Revista Española de Investigación Criminológica

Prevención de la cibervictimización en menores de la provincia de Alicante

Cyber-victimization prevention of minors in Alicante province

Recibido el 30 marzo 2016/Publicado el 5 abril 2017

Samuel Rodríguez Ferrández[1]
Universidad de Murcia

Elena Beatriz Fernández Castejón
Universidad Miguel Hernández de Elche

Rebeca Bautista Ortuño
Universidad Miguel Hernández de Elche

RESUMEN

El objetivo de este estudio es evaluar la eficacia de un programa de prevención dirigido a reducir las tasas de cibervictimización en menores de la provincia de Alicante detectadas en 2014 en un proyecto previo llamado "CiberApp". Para ello se intervino sobre una muestra de 1.575 menores de centros de ESO. La intervención consistió en la realización de 66 sesiones informativas de 50 minutos de duración (59 con los menores y 7 con sus progenitores y educadores). Se ha aplicado un cuestionario diseñado *ad hoc* para medir la frecuencia con la que los participantes llevaban a cabo comportamientos de riesgo en Internet (pretest), así como la frecuencia con la que tenían intención de hacerlo en el futuro (postest). La intervención ha sido eficaz para reducir en los menores la intención de hacer cada una de las conductas de riesgo evaluadas y para potenciar su autoprotección frente a ellas.

[1] La correspondencia debe enviarse a: Samuel Rodríguez Ferrández. Facultad de Derecho, Universidad de Murcia, Santo Cristo 1, Murcia 30001, España. samuel.rodriguez@um.es.

Palabras clave: Cibervictimización; menores; teoría de las actividades cotidianas en el ciberespacio; objetivo adecuado; guardián capaz.

ABSTRACT

The aim of this research is to assess the effectiveness of a prevention program addressed to reduce the children's rates cybervictimization reported in 2014 (in the province of Alicante), from a previous study named "CiberApp". The intervention program included 66 briefings of 50 minutes (59 sessions with minors and 7 with their parents and educators) on a sample of 1,575 children under ESO. A questionnaire designed *ad hoc* to measure the actual frequency of risky behavior on the Internet (pretest) and the intentions of doing these behaviors in the future (post-test) was applied. The intervention has been effective in reducing minors' intentions to make each of the evaluated risk behaviors and promoting their self-protection in front of cybervictimization.

Keywords: Cybervictimization; minors; routine activity theory in cyberspace; suitable target; capable guardian.

1. Introducción

1.1. TIC y relaciones sociales

La popularización de las Tecnologías de la Información y la Comunicación (en adelante TIC) han convertido el ciberespacio en el nuevo referente global de las relaciones interpersonales, tal y como muestran los datos cuantitativos al respecto (Aguilar, 2013). Así, las redes sociales en particular han logrado la convergencia entre servicios de las TIC que hasta el momento estaban separados, como el correo electrónico, la mensajería directa, los chat, la creación de sitios web, los diarios electrónicos, álbumes de fotos, etc. Ello permite a los usuarios controlar el nivel de comunicación con las personas y convierte a las redes sociales en esferas de desarrollo del ocio y de las relaciones sociales en las que el nivel de intimidad plasmado en la Red puede llegar a ser muy alto; adicionalmente, las redes sociales se erigen en un medio integral de gestión de la propia identidad, de la personalidad y de las relaciones sociales, lo cual conlleva innegables ventajas, pero también riesgos (Del Rey, Casas, y Ortega, 2016).

En este sentido, puede afirmarse que todas las esferas personales que, al relacionarse con los demás, pueden ser puestas en peligro en el mundo físico, también aparecen en riesgo en el ciberespacio; y que todas las conductas criminales de ataque a las personas que no requieran de una inmediatez física, también van a acabar realizándose de un modo u otro a través de Internet. Por tanto, dichas esferas personales se ven afectadas por la nueva era de los ataques sociales que se llevan a cabo a través de las TIC. Dichos ataques consisten en distintos tipos de agresiones que perjudican o pueden dañar a cualquier cibernauta que utiliza las nuevas tecnologías sin reparo, introduciendo esferas de su vida personal e íntima en la Red –si bien es cierto que nos ampara un "derecho al olvido digital" (Cobacho y Burguera, 2014)-. Es por esa utilización sin reparos, precisamente, por lo que los menores son un claro grupo de riesgo susceptible de sufrir ciberataques de todo tipo, pero especialmente los referidos al plano social: ciberacoso, *online child grooming*, *sextorsión* o control de la pareja, entre otros. De ahí la importancia de proteger a los menores frente a los posibles ciberataques que pueden sufrir y vulnerar su bienestar personal.

El propósito de este trabajo reside, por consiguiente, en esclarecer cómo influyen en los menores de edad las intervenciones que se pueden llevar a cabo sobre esta problemática, con el objetivo de concienciarles sobre los malos hábitos en Internet y proporcionar estrategias de prevención y afrontamiento del problema, reforzando los factores de protección al respecto. Y ello tras haber estudiado la relevancia del comportamiento en el ciberespacio como clave explicativa de la cibervictimización en nuestro trabajo "CiberApp, estudio sobre el alcance de la cibercriminalidad de los menores de la provincia de Alicante" (Miró et al., 2014); tras plantearse su investigador principal un año antes la necesidad del mismo "para obtener una imagen más clara tanto de la prevalencia de cibervictimización social, como de las razones a las que ésta es debida" en el caso de menores de entre 13 y 18 años (Miró, 2013). Dicha franja de edad, por cierto, acabó ampliándose en su límite mínimo hasta los 12 años en el estudio efectivamente llevado a cabo en 2014. Otros estudios anteriores habían preferido enfocar sus investigaciones, por ejemplo, en la franja de edad comprendida entre los 9 y los 16 años (Garmendia, Garitaonandia, Martínez, y Casado, 2011).

1.2. Programa integral de prevención primaria de la ciberviolencia en menores de la provincia de Alicante

Partiendo de la conceptuación teórica que ha venido formulando Miró (2011; 2012; 2013; 2015) sobre la Teoría de las Actividades Cotidianas de Cohen y Felson (1979) aplicada al ciberespacio, podemos llegar a la siguiente conclusión en términos de prevención de la ciberdelincuencia: la posibilidad de eliminar un ciberataque no sólo hay que buscarla en el tratamiento directo del agresor, sino también (y especialmente) en la educación de la potencial víctima para evitar futuros ataques, además de en la creación de guardianes eficaces. Éste es el motivo por el que el estudio CiberApp (Miró et al., 2014) ha ido mucho más allá de una mera descripción de la prevalencia de la victimización y se centró en identificar los factores de riesgo y de protección asociados a las actividades que de manera cotidiana desarrollan los menores en su uso de las TIC. Es decir, desde qué tipo de herramienta de comunicación usan, si contactan o no con desconocidos, si abren o descargan enlaces de páginas cuya procedencia desconozcan, si reciben control directo por parte de sus padres u otras personas sobre el tiempo y el uso que hacen del ordenador o el teléfono móvil (García Guilabert, 2014) etc.; todo ello debe ser sometido a un exhaustivo examen para comprobar cómo influye cada uno de esos factores en los procesos de victimización.

Una vez establecido este marco, sobre el que se llevó a cabo el estudio en cuestión basado en los hábitos de riesgo en el ciberespacio de los menores de la provincia de Alicante, se parte aquí de la antes mencionada base teórica para poder afirmar la relevancia del actuar del menor internauta que, en su interacción con otros sujetos en el ciberespacio, influye y predispone en mayor o menor medida su propia cibervictimización, tanto económica como social. De hecho, es plausible que los menores perciban su conducta como bastante normal e inevitable y, por ello, no sean especialmente cuidadosos al respecto (Ortega-Ruiz, Del Rey, y Casas, 2012: 305), con tales nefastas consecuencias.

Pues bien, tras el análisis de los resultados obtenidos en el estudio CiberApp (Miró et al., 2014) se acordó la realización de un proyecto de prevención victimal (Morillas, Patró, y Aguilar, 2014) con la intención de trasladar los conocimientos obtenidos no sólo propiamente a las cibervíctimas potenciales (menores), sino también a

padres y educadores. De este modo, se realizó una segunda fase del proyecto, consistente en la intervención de la problemática, por un lado, con el grupo de riesgo, es decir, los menores vulnerables a sufrir ciberataques. Por otro lado, se consideró indispensable lograr la concienciación sobre la problemática de padres y profesionales de la educación, como refuerzo de apoyo para la prevención de este tipo de victimización cibernética. Se llevó a cabo en esta segunda vertiente una guía dirigida a los padres y educadores con el objetivo de concienciar sobre la problemática y ofrecer soluciones prácticas tanto a modo preventivo como interventivo.

Se consideró fundamental para el logro de este objetivo proporcionar herramientas a los educadores y padres por ser el pilar fundamental y la figura educativa que rodea a los menores; por lo que resulta imprescindible informarles de los riesgos a los que se enfrentan los menores que tutelan y, por supuesto, ofrecerles las concretas herramientas que puedan solventar esta problemática surgida de la implementación social de las nuevas tecnologías.

Definir los factores de protección y de riesgo, es decir, conocer las conductas que disminuyen o aumentan el riesgo de ser cibervictimizado, nos permitió realizar un programa integral de prevención según la clasificación del "enfoque bidimensional" de van Dijk y de Waard (1991) donde, además de la intervención preventiva dirigida a evitar que las personas cometan delitos, se propuso dicha intervención también encaminada a evitar que las personas sean víctimas de delitos.

Así pues, este programa de prevención "victimal", en principio dirigido por tanto esencialmente a los menores como cibervíctimas potenciales tiene una orientación básicamente "comunitaria", en tanto busca la prevención a través también de la reducción de "los elementos sociales [...] que les hacen vulnerables y permiten la actividad criminal" (Garrido y López, 1995). La elección de este tipo de programa preventivo se debe a la problemática social que suponen las altas tasas de cibervictimización en menores y, sobre todo, a la gran cifra negra que existe de esta problemática (Miró et al., 2014): es decir, casos que no llegan a hacerse nunca públicos debido, en gran parte, a la vergüenza y el temor a posibles represalias por parte de los menores si desvelasen el ciberataque del que están siendo objetivo; en otras ocasiones ello se debe a la culpabilización que se autoatribuyen por haber establecido y mantenido contacto con alguien desconocido a través de Internet; también puede que no desvelen

su victimización por estar sometido a chantajes y amenazas; e incluso, se puede dar el caso de no hacerlo público por desconocimiento, debido a que ni siquiera son conscientes de que lo que les está ocurriendo es un delito y, por lo tanto, debe ser denunciado.

Concienciar y dotar de habilidades a la sociedad para favorecer la autoprotección y la adopción de conductas responsables en el ciberespacio propicia sin duda que el colectivo de riesgo asuma un papel activo hacia el cambio de comportamiento, al analizar las posibles consecuencias de sus conductas; hecho que con bastante probabilidad se ve reflejado en un descenso de las tasas de victimización en menores, lo cual tratamos de lograr a través de este programa.

1.3. Intervención como medida de prevención primaria: "aprender para saber prevenir y poder proteger"

Este proyecto preventivo de intervención comunitaria prioriza la sensibilización como forma de prevención de los delitos cometidos a través de Internet. Principalmente se basa en un programa de prevención primaria, intentando detener los posibles ataques antes de que ocurran, puesto que siempre es mejor prevenir que responder frente a tales ataques, habiendo ya sufrido sus consecuencias, sobre todo cuando hemos señalado que son muchos los casos que nunca llegan a denunciarse. El Programa CiberApp se basa en las premisas de Aprender para saber Prevenir y poder Proteger. *Aprender* a identificar conductas amenazantes y de riesgo en el ciberespacio y estrategias frente a ellas. En segundo lugar, *Prevenir* posibles ciberataques atendiendo a sus características particulares; y por último, *Proteger* de dichos ataques realizando un uso seguro de las TIC.

El programa se desarrolló durante los meses de noviembre y diciembre del año 2014 en 8 centros de educación secundaria de la provincia de Alicante. Llevar a cabo la intervención en el contexto escolar permitió, por cierto, insistir en las conductas relacionadas con el ciberbullying o ciberacoso escolar; puesto que, en el estudio previo, gran parte de los menores victimizados referían haber sido atacados en múltiples ocasiones por parte de sus compañeros de clase o de compañeros del colegio de otras clases.

Se realizaron un total de 66 sesiones de 50 minutos de duración: 59 sesiones con menores de edades comprendidas, en términos generales que luego se concretarán, entre los 14 y 18 años, en total 1.575 menores (frente a la muestra de 2.038 menores de CiberApp, que incluía a menores de entre 12 a 18 años), 815 chicos y 760 chicas; más 7 sesiones con sus progenitores.

No obstante, el interés del proyecto se centraba en los menores situados en la franja de edad comprendida entre los 14 y 15 años. ¿Por qué? De CiberApp (2014) se extrajeron las tasas más altas de cibervictimización en los menores de 16 a 18 años (Bachiller). Sin embargo, en la búsqueda de la prevención del delito con una intervención principalmente *ex ante*, ésta se centró en los menores de 14 y 15 años (3º y 4º ESO), puesto que a esta edad se adquiere mayor libertad y autonomía en el uso de las TIC a pesar de la falta de experiencia y capacidad para enfrentarse o detectar adecuadamente posibles situaciones de riesgo en Internet. El objetivo, por tanto, es evitar que se instauren hábitos poco seguros en el uso de las TIC; y de este modo prevenir las oportunidades de que los menores se conviertan en víctimas de algún ciberdelito al llegar a la edad de 16-18 años, reduciendo así la tasa de victimización a esa edad de mayor riesgo. Y hay que aclarar adicionalmente que se descartó la intervención con los menores de 12 y 13 años por considerar que son demasiado jóvenes para comprender eficazmente los problemas que pueden surgir en la Red o para medir las consecuencias y responsabilidad de sus actos; además de que, quizás, la intervención podría tener un efecto criminógeno en algunos de estos menores, en parte debido a las diferencias encontradas a estas edades: algunos menores aún se muestran infantilizados y otros, en cambio, muy avanzados para su edad.

Las sesiones teórico-prácticas con los menores se desarrollaban de manera interactiva y participativa. Haciendo uso de apoyo audiovisual (ordenador, proyector, pantalla y un sistema de audio) se hacía especial hincapié en los ciberdelitos económicos (fraude en compra, infección por malware, estafas…) y sociales (ciberacoso, ciberacoso sexual y control de pareja). El contenido de cada sesión abordaba los siguientes puntos: 1) exponer los riesgos y amenazas a los que se enfrentan los menores según sus conductas de riesgo en el ciberespacio, a partir de los datos sobre la prevalencia de las mismas derivadas del estudio anterior (CiberApp); 2) enseñar estrategias que favorezcan un uso seguro de Internet; y 3) facilitar tanto estrategias de

afrontamiento como recursos disponibles para denunciar en el caso de que hubiesen sido o estuviesen siendo víctimas de algún tipo de ciberataque. Para ello se trabajó de forma directa la capacidad empática de los menores, a través de ejemplos reales en los que se tenían que poner en el lugar de la víctima. Se entrenaba la capacidad de afrontamiento, la comunicación, el intercambio de experiencias personales, la habilidad para afrontar situaciones de riesgo, el reconocimiento de situaciones no seguras en Internet, la capacidad para eludir el acoso entre iguales y adultos, y las habilidades de resolución de conflictos. Al finalizar las sesiones, a cada menor se le entregaba un folleto con 10 estrategias de protección en el ciberespacio en el que también se ofrecía información sobre diferentes recursos de apoyo y denuncia en la Red.

En definitiva, se diseñó e implementó con todo ello un programa de intervención psicosocial comunitario para la prevención de la cibervictimización, con una metodología similar a la de otros programas ya validados, como el Cyberprogram 2.0 (aunque específicamente referido al bullying y al ciberbullying; Garaigordobil y Martínez-Valderrey, 2014). Mediante esta intervención se buscaba principalmente potenciar la capacidad de desarrollo y autoprotección de los propios menores, al ser un colectivo vulnerable, carente de habilidades para detectar posibles factores de riesgo a través de Internet y con plena libertad de uso y movimiento en el ciberespacio. Por otro lado, para fomentar la prevención de esta problemática, se potenciaba de igual modo la capacidad de afrontamiento y sentido de competencia de los padres y educadores, que en muchas ocasiones no muestran ningún tipo de control e interés por Internet, considerando que no saben hacer uso de las TIC y que sus hijos son los entendidos en términos digitales. Los resultados del estudio CiberApp (Miró et al., 2014) habían reflejado cómo el control por parte de los padres de las horas y uso que hacen los menores de las TIC disminuía significativamente la probabilidad de ser victimizado.

2. Método

2.1. Objetivos e hipótesis

El objetivo del presente estudio es analizar la eficacia de un programa de intervención diseñado a partir de los resultados obtenidos en el estudio precedente CiberApp, para reducir la intención con la que los menores de la provincia de Alicante llevan a cabo

determinados comportamientos de riesgo en Internet para los distintos tipos de cibervictimización social y económica.

Tras la detección de determinados comportamientos de riesgo de cibervictimización en esta población, la hipótesis de la que se parte es que después de la aplicación de las sesiones del programa se observará una reducción en la intención de llevar a cabo en el futuro los comportamientos de riesgo más frecuentes detectados en el estudio anterior, como: conocer gente en Internet que no se conoce en persona, publicar información personal, enviar información personal a otros, enviar fotos tuyas desnudo o semidesnudo a otra persona, mostrarse desnudo o semidesnudo a través de la webcam, guardar en el dispositivo desde el que se accede a Internet información personal, y descargar archivos o abrir enlaces enviados por desconocidos.

2.2. Muestra

La muestra del estudio estuvo compuesta por 1.574 participantes, de los cuales el 51.7 % eran chicos y el 48.3 % chicas, de edades comprendidas entre los 14 y los 18 años (M=14.8; DT=0.8), todos ellos alumnos de los cursos de 3º y 4º de ESO de los 8 centros que participaron en el proyecto.

Los centros de donde procede la muestra del presente estudio fueron seleccionados aleatoriamente de entre los 20 que participaron en el estudio anterior, en el que los resultados aportaron evidencias empíricas sobre los ciberataques recibidos, de forma continuada, por los menores de entre 12 y 18 años de la provincia de Alicante; y sobre la relación entre dichos ataques y las actividades cotidianas llevadas a cabo en el ciberespacio, permitiendo detectar los factores de riesgo y protección que incrementan o disminuyen el riesgo de ser cibervíctima.

2.3. Variables e Instrumento

Se ha diseñado un cuestionario *ad hoc* para medir la frecuencia con la que en la actualidad los participantes llevaban a cabo comportamientos de riesgo en Internet (pretest), así como para medir la frecuencia con la que tenían intención de hacerlos en el futuro (postest).

Concretamente se preguntó por 7 comportamientos de riesgo para la cibervictimización social (más frecuente en los menores que la económica), en una Escala Likert de 1 a 4 puntos, donde 1=Nunca y 4=Siempre. Las conductas de riesgo especificadas fueron las siguientes:

1. Conocer gente en Internet que no conoces en persona.
2. Publicar información personal (fotos, vídeos, etc.).
3. Enviar información personal a otros (fotos, vídeos, etc.).
4. Enviar fotos tuyas desnudo o semidesnudo a otra persona.
5. Mostrarte desnudo o semidesnudo a través de la webcam.
6. Guardar en el dispositivo desde el que accedes a Internet información personal (fotos, videos, contraseñas, etc.).
7. Descargar archivos o abrir enlaces enviados por desconocidos.

2.4. Procedimiento

El programa de intervención se aplicó desde mediados de noviembre hasta mediados de diciembre del año 2014. El equipo socioeducativo encargado de impartir las sesiones, compuesto por 8 educadores formados en el programa de intervención, se ajustó al día propuesto por cada centro escolar, dentro de la franja horaria de 8:00 a 15:00 h. Se impartieron un total de 59 sesiones, de 50 minutos de duración cada una, con los diferentes grupos de 3º y 4º de ESO de los 8 centros de educación secundaria participantes en el proyecto. La finalidad era exponer los riesgos y amenazas a los que pueden estar expuestos los menores por tener conductas de riesgo en el ciberespacio, aportando estrategias para favorecer un uso seguro de Internet.

La intervención teórico-práctica se apoyó en una presentación visual tras la que además se hacía entrega a cada sujeto de un folleto informativo acerca de cómo prevenir posibles riesgos en Internet y con información sobre recursos de apoyo en la Red. Antes y después de la intervención se tomaron las medidas pre y postest respectivamente.

El tipo de diseño de investigación aplicado es cuasi-experimental, en cuanto a que se ha llevado a cabo una manipulación a través de la aplicación del programa de intervención, pero no se han asignado aleatoriamente los sujetos a diferentes grupos, ya que todos recibieron el tratamiento. Se decidió aplicar este diseño puesto que, como

suele ocurrir cuando se trabaja con poblaciones de menores en contexto escolar, la falta de control en lo que al acceso de la muestra se refiere obligaba a elegir entre aplicar el programa solamente a una parte de la muestra y comparar los resultados con aquellos que no lo recibieron (sabiendo que no se iba a poder acceder a ellos en otro momento), o bien a desarrollar la intervención con todos los alumnos. Por lo tanto, se prescindió así de un grupo control, aplicando un diseño intrasujeto con dos medidas a comparar, una pre y otra post tratamiento.

Para el análisis de datos, sobre el conjunto de la muestra se ha aplicado un análisis descriptivo de cada uno de los ítems en el pre y en el post y, tras el mismo, un contraste de hipótesis sobre medias a partir de la prueba T de Student. Se han aplicado también pruebas T-Student para analizar las diferencias en la frecuencia e intención de seguir realizando cada una de las conductas de riesgo en función del sexo y por grupos de edad.

3. Resultados

3.1. Análisis pre-post con la muestra general

A) Conducta de riesgo 1: *Conocer a gente en Internet que no se conoce en persona*

Los resultados del análisis descriptivo muestran que no es frecuente que los jóvenes conozcan a gente por Internet que desconocen en persona y, tras la aplicación de la intervención, una disminución de la intención de hacerlo en el futuro (Tabla 1 y Figura 1).

Tabla 1.

Descriptivos de la frecuencia con la que los participantes conocen a gente en Internet que no conocen en persona

	% Frecuencias				Descriptivos			
	1	**2**	**3**	**4**	**M**	**DT**	**Min.**	**Máx.**
Pre	37.4	47.9	11.6	3.1	1.80	0.76	1	4
Post	49	40	8.3	2.7	1.65	0.75	1	4

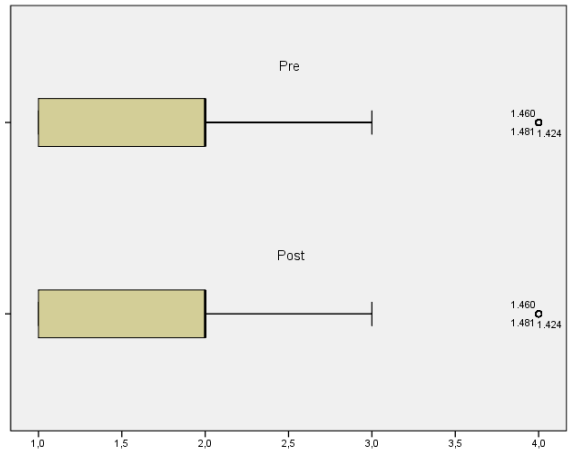

Figura 1: Diagramas de caja de la frecuencia con la que los participantes conocen a gente en Internet que no conocen en persona

Por lo que respecta a los resultados arrojados por la prueba T para muestras relacionadas, los mismos indican que la diferencia observada en la disminución de la intención de conocer a desconocidos por Internet después de la intervención es estadísticamente significativa (T_{1573}=13.24; p<0.000), con un tamaño del efecto mediano (r=0.3).

B) Conducta de riesgo 2: *Publicar información personal*

La frecuencia con la que los jóvenes publican información personal en la Red ha resultado ser una de las mayores de entre todos los comportamientos analizados (Tabla 2 y Figura 2). No obstante, y como ocurría en la conducta anterior, tras aplicar la intervención, se observa una disminución en la intención de seguir haciéndolo. Estas diferencias en las medias han resultado ser estadísticamente significativas (T_{1573}=17.09; p<0.000), obteniéndose además un tamaño del efecto considerable (r=0.4).

Tabla 2.

Descriptivos de la frecuencia con la que los participantes publican información personal en Internet

	% Frecuencias				**Descriptivos**			
	1	**2**	**3**	**4**	**M**	**DT**	**Min.**	**Máx.**
Pre	15.4	39.2	30.9	14.5	2.45	0.92	1	4
Post	22.4	44	23.2	10.4	2.22	0.91	1	4

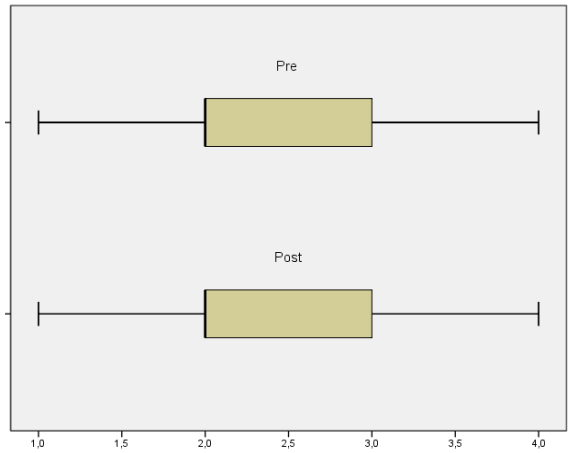

Figura 2: Diagramas de caja de la frecuencia con la que los participantes publican información personal en Internet

C) Conducta de riesgo 3: *Enviar información personal a otros*

En comparación con otras conductas analizadas, los resultados muestran que enviar por Internet información personal a otros es un comportamiento que presentan con menor frecuencia los jóvenes de la muestra (Tabla 3 y Figura 3) y se aprecia además una disminución en la intención de hacerlo en el futuro, tras la intervención. Esas diferencias observadas, entre la frecuencia media con la que los participantes envían por Internet información personal a otros en el presente y la intención de hacerlo en el futuro, son estadísticamente significativas (T_{1573}=14.57; p<0.000), con un tamaño del efecto mediano (r=0.35).

Tabla 3.

Descriptivos de la frecuencia con la que los participantes envían por Internet información personal a otras personas

	% Frecuencias				**Descriptivos**			
	1	**2**	**3**	**4**	**M**	**DT**	**Min.**	**Máx.**
Pre	29.7	39.8	23.4	7.1	2.08	0.9	1	4
Post	38.8	37.4	17.8	6	1.91	0.89	1	4

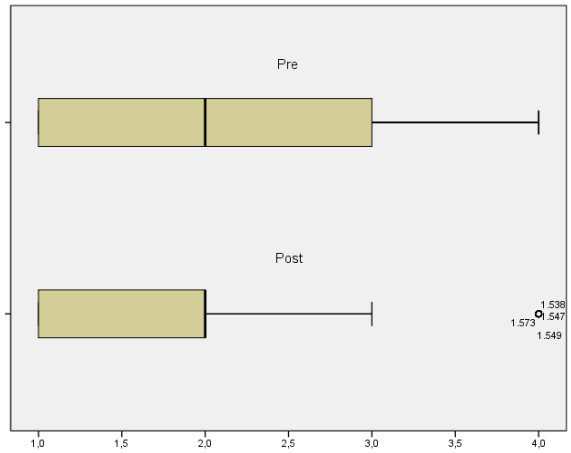

Figura 3: Diagramas de caja de la frecuencia con la que los participantes envían por Internet información personal a otras personas

D) Conducta de riesgo 4: *Enviar fotos desnudo o semidesnudo a otros*

Las frecuencias con las que los jóvenes afirman enviar fotos personales desnudos o semidesnudos es muy baja (Tabla 4), hasta el punto de que aquellos participantes que afirman haberlo hecho alguna vez pueden ser considerados en la distribución como valores atípicos, tal y como se muestra en la Figura 4. No obstante, se vuelven a apreciar, como ocurre con el resto de conductas de riesgo analizadas, una disminución de la intención de hacerlo en el futuro.

Tabla 4.

Descriptivos de la frecuencia con la que los participantes envían por Internet fotos suyas desnudos o semidesnudos a otras personas

	% Frecuencias				**Descriptivos**			
	1	**2**	**3**	**4**	**M**	**DT**	**Min.**	**Máx.**
Pre	88.1	10.4	0.8	0.7	1.14	0.42	1	4
Post	91.3	7.6	0.6	0.5	1.10	0.37	1	4

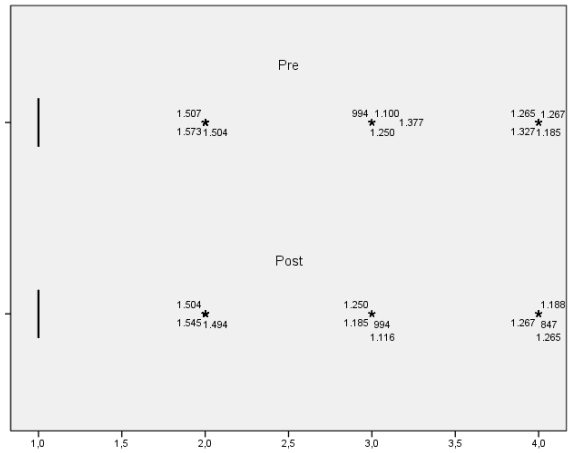

Figura 4: Diagramas de caja de la frecuencia con la que los participantes envían por Internet fotos suyas desnudos o semidesnudos a otras personas

Sin embargo, y aunque las diferencias observadas entre la conducta de enviar fotos por Internet desnudos o semidesnudos en el presente y la intención de hacerlo en el futuro tras la intervención son estadísticamente significativas (T_{1573}=5.46; p<0.000), el bajo tamaño del efecto obtenido (r=0.14) indica que esa diferencia no es clínicamente relevante. Este resultado es coherente con la baja variabilidad observada debida al hecho de que la mayor parte de la muestra, ya desde antes de la intervención, afirmaba no haber llevado a cabo esta conducta nunca.

E) Conducta de riesgo 5: *Mostrarse desnudo o semidesnudo a través de la webcam*

Éste es el comportamiento de riesgo que con menor frecuencia llevan a cabo los sujetos de la muestra de entre todos los analizados. Los resultados del análisis descriptivo evidencian que una tasa todavía mayor de jóvenes afirman no haber llevado a cabo este comportamiento nunca, en comparación con la conducta anterior que ya presentaba una frecuencia muy baja (Tabla 5 y Figura 5).

Tabla 5.

Descriptivos de la frecuencia con la que los participantes se muestran desnudos o semidesnudos a través de la webcam

	% Frecuencias				**Descriptivos**			
	1	**2**	**3**	**4**	**M**	**DT**	**Min.**	**Máx.**
Pre	97.1	1.8	0.4	0.7	1.05	0.31	1	4
Post	97.1	2.2	0.3	0.4	1.04	0.27	1	4

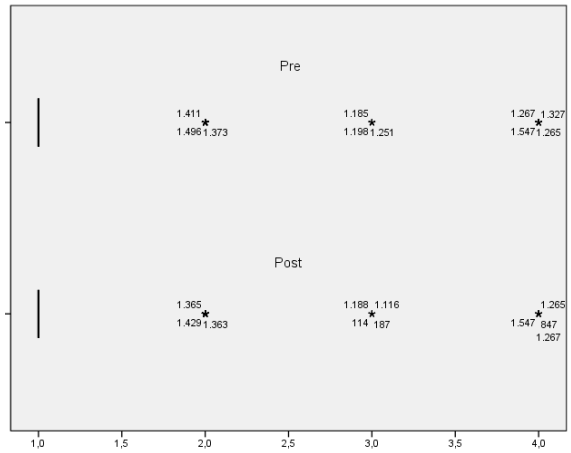

Figura 5: Diagramas de caja de la frecuencia con la que los participantes se muestran desnudos o semidesnudos a través de la webcam

A pesar de que se aprecia una mínima diferencia entre las medias obtenidas antes y después de la intervención, la gran mayoría de jóvenes no han llevado a cabo este comportamiento nunca y tampoco tienen intención de hacerlo en el futuro. Por este motivo, tal y como se sospechaba según lo que ya mostraban los análisis descriptivos, esa mínima diferencia de medias obtenida no ha resultado ser estadísticamente significativa (T_{1573}=1.25; p=0.211).

F) Conducta de riesgo 6: *Guardar en el dispositivo desde el que se accede a Internet información personal*

De entre todos los supuestos analizados, guardar fotos, contraseñas y cualquier otro tipo de información personal en el dispositivo desde el que se accede a Internet es el comportamiento de riesgo que más realizan los jóvenes de la muestra (Tabla 6). Tras la intervención, sin embargo, se observa que se produjo una disminución importante de la intención de seguir haciéndolo en el futuro, como se refleja en la Figura 6.

Tabla 6.

Descriptivos de la frecuencia con la que los participantes guardan en el dispositivo desde el que acceden a Internet información personal

	% Frecuencias				**Descriptivos**			
	1	**2**	**3**	**4**	**M**	**DT**	**Min.**	**Máx.**
Pre	17.8	26.9	21.8	33.5	2.71	1.11	1	4
Post	26.4	30.6	17.2	25.8	2.42	1.14	1	4

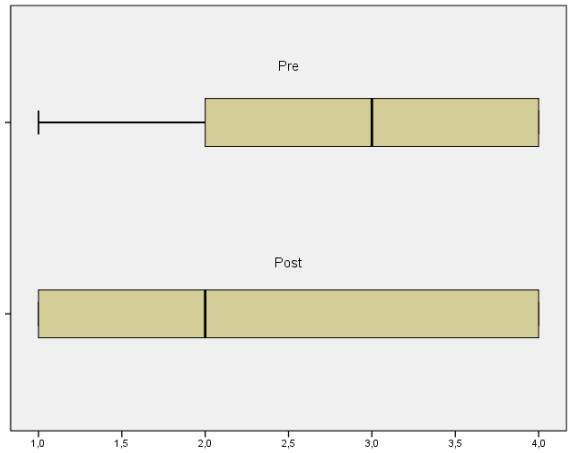

Figura 6: Diagramas de caja de la frecuencia con la que los participantes guardan en el dispositivo desde el que acceden a Internet información personal

Los resultados de la prueba T muestran una diferencia de medias estadísticamente significativa (T_{1573}=17.67; p<0.000), con un tamaño del efecto elevado (r=0.41), que indican que la intervención ha sido efectiva para reducir la intención de seguir realizando esta conducta de riesgo en el futuro.

G) Conducta de riesgo 7: *Descargar archivos o abrir enlaces enviados por desconocidos*

Por último, en cuanto a descargar o abrir archivos enviados por gente desconocida, la frecuencia con la que los jóvenes llevan a cabo este comportamiento no es muy alta, viéndose además reducida tras aplicar la intervención (Tabla 7 y Figura 7).

Tabla 7.

Descriptivos de la frecuencia con la que los participantes descargan archivos o abren enlaces enviados por desconocidos

	% Frecuencias				**Descriptivos**			
	1	**2**	**3**	**4**	**M**	**DT**	**Min.**	**Máx.**
Pre	55	32.9	8.8	3.2	1.60	0.79	1	4
Post	68.1	23.4	5.8	2.7	1.43	0.73	1	4

La diferencia de medias observadas en cuanto a la realización de esta conducta y la intención de seguir llevándola a cabo en el futuro ha resultado estadísticamente significativa (T_{1573}=14.48; p<0.000) y clínicamente relevante (r=0.34).

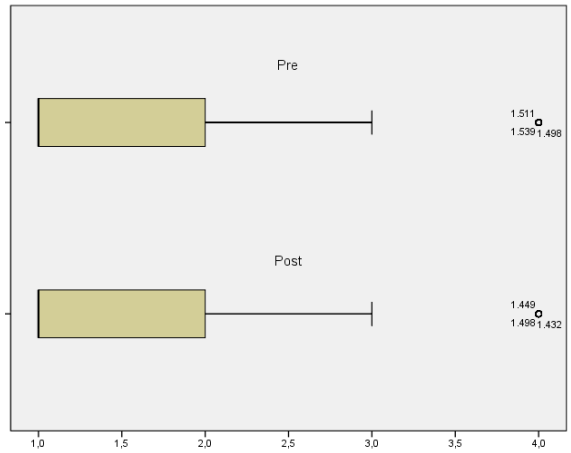

Figura 7: Diagramas de caja de la frecuencia con la que los participantes descargan archivos o abren enlaces enviados por desconocidos

3.2. Análisis de la eficacia de la intervención en función del sexo

En primer lugar, los resultados revelan que existen diferencias en la frecuencia media con la que cada grupo realiza determinados comportamientos. Concretamente, parece ser más habitual en los chicos que en las chicas llevar a cabo conductas de riesgo como conocer gente por Internet que no se conoce en persona, así como descargar o abrir archivos enviados por desconocidos (Tabla 8). Por su parte, es más habitual que ellas publiquen, envíen a otros y guarden información personal en los dispositivos desde los que acceden a Internet.

Por lo que respecta a la intervención aplicada, los resultados obtenidos muestran que fue eficaz para reducir significativamente la intención de llevar a cabo estas cinco conductas en ambos sexos (Tabla 8). Chicos y chicas coinciden en la baja frecuencia con la que envían fotos desnudos o semidesnudos a otros, siendo la intervención más efectiva en chicas, cuya reducción de la intención de seguir haciéndolo en un futuro fue mayor (Tabla 8). En cuanto a la conducta de mostrarse desnudos o semidesnudos a través de la webcam, ambos grupos presentaron una frecuencia de realización tan baja en el pretest que, obviamente, después de la intervención la intención de seguir haciéndolo no pudo verse reducida significativamente en ninguno de los dos sexos (Tabla 8).

Tabla 8.

Diferencias de medias de cada conducta de riesgo antes y después de la intervención según el sexo

Conducta de riesgo*		CHICOS						CHICAS					
		M	**DT**	**T**	**gl**	**p**	**r**	**M**	**DT**	**T**	**gl**	**p**	**r**
1	Pre	1.82	0.77	7	813	0.000	0.13	1.78	0.75	11.81	759	0.000	0.39
	Post	1.71	0.77					1.58	0.72				
2	Pre	2.13	0.87	9.21	813	0.000	0.31	2.78	0.86	14.84	759	0.000	0.47
	Post	1.98	0.85					2.47	0.90				
3	Pre	1.83	0.80	8.22	813	0.000	0.28	2.35	0.93	12.28	759	0.000	0.41
	Post	1.71	0.78					2.13	0.95				
4	Pre	1.14	0.45	1.64	813	0.101	0.06	1.15	0.40	6.30	759	0.000	0.22
	Post	1.12	0.42					1.09	0.30				
5	Pre	1.07	0.37	0.3	813	0.768	0.01	1.03	0.23	1.89	759	0.059	0.07
	Post	1.06	0.34					1.02	0.15				
6	Pre	2.48	1.11	11.83	813	0.000	0.38	2.96	1.06	13.16	759	0.000	0.43
	Post	2.22	1.11					2.64	1.12				
7	Pre	1.66	0.83	9.77	813	0.000	0.32	1.55	0.72	10.76	759	0.000	0.36
	Post	1.49	0.77					1.37	0.66				

Nota. 1. Conocer gente en Internet que no se conoce en persona; 2. Publicar información personal; 3. Enviar información personal a otros; 4. Enviar fotos desnudo o semidesnudo a otros; 5. Mostrarse desnudo o semidesnudo a través de la webcam; 6. Guardar en el dispositivo desde el que se accede a Internet información personal; 7. Descargar archivos o abrir enlaces enviados por desconocidos.

3.3. Análisis de la eficacia de la intervención en función de la edad

En general, y comparando los resultados obtenidos en los tres grupos de edad existentes en la muestra (14 años, 15 años y 16-18 años), la distribución de las frecuencias medias con la que cada grupo realiza cada conducta de riesgo es muy similar y, aunque sin grandes diferencias, la mayoría de comportamientos de riesgo son llevados a cabo con más frecuencia por parte de los jóvenes de mayor edad (Tabla 9, Tabla 10 y Tabla 11). Guardar en el dispositivo desde el que se accede a Internet y publicar información personal son los comportamientos de riesgo que más llevan a cabo los jóvenes, mientras que enviar fotos desnudo y mostrarse de esta forma a través de la webcam son los menos frecuentes, independientemente del grupo de edad.

Tabla 9.

Diferencias de medias de cada conducta de riesgo antes y después de la intervención de los participantes de 14 años

Conducta de riesgo		14 años					
		M	DT	T	gl	p	r
Conocer gente en Internet que no se conoce en persona	Pre	1.73	0.74	8.91	670	0.000	0.33
	Post	1.57	0.73				
Publicar información personal	Pre	2.43	0.93	11.40	670	0.000	0.40
	Post	2.20	0.91				
Enviar información personal a otros	Pre	2.06	0.88	10.13	670	0.000	0.36
	Post	1.87	0.87				
Enviar fotos desnudo o semidesnudo a otros	Pre	1.13	0.44	2.81	670	0.005	0.11
	Post	1.10	0.37				
Mostrarse desnudo o semidesnudo a través de la webcam	Pre	1.05	0.35	2.30	670	0.022	0.09
	Post	1.03	0.25				
Guardar en el dispositivo desde el que se accede a Internet información personal	Pre	2.70	1.14	11.57	670	0.000	0.41
	Post	2.41	1.15				
Descargar archivos o abrir enlaces enviados por desconocidos	Pre	1.55	0.75	9.17	670	0.000	0.33
	Post	1.38	0.69				

En cuanto a la intervención, los resultados muestran que ha sido efectiva para reducir la intención de seguir llevando a cabo en el futuro cada uno de los comportamientos analizados en todos los grupos de edad, con excepción de la conducta de mostrarse ante la webcam desnudo o semidesnudo. Como ocurría en los análisis anteriores (contemplándose toda la muestra y al agrupar por sexos), la frecuencia de partida con la que los jóvenes afirman llevar a cabo esta conducta es tan baja en cada grupo de edad, que las pequeñas reducciones en la intención futura tras la intervención no resultan significativas (Tabla 9, Tabla 10 y Tabla 11).

Tabla 10.

Diferencias de medias de cada conducta de riesgo antes y después de la intervención de los participantes de 15 años

Conducta de riesgo		15 años					
		M	DT	T	gl	p	r
Conocer gente en Internet que no se conoce en persona	Pre	1.83	0.77	8.48	657	0.000	0.31
	Post	1.68	0.73				
Publicar información personal	Pre	2.45	0.91	10.60	657	0.000	0.38
	Post	2.23	0.92				
Enviar información personal a otros	Pre	2.12	0.94	8.99	657	0.000	0.33
	Post	1.96	0.93				
Enviar fotos desnudo o semidesnudo	Pre	1.14	0.40	4.61	657	0.000	0.18

a otros	Post	1.10	0.35				
Mostrarse desnudo o semidesnudo a través de la webcam	Pre	1.03	0.23	-1,00	657	0.318	0.04
	Post	1.04	0.23				
Guardar en el dispositivo desde el que se accede a Internet información personal	Pre	2.78	1.08	11.15	657	0.000	0.40
	Post	2.51	1.12				
Descargar archivos o abrir enlaces enviados por desconocidos	Pre	1.61	0.78	9.36	657	0.000	0.34
	Post	1.44	0.73				

Tabla 11.

Diferencias de medias de cada conducta de riesgo antes y después de la intervención de los participantes de 16 a 18 años

Conducta de riesgo		**16-18 años**					
		M	**DT**	**T**	**gl**	**p**	**r**
Conocer gente en Internet que no se conoce en persona	Pre	1.94	0.77	4.96	244	0.000	0.30
	Post	1.78	0.80				
Publicar información personal	Pre	2.49	0.92	7.08	244	0.000	0.41
	Post	2.24	0.90				
Enviar información personal a otros	Pre	2.03	0.84	5.37	244	0.000	0.33
	Post	1.88	0.85				
Enviar fotos desnudo o semidesnudo a otros	Pre	1.18	0.47	2.44	244	0.015	0.15
	Post	1.13	0.41				
Mostrarse desnudo o semidesnudo a través de la webcam	Pre	1.07	0.37	-0.73	244	0.468	0.05
	Post	1.08	0.39				
Guardar en el dispositivo desde el que se accede a Internet información personal	Pre	2.54	1.09	7.38	244	0.000	0.43
	Post	2.24	1.13				
Descargar archivos o abrir enlaces enviados por desconocidos	Pre	1.75	0.84	6.15	244	0.000	0.37
	Post	1.55	0.81				

4. Discusión y conclusiones

Como hemos destacado más arriba, cuando se llevó a cabo el estudio de CiberApp (2014), se detectaron unas altas tasas de cibervictimización en menores, ante lo cual se planteó el objetivo de colaborar en su reducción a través de esta segunda fase del proyecto que ahora se da a conocer. Así pues, se emprendió el ya explicado proyecto interventivo, centrado en la prevención de la victimización del grupo de menores vulnerable, dándole además una orientación comunitaria con implicación de sus padres y educadores.

Se han obtenido datos estadísticos que permiten afirmar que la intervención aplicada sobre el grupo de menores ha resultado eficaz, pues el efecto es estadísticamente significativo en todos aquellos casos en que la conducta de riesgo

mostraba una frecuencia notable, a los efectos de poder conferirle relevancia clínica. En particular, guardar información personal en el dispositivo desde el que se accede a Internet, publicar información personal, enviar información personal a otros y descargar archivos o abrir enlaces enviados por desconocidos son conductas que, en mayor o menor medida, realizaban los menores; y se ha conseguido un efecto interventivo significativo y relevante en orden a que no las vuelvan a realizar en el futuro. No obstante, sólo se cuenta por el momento para afirmar la eficacia del programa en esta vertiente con los datos que ofrece la comparación entre el pretest y el postest, tras la intervención. Por ello, quizá sólo se podría corroborar plenamente la eficacia del programa realizando dentro de un tiempo un nuevo test, sobre la misma muestra, con el que se obtuviera información sobre la efectividad de los propósitos de los menores tras la implementación del programa. En particular, se podría comprobar así si las tasas de victimización se reducen en el grupo de edad de 16 a 18 años, donde eran más elevadas, por haber logrado evitar la instauración de hábitos poco seguros (o, directamente, de riesgo) en el uso de las TIC.

Con esta vertiente, en todo caso, se ha tratado de trabajar sobre todo en cuanto al objetivo o blanco adecuado como elemento de la TAC aplicada al cibercrimen. Más en concreto, se ha tratado de incidir sobre "los factores relacionados con las actividades cotidianas de la víctima que van a incidir en su cibervictimización" (Miró Llinares, 2013: 15), esencialmente en lo atinente a la introducción de bienes en el ciberespacio y a la autoprotección que incluye el acrónimo ISI (Introduction, Self-protection, Interaction). Así, probablemente, se ha contribuido a potenciar la capacidad de desarrollo y autoprotección de los propios menores, en aras a lograr evitar, o cuanto menos reducir, su cibervictimización.

Por otro lado, en cuanto a la vertiente interventiva referente a padres y educadores, pese a no contar con datos estadísticos sobre la eficacia de la misma (que podrían ser recabados en ese posible nuevo test), se ha tratado de trabajar con ellos sobre la construcción de un "guardián capaz", potenciando posibles factores de protección de la cibervictimización de menores que se habían detectado como posibles víctimas en CiberApp (Miró et al., 2014), en aspectos como el control por parte de los progenitores sobre las horas y el uso del teléfono móvil, el compartir el ordenador con ellos o la limitación del acceso a redes sociales. Así pues, se ha trabajado en la

potenciación de la capacidad de afrontamiento y sentido de competencia de los padres y educadores en orden a la evitación o reducción de la cibervictimización de los menores por ellos tutelados. Aunque es cierto que, para lograr este objetivo plenamente, toda iniciativa educativa dirigida a progenitores en esta materia debería incluir una comprensión contextualizada de la importancia que las TIC tienen en la vida diaria de los menores, con el propósito de facilitarles una visión lo más completa posible de la complejidad que entrañan las conductas de riesgo en la Red (Misha, Cook, Saini, Wu, y MacFadden, 2009).

Otros programas en esta materia ya validados como ConRed han demostrado cumplir con ese doble enfoque, "elevando la toma de conciencia sobre los riesgos, sin alarmar en demasía a los escolares y capacitando a los docentes y padres para que ejerzan su rol de orientadores de la conducta juvenil"; logrando así la disminución de las conductas de riesgo sobre el grupo experimental y aumentando en el seno del mismo la adopción de precauciones y de actitudes de protección, en contraposición al grupo de control (Del Rey, Casas, y Ortega, 2012).

Consideramos que los resultados obtenidos, como en CiberApp (Miró et al., 2014), conforme a la metodología utilizada, pueden ser considerados estadísticamente representativos respecto de la población completa de jóvenes estudiantes de centros de enseñanza secundaria obligatoria y bachillerato de la provincia de Alicante. E, igual que entonces, la similitud de características sociodemográficas que comparte esta provincia con el resto del país, sugiere que la evidencia empírica encontrada en este estudio pueda resultar ser, con alta probabilidad, bastante similar a la referida a menores del resto de España.

En definitiva, en la medida en que con CiberApp (Miró et al., 2014) se pudo aprender cómo se comportan nuestros menores en el ciberespacio en su día a día, y que ello determinaba en muchos casos su cibervictimización, ahora se ha intervenido para intentar prevenir tales casos a través de la protección en varios sentidos: autoprotección del grupo de sujetos vulnerables e, incluso, la necesaria ayuda mutua entre pares (Jiménez, Garmendia, y Casado del Río, 2015); así como también, protección ejercida por vigilantes o guardianes capacitados para esa tarea, teniendo en cuenta las peculiares características de la cibercriminalidad. No obstante, ésta ha constituido la primera experiencia dentro del complejo ámbito de la prevención de la cibervictimización de

menores en nuestro país, que deberá seguir optimizándose con los subsiguientes avances que alcancen las próximas investigaciones científicas que se vayan desarrollando a partir de este momento dentro de este campo.

Agradecimientos

Queremos agradecer al Departamento de Igualdad y Juventud de la Diputación Provincial de Alicante el encargo de realización, mediante un contrato menor de servicios, del "Programa de intervención y prevención de la cibervictimación", así como a los responsables de los centros de educación secundaria de la provincia de Alicante las facilidades para implementarlo, en la misma medida que agradecemos muy sinceramente a los estudiantes y progenitores/tutores su participación.

5. Referencias

Aguilar, M. M. (2013). Los delitos informáticos: cuantificación y análisis legislativo en el Reino Unido. *Cuadernos de Política Criminal*, (110), 221-259.

Cobacho, Á., & Burguera, L. (2014). Responsabilidad de los websmasters y derecho al olvido digital. En J. Valero (Coord.), *La protección de datos personales en Internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica* (pp.381-406). Cizur Menor: Aranzadi.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review*, *44*(4), 588-608.

Del Rey, R., Casas, J. A., & Ortega, R. (2012). El programa ConRed, una práctica basada en la evidencia. *Comunicar: Revista Científica de Comunicación y Educación*, *20*(39), 129-138.

Del Rey, R., Casas, J. A., & Ortega, R. (2016). Impact of the ConRed program on different cyberbullying roles. *Agressive Behavior*, *42*(2), 123-135. doi: 10.1002/ab.21608

Garaigordobil, M., & Martínez-Valderrey, V. (2014). Efecto del Cyberprogram 2.0 sobre la reducción de la victimización y la mejora social en la adolescencia. *Revista de Psicodidáctica*, *19*(2), 289-305. doi: 10.1387/RevPsicodidact.10239

García Guilabert, N. (2014). *Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio*. Tesis doctoral. Universidad de Murcia, España.

Garmendia, M., Garitaonandia, C., Martínez, G., & Casado, M. A. (2011). *Riesgos y seguridad en internet: Los menores españoles en el contexto europeo.* Bilbao: EU Kids Online, Universidad del País Vasco.

Garrido, V., & López, M. J. (1995). *La prevención de la delincuencia: el enfoque de la competencia social*. Valencia: Tirant lo Blanch.

Jiménez, E., Garmendia, M., & Casado del Río, M. Á. (2015). Percepción de los y las menores de la mediación parental respecto a los riesgos en internet. *Revista Latina de Comunicación Social*, (70), 49-68. doi: 10.4185/RLCS-2015-1034

Miró, F. (2011). La oportunidad criminal en el ciberespacio: Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología*, *13*(7), 1-55.

Miró, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid/Barcelona: Marcial Pons.

Miró, F. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. *Revista Española de Investigación Criminológica*, (11), 1-35.

Miró, F. (2015). Cibercrimen y vida diaria en el mundo 2.0. En F. Miró, J. R. Agustina, J. E. Medina, y L. Summers (Eds.), *Crimen, oportunidad y vida diaria. Libro homenaje al Profesor Dr. Marcus Felson* (pp.415-455). Madrid: Dykinson.

Miró, F., García, N., Castro, F. J., Díez, T., Fernández, E. B., Martín, B., Ruiz, M. M. (2014). *CiberApp. Aprender, Prevenir, Proteger. Estudio sobre el alcance de la cibercriminalidad contra menores de la provincia de Alicante*. Elche: Crímina.

Misha, F., Cook, C., Saini, M., Wu, M. J., & MacFadden, R. (2009). Interventions for children, youth, and parents to prevent and reduce cyber abuse. *Campbell Systematics Reviews*, (2), 1-54. doi: 10.4073/csr.2009.2

Morillas, D. L., Patró, R. M., & Aguilar, M. M. (2014). *Victimología: un estudio sobre la víctima y los procesos de victimización* (2ª Ed.). Madrid: Dykinson.

Ortega-Ruiz, R., Del Rey, R., & Casas, J. A. (2012). Knowing, building and living together on Internet and Social Networks: the ConRed Cyberbullying Prevention Program. *International Journal of Conflict and Violence*, *6*(2), 303-312.

van Dijk, J. J. M., & de Waard, J. (1991). A two-dimensional typology of crime prevention projects: With a bibliography. *Criminal Justice Abstracts*, *23*(3), 483-503.

Samuel Rodríguez Ferrández es Profesor Contratado de Derecho Penal y Subdirector de Investigación y Transferencia de Resultados en el Centro de Estudios Criminológicos "CICUM" de la Universidad de Murcia.

Elena Beatriz Fernández Castejón es Profesora Ayudante de Derecho Penal e Investigadora del Centro "Crímina" para el Estudio y Prevención de la Delincuencia de la Universidad Miguel Hernández de Elche.

Rebeca Bautista Ortuño es Profesora Ayudante de Psicología Básica e Investigadora del Centro "Crímina" para el Estudio y Prevención de la Delincuencia de la Universidad Miguel Hernández de Elche.