En relación con la prevención del ciberacoso, y ya que este peligro relativo al uso de Internet es una forma de manifestación del acoso a través de las Nuevas Tecnologías, a continuación se presentan las líneas generales de la normativa específica de convivencia escolar en la comunidad de Castilla y León.

B.1. El Decreto 51/2007, de 17 de mayo, por el que se regulan los derechos y deberes de los alumnos y la participación y los compromisos de las familias en el proceso educativo, y se establecen las normas de convivencia y disciplina en los Centros Educativos de Castilla y León.

El Decreto regula, por una parte, derechos y deberes de los alumnos y, por otra, la necesaria implicación de las familias en el proceso educativo estableciendo, al mismo tiempo, las normas de convivencia y disciplina en los centros educativos no universitarios, sostenidos con fondos públicos, de Castilla y León.

De esta forma los principales aspectos que incorpora el Decreto quedan reflejados en los principios informadores del mismo:

a) La importancia de la acción preventiva como mejor garantía para la mejora de la convivencia escolar.

b) La responsabilidad de todos y cada uno de los miembros de la comunidad educativa para conseguir un clima escolar adecuado.

c) El necesario refuerzo de la autoridad del profesor para un correcto desarrollo del proceso educativo.

d) La necesidad de una colaboración e implicación de los padres o tutores legales del alumno en la función tutorial del profesor.

e) La relevancia de los órganos colegiados y de los equipos directivos de los centros en el impulso de la convivencia y en el tratamiento de los conflictos.

Por su especial relación con el ciberacoso, es importante tener en cuenta el artículo 6 del Decreto que se refiere al derecho de todo el alumnado a ser respetado: “Todos los alumnos tienen derecho a que se respeten su identidad, integridad y dignidad personales”.

Se recogen, a continuación, los aspectos que implican el respeto a dicho derecho.

a) La protección contra toda agresión física, emocional o moral.

b) El respeto a la libertad de conciencia y a sus convicciones ideológicas, religiosas o morales.

c) La disposición en el centro de unas condiciones adecuadas de seguridad e higiene, a través de la adopción de medidas adecuadas de prevención y de actuación.

d) Un ambiente de convivencia que permita el normal desarrollo de las actividades académicas y fomente el respeto mutuo.

e) La confidencialidad en sus datos personales sin perjuicio de las comunicaciones necesarias para la Administración educativa y la obligación que hubiere, en su caso, de informar a la autoridad competente.

B.2. La Orden EDU/1921/2007, de 27 de noviembre, establece las medidas y las actuaciones para la promoción y mejora de la convivencia en los centros educativos de Castilla y León, desarrolla el Decreto 51/2007, en aspectos como la promoción y mejora de la convivencia en relación con los recursos necesarios para su fomento en los centros docentes, así como las medidas necesarias de coordinación, seguimiento y evaluación en los diferentes niveles de la Administración.

a) Establece el protocolo de actuación

b) Medidas de seguridad en los centros educativos.

Colaboración con los órganos administrativos que tengan competencias en materia de seguridad pública y ciudadana, la adopción de medidas preventivas de seguridad tanto en el interior del recinto escolar como en el entorno del mismo.

c) Seguridad jurídica de los miembros de la comunidad educativa.

Protección y asistencia jurídica del personal docente, de administración y servicios y de los inspectores de educación en el desarrollo de sus funciones. Se incluirán las medidas precisas para aquellos casos en los que se haya iniciado contra los anteriores miembros de la comunidad educativa un proceso judicial, derivado de su actuación profesional.

B.3. Circular de 27 de diciembre de 2006 de la Secretaría General de la Consejería de Educación, sobre la implantación del servicio de asistencia jurídica para profesores, inspectores y alumnos de centros educativos sostenidos con fondos públicos de Castilla y León.

Además de la asistencia judicial que DECRETO 203/1997, de 23 de octubre, establece para el personal al servicio de la Administración Autonómica, la Circular de 27 de diciembre de 2006 ofrece asistencia jurídica a profesores y alumnos que hayan sido víctimas de cualquier tipo de violencia. Como aparece en el texto de la misma, la Consejería de Educación entiende que la defensa de los derechos y el cumplimiento de deberes necesita en ocasiones, por sus especiales características, de un apoyo adecuado que vaya más allá del que es posible brindar desde el ámbito educativo, aportando la necesaria asistencia legal a los afectados.

Entre otros aspectos, la Circular establece el procedimiento y documentación necesaria para solicitar la asistencia jurídica.

A continuación, en la siguiente página, se presenta, a modo de esquema, el procedimiento de actuación ante situaciones de conflicto provocadas por la utilización inadecuada de las nuevas tecnologías (Internet, teléfonos móviles) y especialmente en casos de ciberacoso, ciberabuso y otras situaciones de ciberagresión.

PROCEDIMIENTO DE ACTUACIÓN ANTE SITUACIONES DE CONFLICTO PROVOCADAS POR LA UTILIZACIÓN INADECUADA DE LAS NUEVAS TECNOLOGÍAS (INTERNET, TELÉFONOS MÓVILES) Y ESPECIALMENTE EN CASOS DE CIBERACOSO, CIBERABUSO Y OTRAS SITUACIONES DE CIBERAGRESIÓN.

¿EN QUÉ MOMENTO?	¿A QUIÉN AFECTA?	¿DÓNDE OCURRE?	¿SE CONOCE AL AUTOR?	¿QUÉ PUEDE HACER?	NORMATIVA Y RECURSOS APLICABLES	¿QUIEN LO TIENE QUE HACER?
Inmediatamente que nos enteremos de que está ocurriendo	PROFESORADO	EN EL CENTRO	SI	Aplicación del "Procedimiento de actuación ante situaciones de conflicto que afecten a la convivencia escolar" (Anexo de la Orden EDU/1921/2007)	DECRETO 51/2007, de 17 de mayo Artículo 35.– Actuaciones inmediatas. Artículo 36.– Competencia.	Cualquier profesor afectado o no.
					DECRETO 51/2007, de 17 de mayo Artículo 37 a 39 y artículos 32 y 50 (entre otros).	Director de oficio o a instancia del profesor afectado o de otro.
			SE CONOZCA Ó NO	Denuncia en aquellos casos en los que sus características o gravedad lo requiera.	Actuaciones policiales y/o judiciales.	Profesor afectado
				Solicitud de asesoramiento a través del Programa de Asistencia Jurídica de la Consejería de Educación en los casos de denuncia.	ORDEN EDU/1921/2007, de 27 de nov. Artículo 7.– Seguridad jurídica de los miembros de la comunidad educativa. (Teléfono 012).	Profesor afectado
		FUERA DEL CENTRO	SE CONOZCA Ó NO	Denuncia en aquellos casos en los que sus características o gravedad lo requiera.	Actuaciones policiales y/o judiciales.	Profesor afectado
				Solicitud de asesoramiento a través del Programa de Asistencia Jurídica de la Consejería de Educación en los casos de denuncia.	ORDEN EDU/1921/2007, de 27 de nov. Artículo 7.– Seguridad jurídica de los miembros de la comunidad educativa. (Teléfono 012).	Profesor afectado
	ALUMNADO	EN EL CENTRO	SI	Aplicación del "Procedimiento de actuación ante situaciones de conflicto que afecten a la convivencia escolar" (Anexo de la Orden EDU/1921/2007)	DECRETO 51/2007, de 17 de mayo Artículo 35.– Actuaciones inmediatas. Artículo 36.– Competencia.	Cualquier profesor afectado o no.
					DECRETO 51/2007, de 17 de mayo Artículo 37 a 39 y artículos 32 y 50 (entre otros).	Director de oficio o a instancia del alumno afectado o de un profesor.
			SE CONOZCA Ó NO	Denuncia en aquellos casos en los que sus características o gravedad lo requiera.	Actuaciones policiales y/o judiciales.	Alumno afectado (sus familiares en caso de menores). También, en algunos casos, el Director o un profesor.
				Solicitud de asesoramiento a través del Programa de Asistencia Jurídica de la Consejería de Educación en los casos de denuncia.	ORDEN EDU/1921/2007, de 27 de nov. Artículo 7.– Seguridad jurídica de los miembros de la comunidad educativa. (Teléfono 012).	Alumno, familiares, profesor o Director del centro según casos.
		FUERA DEL CENTRO	SE CONOZCA Ó NO	Denuncia de aquellos casos en los que las características lo hagan preciso.	Actuaciones policiales y/o judiciales.	Alumno afectado (sus familiares en caso de menores). También, en algunos casos, el Director o un profesor.
				Solicitud de asesoramiento a través del Programa de Asistencia Jurídica de la Consejería de Educación en los caso de denuncia.	ORDEN EDU/1921/2007, de 27 de nov. Artículo 7.– Seguridad jurídica de los miembros de la comunidad educativa. (Teléfono 012).	Alumno, familiares, profesor o Director del centro según casos.
Con posterioridad al conocimiento de la situación.	En aquellas situaciones en las que las características o número de los casos lo haga preciso se elevará informe a la Fiscalía.					Administración Educativa.

VI. El fomento de un buen uso de los medios informáticos

VI. EL FOMENTO DE UN BUEN USO DE LOS MEDIOS INFORMÁTICOS

A. Fundamentación y presentación del capítulo

Las generaciones recientes de adolescentes españoles han crecido de manera simultánea al desarrollo de una Red evolucionada, de carácter marcadamente social, implantada en los hogares con la naturalidad de un simple elemento de comunicación, información o diversión.

Sin embargo, y a pesar de la aparente familiaridad de los jóvenes con esta nueva tecnología y de la sensación de control o inocuidad que experimentan, la red se desarrolla cualitativa y cuantitativamente en direcciones no siempre deseables, y a una velocidad que hace difícil el establecimiento de medidas mitigadoras de los posibles impactos perjudiciales sobre el crecimiento emocional y personal de los adolescentes.

Todo esto refleja un panorama en el que todos, padres e hijos, son nuevos. Faltan pautas y criterios de actuación válidos, homogéneos y ejecutables realmente por unos y por otros. En tanto en cuanto no estén claras estas bases de actuación, los jóvenes parecen enfrentarse sin recursos a este nuevo entorno, mientras que los padres tienden a reaplicar las soluciones del mundo físico al mundo virtual.

Por ello, se hace necesario el desarrollo de actuaciones que, preservando y potenciando el uso y disfrute de las tecnologías de la información, eliminen los usos no deseados y minimicen los impactos que puedan ser lesivos para cualquiera de los miembros de la comunidad educativa o de la sociedad en general.

El fomento de hábitos de responsabilidad en el uso de la tecnología dentro del entorno educativo es una garantía para el avance hacia una sociedad de la información a la medida del ser humano.

En este sentido, el presente capítulo se enfoca a la elaboración de recomendaciones referentes a la gestión de la seguridad informática y los códigos cívicos para el buen uso de los medios informáticos en los centros educativos. Por ello, el capítulo está compuesto por tres subcapítulos.

En una primera parte, se presentan, de forma general, las principales acciones de información, formación y sensibilización a poner en marcha para fomentar un uso adecuado de los medios informáticos y de Internet.

A continuación, en la segunda parte, se presentan las distintas estrategias en materia de seguridad informática y configuración de equipos informáticos, como por ejemplo el filtrado de los contenidos para aumentar la seguridad frente a accesos exteriores no autorizados.

La última parte de este capítulo constituye una guía muy práctica sobre las distintas tecnologías utilizadas por los jóvenes para comunicarse, para encontrar información o, simplemente, para divertirse y una serie de códigos éticos y cívicos de buen uso de estas Nuevas Tecnologías, con el objetivo de fomentar la seguridad de los niños y un uso apropiado, orientado al aprendizaje.

B. Las acciones de información, formación y sensibilización ante los riesgos de las Nuevas Tecnologías

El presente apartado se configura como una guía de normas básicas, dirigida a todos los sectores de la comunidad educativa, que aporta información actualizada sobre la naturaleza, riesgos y consecuencias del mal uso de las redes informáticas así como sobre las pautas adecuadas de protección y uso correcto.

Esta información se presentará también, de forma más práctica, como guías de recomendaciones para el buen uso de los medios informáticos, atendiendo a las singularidades de cada uno de los sectores destinatarios: los alumnos, las familias, los centros educativos y los profesores.

Entre los principales objetivos que se persiguen a través de estas acciones, se pueden citar:

a) Fomentar un uso responsable de las Nuevas Tecnologías de la información y comunicación que promueva una relación con la tecnología que no vulnere derechos y que incremente el crecimiento personal de los usuarios.

b) Reducir y proteger frente a los posibles riesgos derivados del uso de las Tecnologías de la Información.

c) Fomentar valores y actitudes de comportamiento cívico en entornos tecnológicos.

d) Fomentar el establecimiento de un protocolo de contacto con otras entidades, públicas o privadas del ámbito de las Nuevas Tecnologías.

e) Ofrecer una formación específica sobre el ciberacoso a todos los colectivos de la comunidad educativa.

Las acciones de sensibilización de la comunidad educativa, en relación a los diferentes riesgos de las Nuevas Tecnologías, se estructuran en tres tipos de acciones específicas:

1. Acciones informativas, dirigidas a profesores, alumnos, padres y centros, etc.

Este tipo de acciones están orientadas a ofrecer información específica, clave a los distintos protagonistas de la comunidad educativa en relación a los riesgos a los que se pueden enfrentar los menores en la red y, sobre todo, la forma de afrontar los mismos.

El estudio elaborado por INTECO[6], sobre los hábitos seguros de los menores de 18 años en el uso de las Nuevas Tecnologías, confirma que los adultos tienen pocos conocimientos sobre los riesgos a los que se exponen sus hijos a la hora de utilizar Internet. Lo que más les preocupa es el riesgo de dependencia o uso abusivo, por delante del resto de situaciones: virus, acoso sexual, interacción con desconocidos, acceso a contenidos inadecuados, etc.

Por otro lado, el mismo estudio determina que los padres de los niños españoles de 10-16 años reúnen las aptitudes y la formación suficientes como para absorber formación relacionada con las Nuevas Tecnologías (son jóvenes, usuarios de Internet, y tienen formación) y, además, están implicados en los hábitos Nuevas Tecnologías de sus hijos (establecen normas, controlan de algún modo su navegación, muestran preocupación ante los riesgos).

En este sentido, las acciones informativas se deben adaptar a las necesidades formativas de cada colectivo, reforzando la información sobre los riesgos menos conocidos en cada caso (el estudio muestra que hay ciertos riesgos que son en mayor medida conocidos por los niños y que los padres desconocen, por ejemplo lo relativo al ciberacoso, y otros donde se apreciaba la tendencia contraria).

El Grupo Interdisciplinar para el buen uso de los medios informáticos de la Junta de Castilla y León recomienda la puesta en marcha de acciones informativas mediante enlaces a documentos específicos o páginas web desde el Portal de Educación de Castilla y León, mediante las páginas web de los centros educativos o desde el Sistema de Información Administrativo Único (SIAU).

2. Acciones de formación

En coherencia con las acciones informativas, la acción formativa debe proporcionar pautas concretas para identificar los riesgos asociados al uso de Internet y la forma de afrontarlos.

En este sentido, es importante ofrecer una información eficaz que permita a todos los colectivos de la comunidad educativa sentirse seguros y cómodos en la utilización de las Nuevas Tecnologías. Por tanto, la formación sobre riesgos existentes en las Nuevas Tecnologías debe ser rigurosa y práctica, ya que muchos estudios han demostrado que tanto niños como adultos tienen un nivel adecuado de conocimiento de las Nuevas Tecnologías. Por ello, las acciones formativas se deben configurar en base a una comunicación que aporte seguridad al usuario.

---

[6] INTECO (2009): *Estudio sobre los hábitos seguros en el uso de las NUEVAS TECNOLOGÍAS por niños y adolescentes y e-confianza de sus padres*. Observatorio de la Seguridad de la Información

Por otro lado, es fundamental reforzar la formación sobre las medidas efectivas de respuesta ante la incidencia de un problema de seguridad. Estas acciones, responsabilidad tanto de las Administraciones Públicas como de la industria, deben ir más allá de las medidas técnicas (apagar el ordenador, formatear el equipo, etc.), ya que estudios sobre la materia demuestran que tanto adultos como los niños desconocen las otras acciones que deben implementar ante una incidencia de seguridad.

En este sentido, el Grupo Interdisciplinar recomienda la participación de todos los colectivos en el Programa Aprende, promovido la Consejería de Fomento, en colaboración con la Consejería de Educación de la Junta de Castilla y León, a través de cual los centros educativos se convierten en el punto de encuentro de jornadas TIC (Tecnologías de la Información y la Comunicación). Alumnos y padres interesados en el uso inteligente de las tecnologías pueden realizar talleres formativos e informativos que permitan seguir avanzando en la Sociedad del Conocimiento, de manera segura e inteligente. En este sentido, los centros educativos se convierten en el marco imprescindible en el que se llevarán a cabo los talleres informativos para la prevención de riesgos en el uso de las Tecnologías de la Información y la Comunicación (TIC) por parte de los menores y talleres de formación.

Por otro lado, también se recomienda la organización de cursos de formación sobre acoso escolar computables para el reconocimiento de sexenios o habilitación como cargo directivo, cursos específicos de formación para Equipos Directivos de los centros, acciones formativas desarrolladas por los Departamentos de Orientación, recursos y juegos educativos en el escritorio virtual de los alumnos.

3. Acciones de sensibilización

Las acciones de sensibilización deben estar orientadas no solamente a los menores, sino que deben fomentar una implicación activa también por parte de los sus padres y educadores, así como de otros miembros de la comunidad educativa. El principal objetivo de las acciones de sensibilización es que toda la comunidad educativa conozca los riesgos del uso de las Nuevas Tecnologías y ponga en práctica las medidas adecuadas para asegurar una navegación segura en la red y un uso adecuado de estas tecnologías.

En este sentido, el Grupo Interdisciplinar de la Consejería de Educación de Castilla y León ha recomendado la puesta en marcha de distintas acciones de sensibilización dirigida a toda la comunidad educativa. Entre ellas, se pueden citar:

- Avisos en el inicio de los equipos de los centros educativos sobre normas de uso adecuado de los equipos.
- Utilización de las ventanas educativas de los centros.
- Puesta en marcha de campañas de mensajes por bluetooth.

- Descarga de salvapantallas para el alumnado.
- Avisos por correo-e o correo postal.
- Elaboración de carteles con información general,
- Elaboración de carteles con un decálogo para aulas de informática y bibliotecas escolares, folletos o dípticos con información dirigida a grupos concretos.
- Entrega de flyers junto a los boletines de evaluación trimestrales.
- La elaboración y puesta en marcha de planes de actuación y difusión en los medios usados por la comunidad educativa (foros, programas de mensajería instantánea –MSN–, redes sociales virtuales –Tuenti–, entre otros).
- Inclusión en la propuesta de guión de la presentación de avisos en escritorios virtuales, descargas de salvapantallas institucionales atractivos relacionados con el acoso, y la vinculación con los planes de acogida.

A nivel de Administraciones Públicas, las acciones de concienciación y sensibilización de la población se han materializado en varias iniciativas: elaboración de guías y materiales didácticos e interactivos, difusión de buenas prácticas, publicación de estudios, creación de páginas web, realización de charlas, seminarios y cursos, etc.

En cuanto al nivel nacional, se pueden citar las siguientes iniciativas:

1) Chavales. Iniciativa promovida por Red.es. Web: http://chaval.red.es

Se trata de un portal orientado a niños de 6 a 13 años, dividido en tres tramos de edad: de 6 a 9 años, de 9 a 11 años y de 11 a 13 años. En estas secciones se pueden encontrar ciberconsejos, cibernormas, y otra información sobre el uso de la mensajería instantánea, los chats, los móviles, el intercambio de ficheros, etc. dirigidas a la orientación del menor. Además incluye una selección de enlaces de ocio educativo con un enfoque participativo.

También ofrece a padres y educadores información y documentación sobre la seguridad en el uso de las Nuevas Tecnologías.

2) Proyecto Secukid. Iniciativa promovida por AETICAL dentro del programa Déd@lo, INTECO y Pantallas Amigas. Web: http://www.secukid.es

Se trata de un juego de inteligencia para móviles que persigue transmitir conceptos básicos sobre seguridad en el uso de las Nuevas Tecnologías a niños y adolescentes a partir de 11 años. El juego, que simula un

ambiente cibernético, comprende cinco niveles: virus, troyanos y gusanos, programas espía, ciberbullying y grooming.

3) Proyectos Tic-Tac y Chiquimadrid. Iniciativas promovidas por el Ayuntamiento de Madrid, a través del Área de Gobierno de Economía y Empleo, con el apoyo del Plan Avanza del Ministerio de Industria, Turismo y Comercio. Webs: http://www.tic-tac.es y http://www.chiquimadrid.es

El proyecto "Tic-Tac" (Tiempo para educar a través de las TIC) tiene como objetivo proporcionar a la comunidad educativa la información que necesitan para fomentar un uso responsable y seguro de las Nuevas Tecnologías. La web dispone de un apartado para madres y padres, otro para educadores y otro para niños, con numerosos juegos. Además, también encontramos un consultorio con las dudas principales sobre el uso que se debe hacer de Internet, así como una guía multimedia muy útil para los padres. Como complemento, el proyecto "ChiquiMadrid "está más centrado en contenidos y juegos educativos para los niños, ofreciéndoles al mismo tiempo unos consejos muy útiles sobre el uso correcto de Internet, como elemento educativo y de ocio.

4) Wild Web Woods. Iniciativa promovida por el Consejo de Europa. Web: http://www.wildwebwoods.org

Se trata de un juego diseñado para que los más pequeños entiendan el funcionamiento de Internet y para enseñarles unas nociones técnicas que les ayudarán a convertirse en unos internautas prudentes. Además de divertirse, los niños reciben información sobre seguridad en la Red, ya que el juego está basado en el manual del Consejo de Europa titulado "Manual de conocimientos de Internet", que contiene datos y consejos prácticos para padres y profesores.

5) Internet Segura. Iniciativa promovida por IQUA. Web: http://www.internetsegura.net

Se trata de un programa de sensibilización creado por IQUA, que tiene como misión promover el uso seguro de Internet contribuyendo a generar una cultura de responsabilidad, que permita a los niños y adolescentes beneficiarse cada vez más de este nuevo medio. El portal se dirige a padres, educadores y también a los menores. Contiene amplia información sobre los beneficios y los riesgos de Internet, sobre las herramientas de control que existen, las líneas directas y una serie de recomendaciones para padres y niños.

6) Pantallas Amigas. Iniciativa de EDEX e Integral de Medios. Web: http://www.pantallasamigas.net

Sus actuaciones se centran principalmente en la edición de publicaciones y materiales didácticos, la celebración de jornadas divulgativas o la creación de un centro digital de noticias y documentación. El portal incluye un catálogo con recursos educativos para un uso seguro de Internet y las Nuevas Tecnologías para

los menores, que incluyen guías y packs multimedia de carácter educativo sobre Internet, Telefonía móvil y videojuegos.

7) Proyecto Internet Sin Riesgos. Iniciativa de CEDETEL, con la colaboración de TRALALERE y con el apoyo del Ministerio de Industria, Turismo y Comercio dentro del Plan Avanza y de la Consejería de Fomento de la Junta de Castilla y León. Web: http://www.internetsinriesgos.es/index.html

El proyecto Internet sin Riesgos nace con el objetivo de sensibilizar a los niños sobre los riesgos de Internet y transmitirles buenas prácticas de uso, además de sensibilizar e informar a los padres y educadores para que sepan proteger a los menores. Internet sin Riesgos va dirigido a niños de entre 7 y 12 años, a sus familiares (principalmente sus padres), a educadores y a monitores y dinamizadores de cibercentros, centros cívicos y asociaciones.

8) Programa Aprende. Consejería de Fomento, en colaboración con la Consejería de Educación de la Junta de Castilla y León

A través de este Programa, los centros educativos se convierten en el punto de encuentro de jornadas TIC: El proyecto consiste fundamentalmente en una serie de talleres formativos e informativos desarrollados en los propios centros escolares y que están dirigidos principalmente a los padres y a los alumnos. En estos talleres, se asesora sobre el alcance que tienen las Nuevas Tecnologías en la sociedad y en la educación en valores, para lo cual se realizarán ejercicios prácticos con el fin de ayudar a los padres a orientar y controlar el uso que de ellas hacen sus hijos.

9) "Guía sobre el uso inteligente de las nuevas tecnologías". Dirección General de Telecomunicaciones, Consejería de Fomento, Junta de Castilla y León

La "Guía sobre el uso inteligente de las nuevas tecnologías" pretende ser una ayuda para padres y educadores, en el ámbito de las Nuevas Tecnologías, que, día a día, están cambiando la manera en que vivimos, nos relacionamos y aprendemos. Con ella, se busca educarlos, orientarlos y dotarles de los recursos necesarios para que sepan cómo reaccionar y qué medidas tomar ante las situaciones de riesgo.

En cuanto a las líneas de denuncia, las autoridades públicas deben continuar difundiendo eficazmente la existencia de los canales de denuncia existentes:

a) Protégeles. Web: http://www.protegeles.com

Protégeles es una Asociación sin ánimo de lucro dedicada a la seguridad de los menores en Internet. Constituye el nodo español de sensibilización dentro de la red europea INSAFE promovida directamente por la Comunidad Europea. La asociación funciona como una Línea de Denuncia que además de realizar un

seguimiento y comprobación de las informaciones recibidas, realiza una búsqueda proactiva orientada a la eliminación de páginas de pornografía infantil en Internet. Protégeles también organiza y gestiona "líneas de ayuda" o "helplines", para asistir profesionalmente a menores objeto de acoso escolar ("bullying" o "ciber-bullying") www.acosoescolar.info o que padecen trastornos de conducta alimenticia como la anorexia y la bulimia www.anaymia.com y www.masqueunaimagen.com.

b) ACPI: Acción contra la Pornografía Infantil. Web: http://www.asociacion-acpi.org

La Asociación ACPI (Acción contra la Pornografía Infantil) es una ONG cuyo objetivo es luchar contra la explotación sexual de menores: pornografía infantil, prostitución infantil y turismo sexual. Colabora con la ONG Protégeles compartiendo su línea de denuncia. ACPI es miembro de la organización internacional ECPAT Internacional, miembro español de la European Federation for Missing and Sexually Exploited Children y miembro del INHOPE europeo.

c) AGPD. Agencia Española de Protección de Datos. Web: http://www.agpd.es

Entre algunas de sus funciones principales están atender las peticiones y reclamaciones formuladas por las personas afectadas, proporcionar información de manera presencial, telefónica y escrita a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal, velar por el cumplimiento de los términos que establece la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, velar por el cumplimiento del artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

d) Grupo de delitos informáticos de la Guardia Civil. Web: www.gdt.guardiacivil.es

El Grupo de Delitos Telemáticos fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se sirven de Internet o de las Nuevas Tecnologías para su comisión. Este grupo de trabajo integrado dentro del cuerpo de la Guardia Civil tiene como misión llevar a cabo todas aquellas investigaciones relacionadas con la delincuencia informática que le encomienden las Autoridades judiciales o que conozca por comunicaciones y denuncias de los ciudadanos, que por su importancia o relevancia social, dificultad técnica o número de afectados, aconsejen la dedicación de los recursos materiales y humanos más técnicos de la Guardia Civil.

e) IQUA: Internet Quality Agency. Web: http://www.iqua.net

La Agencia de Calidad de Internet (IQUA - Internet Quality Agency), es una entidad de ámbito estatal con vocación Internacional, sin ánimo de lucro, que trabaja en la mejora y la calidad en Internet.

Sus ámbitos de actuación son los siguientes:

- Velar por la calidad de Internet. IQUA ha firmado un acuerdo con la Asociación de Clasificación de Contenidos de Internet (ICRA), para impulsar la protección de los menores ante los contenidos perjudiciales en Internet mediante el sistema del autoetiquetado de las páginas web y del filtrado posterior, convirtiéndose en el representante único de ICRA en España y Andorra.
- Otorgar un sello que acredite la calidad de las páginas web.
- Defender los derechos de los usuarios de la red.
- Resolver extrajudicialmente conflictos relacionados con Internet.

Asimismo, IQUA participa con ICRA y siete organizaciones europeas más, en el Proyecto Quatro (Quality Assurance and Content Description), financiado por la Unión Europea en el marco del Programa Europeo Safer Internet. Este proyecto tiene el objetivo de ayudar a los usuarios de Internet a encontrar aquello que buscan, confiar en aquello que encuentran y evitar cualquier tipo de material que, por el motivo que sea, no quieren ver.

f) INTECO. Web: http://www.inteco.es

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), promovido por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología. Tiene un doble objetivo: contribuir a la convergencia de España con Europa en la Sociedad de la Información y promover el desarrollo regional.

g) Red.es. Web: http://red.es

Red.es es una entidad pública empresarial adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información.

Entre sus funciones destacan:

- Impulsar el desarrollo de la Sociedad de la Información mediante la ejecución de programas definidos en el Plan Avanza para la convergencia con Europa y entre Comunidades Autónomas.
- Analizar la Sociedad de la Información a través del Observatorio de las Telecomunicaciones y de la Sociedad de la Información.
- Ofrecer asesoría y apoyo específico a la Administración General del Estado.
- Gestionar el registro de nombres de dominios ".es".

Dentro del Plan Avanza, desde Red.es se promueven actuaciones para el fomento de las buenas prácticas en el uso de las Tecnologías de la Información y la Comunicación (TIC).

C. La gestión de la seguridad informática

La implantación, desarrollo y expansión de Internet en los más diversos ámbitos de la sociedad ha procurado indudables ventajas: la universalización del conocimiento, el acceso a la información, o la adquisición de una nueva dimensión de la comunicación y las relaciones laborales o sociales que son, entre otras, conquistas históricas que han supuesto un salto cualitativo en la estructura de nuestra civilización.

Por otro lado, la aparición y proliferación en la red de servicios dirigidos, no ya al mundo científico o empresarial, sino al receptor individual demandante de información o de ocio, ha favorecido notablemente la presencia de equipos informáticos en los hogares españoles.

Sin embargo, y en equilibrada contraposición a este enfoque positivista de la “red de redes”, el carácter instrumental de Internet no le permite gozar intrínsecamente de las cualidades de bondad o maldad. La inexistencia de condicionantes físicos o legales ha transmutado a Internet en un reflejo fiel pero ilimitado de la naturaleza humana, con sus luces y sus sombras; y los “navegadores” han dejado de ser un mero icono en el monitor para convertirse en potentes telescopios al alcance de todos los públicos, escudriñando a través de una ventana indiscreta elevada a su máxima expresión, de un espejo mágico perdido en el ciberespacio a la espera de ser encontrado por una mente curiosa, adulta.

Ante esta realidad dual, corresponde a los adultos velar por la integridad y el desarrollo emocional armónico de los menores de edad a su cargo, tutelando el uso que éstos hacen de la red o poniendo los medios necesarios para su seguimiento; corresponde a los menores adquirir criterios que les permitan discernir los contenidos que se les ofrecen en la red y considerar la conveniencia de acceder a ellos.

Para ayudarnos en esta tarea, ya seamos adultos o menores de edad, existen herramientas básicas de control de acceso que los programas navegadores o las aplicaciones del propio sistema operativo ofrecen, para evitar tanto el acceso voluntario o involuntario a páginas web con contenidos inapropiados, como el acceso no autorizado a nuestro equipo informático de páginas web no deseadas.

Por ello, con este apartado, se persigue la consecución de los siguientes objetivos:

a) Controlar el acceso a contenidos inapropiados.

b) Evitar la infección por virus informáticos de los equipos de los centros escolares.

c) Aportar los medios técnicos para facilitar, en los centros educativos y en el hogar, un seguimiento de los contenidos a los que acceden los menores en Internet.

d) Informar a los Centros de las medidas a adoptar para conseguir entornos seguros.

e) Elaboración de material de buena praxis en el uso de medios y recursos informáticos:

- Configuración de los ordenadores para acceso a Internet seguro.
- Configuración de redes seguras.
- Utilización de Software.
- Recomendaciones desde el punto de vista funcional – organizativo.
- Uso eficiente de los ordenadores.

En relación con estos objetivos, el Grupo Interdisciplinar aportó una serie de recomendaciones relativas a la seguridad de los equipos informáticos en los centros educativos, que se presentan a continuación.

1. La seguridad de los ordenadores

1.1. Contraseña de los usuarios

- No eliminar nunca las contraseñas de los usuarios de los equipos. Se pueden cambiar y personalizar.
- No dejar equipos con perfil administrador abierto. De esta forma, evitamos que personas no autorizadas puedan acceder a determinados contenidos.
- Se recomienda utilizar contraseñas de al menos 8 caracteres alfanuméricos.
- Utilizar el perfil del administrador del equipo sólo en caso de querer realizar modificaciones permanentes en el equipo, como instalación de programas, cambios en determinadas configuraciones, etc. Se recomienda que una vez hechas estas modificaciones se cierre la sesión y se cambie a un perfil usuario.

1.2. La configuración del Navegador y el Firewall

Se recomienda configurar los exploradores de forma segura, facilitando pondrá un link en que aparecerán instrucciones concretas para la configuración de los distintas aplicaciones que usen los centros (Explorer, Firefox, etc.).

1.3. La configuración de las redes inalámbricas

Las redes inalámbricas deben estar obligatoriamente protegidas por contraseña. La presencia de uno o varios puntos de acceso sin la debida protección puede propiciar la entrada en la red de personal ajeno al centro.

2. La gestión de las aulas de informática

- Publicar en las aulas de informática, en las zonas donde haya ordenadores fijos, y junto a los equipos portátiles, un pequeño resumen de las indicaciones sobre el buen uso.
- Antes de iniciar la clase, comprobar que todos los ordenadores se han accedido con el perfil adecuado (alumno/profesor), y que tiene el antivirus y el firewall activo.
- Al finalizar la clase, eliminar todos los archivos temporales, cookies, etc. (poner un link con instrucciones en función del tipo de explorador)
- Antes de abandonar el aula, el encargado del aula deberá comprobar que todos los equipos han sido apagados.
- Cerrar las aulas cuando no se estén usando. En caso de utilización de las aulas fuera del horario lectivo, se recomienda la presencia de una persona responsable en las mismas.
- Si no existen en el Reglamento de Régimen Interior del centro, se deben establecer unas pautas de uso de los equipos informáticos por parte de cualquier miembro de la comunidad educativa, especialmente por el profesorado y alumnado.

3. La política general de descargas e instalación de software

3.1. La instalación de software en los equipos del centro

- Todo el software que se encuentra preinstalado en los equipos que se suministran al centro está licenciado y registrado a nombre de la Consejería de Educación de la Junta de Castilla y León.
- Queda totalmente prohibida la instalación y utilización de cualquier software siempre que no se disponga de licencia. El profesor que instale, o encargue la instalación, de cualquier software se responsabilizará de que el software sea legal, registrado y de que dispone del número de serie.
- No se permitirá la instalación de ningún tipo de software a los alumnos.

- Queda prohibido instalar cualquier software fuera de los fines docentes–educativos, se encuentre éste licenciado o no. En este sentido, hay que prestar especial atención a los programas "Peer to peer" (P2P) utilizados para el intercambio de ficheros, y a los accesos a los chats.
- Sí estarán permitidos programas de mensajería instantánea tipo Messenger.

D. Los códigos cívicos para el buen uso de los medios informáticos en los centros educativos

Actualmente, los niños y los jóvenes son citados como los "nativos digitales"7: ciudadanos nacidos en un mundo digital, que crecen rodeados y sumergidos en la tecnología y todos los instrumentos de la era digital. Su confianza en la utilización de la tecnología es, habitualmente, muy alta, pero su conocimiento y percepción de los posibles riesgos puede ser bajo. Por ello, tiene sentido enseñar a los niños a utilizar de forma responsable estas tecnologías de muy pequeñas, y, definitivamente, cuando empiezan el colegio.

A pesar de los beneficios educativos y sociales ofrecidos por las Nuevas Tecnologías, existen, desgraciadamente, algunos riesgos, especialmente para los niños y los jóvenes. Como en cualquier otra área de la vida, los niños son especialmente vulnerables y se exponen al peligro, sea intencionadamente o no, cuando utilizan Internet y otras tecnologías.

Aunque la supervisión de los adultos es una solución preferible, no es totalmente realista o práctica, especialmente fuera de los centros educativos. Por ello ,es necesario poner en alerta a los niños y los jóvenes sobre los riesgos que pueden encontrar al navegar en Internet, ofreciéndoles ayuda para desarrollar un comportamiento responsable y seguro en la utilización de las Nuevas Tecnologías, sea en los centros, en casa o en cualquier otro sitio.

Al considerar los aspectos relacionados con el uso de las TICs, los centros educativos deben tener en cuenta la edad y el conocimiento de sus alumnos sobre estas tecnologías: aunque el mensaje central sobre la seguridad debe ser el mismo, los métodos de presentación tienen que ser distintos.

Los aspectos sobre los cuales se debería poner especial énfasis en la seguridad podrían ser agrupados, globalmente, en cuatro categorías:

a) El contenido.

[7] Ofcom (2006): *The communication market 2006.*

b) El contacto.

c) El comercio.

d) La cultura.

A. El contenido

Al utilizar Internet u otros servicios y tecnologías on-line, existe el riesgo de que los niños y los jóvenes sean expuestos a contenidos inapropiados. Esto puede ser material pornográfico, que contiene violencia, que anima a actividades ilegales o peligrosas, o que es, simplemente, inadecuado para su edad. Uno de los beneficios clave de Internet es que está abierto a todo el mundo, pero, desgraciadamente, esto significa que aquellas personas con puntos de vista políticos extremistas, racistas o sexistas tienen una gran libertad de expresión a través de este medio.

Los centros educativos ofrecen, en algún medida, un cierto nivel de protección frente a este tipo de contenido, pero hasta los programas de filtrado instalados en los equipos informáticos del centro no ofrecen siempre un 100% de seguridad. La supervisión y el control en clase puede ser de gran ayuda, pero este mismo nivel de vigilancia no se puede extender a todos los lugares en donde los niños y los jóvenes utilizan Internet.

Es normal que los niños se crean todo lo que leen en Internet, y muchas veces el contenido online parece ser tan fiable como los escritos oficiales. Por ello, es importante que los centros educativos fomenten la alfabetización digital en todos los sentidos, enseñando a los jóvenes a ser críticos y a poder discriminar entre los distintos materiales que encuentran en Internet y la información que reciben a través de los servicios de "contacto directo", tales como el correo electrónico, el chat o las redes sociales.

Los niños deberían ser conscientes de los riesgos a los que se someten al consultar ciertos tipos de contenido en Internet. Estos riesgos incluyen los virus informáticos, el adware y el spyware. Por ello, es importante enseñarles a cuestionar siempre la fuente y la fiabilidad de cualquier contenido que consultan o descargan y a conocer y saber utilizar las distintas soluciones tecnológicas para minimizar estos riesgos.

B. El contacto

Los riesgos asociados con el contacto son, probablemente, los que reciben más atención por el temor del peligro físico.

Una minoría de delincuentes utiliza Internet y los servicios asociados, como los chats, los juegos y las redes sociales, para relacionarse con los niños y los jóvenes. La intención de estas personas es establecer y

desarrollar relaciones con los jóvenes con el único propósito de persuadirles en actividades sexuales. Los pedófilos, muchas veces, se dirigen hacia un público específico, presentándose como personas jóvenes con intereses y preferencias similares para poder establecer una amistad virtual.

Estas amistades se desarrollan con el paso de los meses o los años, a medida que el pedófilo se gana la confianza de la persona joven, avanzando hacia otras formas de contacto, como los mensajes de teléfono, como una fase previa al encuentro cara a cara. Estas técnicas se conocen como "seducción online", "grooming", etc.

Existe también el riesgo de que mientras están navegando, los niños pueden ofrecer información personal, o establecer citas con personas que han conocido online, y, por tanto, están arriesgando su seguridad o la de su familia o amigos.

Por tanto, parece que las Nuevas Tecnologías ofrece un anonimato a través del cual los acosadores pueden atormentar a sus víctimas a cualquier hora del día o noche. Esta forma de acoso, conocida como ciberacoso, puede afectar a su autoestima y peligrar, por tanto, su bienestar psicológico. Puede que la seguridad física de estos niños no esté en peligro, pero pueden recibir mensajes a través del correo electrónico, del chat o los mensajes de texto, o pueden ser el objetivo de páginas web o perfiles de redes sociales que les hacen avergonzarse, estar tristes, deprimidos o asustados.

C. El comercio

En la utilización de las Nuevas Tecnologías, también existe el riesgo de que los niños puedan hacer transacciones que pueden tener graves consecuencias económicas o comerciales.

El comercio electrónico está continuamente creciendo, y existe el riesgo de que los niños puedan ofrecer información personal cuando navegan, como por ejemplo, los detalles de la tarjeta de crédito de los padres. Esto puede tener consecuencias económicas inesperadas.

El correo basura o el spam puede contener ofertas que parecen demasiado interesantes para perdérselas, mientras que el phishing puede engañar a los niños (y a sus padres) para divulgar información personal o financiera que podría ser utilizada para el robo de identidad.

D. La cultura

Los niños y los jóvenes necesitan una educación y asesoría permanente para la apropiación y el refuerzo de los mensajes de seguridad informática.

Al utilizar las Nuevas Tecnologías, existe también el riesgo de que los niños se vean implicados en actividades inapropiadas o antisociales. Igual que en el mundo real, los grupos se crean rápidamente en el mundo virtual, y este tipo de actividades pueden empezar como una diversión sin posibilidad de daños, como por ejemplo, hacer pública una opinión opuesta a la de otro miembro de un chat. Pero estos comportamientos pueden llegar rápidamente a ser algo mucho más serio. Por ello, se debe enseñar a los niños y a los jóvenes a respetar la opinión y la integridad de los otros usuarios, de la misma manera que en la vida real.

Un área de creciente preocupación últimamente es el comportamiento apropiado en los entornos Web 2.0, es decir en las redes sociales y los blogs. Estos servicios permiten a las personas publicar, colaborar y compartir información de muchas formas. Aunque muchas redes sociales de este tipo tienen restricciones de edad para los nuevos miembros (habitualmente, los usuarios tienen que tener 13 o 14 años para poder registrarse), en ocasiones, no tienen estos tipos de mecanismos, y por tanto, los niños pueden mentir sobre su edad para crear un perfil, mientras que otras redes sociales no tienen ninguna restricción en cuanto a la edad. Por otra parte, en los últimos años han aparecido muchas redes sociales dirigidas especialmente a los niños, que suelen tener un fuerte enfoque en la seguridad informática.

En los entornos Web 2.0, los niños y los jóvenes ya no son solamente receptores de contenido descargado en la red, pero son también participantes activos en el mundo virtual, subiendo contenido al que puede tener acceso una audiencia mundial. En muchos casos, los nuevos usuarios publican información detallada sobre su vida personal y sus rutinas diarias, información de contacto, fotografías y vídeos, sin tener en cuenta las posibles implicaciones del contenido que se publica (que puede ser, a veces, sexualmente provocativo) y de la permanencia de sus perfiles. Por desgracia, en estos sitios también puede aparecer el acoso, la calumnia y las humillaciones de los otros.

El plagio y el copyright también son aspectos culturales clave, especialmente en relación con los trabajos escolares y la descarga de música o juegos, tan populares en muchos servicios de distribución de documentos. Los niños deben comprender que estas actividades pueden tener consecuencias morales, legales y económicas muy serias –la persona más joven, conocida hasta ahora, juzgada por compartir documentos en Internet (en los Estados Unidos) tenía solamente 12 años.

También existe el riesgo de que los niños se obsesionen con las Nuevas Tecnologías, abandonando sus relaciones y el contacto con su familia, como resultado del tiempo que utiliza para estar conectado.

Por todo ello, es importante enseñar a los niños y a los jóvenes cómo ser críticos y discriminar entre los usuarios de los servicios online. Tienen que aprender a valorar el material que encuentran navegando y las relaciones que crean a través de los servicios de “contacto directo”. En el momento en el que aprenden a discernir y a utilizar su propio juicio para determinar lo que es bueno y lo que es malo, es cuando la seguridad

de los niños y los jóvenes es más duradera y está mejor posicionada frente a los nuevos riesgos. Por ello, es esencial que la alfabetización digital tenga en consideración todos estos aspectos culturales.

Para hacer frente a todos estos riesgos, a continuación se presentan una serie de pautas relativas al uso de las diferentes tecnologías que utilizan, hoy en día, los alumnos para comunicarse, para buscar información o para divertirse.

1. El uso de Internet

1.1. El contexto

Internet facilita el acceso de los usuarios a la obtención de información y recursos, para comunicar con otros y para publicar información. Consiste en un sistema mundial de redes de ordenadores, en el cual los usuarios de ordenadores pueden, si tienen permiso, acceder a la información disponible en otros ordenadores de la red.

La cantidad de información disponible en Internet es muy amplia y puede ser realmente intimidante, especialmente cuando buscas algún tipo de información específica. Los motores de búsqueda te pueden ayudar a refinar tu búsqueda.

1.2. Los beneficios

Internet facilita el acceso a una gran variedad de material cultural, educativo e intelectual, que de otra forma no está disponible gratuitamente o fácilmente, y representa un recurso muy potente para el aprendizaje. El acceso es extendido a recursos mucho más allá del centro –a los museos, las galerías y las organizaciones de cualquier tipo. Los recursos pueden presentarse de forma interactiva de manera que los alumnos pueden experimentar y ver cómo funcionan las cosas. Internet también es una excelente fuente de información para los niños, especialmente en cuanto a aspectos más íntimos, sobre los que no quieren hablar cara a cara.

Internet ofrece también medios eficientes para comunicar, que incluyen las videoconferencias, eliminando así muchas barreras a la comunicación.

1.3. Los riesgos asociados al uso de Internet

Aunque la red puede ser una herramienta educativa muy útil, existen algunos riesgos en su utilización. Algún contenido, como la pornografía, el material violento, o la información que impulsa las actividades ilegales, es claramente inapropiado para los niños y los jóvenes. Por otro lado, aunque la adecuación de algunas páginas

web es fácil de juzgar, otras páginas pueden parecer apropiadas en la superficie, pero el contenido puede ser poco fiable o apropiado. Algunos sitios comerciales también pueden ser inapropiados para los niños.

También se cuestiona la fiabilidad, la credibilidad y la validez de la información contenida en algunas páginas web. En el entorno del centro educativo, los profesores pueden evaluar el valor educativo de una página web, y los alumnos tienen que aprender a valorar críticamente los materiales que encuentran.

1.4. Las estrategias para un uso seguro de Internet

1.4.1. Políticas de buen uso

Como parte de su responsabilidad para asegurar un uso seguro de Internet, los centros educativos deben desarrollar una política de buen uso de esta tecnología.

Una política de buen uso ofrece un marco para el uso seguro y responsable de Internet en el centro, y puede ofrecer asesoría a los alumnos y a los padres para utilizar Internet en casa. Normalmente, a través de estas pautas, se configuran los comportamientos seguros y responsables de los alumnos, los procedimientos para informar sobre el material inapropiado, e información sobre cómo proteger los equipos informáticos, por ejemplo, de los virus.

La política debería proveer cobertura para una gran variedad de Nuevas Tecnologías que pueden ser utilizadas, tanto dentro como fuera del centro, como pueden ser el correo electrónico, el chat, la mensajería instantánea, los webcams, los blogs y las redes sociales.

El tono de estas políticas se debe adecuar a la edad de los alumnos: los centros pueden crear diferentes versiones de la estas normas para diferentes grupos de edad.

1.4.2. La evaluación de los materiales de la red

Aunque existe una gran variedad de información fiable en la red, también existe una gran cantidad de información incorrecta, no actualizada o seriamente sesgada. La popularidad de los instrumentos colaborativos de autorización, como son los blogs y los wikis, está aumentando, permitiendo a los visitantes añadir, editar o eliminar contenido, muchas veces sin necesidad de registrarse. Si bien estos recursos pueden ser muy valiosos, contribuyendo a la creación de un gran cuerpo de conocimiento, existe todavía el riesgo que este tipo de contenido sea incorrecto.

De forma similar, no todos los materiales educativos son apropiados a la edad de los alumnos: puede que hayan sido desarrollados para una audiencia distinta. Por ello, es necesaria una evaluación crítica de los

recursos de la red para determinar su fiabilidad y su exactitud. Los alumnos tienen que aprender el valor de este proceso como parte central del desarrollo de sus competencias digitales.

Al evaluar los materiales, los alumnos deberían cuestionar los siguientes aspectos:

- ¿Quién ha publicado el contenido? La dirección URL nos puede dar algunas pistas.
- ¿Cuál es el origen del contenido? Puede proceder de una fuente distinta de la persona que lo haya publicado. ¿Tiene permiso para hacerlo? ¿Está libre de las restricciones de copyright?
- ¿El contenido está actualizado?
- ¿El contenido es fácil de leer y entender?
- ¿Presenta solamente un punto de vista?
- ¿Ofrece el contenido todo lo que necesito?
- ¿Los enlaces son útiles?

1.4.3. El filtrado de los contenidos

La mayoría de los servicios educativos proveedores de Internet ofrecen también un servicio de filtrado de contenidos de Internet. Esta herramienta ayuda a prevenir el acceso a un contenido no deseado y puede filtrar otros servicios, como por ejemplo, el correo entrante y saliente. Otros programas informáticos adicionales se pueden utilizar en los centros para complementar este servicio. Muchas herramientas de filtrado también están disponibles para los usuarios de Internet en casa.

Es importante recordar que, aunque los sistemas de filtrado son herramientas muy eficaces, no son completamente infalibles; por ello, estas herramientas se tienen que complementar con un enfoque responsable sobre la utilización de Internet en cualquier momento.

1.4.4. Los útiles de búsqueda de Internet

La red ofrece una gran cantidad de información en una gran variedad de formatos. Sin embargo, la extensión de Internet puede representar un inconveniente muy grande; son necesarias una serie de útiles y técnicas de búsqueda para localizar la información de forma rápida y fácil.

Los motores de búsqueda ofrecen una forma de navegar en Internet utilizando palabras clave. Aunque con solamente escribir una palabra clave o frase en un motor de búsqueda, se ofrece rápidamente una lista de páginas web que contienen esa palabra, sin embargo el inmenso volumen de enlaces es impracticable y el

nivel de los potenciales enlaces útiles es muy bajo. Por ello, los alumnos deben conocer y aprender los principios de una búsqueda eficiente como parte del desarrollo de las competencias digitales clave.

Para una búsqueda exitosa en Internet, es necesaria una planificación cuidadosa y una definición de las necesidades exactas de información. La mayoría de los motores de búsqueda ofrecen técnicas avanzadas de búsqueda que permiten a los usuarios definir sus búsquedas de forma más precisa. Aunque los comandos de búsqueda pueden variar entre los distintos motores de búsqueda, los conceptos siguen siendo los mismos, y de esta forma las habilidades adquiridas son transferibles.

Como alternativa a la búsqueda por palabras clave, un directorio o una búsqueda basada en un menú que cataloga la información de la red en tópicos, empezando por los menús de tópicos generales que se refinan gradualmente a través de las elecciones del usuario hasta que se encuentra la información relevante. Una búsqueda basada en un menú puede ofrecer un método estructurado de búsqueda, pero produce una lista que comprende solamente aquellas páginas web indexadas por el proveedor del motor de búsqueda.

Muchos motores de búsqueda ofrecen opciones de filtrado para eliminar las páginas web inadecuadas y la publicidad de los resultados de la búsqueda; existen también motores de búsqueda dirigidos especialmente a los niños y a las familias.

1.4.5. La adaptación de los buscadores de la red

La mayoría de los buscadores de la red ofrecen opciones de adaptación para permitir ajustes de seguridad, privacidad y contenido de las búsquedas.

2. El uso del correo electrónico

2.1. El contexto

El correo electrónico representa una excelente forma para enviar mensajes a través de Internet. Cualquier material se puede adjuntar o incluir al correo, tales como texto, imagen, sonido, animaciones o películas.

2.2. Los beneficios

El correo electrónico puede ser un instrumento extremadamente valioso en los centros educativos, impulsando el desarrollo de las habilidades comunicativas y transformando el proceso de aprendizaje abriendo posibilidades que, de forma tradicional, no existirían.

Los profesores han informado que el uso del correo electrónico ayuda a los alumnos a tener más cuidado con su ortografía (un correo con una dirección incorrectamente escrita no llegará al destinatario) y más precisos con las palabras que utilizan, ya que fomenta la brevedad y la claridad de los mensajes.

El correo electrónico puede ser realmente gratificante para los alumnos con necesidades educativas especiales. Los alumnos con discapacidad física o cognitiva pueden necesitar mucho tiempo para elaborar los mensajes, pero los destinatarios no sabrán que han tenido dificultades. Los alumnos con discapacidad auditiva pueden encontrar en el correo electrónico un canal alternativo de comunicación muy accesible.

2.3. Los riesgos

A pesar de estas ventajas, el correo electrónico está abierto al abuso, que puede presentar bajo distintas formas:

2.3.1. El spam, spoofing, phising y pharming

El spam es correo electrónico no deseado, muchas veces de fuentes no familiares. El spam contiene, muchas veces, contenido inapropiado, como la publicidad engañosa - posiblemente bajo la pretensión de un premio– o la pornografía. Los spammers reúnen direcciones de correo electrónico de páginas web y grupos de discusión, pero existen también empresas especializadas en la creación de listas de correo de distribución.

El spoofing de los correos electrónicos se utiliza para avergonzar al destinatario, para supervisar el origen de los correos contenedores de virus y, a veces, para obtener información importante de los receptores de spam.

El spam y el spoofing son prácticas similares conocidas bajo el nombre de “phishing” o “pharming”. Estos correos electrónicos y páginas web imitan la marca y la identidad de bancos o empresas financieras conocidas con el objetivo de engañar a la gente para revelar información financiera personal, que se utiliza después de forma fraudulenta. El robo de identidad puede tener serias consecuencias económicas.

2.3.2. El flaming

Este término se utiliza para definir a los correos violentos o abusivos que se envían de una persona a otra, muchas veces en el contexto de un grupo de discusión o los chats.

2.3.3. El acoso

El correo electrónico puede facilitar el acoso entre los niños, siendo víctimas de mensajes no deseados u obsesivos.

2.3.4. El “bombing” o el bombardeo

Una “bomba” es un programa que intenta quebrar otro programa. Un correo electrónico bomba es un mensaje muy grande de correo, o un volumen muy grande de mensajes, enviados con la intención de quebrar el programa de correo electrónico del receptor.

2.3.5. Los virus

Un virus de ordenador puede causar problemas serios, posibilitando la destrucción de archivos y permitiendo el acceso de los piratas informáticos al disco duro del ordenador. Los virus se pueden transmitir a través de los archivos adjuntos al correo electrónico. También se pueden enviar desde correos electrónicos falsos que aparecen como si fueran enviados desde personas que conocemos.

2.3.6. Los proveedores de servicios de correo electrónico de la red

Algunas cuentas gratis de correo electrónico incorporan peligros inherentes. Algunos proveedores permiten que las direcciones de correo electrónico estén compartidas con otras personas, elevando así el riesgo de recibir spam. Sin embargo, muchos servicios de correo electrónico ofrecen herramientas anti-spam muy eficaces, aunque muchas veces estas herramientas son opcionales.

2.4. Las estrategias para un uso seguro

Cuando los niños utilizan el correo electrónico, tienen el riesgo de recibir mensajes inapropiados. Por ello, los alumnos deberían aprender a adoptar un comportamiento adecuado cuando reciben este tipo de mensajes. Es importante enseñarles y explicarles que, a este tipo de mensajes, no deben responder, sino cerrar el mensaje y buscar consejo a los profesores. Esto permite al profesor verificar el mensaje, hablar sobre algunos aspectos, y tranquilizar al alumno, explicándole que no es su culpa.

Por otro lado, los alumnos también deben aprender a utilizar correctamente el correo electrónico y a desarrollar protocolos adecuados para escribir mensajes.

A continuación, se presentan algunos aspectos a considerar a la hora de asegurar un uso seguro del correo electrónico:

2.4.1. Políticas de buen uso

Además de ofrecer una guía para un uso adecuado de Internet, una política de uso seguro de los medios informáticos en los centros debe también ofrecer unas recomendaciones claras para el uso del correo electrónico. Estas pueden incluir orientación sobre el tono apropiado y el lenguaje a utilizar en los correos electrónicos, políticas sobre el uso de las cuentas de correo electrónico, y medidas para proteger la red del

centro de los virus informáticos. Por otro lado, los centros educativos deberían compartir estas orientaciones con los padres para proveer a los alumnos de un marco general para un uso seguro del correo electrónico también fuera del centro escolar.

2.4.2. Las cuentas de correo electrónico

La mayoría de los centros educativos deberían limitar el uso del correo electrónico dentro del centro por motivos de gestión, pero, en todo caso, es importante tener mucho cuidado que los alumnos no puedan ser identificados a través de su cuenta de correo, fuera del centro educativo.

Una cuenta de correo electrónico de clase o de grupo puede ser la solución más apropiada para los alumnos más jóvenes. Las cuentas individuales se pueden crear a medida que los alumnos adquieren las habilidades apropiadas y el conocimiento necesario para comprender las implicaciones de seguridad informática. Muchos centros empiezan a utilizar los entornos virtuales de aprendizaje que utilizan el correo electrónico dentro del centro; sin embargo, a estos entornos se puede tener acceso también desde fuera del centro. En este sentido, hay que tener mucho cuidado con el uso del correo electrónico fuera del sistema interno de correo.

2.4.3. Los proveedores de servicios de correo electrónico de la red

Los centros educativos normalmente prohíben el uso de las cuentas gratis de correo electrónico dentro de la escuela. Sin embargo, algunos alumnos lo pueden utilizar fuera del centro. Por ello, es importante enseñarles a verificar los acuerdos de privacidad de tales servicios y a no consentir que sus datos personales sean compartidos con tercios, para minimizar la cantidad de spam que puedan recibir.

2.4.4. El acoso a través del correo electrónico

Es importante que los alumnos conozcan las características del acoso a través del correo electrónico, los efectos que puedan tener sobre el receptor, pero también estrategias para manejar este tipo de situaciones.

2.4.4. Los servicios de filtrado

De la misma manera que el acceso a Internet puede ser filtrado, los mensajes de correo electrónico también deberían tener filtros en contra de los contenidos inapropiados y el spam. Es importante recordar que aunque estos servicios de filtrado son eficaces, no son infalibles, y, por tanto, el uso de estos programas debe ir siempre acompañado de una guía de uso responsable del correo electrónico.

2.4.5. Los virus

Los ficheros adjuntos al correo electrónico deberían siempre ser tratados con precaución. Algunos virus se adjuntan al mensaje sin el conocimiento del remitente: si una dirección de correo electrónico es objeto del

spoofing, entonces los mensajes con virus pueden aparecer como si hubiesen sido enviados por personas que conocemos o en las que confiamos. El antivirus debería utilizarse siempre para revisar el correo saliente y el correo entrante, y, especialmente, a la hora de abrir o descargar ficheros adjuntos.

3. El uso del chat y de los servicios de mensajería instantánea

3.1. El contexto

El chat es una forma de comunicación a tiempo real con otras personas, a través de Internet, en espacios virtuales de encuentro específicos. Existen muchos sitios de chat disponibles en Internet. Pueden formar parte de una página web, constituyéndose así como una opción dentro de los juegos o un servicio ofrecido por el proveedor de Internet.

Habitualmente, los usuarios deben registrarse, eligiendo un nombre de usuario y una contraseña; el nombre de usuario es, muchas veces, un seudónimo o un nombre falso.

Normalmente, en estos sitios, existe una lista de los usuarios que están conversando, y cuando entran nuevos usuarios, se advierte a todo el mundo de su entrada en el chat. Para contribuir a la conversación, el usuario puede escribir un mensaje en la ventana de conversación, y el mensaje se mostrará en la pantalla para que todo el mundo lo vea y para que respondan si quieren.

Los usuarios también pueden entrar en un sitio de chat sin tener que contribuir a la discusión, viendo lo que los otros están diciendo. Esto se conoce como *acecho* (lurking, en inglés), una práctica aceptada que representa una buena forma de familiarizarse con el funcionamiento del chat.

Muchos sitios de chat ofrecen también espacios privados para que los usuarios puedan conversar sin que los otros usuarios vean su discusión.

Algunos sitios de chat son públicos, pudiendo acceder a ellos cualquier persona, mientras que otros son privados y pueden utilizarlos solamente por personas invitadas y grupos específicos.

Los servicios de mensajería instantánea es una forma de chat online, privada entre dos personas. No están moderados, y no pueden ser utilizados por otros usuarios. Cuando envías un mensaje instantáneo, llega casi de inmediato a la persona a la que lo envías, apareciendo en la pantalla de su ordenador. Algunos servicios permiten enviar archivos o realizar conversaciones de voz a través de Internet. La mensajería instantánea se conoce también como“IM” o “IMing”. MSN Messenger, Internet Relay Chat y ICQ son algunos ejemplos de programas de mensajería instantánea.

Para poder utilizar este tipo de servicio, es necesario instalar un programa específico en el ordenador, y utilizar una lista de contactos con los que puedes intercambiar mensajes. Habitualmente, tienes que invitar a personas para que aparezcan en tu lista de contactos, pero también aceptar aparecer en la lista de otras personas.

3.2. Los beneficios

Aunque considerados principalmente como una actividad de ocio, los sitios de chat pueden ofrecer también beneficios educativos. Los alumnos pueden conversar con sus iguales de cualquier sitio del mundo, en tiempo real, para compartir experiencias, estilos de vida y trabajar en colaboración. Los chats online tienen, frecuentemente, un anfitrión, tales como un empresario o un personaje de televisión, permitiendo el acceso a una gran cantidad de información y experiencias que no estarían disponibles de otra manera para los alumnos. La mensajería instantánea puede, igual que el chat, ofrecer muchos beneficios como método de comunicación instantáneo y eficiente.

3.3. Los riesgos

Los sitios de chat presentan aspectos de anonimato, de forma que los niños pueden hablar, muchas veces, sobre cosas que normalmente no tendrían la confianza de decir cara a cara. Pueden fingir ser otra persona: mayor, más inteligente y más popular. Aunque esto constituye un aspecto positivo para muchas personas, otros usuarios pueden abusar de estas opciones. El uso de seudónimos está aceptado y recomendado en los sitios de chat y, aunque esto asegura tu anonimato, también significa que nunca puedes estar seguro de con quien estás hablando.

Los sitios de chat han atraído, desgraciadamente, a delincuentes, especialmente a los pedófilos que utilizan el anonimato para acosar a los niños, desarrollando relaciones online con el único objetivo de persuadirles en realizar actividades sexuales.

Igual que en las escuelas, en los sitios de chat se pueden formar grupos. Estos grupos utilizan muchas veces una serie de acrónimos para hacer sus conversaciones privadas y excluir a otros. Desafortunadamente, esto también puede llevar al acoso.

En el caso de la mensajería instantánea, los usuarios están informados cuando un usuario está conectado. Sin embargo, si se utiliza en un ordenador compartido, el servicio de mensajería instantánea puede conectarse de forma automática cuando otro usuario se conecta a Internet, confundiendo a los otros usuarios sobre quién está conectado.

Existe también un aspecto relacionado con la privacidad en cuanto a los detalles requeridos para registrarse en un servicio de mensajería instantánea. Esta información podría estar disponible para otras personas.

3.4. Las estrategias para un buen uso

Muchos centros educativos limitan el acceso a este tipo de servicios, de forma que muchos de estos aspectos relativos a estos servicios están asociados, principalmente, a su uso en casa. Sin embargo, es importante que los alumnos sean conscientes de los riesgos y las formas de evitarlos, como parte del desarrollo de sus competencias digitales.

3.4.1. Políticas de buen uso

Las políticas de uso adecuado de los centros deberían incluir también orientaciones sobre la utilización del chat y de la mensajería instantánea, tanto dentro de las escuelas como fuera. Esta información se debe compartir con los padres, especialmente porque el uso de estas tecnologías, con sus riesgos asociados, se realiza más a menudo fuera del centro educativo.

3.4.2. La privacidad de los datos personales

Cualquier persona que utiliza el chat o la mensajería instantánea debería tener cuidado con la cantidad de información personal que revelan cuando se conectan. Es fundamental recordar a los niños que, aunque sientan que conocen muy bien la persona con la que están conversando, hay que tener cuidado cuando se habla sobre aspectos íntimos. La “información personal” va más allá de los detalles evidentes como el nombre, la edad y la dirección, hasta información sobre el nombre de los amigos, actividades extra escolares, o detalles sobre la localización –estos detalles, reunidos, pueden formar un perfil muy minucioso de la persona. Esto lleva a la identificación o, incluso, el contacto de la persona en cuestión.

Si el registro es necesario para utilizar el chat o la mensajería instantánea, los alumnos se deben asegurar de que ofrecen la menor cantidad de información personal posible, pero también deben tener mucho cuidado con los acuerdos de privacidad para que sus datos personales no estén disponibles públicamente. Por otro lado, los alumnos deberían elegir no aparecer en el listado de miembros, ya que, de esta forma, su información personal será disponible para todo el mundo.

3.4.3. Los chats moderados

Algunos sitios de chat están monitorizados o moderados. Esto significa que existe sea una persona que supervisa todo lo que se dice y se asegura de que los contribuyentes hablan sobre el tema establecido (monitorización proactiva), sea una tecnología que controla la conversación y advierta al moderador si detecta alguna conversación inapropiada (monitorización reactiva).

La moderación proactiva es mejor en el contexto educativo, porque el moderador puede entrar en la conversación y asegurarse de que todo lo que se dice está dentro del tema del chat.

Además, todos los sitios buenos de chat tendrían que tener una declaración y una política clara sobre la privacidad, un archivo de las conversaciones anteriores y una guía sobre los temas previstos.

Fuera del centro educativo, es muy probable que los niños encuentren sitios de chat inapropiados; por eso, es esencial que sean conscientes de los riesgos y puedan adoptar un comportamiento seguro y responsable a la hora de utilizar estos servicios.

3.4.4. El acoso

Los alumnos deberían saber qué hacer si sufren acoso en un sitio de chat. En este sentido, no deberían responder con violencia, sino guardar una copia de la conversación para poder utilizarla para denunciar la situación. Para ello, se debe contactar con los moderadores de los chat para recabar cuanto más información posible sobre el acosador, como por ejemplo, el nombre de usuario, la fecha y la hora del suceso, etc.

A partir de aquí, los proveedores de servicios de Internet pueden empezar a poner en marcha las acciones adecuadas a la situación, como advertir al acosador de que este tipo de comportamiento es inaceptable o prohibir completamente la participación de este usuario en el chat.

En el caso de la mensajería instantánea, los usuarios deben contactar con el proveedor del servicio, ofreciendo como información el nombre de usuario, la fecha y la hora, y otros detalles de la situación sufrida. A partir de este momento, el proveedor del servicio debe poner en marcha acciones adecuadas, que pueden incluir una advertencia o la desconexión del usuario acosador del servicio de mensajería instantánea.

3.4.5. Las listas de contactos

Es aconsejable que los alumnos añadan a su lista de contactos solamente a aquellas personas que conocen; por otro lado, debería siempre utilizarse un servicio de mensajería instantánea que evita que otras personas se añadan a la lista de contactos sin la autorización del propietario de la cuenta.

3.4.6. La conexión automática

Muchos programas de mensajería instantánea se conectan automáticamente al servicio cuando los usuarios tienen acceso a Internet. Por ello, los niños deberían siempre verificar que la persona con la que están conversando es realmente la persona que creen que es. También es posible ajustar la privacidad de la cuenta de los programas de mensajería instantánea para pedir siempre una contraseña antes de que un nuevo usuario se conecte. Por otro lado, algunos programas de mensajería instantánea ofrecen a sus usuarios la posibilidad de conectarse de forma invisible si no quieren recibir mensajes.

3.4.7. Los virus

Es importante tener mucho cuidado también con los virus a la hora de enviar y recibir ficheros adjuntos a través de la mensajería instantánea e, igual que con el correo electrónico, estos ficheros deben ser siempre revisados con el antivirus.

4. El uso de los programas de interacción social

4.1. El contexto

La aparición de los instrumentos de interacción social es, quizás, uno de los avances más grandes del mundo virtual, en los últimos años.

Los blogs fueron unos de los primeros útiles de este tipo que ofrecen la posibilidad de crear diarios virtuales. Estos fueron seguidos por los blogs móviles (blogs enviados desde un teléfono móvil), los wikis (páginas web colaborativas y modificables), etc. Estos instrumentos impulsan y ganan valor a través de la interacción social, y ofrecen oportunidades para la manifestación de la inteligencia colectiva.

El concepto de "red social" o "Web 2.0" es normalmente utilizado para describir las comunidades virtuales en las cuales el contenido, como por ejemplo, los textos, las fotos, la música y los videos, lo crean y lo comparten los usuarios. Las características adicionales de estos útiles permiten a los usuarios crear perfiles, publicar comentarios, intercambiar mensajes instantáneos y desarrollar listas de amigos. Ejemplos de comunidades de redes sociales incluyen sitios web como Facebook, Tuenti, MySpace, Bebo, etc. y aquellos que se centran en tipos específicos de contenido o intereses, tales como Flickr (en donde se comparten fotos) y Youtube y Google Video (en donde se comparten videos).

La popularidad de los sitios de redes sociales es sorprendente. Los datos arrojados por el último informe realizado por comScore -empresa líder en la medición del mundo digital– sobre la utilización de las redes sociales en España y Europa en el año 2008[8], demuestran que más del 74% de los internautas europeos han visitado por lo menos una red social en el último año, mientras que en España este porcentaje se eleva al 73,7% de los internautas. Esto significa que casi 13 millones de españoles han utilizado esta herramienta durante el último año, un incremento de casi 41% con respecto al año 2007.

[8] http://www.comscore.com/press/release.asp?press=2733

Aunque la mayoría de las comunidades de redes sociales tienen restricciones de edad para los nuevos usuarios (normalmente, deben ser mayores de 13 o 14 años para poderse registrar), hay muchos otros sitios web que no tienen implementados mecanismos de verificación de la edad y, por tanto, los niños pueden simplemente mentir sobre su edad para crear un perfil, mientras que otros sitios web no imponen restricciones de edad en ningún caso. Por otro lado, existen redes sociales, que cada vez tienen una mayor presencia y que se dirigen a grupos específicos, entre ellos, a niños y jóvenes, y en donde se pone mucho énfasis en la seguridad informática.

4.2. Los beneficios

Los instrumentos de interacción social ofrecen nuevas oportunidades para expresarse, permitiendo a los usuarios crear comunidades, colaborar, experimentar, compartir y aprender en un mundo virtual. Estas herramientas han sido muy bien recibidas por los jóvenes, ya que representan una excelente fuente de información y divertimento, que utiliza, además, la aprobación y los comentarios críticos del trabajo que se crea. Estos útiles pueden ofrecer también excelentes beneficios educativos a través de los entornos virtuales de aprendizaje, que permite un aprendizaje flexible y accesible online para los alumnos.

4.3. Los riesgos

Es importante recordar que las comunidades de redes sociales no son entornos solamente dirigidos a los jóvenes. Son espacios públicos tanto para adultos como para jóvenes, y el contenido publicado lo puede consultar una audiencia mundial.

A pesar de que las redes sociales animan a los jóvenes a ser usuarios creativos en Internet, publicando contenido y no siendo consumidores pasivos, lo que se está publicando necesita atención especial. La preocupación se mueve desde el contenido que descargan los niños al contenido que se sube a la red.

Algunos jóvenes publican información detallada sobre sus vidas personales, incluyendo datos de contacto, detalles sobre sus rutinas diarias, fotografías y videos, ofreciendo, de esta forma, un catálogo online para los que buscan explotar a los niños y a los jóvenes, sea con intenciones sexuales o para el robo de identidad. Además, se han registrado casos en los cuales los jóvenes han publicado contenido inapropiado, como por ejemplo, fotos y videos propios, aparentemente inconscientes de la visibilidad y de la permanencia de este contenido, mucho más tiempo después de que sus perfiles habían sido actualizados o suprimidos. Por otro lado, desgraciadamente, los sitios de redes sociales pueden también constituir una plataforma ideal para la manifestación del acoso y la humillación de otros usuarios.

Actualmente, los mejores sitios de redes sociales toman muy seriamente en consideración estos aspectos, ofreciendo orientaciones y normas de buenas prácticas y animando a los usuarios a denunciar el abuso.

En este sentido, en el marco europeo, 17 grandes empresas informáticos han firmado el 10 de febrero de 2009, en el día del Internet Seguro en Europa, organizado por la Comisión Europea, un acuerdo para mejorar la seguridad de los menores de 18 años que utilizan los sitios de redes sociales. Entre las empresas que han firmado este pacto, se incluyen Arto, Bebo, Dailymotion, Facebook, Giovani.it, Google/YouTube, Hyves, Microsoft Europe, Myspace, Nasza-klaza.pl, Netlog, One.lt, Skyrock, StudiVZ, Sulake/Habbo Hotel, Yahoo!Europe, y Zap.lu. Estas empresas se comprometieron a poner restricciones para el uso de las redes sociales por parte de niños demasiado jóvenes para utilizar sus servicios, así como a colocar en su sitio un 'Informe de abuso' accesible y fácil de usar. También hicieron públicas sus intenciones de hacer claramente visibles las opciones de elegir entre diferentes grados de protección de la intimidad en cuanto a los accesos a los perfiles. Por último, los perfiles de los menores serán dados de alta automáticamente en modo privado, accesible sólo a los 'amigos' e inaccesibles desde los buscadores.

4.4. Las estrategias para un buen uso

Actualmente, hay mucho debate sobre el acceso a las comunidades de redes sociales dentro del ámbito educativo. Las decisiones sobre permitir o no el acceso dentro de los centros se realizan, normalmente, a nivel local, basadas en necesidades, aspectos y riesgos locales. Muchos centros utilizan los blogs para conseguir un efecto educativo positivo, enseñando a los niños a construir competencias y habilidades comunicativas eficaces.

Sin embargo, está claro que si el uso de estas herramientas está prohibido dentro de los centros, los jóvenes van a seguir accediendo a ellas fuera de estos establecimientos. El eurobarómetro realizado por la Comisión Europea en el año 2008, sobre el uso seguro de Internet desde la perspectiva de los padres[9], demuestra que en la mayoría de todos los estados miembros de la Unión Europea, por lo menos dos tercios de los padres dijeron que sus hijos utilizan Internet. Por otro lado, los niños cuyos padres eran usuarios frecuentes de Internet, lo eran ellos también, mientras que la mitad de los padres que no utilizaban Internet dijeron que sus niños sí tenían acceso a Internet.

[9] European Commission (2008): Flash Eurobarometer "Towards a safer use of Internet for children in the EU – a parents´perspective". http://ec.europa.eu/information_society/activities/sip/surveys/quantitative/index_en.htm

Esta carencia general de concienciación de los padres sugiere que la responsabilidad para enseñar a los jóvenes a utilizar las herramientas de interacción social recae sobre los centros educativos. Estrategias clave para un uso seguro de estas herramientas incluyen:

4.4.1. Respetar las restricciones de edad

La mayoría de los sitios de redes sociales tienen restricciones de edad para sus miembros. A la hora de registrarse en uno de estos sitios, los usuarios deben estar de acuerdo con los términos y las condiciones expuestas –muchas páginas web rescinden algunas cuentas si creen que sus usuarios no cumplen con las condiciones de edad. Por ello, es importante buscar y utilizar herramientas de interacción social desarrolladas por organizaciones fiables específicamente para los niños –muchas de estas herramientas ofrecen experiencias sociales para los niños dentro de un entorno seguro y moderado.

4.4.2. Guardar la información personal

Los alumnos deben aprender a guardar la información personal cuando utilizan las herramientas de interacción social, pero también a proteger la información personal de otros. Esto no incluye solamente los datos evidentes como el nombre, la dirección, el número de teléfono y el nombre del centro al que acude, sino también los detalles menos evidentes como lugares preferidos para quedar con los amigos, información sobre los amigos, actividades extra escolares, ya que todo ello se puede utilizar para reconstituir un perfil exhaustivo de identificación del usuario.

Es importante animar a los niños y a los jóvenes a utilizar las características de privacidad que ofrecen las redes sociales, permitiendo el acceso solamente a aquellas personas que conocen también en el mundo real. La privacidad se extiende también a las direcciones de correo electrónico: los usuarios de las redes sociales deberían crear una dirección de correo electrónico anónima que se podría eliminar o cambiar con facilidad, para prevenir el acoso o la recepción de mensajes inadecuados.

4.4.3. Publicar contenidos de forma responsable

Los jóvenes necesitan aprender a ser editores responsables dentro del mundo de las redes sociales. Por ello, deben saber valorar la longevidad del contenido que publican y comprender que cualquier contenido que suben a la red está fuera de su control desde el momento en el que se publica, ya que el contenido online se puede leer, copiar, compartir y manipular con facilidad y rapidez en el mundo virtual.

Por otro lado, los niños deben aprender a respetar los derechos de los otros usuarios, no publicar información que puede comprometer su identidad o seguridad y evitar ser maliciosos o abusivos con los otros en sus interacciones. Además, es importante que los niños aprendan también a valorar los derechos de propiedad

intelectual de los otros cuando publican algo en Internet, asegurándose siempre de que las imágenes, los vídeos o la música que incorporan a sus perfiles no están protegidos por los derechos de autor.

4.4.4. Guardar a los amigos online en el mundo virtual

Algunos jóvenes tienen cientos de amigos online. Por ello, los jóvenes deben aprender a distinguir entre las personas que conocen, ya que los amigos online no son amigos verdaderos, y nunca pueden estar seguros de que son quienes realmente dicen que son. En este sentido, los niños no deberían nunca divulgar información personal que podría identificarles y podría ser utilizada en contra suyo en el futuro. También deben ser conscientes que los "consejos amistosos" de los amigos online podrían ser utilizados como una forma de manipulación. Como pasa con cualquier otra herramienta de contacto online, cuando utilizan las redes sociales, nunca deberían citarse con personas que solamente han conocido a través de Internet.

4.4.5. Limitar el tiempo utilizado para estar conectado

Es fundamental animar a los niños a limitar su tiempo utilizado para estar conectada a Internet, gestionando y equilibrando el tiempo empleado para las redes sociales con el tiempo dedicado a los amigos y a las actividades sociales del mundo real.

4.4.6. Utilizar los consejos prácticos de seguridad

Muchos de las páginas de redes sociales se toman muy en serio los aspectos relativos a la seguridad de sus usuarios. Por ello, es importante aconsejar a los niños a buscar información y consejos sobre la seguridad en los sitios que están utilizando, respetar las normas y las condiciones de los distintos sitios, pero también utilizar las opciones de denuncia de abusos que ponen a su disposición.

5. El uso de los servicios de intercambio de ficheros

5.1. El contexto

Los servicios de intercambio de ficheros, conocidos también como redes peer-to-peer (P2P), utilizan configuraciones de distribución de la red para permitir a sus usuarios compartir información en distintos formatos. Los usuarios se conectan uno con el otro de forma directa, sin la necesidad de que exista un punto central de gestión de las interacciones. Los programas de intercambio de ficheros se utilizan habitualmente para descargar y compartir música, imágenes, programas informáticos, vídeos, juegos y documentos.

Muchos de los programas de intercambio de ficheros están disponibles en Internet. Las aplicaciones informáticas más conocidas de este tipo son Kazaa, eMule y LimeWire. Algunos son gratis, mientras que otros perciben un coste nominal para descargar el programa.

Algunas versiones gratis de estos programas incluyen banners y publicidad, spyware, etc. Los programas que perciben costes por su descarga normalmente no incluyen este tipo de complementos, pero si ofrecen otras facilidades, tales como los chats con voz y el Internet Relay Chat.

5.2. Los beneficios

Las redes de intercambio de ficheros, como los servicios de chats, pueden desarrollar el sentido de comunidad entre sus usuarios, especialmente en áreas como los juegos. El uso de las redes de intercambio está pensado como una actividad recreativa; es poco probable de que pueda tener alguna aplicación en el entorno educativo, aunque esta situación puede cambiar en el futuro.

5.3. Los riesgos

Existen varias preocupaciones relacionadas con el intercambio de documentos:

5.3.1. La propiedad intelectual

Un riesgo clave de las redes de intercambio de ficheros es que la disponibilidad de muchos de los ficheros disponibles es ilegal y, por tanto, aquellos que descargan esos ficheros están infringiendo los derechos de propiedad intelectual. Existen, sin embargo, un número importante de sitios web autorizados, como Napster o iTunes, en donde los ficheros pueden ser descargados a cambio de un pequeño precio, sin necesidad de infringir la ley.

5.3.2. La exposición a contenidos inapropiados

Al utilizar los servicios de intercambio de ficheros, existe el riesgo de que los niños se puedan exponer a un contenido inapropiado o ilegal. Esto se puede presentar en forma de canciones con letra inapropiada para su edad o demasiado explícita, o imágenes o vídeos que tienen títulos o descripciones incorrectas o que pueden confundir. Desgraciadamente, algunos usuarios de las redes P2P suben a la red contenido pornográfico u ofensivo, disimulado el fichero con un título “inocente”, como el nombre del último estreno en películas familiares, para atraer a los más jóvenes.

5.3.3. La exposición a contactos inapropiados

Muchas aplicaciones P2P ofrecen servicios adicionales, tales como el chat con voz y el Internet Relay Chat. Por ello, se deberían aplicar las mismas reglas que cuando se utilizan los chats o cualquier otro medio de comunicación: no ofrecer datos personales y si cualquier conversación te hace sentir incómodo, abandona esa discusión y no respondas. También puede ser prudente cambiar de nombre de usuario.

5.3.4. Los virus y los piratas informáticos

Los usuarios de las redes P2P se exponen a un alto nivel de riesgo por infecciones de virus informáticos e intentos de pirateo. A la hora de afiliarse a una red de este tipo, se pregunta al usuario cuál es el directorio del disco duro que se utilizará para permitir que los otros usuarios tengan acceso, pero es muy difícil asegurar que el resto del ordenador estará completamente seguro.

5.4. Las estrategias para un buen uso

Dado que, actualmente, es muy poco probable que las redes P2P tengan alguna aplicación en el entorno educativo, los centros educativos podrían decidir bloquear la instalación de los programas de intercambio de ficheros en las redes de los centros. Sin embargo, es muy probable que los niños accedan a estas redes en otros contextos. Por ello, el centro educativo tiene la obligación de educar a sus alumnos con respecto a estos aspectos.

5.4.1. Utilizar siempre solamente servicios autorizados

Como ya se ha comentado anteriormente, la descarga de copias no autorizadas de ficheros es ilegal y puede tener serias consecuencias jurídicas y legales. Sin embargo, existen muchos servicios que ofrecen una descarga legal de ficheros a cambio de un pequeño coste. Por otro lado, hay que tener cuidado también con estas transacciones, ya que pueden tener implicaciones económicas importantes para los niños.

5.4.2. Utilizar los instrumentos de filtrado

Muchas aplicaciones P2P, tales como Kazaa, ofrece un servicio de filtrado basado en datos descriptivos, para excluir ficheros que puedan tener contenido ofensivo o pornográfico. Sin embargo, este tipo de filtros son efectivos solamente si el creador de la lista tiene el tiempo y la voluntad de hacerlo; algunos creadores de este tipo de listas adjuntan palabras que pueden confundir como forma para distribuir contenido inapropiado.

Algunos programas P2P permiten también bloquear un tipo específico de fichero, como pueden ser las imágenes o el vídeo, o los ficheros ejecutables con extensiones del tipo .exe, .vbs o .scr, que pueden

contener virus. Es importante recordar que algunos programas de filtrado para el uso del Internet en casa no permite el bloqueo del acceso a las aplicaciones de intercambio de ficheros.

5.4.3. La seguridad

Cualquier persona que esté utilizando programas de intercambio debería asegurarse de que todos los ficheros descargados estén inspeccionados con el antivirus, y que el servicio de firewall está funcionando adecuadamente.

ANEXOS

GLOSARIO

A

ADSL: Línea de suscripción digital asimétrica. Tecnología para transmitir información digital a elevados anchos de banda. La tecnología ADSL provee una conexión permanente y de gran velocidad.

Antivirus: Programa que busca y elimina los virus informáticos que pueden haber infectado un ordenador.

Archivo adjunto: Archivo que acompaña un mensaje de correo electrónico. Es apropiado para el envío de imágenes, sonidos, programas y cualquier otro tipo de información.

Avatar: Representación gráfica que se asocia a un usuario para su identificación.

B

Backup: Copia de seguridad. Acción de copiar documentos, archivos o ficheros de tal forma que puedan recuperarse en caso de fallo en el sistema

Bajar: Descargar un contenido de algún punto de Internet al ordenador del usuario.

Banner: Anuncio de dimensiones relativamente pequeñas que se muestra en una página web con fines publicitarios.

Blog (Web log): Tipo de página web que se utiliza como diario (puede ser particular, colectivo o de una empresa).

Browser: Aplicación informática que permite acceder a la información gráfica, textual y multimedia en la Web.

Buscador, motor de búsqueda: Es un programa, ubicado en un sitio de Internet, que recibe un pedido de búsqueda, lo compara con las entradas de su base de datos y devuelve el resultado. Algunos de los más conocidos son: Google, Yahoo, Altavista, Lycos, Infoseek

C

Chat: charla. Servicio de Internet que permite a dos o más usuarios conversar on-line mediante el teclado.

Chat room: Habitación virtual o espacio en el que chatear. Los chats se suelen organizar por temas o intereses.

Ciber-: Este prefijo, unido a casi cualquier palabra, la relaciona con el mundo de Internet: cibernauta, ciberpunk, ciberexperiencia, cibersexo, etc.

Colgar: Por un lado, puede hacer referencia el hecho de que el ordenador se quede bloqueado o parado. Colgar o subir un archivo en Internet es transmitir dicho archivo de un ordenador a la Web.

D

Descarga: Acción mediante la cual se graba información existente en una red en algún dispositivo de almacenamiento de nuestro ordenador.

Disco duro: Es una unidad de almacenamiento fijo, en él se guarda la información de manera permanente, la cual puede ser modificada o borrada. Otro parámetro de acceso importante es el tiempo medio de acceso, que indica la rapidez con la que se lee la información.

E

e-mail: Correo electrónico es el servicio más básico, antiguo y utilizado dentro de Internet. La mensajería electrónica es el medio más rápido y eficaz de comunicación. Permite intercambiar mensajes, programas, videos, imágenes, etc.

F

Firewall: Mecanismo de seguridad que impide el acceso a una red. Cortafuegos.

Foro: Es un grupo de discusión online que cuenta con un servicio automatizado de mensajes. Normalmente existe un moderador en cada foro para regular el mismo.

H

Hacker: Persona que penetra en las redes e intenta tener acceso a zonas o contenidos reservados. En sentido amplio, persona hábil en el uso de las redes, aunque no cometa actos delictivos.

I

Internet: red de redes. Sistema mundial de redes de ordenadores interconectados. Fue concebido a fines de la década de 1960 por el Departamento de Defensa de los Estados Unidos; más precisamente por la ARPA. Se lo llamó primero ARPAnet y fue pensado para cumplir funciones de investigación. Su uso se popularizó a

partir de la creación de la Wold Wide Web. Actualmente es un espacio público utilizado por millones de personas en todo el mundo como herramienta de comunicación e información.

Intranet: Es una red privada existente dentro de una empresa u organización.

L

Link: enlace. Imagen o texto destacado, mediante subrayado o color, que lleva a otro sector del documento o a otra página web, hipervínculo.

Lista de distribución: Relación de direcciones electrónicas que conforman un grupo de trabajo o de interés y a cuyos propietarios se remiten simultáneamente determinados mensajes a través del correo electrónico.

N

Navegador: Programa para recorrer la World Wide Web. Algunos de los más conocidos son Microsoft Internet Explorer, Mozilla Firefox y Opera.

Nick o nickname: Apodo que se suele utilizar en cualquier tipo de comunicación a través de la Red, “apodo”.

Nombre de usuario (Username): Nombre inteligible que identifica al usuario de un sistema o de una red.

O

Online: en línea, conectado. Estado en que se encuentra un ordenador cuando se conecta directamente con la Red a través de un dispositivo, por ejemplo, un módem.

P

P2P: “Peer to peer”, sistema de comunicación bilateral exclusiva entre dos o más personas a través de Internet con la finalidad de intercambiar información y archivos.

Página web: una de las páginas que componen un sitio de la World Wide Web. Un sitio web agrupa un conjunto de páginas afines. A la página de inicio se la llama “home page”.

Password: contraseña.

R

Red: Sistema de comunicación de datos que conecta entre sí sistemas informáticos.

Realidad virtual: Tecnología informática y de comunicaciones que sumerge al usuario en un entorno virtual de naturaleza espacio – sensitiva por medio artificiales que le permiten actuar con el sistema de forma interactiva.

S

Sistema operativo: Programa que administra los demás programas en un ordenador.

Software: Término general que designa los diversos tipos de programas usados en computación.

Spam: Consiste en el envío masivo, indiscriminado y no solicitado de publicidad a través de las cuentas de correo electrónico.

Spyware: Software instalado en un ordenador que recoge información sobre el usuario que lo utiliza sin su conocimiento, para enviarlo vía Internet a quien luego vende la información o la usa para realizar estadísticas o para posteriores acciones como spam, por ejemplo.

T

Troyano: Programa que contiene código dañino dentro de datos aparentemente inofensivos.

U

Upload: Significa lo mismo que “colgar”, es decir, es el proceso de transferir información desde un ordenador personal a alguna red.

URL (universal Resource Locator): Localizados Universal de Recursos. Es el término técnico que se utiliza para referirse a una dirección de Internet. Cada URL es único y está formado por varias partes. (ej. http://www.jcyl.es)

V

Virus: Pequeño programa que “infecta” una computadora; puede causar efectos indeseables y hasta daños irreparables.

Y

Youtube: Sitio web (www.youtube.com) en el que se alojan millones de videos y que permite la subida de videos por parte de los usuarios.

ENLACES DE INTERÉS

I. Instituciones

1. Ministerio de Educación, Política Social y Deporte: http://www.mepsyd.es/portada.html
2. Brigada de Investigación Tecnológica: http://www.policia.es/bit/
3. Instituto Nacional de Tecnologías de la Comunicación: www.inteco.es
4. Instituto Superior de Formación y Recursos en Red para el Profesorado: http://www.isftic.mepsyd.es/
5. Asociación de Internautas: http://www.internautas.org/
6. Agencia Española de Protección de Datos: https://www.agpd.es/portalweb/index-ides-idphp.php
7. Asociación Española de Pediatría: http://www.aeped.es/index.htm
8. Fundación CTIC: http://www.ctic.es/web/contenidos/es/index.html
9. Observatorio de Contenidos Televisivos Audiovisuales: http://www.iniciativaocta.org/
10. Asociación ACPI: http://www.asociacion-acpi.org/
11. Fundación Telefónica: http://www.fundacion.telefonica.com/index.htm
12. Agencia de Calidad de Internet: http://www.iqua.net/
13. Asociación Española de Usuarios de Internet: http://aui.es/
14. Asociación de Clasificación de Contenidos de Internet (ICRA): http://www.fosi.org/icra/
15. El Portal de Sociedad de la Información de la Unión Europea: http://ec.europa.eu/information_society/index_en.htm
16. International Association of Internet Hotlines (INHOPE) es la asociación internacional de líneas directas de Internet y fue fundada en 1999 dentro del Plan de Acción para un uso más seguro de Internet de la Comisión Europea.: https://www.inhope.org/en/index.html
17. Safer Internet Programme (Comisión Europea): http://ec.europa.eu/information_society/activities/sip/index_en.htm
18. Plan Avanza: http://www.planavanza.es/

19. Asociación dedicada a la seguridad infantil en Childnet International: http://www.childnet-int.org/
20. Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información: http://observatorio.red.es/index.action
21. Observatorio de Sociedad de la Información en Castilla y León: http://www.orsi.es

II. Páginas web

1. CapitanNet. Iniciativa apoyada por el Ministerio de Ciencia y Tecnología y promovida por el Comité español de la UNICEF para fomentar el uso seguro de internet por los niños, con consejos para padres y educadores. http://www.capitannet.com
2. Seguridad en la Red: http://www.seguridadenlared.org/
3. Protégeles: Línea de denuncia: http://www.protegeles.com/
4. Internet sin Acoso: http://www.internetsinacoso.com/
5. Sin Acoso: http://sinacoso.es/
6. Tecnoadicciones: línea de ayuda para problemas de adicción a las Nuevas Tecnologías: http://www.tecnoadicciones.com/
7. Líneas de ayuda: http://www.lineasdeayuda.info/
8. Portal del menor: http://www.portaldelmenor.es/
9. SID´09: Día Internacional de la Internet Segura: http://www.internetsegura2009.com/. Desarrollada por la Agencia de Calidad de Internet para la sensibilización y la promoción del uso seguro de Internet, para que menores y adolescentes puedan disfrutar de los beneficios que les ofrece la red.
10. Exprime la Red: http://www.exprimelared.com/
11. Ciberfamilias: http://www.ciberfamilias.com/index.htm
12. Cibercentro amigo: http://www.cibercentroamigo.com
13. Cibercentinelas: Luchar contra la pornografía infantil, buscar niños desaparecidos, anular foros de pedófilos y otras muchas acciones son las que llevan a cabo en esta página. http://www.cibercentinelas.org
14. Educared: http://www.educared.net/

15. Chavales, esta es nuestra web: http://chaval.red.es/index.jsp
16. Insafe: http://www.saferinternet.org/ww/en/pub/insafe/index.htm
17. Iníciate online. Junta de Castilla y León: http://iniciateonline.jcyl.es
18. Portal de Educación. Junta de Castilla y León: http://www.educa.jcyl.es
19. Proyecto Internet sin riesgos: http://www.internetsinriesgos.es
20. Pantallas Amigas: http://www.pantallasamigas.net/
21. Internet Segura: http://www.iqua.net/?go=R3KV5eGGiY9LhQDuPXV3ex72Rig=
22. The Quatro Plus Project: Proyecto financiado por la Unión Europea, el proyecto Garantía de Calidad y Descripción de Contenidos (Quality Assurance and Content Description, Quatro), que se lleva a cabo en el marco del Programa Europeo Safer Internet, tiene el objetivo de ayudar a los usuarios de Internet a encontrar aquello que buscan, confiar en aquello que encuentran y evitar cualquier tipo de material que, por el motivo que sea, no quieren ver. http://www.quatro-project.org/
23. El Programa *Safer Internet* de la Unión Europea: http://ec.europa.eu/information_society/activities/sip/index_en.htm
24. Ciberbullying: Acoso entre menores por medio de Nuevas Tecnologías: http://www.ciberbullying.net/
25. SafeKids: http://www.safekids.com/