GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

red.es

Seguridad TIC y menores de edad

GUÍA DIDÁCTICA II JORNADAS FORMATIVAS FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO

Febrero 2016

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

SECRETARÍA DE ESTADO DE SEGURIDAD

red.es

GUÍA DIDÁCTICA _ SEGURIDAD TIC Y MENORES DE EDAD

II JORNADAS FORMATIVAS

Febrero 2016

Introducción

Red.es es una entidad pública empresarial adscrita al Ministerio de Industria, Energía y Turismo (MINETUR), que desarrolla un extenso conjunto de programas para que la sociedad española se beneficie al máximo de las posibilidades que ofrecen las Tecnologías de la Información y la Comunicación (TIC).

Esta entidad lleva a cabo el plan de formación denominado "***Capacitación en materia de Seguridad TIC para padres, madres, tutores y educadores de menores de edad***", enmarcado dentro de la "*Agenda Digital para España*", aprobada en febrero de 2013 por el Consejo de Ministros.

En el marco de este plan de capacitación, entre los meses de febrero y marzo de 2015, impartimos unas jornadas formativas de **Seguridad TIC y menores de edad** dirigidas a las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE), en virtud del convenio de colaboración suscrito entre la Secretaría de Estado de Seguridad (Ministerio del Interior) y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (Ministerio de Industria, Energía y Turismo); enmarcándose dentro del citado plan de capacitación emprendido por Red.es.

Tras el elevado grado de satisfacción en el primer programa y la necesidad de continuar esta línea de formación, se plantea llevar a cabo unas segundas jornadas formativas dirigidas este colectivo, presentando en este documento la guía didáctica.

Destinatarios. Público objetivo

Las segundas jornadas formativas están dirigidas al personal de las Fuerzas y Cuerpos de Seguridad del Estado del Ministerio del Interior (Cuerpo Nacional de Policía y Guardia Civil) que imparten o quieren impartir charlas a menores de edad sobre los riesgos en Internet y el uso de las TIC, en el marco del Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos[1]; que pretende potenciar actuaciones preventivas en relación con los riesgos a los que se ven sometidos los menores y los jóvenes, en temas tan importantes como el uso de Internet y las nuevas tecnologías, entre otros. El número de participantes previsto es entre 100 y 110 alumnos/as.

Objetivos de aprendizaje

Las jornadas de formación se plantean con los siguientes objetivos de aprendizaje:

- Conocer el estado actual de los principales riesgos a los que se enfrentan los menores de edad en el uso de las TIC e Internet.
- Aprender estrategias y pautas didácticas para abordar los riesgos en materia de seguridad TIC para menores de edad.
- Disponer de recursos, materiales y herramientas para facilitar la labor didáctica, en materia de seguridad TIC y menores.
- Compartir experiencias formativas en materia de seguridad TIC y menores de edad.

Contenidos / Áreas temáticas (unidades didácticas)

Los contenidos del programa de formación atienden a estas **áreas temáticas** (unidades didácticas / temas):

- Ciberacoso escolar (*ciberbullying)*.
- *Grooming*.

[1] Ministerio del Interior. Instrucción nº 7/2013 de la Secretaría de Seguridad, sobre el "Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos". Recuperado de: http://www.interior.gob.es/documents/642012/1568685/Instruccion_7_2013.pdf/cef1a61c-8fe4-458d-ae0d-ca1f3d336ace

- *Sexting*.
- Gestión de la privacidad e identidad digital.
- Suplantación de identidad.
- Comunidades peligrosas en línea.
- Cambios legislativos en relación con las TIC.

Metodología didáctica

El programa se plantea a través de una modalidad *blended-learning*, combinando formación online junto con un circuito de talleres presenciales y una sesión plenaria, con una duración total de 37 horas lectivas.

Formación online

Las jornadas formativas contemplan una ***primera fase online*** que se desarrolla durante dos semanas en modalidad curso MOOC (*Massive Open Online Course*, curso en línea masivo y abierto), a través de la plataforma que Red.es pone a disposición como canal de capacitación online.

En este entorno, el alumnado dispondrá de los contenidos interactivos y podrá realizar las diferentes actividades virtuales planteadas (trabajo personal y seguimiento/lectura de materiales).

En esta primera fase online, el alumnado dispondrá de las primeras 6 unidades didácticas (temas o lecciones), centrándose cada una de ellas en uno de los riesgos TIC para los menores de edad. Cada unidad dispone de los siguientes recursos didácticos:

- Presentación unidad didáctica (vídeo).
- Guía de estudio.
- Objeto de aprendizaje multimedia: conceptualización, diagnóstico, respuesta y prevención del riesgo TIC.
- Materiales complementarios: monográfico, unidades didácticas (para educadores) y juegos/actividades hogar (para padres/madres).

Por otro lado, tras las sesiones presenciales se plantea una ***segunda fase online*** donde los participantes tendrán que elaborar una actividad práctica obligatoria, completando así el programa formativo.

Plan de actividades online:

Por un lado, los estudiantes tendrán que realizar una serie de actividades que ayuden a valorar su nivel de aprendizaje, consideradas como de ***trabajo personal***; donde se incluyen:

- Breves actividades de cada unidad, planteadas como "**Retos semanales**" que tendrán un carácter optativo, ayudando a fomentar la participación en la plataforma online.
- **Cuestionario** de evaluación de cada unidad/tema.
- **Actividad práctica final** dentro del entorno del curso MOOC (en la segunda fase online). Esta actividad la tendrán que realizar los estudiantes de forma obligatoria, poniendo en valor todo lo aprendido en la fase online inicial y en las sesiones presenciales. Para ello se les ofrecerá la posibilidad de elegir entre dos tipos de actividades que describimos más adelante.

Por otro lado, como parte del plan de actividades, se contemplan las relacionadas con la ***lectura de los materiales y contenidos*** del curso.

La dedicación total al estudio de la formación online es de **25 horas lectivas**.

Formación presencial

Las sesiones presenciales se plantean eminentemente prácticas, a través de un circuito de talleres. En cada taller práctico abordaremos un riesgo TIC de los planteados, con una duración de 1,5 horas, ofreciendo **estrategias didácticas** (formación de formadores), así como propuestas y recomendaciones para facilitar a los estudiantes su labor docente a la hora de impartir los riesgos ante los menores de edad.

Por otro lado, se plantea una sesión plenaria donde se abordarán los recientes cambios legislativos operados en el Código Penal en relación con las tecnologías.

Las jornadas presenciales se desarrollarán durante tres días. El grupo de alumnos/as se dividirá en cuatro sub-grupos y cada uno de ellos irá rotando por cuatro aulas, donde en cada una de ellas se aborda uno de los riesgos.

A continuación presentamos la propuesta de planificación y estructura de las sesiones presenciales:

	JORNADA 1: 19 abril de 2016			
09:30-10:00	Llegada y acreditación alumnado.			
10:00-10:30	Presentación e inauguración de las jornadas.			
	Aula 1: *Ciberbullying*	Aula 2: *Grooming*	Aula 3: *Sexting*	Aula 4: Gestión privacidad
10:30-12:00	Grupo A	Grupo B	Grupo C	Grupo D
12:00-12:45	Descanso			
12:45-14:15	Grupo B	Grupo A	Grupo D	Grupo C
14:15-16:15	Almuerzo			
16:15-17:45	Grupo C	Grupo D	Grupo A	Grupo B

	JORNADA 2: 20 abril de 2016			
	Aula 1: *Ciberbullying*	Aula 2: *Grooming*	Aula 3: *Sexting*	Aula 4: Gestión privacidad
10:00-11:30	Grupo D	Grupo C	Grupo B	Grupo A
11:30-12:15	Descanso			
	Aula 1: Suplantación identidad	Aula 2: Comunidades peligrosas	Aula 3: Comunidades peligrosas	Aula 4: Suplantación identidad
12:15-13:45	Grupo A	Grupo B	Grupo C	Grupo D
13:45-16:00	Almuerzo			
16:00-17:30	Grupo B	Grupo A	Grupo D	Grupo C

	JORNADA 3: 21 de abril de 2016 (todos los grupos)
10:00-11:30	**Sesión plenaria: Cambios legislativos en relación con las tecnologías**
11:30-12:00	Descanso
12:00-12:30	**Presentación repositorio de contenidos** (Ministerio del Interior)
12:30-13:30	Cierre y clausura de las jornadas.

Instalaciones sesiones presenciales

El circuito de talleres presenciales (jornadas 1 y 2) se llevará a cabo en la sede de la Dirección General de la Guardia Civil situada en la calle de Guzmán el Bueno, 110, 28003 Madrid. La tercera jornada se llevará a cabo en las instalaciones de la Secretaría de Estado de Telecomunicaciones y Sociedad de la Información (Ministerio de Industria, Energía y Turismo, calle del Capitán Haya, 41, 28020 Madrid).

Equipo docente

Los talleres presenciales serán impartidos por un equipo de docentes especializados en las áreas temáticas a impartir. A continuación presentamos sus referencias y talleres que imparten:

D. Manuel Ransán Blanco

Coordinador del Área de Menores OSI en INCIBE (2007-2013, 2015 - actualidad): definición, ejecución y gestión de programas para la sensibilización y formación en el

uso seguro y responsable de las TIC. Consultor de seguridad TIC y protección de menores en Internet para Red.es (2013-2015): soporte para el desarrollo de las políticas públicas marcadas por la Agenda Digital para España y el Plan de Confianza en el Ámbito Digital. Impartición de jornadas y talleres a padres, menores, educadores y profesionales. Formación de formadores. Coautor de la «Guía clínica sobre el ciberacoso para profesionales de la salud» y autor de la «Guía de mediación parental en Internet». CISSP por ISC2 y CISM por ISACA.

Talleres que imparte: Ciberacoso escolar (*Ciberbullying*) y Suplantación de identidad (Aula 1 del calendario)

D. Ángel Pablo Avilés García de la Rosa.

Guardia Civil en la Unidad Central Operativa – Policía Judicial (Grupo de Delitos Telemáticos de la Guardia Civil). Editor del blog http://elblogdeangelucho.com y autor del libro: "X1Red+Segura Informando y Educando.

Participa en eventos, jornadas y congresos de seguridad informática con la intención de trasladar la seguridad a usuarios no técnicos. Forma parte de la organización de la iniciativa X1RedMasSegura, mediante la que se imparten charlas y talleres gratuitos dirigidos a usuarios finales de Internet sin conocimientos técnicos. Haciendo especial incidencia con las actividades dirigiéndolas a personas mayores, niños y personas con discapacidad.

Talleres que imparte: *Grooming* y Comunidades peligrosas en línea (Aula 2 del calendario)

D. David Cortejoso Mozo.

Psicólogo Sanitario y Enfermero del Trabajo, Máster en Terapia de Conducta y Trastornos de la Personalidad, Profesor Universitario en la Universidad Isabel I, Director del I Experto Universitario en Educación para la Seguridad TIC en Menores en la Universidad Isabel I, Vicepresidente de Helptic Asociación de Afectados por el uso de las TIC, Miembro de la Sociedad Española de Criminología y Ciencias Forenses, Docente colaborador para el Gobierno de Canarias en los riesgos de las nuevas

tecnologías, creador de la web bullying-acoso.com y docente de menores, padres, madres y educadores en los riesgos de las TIC durante los últimos 5 años.

Talleres que imparte: *Sexting* y Comunidades peligrosas en línea (Aula 3 del calendario)

D. Andrés Calvo Medina.

Jefe de Área de Autorizaciones. Responsable de Seguridad. Secretaría General de la Agencia Española de Protección de Datos.

Funcionario de la Administración General del Estado desde el año 1.982 ha ocupado puestos de índole técnica en la Escala de Tecnicos Auxiliares de Informatica, Cuerpo de Científicos Especializados del INTA y Cuerpo de Científicos Superiores de la Defensa.

La mayor parte de su trayectoria profesional ha sido dedicada a la Seguridad de las TIC, siendo responsable de seguridad TIC en el Instituto Nacional de Técnica Aeroespacial y en la actualidad en la Agencia Española de Protección de Datos. Además de su experiencia como responsable de seguridad en la Agencia Española de Protección de Datos (AEPD) ha prestado servicio en la Subdirección General de Inspección donde ocupando puesto de Inspector y Jefe de Área de Instrucción ha sido coordinador de equipo de inspección-instrucción durante más de cinco años.

En la actualidad, además de las tareas propias del Responsable de Seguridad de la AEPD, trabaja en la consecución de los objetivos que el plan estratégico recientemente publicado ha marcado con relación a los menores y cuyos materiales vienen publicándose en la web www.tudecideseninternet.es elaborando guías para menores y educadores, participando en el diseño de juegos para divulgar la protección de datos entre los menores y, en general, participando en el rediseño del sitio web de menores antes indicado que la Agencia Española de Protección de Datos junto con el Ministerio de Educación (INTEF) ponen a disposición del menor y la comunidad educativa. Además de estas labores forma parte de la Unidad de Evaluación de Estudios Tecnológicos de la AEPD donde también colabora con relación a las líneas marcadas por el antes mencionado plan estratégico y más concretamente en relación con el análisis de procesos de Big Data en nuestro país.

Durante estos años ha participado en tareas de formación dentro del ámbito del plan de formación contínua del Ministerio de Defensa y participa activamente en los procesos de formación relacionados con protección de datos en el ámbito de la Administración General del Estado además de realizar ponencias de carácter nacional e internacional en materia de protección de datos y riesgos en el tratamiento de datos personales. Por otra parte, como licenciado en filología inglesa adquirió conocimientos pedagógicos y experiencia docente en la enseñanza de la lengua inglesa con alumnos de enseñanza secundaria."

Talleres que imparte: Gestión de la privacidad e identidad digital y Suplantación de identidad (Aula 4 del calendario)

Práctica final

Como hemos comentado anteriormente, tras las sesiones presenciales el alumnado tendrá que realizar una actividad práctica, que estará descrita detalladamente en la plataforma de teleformación.

Como actividad final se propondrá dos opciones para que el alumnado pueda elegir una de ellas. A continuación presentamos dichas actividades:

A lo largo del curso hemos estudiado los principales riesgos derivados del uso de las TIC y sobre cómo estos pueden afectar a nuestros menores de edad. Además, hemos compartido experiencias, recursos y materiales en las sesiones presenciales orientadas a facilitar la impartición de estos temas en el marco del Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos.

Como actividad práctica final del curso te proponemos dos opciones, debiendo elegir y realizar sólo una de ellas:

OPCIÓN A: DECÁLOGO SEGURIDAD TIC PARA MENORES DE EDAD

Instrucciones: **ELABORE UN DECÁLOGO CON LOS 10 CONSEJOS MÁS IMPORTANTES QUE LE DARÍA A UN/A MENOR DE EDAD PARA PREVENIR LOS DIFERENTES RIESGOS TIC.**

Es importante que incluya en el decálogo consejos de cada uno de los riesgos analizados a lo largo del curso y que pueda utilizarlo posteriormente para sus sesiones enmarcadas en el Plan Director.

(Elabore el decálogo en un documento de texto indicando su nombre y apellidos. Envíelo por e-mail a la dirección menoresformacion@red.es, indicando en el asunto: "Actividad práctica final SEG_TIC_005 (su nombre y apellidos)". **La fecha tope de entrega es el 30 de abril de 2016**).

OPCIÓN B: PRESENTACIÓN RIESGO TIC Y MENORES DE EDAD

Instrucciones: **SELECCIONE UNO DE LOS SEIS RIESGOS TIC Y ELABORE UNA PRESENTACIÓN (TIPO POWER POINT, ENTRE 5/8 DIAPOSITIVAS) PARA PRESENTAR DICHO RIESGO A UN GRUPO DE MENORES DE UN CENTRO EDUCATIVO.**

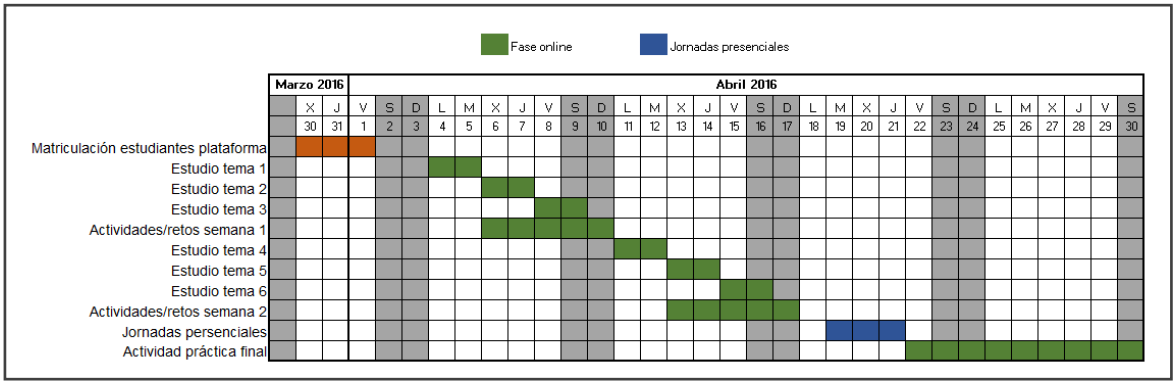
En la presentación es importante que identifique la edad de los menores (infantil, primaria o secundaria), el riesgo/tema seleccionado y su nombre/apellidos. Así mismo, debe abordar tanto la descripción del riesgo como pautas y recomendaciones de prevención y actuación; teniendo en cuenta que la finalidad es utilizarlo posteriormente en sesiones enmarcadas en el Plan Director.

(Elabore la presentación y envíela por e-mail a la direccion menoresformacion@red.es, indicando en el asunto: "Actividad práctica final SEG_TIC_005 (su nombre y apellidos)". **La fecha tope de entrega es el 30 de abril de 2016**).

Nota importante: Se comprobará que los trabajos presentados no sean iguales o presenten total similitud en su contenido. Si este caso es detectado, dichos trabajos no serán evaluados, considerándose como no superado en la evaluación del curso.

Planificación

Las jornadas formativas se desarrollarán a lo largo del mes de abril de 2016, conforme al siguiente calendario[2]:



[2] Las unidades didácticas (fase online) estarán todas disponibles desde el inicio, con idea de que el estudiante pueda organizar su propio proceso de aprendizaje. En la planificación se reflejan de forma escalonada con el fin de orientar/facilitar el estudio para los alumnos/as.

ANEXO 1: CANAL DE CAPACITACIÓN ONLINE (CURSO MOOC)

La fase online del programa se desarrolla a través de un curso MOOC (Massive Open Online Course, *-curso en línea masivo y abierto-*), en el **canal de capacitación online** que Red.es ha puesto en marcha en el marco del programa de capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad.

[http://formaciononline.chaval.es]

Estructura de contenidos

Junto con la presentación del curso y la guía didáctica general, el apartado de **contenidos** del curso consta de las seis unidades didácticas o temas (riesgos TIC objeto de estudio en el programa de formación).

Gamificación: "*competición sana*"

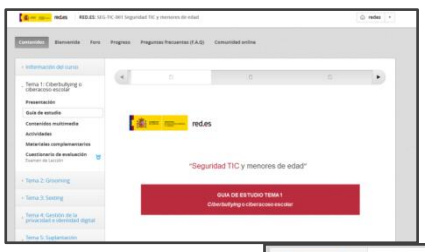
El curso cuenta con un sistema de gamificación ("competición sana") cuyo objetivo es estimular y motivar el aprendizaje del alumnado. A lo largo de los objetos de aprendizaje (contenidos multimedia) de los diferentes temas de estudio, el estudiante podrá ir consiguiendo puntos como premio a su esfuerzo, en forma de "estrellas", a medida que vaya respondiendo correctamente a preguntas y cuestiones que se les plantea.

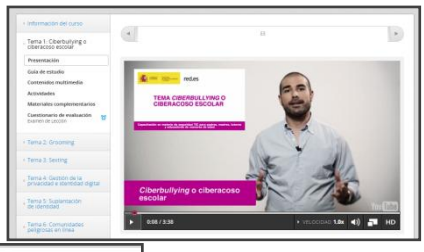
En la sección de gamificación podrá ir viendo las estrellas que va consiguiendo. Cuantas más estrellas adquiera, más posibilidades tendrá de aparecer en los primeros puestos del ranking que se muestran al final de la página. Este sistema de gamificación es simplemente un juego, por lo que la calificación no depende de ello, tan sólo se pretende fomentar la participación y recompensar el esfuerzo y dedicación.

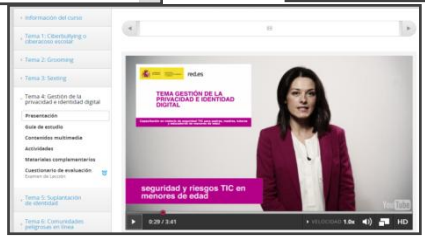
Unidades didácticas / temas del curso MOOC

Cada uno de los temas consta de los siguientes recursos didácticos:

- Presentación (vídeo).
- Guía de estudio.
- Contenido multimedia: objeto de aprendizaje multimedia.
- Recursos complementarios y Cuestionario de evaluación.



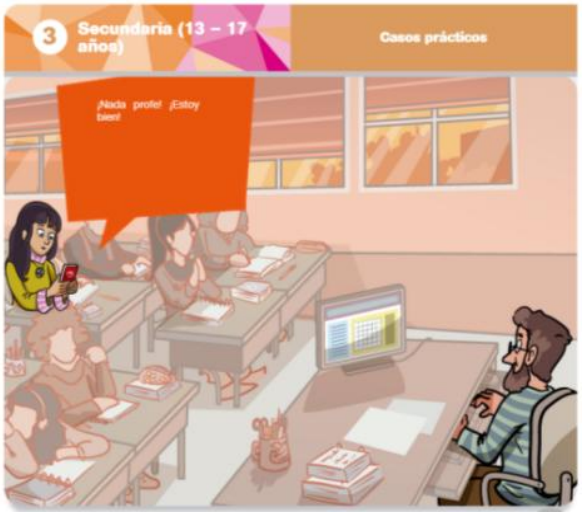




Contenidos multimedia: Objeto de Aprendizaje

Los contenidos de estudio de cada tema se presentan a través de objetos de aprendizajes multimedia, de forma interactiva y parte de ellos se abordan a través de **casos prácticos** que ilustran situaciones relacionadas con cada riesgo, permitiendo al estudiante elegir una "ruta" en función de la etapa educativa (primaria o secundaria) y del entorno (escolar o familiar).

Los contenidos están organizados siguiendo una secuencia lógica y flexible, de forma que permitirá al alumnado acceder de forma fácil a todas las partes del contenido.




Casos prácticos
Primaria (6 – 12 años)
Buenos días María, es muy temprano aún. ¿Cómo es que ya estás levantada? ¿No has dormido bien?


Casos prácticos
Primaria (6 – 12 años)
Ana quiero ver cómo eres, seguro que eres muy guapa. ¿me mandas una foto tuya, yo te envío un mía?


1 Definición y descripción del riesgo
Características del acoso escolar o ciberbullying
Según esta definición, podemos ver las siguientes características:
Daño
Intencional
Repetido
Medios digitales
Medios digitales
El acoso se realiza a través de ordenadores, teléfonos, y otros dispositivos digitales, lo que lo diferencia del acoso tradicional.
El ciberbullying o ciberacoso escolar es un tipo concreto de ciberacoso aplicado en un contexto en el que únicamente están implicados menores.
De forma más detallada podemos definir el ciberbullying o ciberacoso escolar como: «el daño intencional y repetido infligido por parte de un menor o grupo de menores hacia otro menor mediante el uso de medios digitales».
¿Qué agentes están implicados en el ciberbullying o ciberacoso escolar?
Adultos y menores
Solo adultos
Menores
Ninguna respuesta es correcta
Enviar

ANEXO 2: CONTENIDOS FORMATIVOS SEGURIDAD TIC Y MENORES DE EDAD

Como contenidos complementarios en esta formación, ponemos a disposición del alumnado los materiales formativos generados en el programa de capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad (Red.es).

Tipos de materiales

Para cada uno de los riesgos TIC que se trabajarán en las jornadas formativas, así como para otros temas tales como: Netiqueta, acceso a contenidos inapropiados, tecnoadicciones, protección ante virus y fraudes o mediación parental, está disponible el siguiente contenido en formato de documento portátil (pdf):

MONOGRÁFICO

- Marco de referencia con información clara y concisa sobre cada uno de los riesgos TIC: diagnóstico, prevención y actuación.

UNIDADES DIDÁCTICAS

- Recursos didácticos dirigidos a educadores para trabajar cada tema con los menores en las aulas (por etapas educativas).

JUEGOS PARA EL HOGAR

- Actividades dirigidas a padres y madres para trabajar cada tema con los menores en el entorno familiar (por etapas educativas).

Estos materiales están disponibles para su descarga gratuita (bajo licencia *Creative Commons*) desde el portal del proyecto: http://formacion.chaval.es

Así mismo, los contenidos multimedia (**Objeto de Aprendizaje Multimedia**); trabajados en la fase online, están disponibles en formato HTML5 para que puedan ser integrados en web, intranets o repositorios, una vez finalice el plan formativo.