CRÍMINA

Centro para el estudio y
prevención de la delincuencia

INFORME DE RESULTADOS DEL PROYECTO SAF_*e*. CIBERVICTIMIZACIÓN Y HÁBITOS DE USO DE LAS TIC E INTERNET DE LOS ALUMNOS DE ENSEÑANZA NO UNIVERSITARIA DE CASTILLA Y LEÓN

EQUIPO INVESTIGADOR

Investigadores principales

Fernando Miró Llinares

Elena Beatriz Fernández Castejón

Investigadores

Ana Páez Mérida

Asier Moneva Pardo[1]

Nazaret Alonso Núñez

Apoyo a la investigación

Ana Belén Gómez Bellvís

Cordelia Estévez Casellas

Francisco Javier Castro Toledo[2]

Estudio encargado por el Servicio de Educación Infantil, Básica y Bachillerato. Dirección General de Política Educativa Escolar. Consejería de Educación de Castilla y León. Año 2017-2018.

---

[1] El trabajo de este investigador ha sido financiado con fondos de las ayudas para la Formación de Profesorado Universitario (FPU) del Ministerio de Educación, Cultura y Deporte del Gobierno de España, con referencia FPU16/01671.

2 Este investigador ha recibido el apoyo del Instituto Nacional de Ciberseguridad (INCIBE) en el marco de las "Ayudas para la excelencia de los equipos de investigación avanzada en ciberseguridad" (ref. INCIBEI-2015-02480).

ÍNDICE

I. INTRODUCCIÓN..... 7

II. ESTAMOS EN LAS AULAS, ESTAMOS EN EL CIBERESPACIO 8

2.1 El ciberespacio: otra realidad 8

2.2 Cibervictimización en menores.....11

2.3 Cibervictimización y su incidencia en el ámbito escolar 13

2.4 Cibercriminalidad y cibervictimización en España: situación actual 16

2.4.1 Cibercriminalidad..... 16

2.4.2 Cibervictimización..... 19

III. SAF_e: PROTOCOLO DE ACTUACIÓN SOBRE USO SEGURO DE LAS TIC, CONVIVENCIA ESCOLAR Y RIESGOS DE INTERNET EN CASTILLA Y LEÓN..... 22

IV. RESULTADOS..... 27

4.1 CIBERATAQUES SOCIALES AUTOINFORMADOS POR LOS ALUMNOS.....29

4.1.1 Ciberacoso 29

4.1.2 Ciberacoso sexual 30

4.1.3 Control de pareja..... 32

4.2 CIBERATAQUES QUE AFECTAN A LOS JÓVENES DE CASTILLA Y LEÓN.....33

4.2.1 Ciberataques económicos 34

a) Fraude en compra 36

b) Infección por malware 41

c) Pérdida de archivo por infección por malware 43

d) Scam.....45

e) Spam 47

4.2.2 Ciberataques sociales 49

a) Ciberacoso....50

b) Ciberacoso sexual....106

c) Control de pareja a través de las TIC....146

4.3 CONDUCTAS DE USO DESVIADO DE INTERNET Y LAS TIC DE LOS JÓVENES DE CASTILLA Y LEÓN....157

4.3.1 Uso abusivo de Internet y las TIC....158

4.3.2 Otras conductas desviadas....160

4.4 PERCEPCIÓN Y CONOCIMIENTO DE LOS DOCENTES SOBRE LOS CIBERATAQUES Y USO DESVIADO DE INTERNET QUE AFECTAN A LOS JÓVENES DE CASTILLA Y LEÓN....166

4.4.1 Percepción de los docentes sobre la existencia de cibervictimización y uso desviado de Internet entre sus alumnos....167

a) Ciberacoso....168

b) Ciberacoso sexual....169

c) Control de pareja a través de las TIC e Internet....171

d) Ciberataques económicos....172

e) Uso desviado de Internet....173

4.4.2 Conocimiento directo de los docentes sobre la existencia de cibervictimización y uso desviado de Internet entre sus alumnos....175

a) Ciberacoso....176

b) Ciberacoso sexual....179

c) Control de pareja a través de las TIC e Internet....182

c) Ciberataques económicos....185

e) Uso desviado de Internet....187

4.5 HÁBITOS EN EL USO DE LAS TIC DE LOS JÓVENES DE CASTILLA Y LEÓN....189

4.5.1 Uso de las Tecnologías de la Información y la Comunicación....190

a) Uso del ordenador....190

b) Uso del móvil y la tablet....193
4.5.2 Uso de las herramientas de comunicación.... 195
a) Redes sociales....195
b) Correo electrónico....200
c) Blogs, vídeo blogs y cuentas de YouTube....201
d) Videollamadas....203
e) Webs de contacto....204
4.5.3 Actividades cotidianas de los jóvenes en Internet.... 206
a) Comprar por Internet....206
b) Facilitar datos personales....207
c) Contactar con desconocidos....208
d) Abrir enlaces o descargar archivos de Internet....210
e) Realizar comportamientos sexuales online....212
f) Jugar online....215
g) Guardar información en el ordenador y el móvil....216
h) Usar antivirus....217
i) Usar contraseñas....218
4.6 SUPERVISIÓN PARENTAL DEL USO DE LAS TIC....219
4.7 MECANISMOS DE PREVENCIÓN E INTERVENCIÓN DE LOS CENTROS EDUCATIVOS ANTE CASOS DE CIBERVICTIMIZACIÓN Y USO DESVIADO DE INTERNET....222
4.7.1 Mecanismos de prevención de los riesgos de Internet y del uso desviado existentes en los centros educativos.... 223
a) Mecanismos de prevención de los riesgos de Internet....224
b) Mecanismos de prevención del uso desviado de Internet....229
4.7.2 Mecanismos de intervención sobre los riesgos de Internet y el uso desviado en los centros educativos.... 234

a) Mecanismos de intervención en el ciberacoso.....235

b) Mecanismos de intervención ante el ciberacoso sexual 239

c) Mecanismos de intervención en el control de pareja a través de las TIC e Internet.244

d) Mecanismos de intervención en la cibervictimización económica 249

e) Mecanismos de intervención ante conductas desviadas en el uso de Internet.....254

V. RECAPITULACIÓN Y CONCLUSIONES 259

VI. REFERENCIAS 265

VII. ÍNDICE DE GRÁFICOS 266

VIII. ÍNDICE DE TABLAS.....281

I. INTRODUCCIÓN

Saf_*e* nace de la necesidad de conocer la realidad actual sobre los hábitos de uso y riesgo de Internet que tienen los alumnos de enseñanza no universitaria de la comunidad autónoma de Castilla y León, lo que permitirá, posteriormente, la elaboración de un protocolo de actuación del uso seguro de las TIC.

El presente informe, por tanto, consiste en una presentación de los principales resultados obtenidos sobre las cifras de cibervictimización y los hábitos de uso de las TIC e Internet de los alumnos mencionados anteriormente. Más concretamente, este informe se divide en tres grandes capítulos. El primero de ellos (capítulo "*II. El ciberespacio*") es una contextualización teórica sobre lo que es el ciberespacio y la ciberdelincuencia. Al mismo tiempo, dicha conceptualización se apoya en datos estadísticos a nivel español que muestran la realidad actual de este fenómeno en nuestro país.

El segundo capítulo (apartado "*III. Saf_*e*: Protocolo de actuación sobre uso seguro de las TIC, convivencia escolar y riesgos de Internet en Castilla y León*") hace referencia al propio proyecto Saf_*e*, ya que en él se detalla qué es este proyecto, en qué consiste, qué objetivos persigue y cómo está estructurado.

Finalmente, en el último de los capítulos (apartado "*IV. Resultados*"), que es el más extenso, se presentan los resultados obtenidos tras el análisis de los datos recogidos gracias a los cuestionarios cumplimentados tanto por los alumnos de enseñanza no universitaria de Castilla y León (5º y 6º de educación primaria, 1º, 2º, 3º y 4º de educación secundaria obligatoria, 1º y 2º de bachillerato y ciclos formativos de grado medio), como por sus profesores. Entre los resultados se encuentra información sobre las cifras de cibervictimización de estos alumnos, sus hábitos en el uso de las TIC e Internet y los mecanismos de prevención e

intervención de la ciberdelincuencia disponibles en los centros educativos, entre otros datos relevantes.

II. ESTAMOS EN LAS AULAS, ESTAMOS EN EL CIBERESPACIO

2.1 El ciberespacio: otra realidad

Actualmente, vivimos en una sociedad donde las TIC (Tecnologías de la Información y la Comunicación) tienen un papel muy importante, tanto que muchas veces llegan a convertirse en necesarias para la vida cotidiana. Para muchas personas es inconcebible vivir en una realidad en la que no existan móviles, ordenadores y, por supuesto, Internet. Esta realidad, que se presenta como un ámbito de interacción social distinto al físico, es el llamado ciberespacio, el cual no está situado en ningún sitio en concreto y en el que no existen fronteras. Además, en él existe mucha libertad de movilidad, es decir, el usuario puede navegar por Internet de la forma que quiera y cuando quiera y, así, encontrar lo que desee. En otras palabras, no hay censuras (Miró, 2013).

La información en el ciberespacio se propaga de manera inmediata y puede llegar a cualquier parte del mundo en cuestión de segundos. Ello facilita la comunicación entre personas que se encuentran en lugares distintos, en zonas horarias diferentes e incluso que no comparten un mismo idioma (Miró, 2013). Todas estas ventajas hacen que cada vez más gente integre el mundo virtual en su vida diaria, sobre todo aquellas personas que nacieron cuando el ciberespacio aun no existía y no ofrecía el abanico de posibilidades que ofrece hoy en día.

En contraposición al grupo de personas mencionado al final del párrafo anterior, hay un grupo de personas que sí ha nacido con este mundo a su alcance: son los llamados nativos digitales (Prensky, 2010) o Generación Z. Para ellos, el ciberespacio no es en absoluto nuevo, sino que es una parte integrada en sus

vidas. Ello hace que sepan manejarse con naturalidad y soltura en él y que muchas veces no sean conscientes de los riesgos reales que conlleva.

El ciberespacio, como se acaba de introducir en el párrafo anterior, y al igual que sucede con el espacio físico, presenta una serie de riesgos que pueden afectar negativamente a las personas. Sin embargo, estos riesgos, que se relacionan principalmente con la posibilidad de ser víctima de un delito, son distintos a los que pueden encontrarse en el espacio físico, ya que la delincuencia se ha adaptado a este nuevo mundo y ha tomado otras formas. De hecho, las oportunidades delictivas que ofrece el ciberespacio son muchas veces mayores que en otros ámbitos. Algunos ejemplos de la adaptación de la delincuencia al mundo virtual los encontramos en la creación de nuevos delitos que solo pueden cometerse a través de Internet, como por ejemplo el *hacking* o las infecciones de *malware.* Otros ejemplos los encontramos en delitos que se han adaptado a las nuevas tecnologías, como son el ciberacoso o las estafas.

Otro dato que demuestra que la ciberdelincuencia es distinta a la delincuencia tradicional es que es más difícil investigar un delito cometido en el ciberespacio que en la vida real, ya que existen más oportunidades de ocultar información o escapar de la legalidad debido, precisamente, a su carácter anónimo, su falta de fronteras espacio-temporales y la total libertad que tiene el usuario para actuar como quiera.

En este sentido, la teoría de las Actividades Rutinarias de Cohen y Felson (1979) cobra un papel muy relevante en la explicación de la cibercriminalidad. Por como está configurado el ciberespacio, y tal y como indica Miró (2013), éste incrementa la posibilidad de que la víctima y el delincuente coincidan, por lo que existe un riesgo elevado de cibervictimización. Paradójicamente, ello también significa que la víctima tiene un mayor poder para evitar el ciberataque, ya que ella, a través de las actividades que desarrolla en el ciberespacio y sus hábitos de

uso del mismo, puede disminuir la probabilidad de convertirse en víctima. Por el contrario, también puede aumentar esta probabilidad haciendo un mal uso de las TIC e Internet.

Según Miró (2012), existen distintos tipos de ciberdelincuencia: la económica y la social. La ciberdelincuencia económica está compuesta por todo el conjunto de delitos cometidos a través del ciberespacio con la finalidad de obtener una ganancia patrimonial. Es decir, en este tipo de delitos existe una intención económica detrás de la comisión de la conducta. Algunos ejemplos de este tipo de ciberdelincuencia son el *scam*, el *spam*, la infección y pérdida de archivos por infección por *malware* y el fraude online, entre otros[3].

La ciberdelincuencia social, en cambio, hace referencia al conjunto de delitos que causan un daño a bienes jurídicos privados como pueden ser la intimidad, la libertad sexual o la libre formación de la sexualidad. En este tipo de ciberdelincuencia no existe intención de obtener una ganancia económica, sino que se dañan esferas privadas/personales de la persona. Algunas de las conductas que entran dentro de este tipo de ciberdelincuencia son el ciberacoso, dentro del cual pueden incluirse el *ciberbullying* o el *cyberstalking*, el ciberacoso sexual, llamado *cybergrooming* si se realiza contra menores, y el control por parte de la pareja o la expareja a través de las TIC e Internet[4].

[3] En el capítulo IV de este informe, y más concretamente en el apartado "*4.2 Ciberataques que afectan a los jóvenes de Castilla y León"* se especifica en qué consiste cada uno de estos ciberataques.

[4] Estas conductas, al igual que las que se integran dentro de la ciberdelincuencia económica, se explican con mayor detalle en el apartado "*4.2 Ciberataques que afectan a los jóvenes de Castilla y León".*

Como se verá posteriormente, en este estudio se analizan con detalle las distintas conductas que se incluyen en ambos tipos de ciberdelincuencia y en qué medida afectan a los alumnos de enseñanza no universitaria de la comunidad autónoma de Castilla y León.

2.2 Cibervictimización en menores

Existe un ámbito del ciberespacio que preocupa especialmente a la población: la cibervictimización de los jóvenes, es decir, el hecho de que los más jóvenes sean víctimas de delitos cometidos a través del mundo virtual. Esta preocupación se debe a la condición de colectivo vulnerable que tiene este sector de la población, el cual, además, se ve más expuesto a las amenazas del ciberespacio porque suele ser menos consciente de los riesgos reales que conlleva y desconoce las medidas que debe adoptar para protegerse de los ciberataques. Además, el hecho de que los jóvenes hagan un gran uso de las tecnologías, sobre todo del móvil y el ordenador, hace que pasen muchas horas al día navegando por Internet, lo que se convierte en un factor de riesgo para la cibervictimización (García, 2017).

A pesar de la preocupación por la cibervictimización de este colectivo, los adultos, y especialmente los padres, madres y educadores, en la medida que les competa, no supervisan lo que los jóvenes hacen en Internet (García, 2017). En otras palabras, existe poco control parental sobre las actividades desarrolladas en el mundo virtual. Ello podría explicarse, en parte, porque los adultos tampoco conocen la realidad del ciberespacio, no están bien informados sobre cómo enfrentar los riesgos y problemas derivados de su utilización y, en consecuencia, no saben cómo actuar ante casos de ciberdelincuencia.

Tal y como se ha ido introduciendo en apartados anteriores, la población joven se expone a una serie de riesgos al interactuar en el ciberespacio. Citando de

nuevo la reformulación que hace Miró (2013) de la Teoría de las Actividades Rutinarias de Cohen y Felson (1979), los jóvenes, al realizar ciertas conductas y llevar a cabo algunas actividades en el ciberespacio, pueden aumentar su propio riesgo de ser víctimas de un ciberataque. De hecho, Miró (2013) apunta que "la víctima es elemento clave en la producción del evento delictivo particularmente en Internet, ya que determina su propio ámbito de riesgo al incorporar determinados bienes al ciberespacio, al interaccionar con otros y particularmente con desconocidos, y al no utilizar todas las posibles medidas de autoprotección" (p. 30).

Algunos de los factores generales que aumentan el riesgo de ser víctima de un ciberataque son contactar con desconocidos, publicar información personal o simplemente interactuar en el ciberespacio. Si se concreta más en un ciberataque específico como, por ejemplo, el ciberacoso, el cual tiene una gran incidencia y prevalencia en los centros educativos (García, 2017), se destaca que algunos de los factores de riesgo se relacionan con el uso de las redes sociales, la cesión voluntaria de información personal o privada y pasar muchas horas navegando por Internet, sobre todo si se hace en espacios físicos alejados de la supervisión de los padres (por ejemplo, que el joven haga uso de Internet en su cuarto o en zonas del hogar donde no haya ningún adulto presente que pueda controlarlo) (García, 2017).

Es importante conocer los riesgos a los que se exponen los más jóvenes para poder dirigir una intervención adecuada a sus necesidades. Ejemplo de ello es el programa de prevención desarrollado por Rodríguez, Fernández y Bautista (2017), un programa de prevención victimal basado en los resultados del estudio CiberApp desarrollado por Crímina en el año 2014. Este programa tiene un enfoque bidimensional y una orientación comunitaria y pretende prevenir tanto la cibervictimización como la ciberdelincuencia. Se trata, además, de un

programa de prevención primario basado principalmente en la sensibilización y concienciación de los riesgos del ciberespacio.

Profundizando un poco más en el programa mencionado en el párrafo anterior, cabe destacar que las sesiones se basaron, primero, en exponer los riesgos relacionados tanto con los ciberdelitos económicos (fraude en compra, infección por *malware*, estafas, etc.) como con los sociales (ciberacoso, ciberacoso sexual y control de pareja) y, segundo, en aportar estrategias para favorecer el uso seguro de Internet, la denuncia y el afrontamiento de los ciberataques (Rodríguez, Fernández y Bautista, 2017).

En definitiva, este apartado deja constancia de la preocupación que existe en la sociedad sobre los distintos ciberataques que afectan a los más jóvenes, aunque la realidad muestra que los propios adultos desconocen los riesgos que conllevan las TIC e Internet y cómo prevenirlos.

2.3 Cibervictimización y su incidencia en el ámbito escolar

Lejos quedan ya los inicios de la preocupación de las diferentes sociedades por el fenómeno del *bullying* acuñado por Olweus (1978), quien definió el constructo como una situación de violencia persistente en el tiempo, física o mental, que es sostenida por uno o varios menores de un mismo centro escolar sobre otro alumno, al cual han escogido como foco de sus ataques, encontrándose éste en una situación de indefensión.

Más de dos décadas después de que autores tan relevantes como el mencionado anteriormente empezasen a considerar el *bullying* como un problema, en España sigue habiendo una falta de estudios que analicen este fenómeno. Cerezo (2009) es una de las autoras que arroja luz sobre la incidencia de este fenómeno en los centros escolares del territorio español. En su investigación, la autora determina

que el *bullying* se produce en todos los centros objeto de estudio y que su incidencia alcanza al 23% de los menores estudiados.

Hoy en día, a pesar de los conocimientos adquiridos y de los esfuerzos realizados para acabar con este tipo de violencia en las aulas, siguen existiendo casos alarmantes que preocupan notablemente no sólo a padres y educadores, sino al conjunto de la sociedad española. Basta con recordar el suceso acaecido hace poco más de un año en Palma de Mallorca, donde una menor de 8 años recibía una paliza por parte de 12 de sus compañeros de colegio, ocasionándole un desprendimiento de riñón en lo que parecía ser la culminación de una serie de insultos y menosprecios sufridos por la víctima con frecuencia[5]. Debemos recordar que casos tan mediáticos como éste son la punta de un *iceberg*, ya que la mayoría de las dinámicas de acoso escolar permanecen relegadas a un segundo plano que permite que éstas pasen desapercibidas para la totalidad de la ciudadanía española, lo que no significa que no existan.

No obstante, las dinámicas violentas reflejadas en las aulas han dado un salto cualitativo adecuándose a las TIC, al igual que lo han hecho los demás aspectos de la vida de las personas. De este modo, se conforma lo que hoy conocemos como *cyberbullying,* que puede presentarse como una continuidad del acoso iniciado en el espacio físico o como una modalidad de acoso escolar que se inicia y se mantiene únicamente a través de las nuevas tecnologías (Hernández-Prados y Solano-Fernández, 2007).

En CiberApp, el primer estudio sobre el alcance de la cibervictimización en menores del territorio nacional, realizado por el Centro Crímina en la provincia

[5] El Periódico de Palma de Mallorca recogía el suceso el 7 de diciembre de 2016. Facilitamos el acceso al mismo a través del siguiente enlace: http://www.elperiodico.com/es/sociedad/20161007/hospitalizada-nina-ocho-anos-paliza-doce-companeros-colegio-mallorca-5471599

de Alicante (2014), se obtuvieron resultados que indicaban que el 33,9% de los menores alicantinos sufría insultos o ridiculizaciones reiteradas por parte de sus compañeros de clase, y un 21,3% de los mismos era atacado de este modo por parte de los compañeros de otras aulas. Respecto a la vertiente sexual del ciberacoso, los menores aseguraban haber sufrido acoso repetido a través de mensajes de carácter sexual por uno o varios compañeros de clase en el 7,9% de los casos y el 10,2% de los menores victimizados por esta modalidad delictiva aseveraban haber sido atacados por compañeros de otras clases.

Durante el año 2016, en el estudio llevado a cabo por Crímina en Extremadura (CiberEduca2.0), se obtuvieron resultados que indicaban nuevamente que los menores seguían siendo víctimas de ciberataques por parte de sus compañeros de colegio. A modo de ejemplo, basta con mencionar que el 45% de los menores extremeños que sufría marginación o exclusión a través de las TIC era victimizado por sus propios compañeros de clase, mientras que un 27,5% de los mismos sufría esta misma conducta por parte de uno o varios alumnos de otras clases.

A pesar de ello, no debemos restar importancia a los ciberataques realizados por personas ajenas al ámbito escolar del menor, puesto que en la medida en que un hecho afecta directamente a un sujeto, también puede llegar a afectar al resto de facetas de su vida, incluyendo, por tanto, el colegio. No olvidemos que los menores de edad pasan gran parte del día en los centros académicos, lo que sitúa a los profesores en una posición de privilegio a la hora de detectar posibles cambios en los jóvenes que pueden ser consecuencia de una potencial victimización.

Algo similar sucede con la tendencia de los menores a utilizar las TIC e Internet, lo cual puede convertirse en un problema si no se utilizan correctamente. En concreto, uno de estos problemas es el abuso de las TIC e Internet. Aunque este abuso no tenga lugar en las aulas, puede tener consecuencias muy negativas en

la trayectoria escolar del joven, ya que puede interferir en las horas de sueño o en las horas de estudio y, en consecuencia, afectar al rendimiento escolar, tal y como manifiestan De Gracia, Vigo, Fernández y Marcó (2002) o Echeburúa y De Corral (2010).

En definitiva, los datos arrojados por las investigaciones predecesoras a Saf_*e* ponen de manifiesto que es necesario ampliar los estudios de cibervictimización a las pautas de prevención e intervención que contemplan los centros académicos para hacer frente a problemáticas tan actuales como son la cibervictimización y los riesgos de Internet.

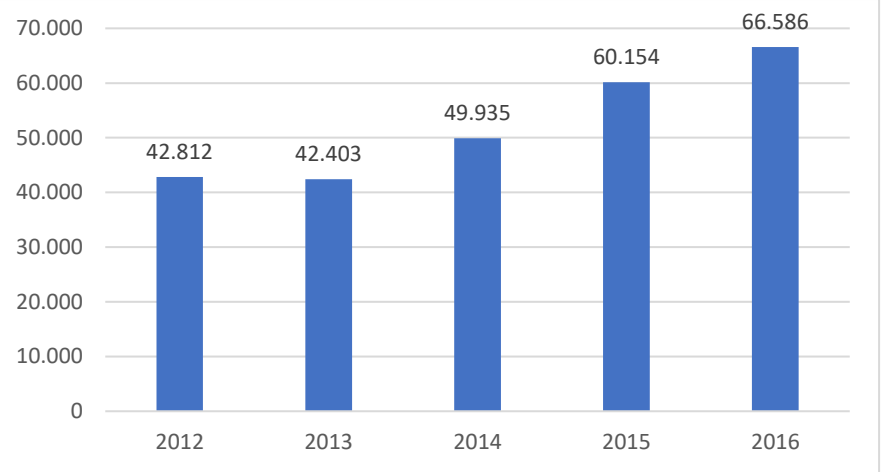
2.4 Cibercriminalidad y cibervictimización en España: situación actual

2.4.1 Cibercriminalidad

Es difícil saber cómo es la situación actual de la ciberdelincuencia en España, ya que existen pocos datos al respecto y los que hay son poco exactos. A pesar de ello, existen algunas fuentes oficiales de información que pueden ofrecer una imagen orientativa sobre este escenario. Una de estas fuentes procede del Ministerio del Interior, que desde 2013 realiza estudios sobre la cibercriminalidad en España a partir de los datos procedentes del Sistema Estadístico de Criminalidad (SEC), quien a su vez recoge datos obtenidos por las Fuerzas y Cuerpos de Seguridad del Estado, en adelante FCSE, (Guardia Civil y Cuerpo Nacional de Policía), la Policía Foral de Navarra y algunos Cuerpos de Policía Local. El principal inconveniente de esta fuente de información es que excluye algunos cuerpos de policía autonómicos y locales, lo que conlleva una no adecuación de los datos a la realidad. Por ello, es necesario disponer de otras fuentes oficiales, así como estudios empíricos que complementen la información aportada por las primeras.

Profundizando en los datos, en el gráfico 1 se muestra un aumento de los hechos conocidos sobre cibercriminalidad desde el 2012 hasta el 2016, lo que a primera vista podría indicar un aumento de este tipo de delincuencia. Sin embargo, debemos tomar con cautela estos datos, ya que lo que podrían mostrar es que existe una mayor visibilidad de los delitos en este ámbito y no un aumento de los mismos.

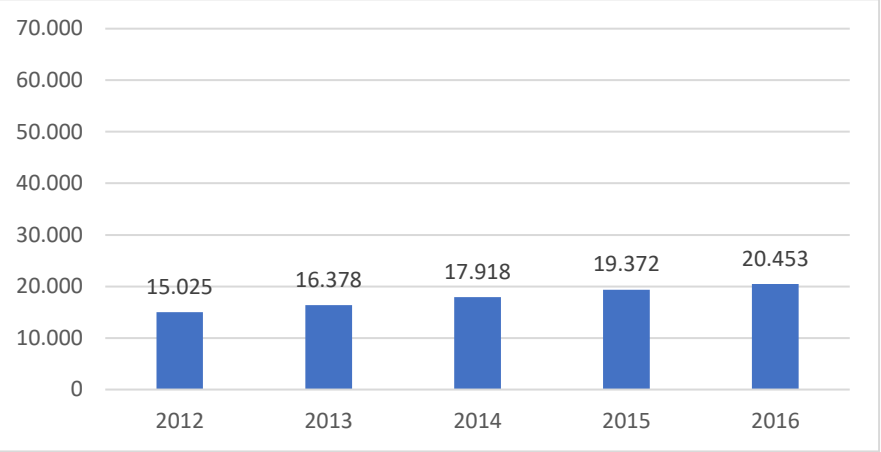
Gráfico 1. *Evolución global de los hechos conocidos sobre cibercriminalidad entre 2012 y 2016*



*Fuente: Elaboración propia a partir de los datos de los Estudios sobre la cibercriminalidad en España de los años 2015 y 2016 (Ministerio del Interior).

En cuanto a los datos esclarecidos, se observa que también ha habido una tendencia al alza en los últimos 5 años, tal y como se muestra en el gráfico 2. Ello muestra que, aun sin importar si el resultado final de la investigación es la determinación de la existencia real de un hecho delictivo o no, cada año se consiguen esclarecer más casos, lo que podría indicar una mayor involucración del sistema en la persecución de la cibercriminalidad.

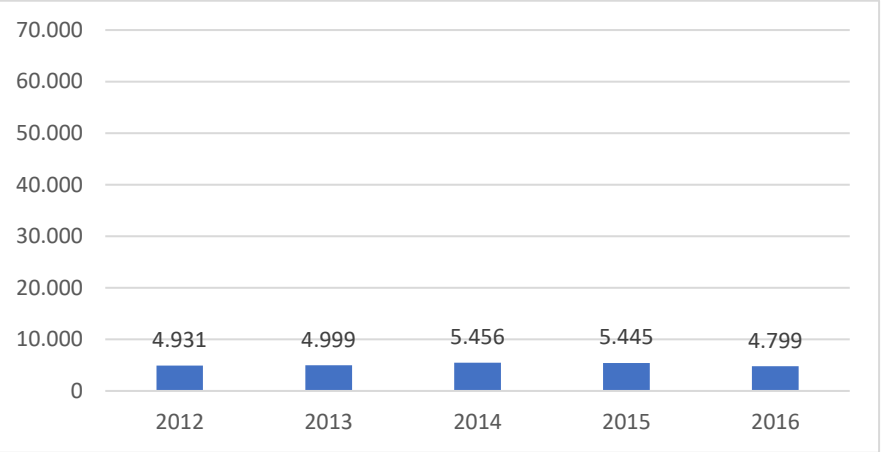
Gráfico 2. *Evolución global de los hechos esclarecidos entre 2012 y 2016*



*Fuente: Elaboración propia a partir de los datos de los Estudios sobre la cibercriminalidad en España de los años 2015 y 2016 (Ministerio del Interior).

En cuanto al global de detenciones e imputaciones, se observa que los datos varían un poco más respecto a las dos ilustraciones anteriores. En el gráfico 3 se muestra que en 2014 y 2015 el número de detenciones e imputaciones aumentó, mientras que en 2016 éste descendió incluso a valores más bajos que los de 2012. De nuevo, ello no indica que la ciberdelincuencia haya aumentado o disminuido. Por otra parte, podría indicar cambios a la hora de valorar la ciberdelincuencia o un cambio de las leyes penales.

Gráfico 3. *Evolución global de las detenciones e imputaciones entre 2012 y 2016*

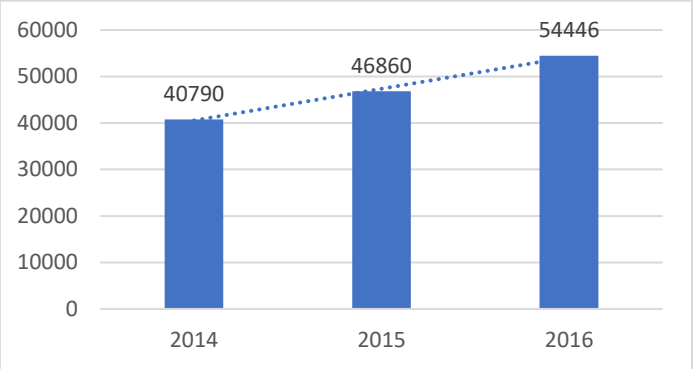


*Fuente: Elaboración propia a partir de los datos de los Estudios sobre la cibercriminalidad en España de los años 2015 y 2016 (Ministerio del Interior).

2.4.2 Cibervictimización

Como bien se ha comentado anteriormente, es difícil obtener datos sobre las cifras de ciberdelincuencia. Sin embargo, aún es más difícil obtenerlos acerca de la cibervictimización, es decir, el número de víctimas por ciberataques. De hecho, aunque el Ministerio del Interior de España comenzó a realizar estudios sobre cibercriminalidad en el año 2013, no fue hasta el 2014 cuando comenzó a introducir cifras sobre cibervictimización. En el gráfico 4 se observa que desde 2014 hasta 2016 se ha producido un aumento en más de 10.000 víctimas por delitos cometidos en el ciberespacio.

Gráfico 4. *Evolución de cibervictimización registrada en España entre 2014 y 2016*



*Fuente: Elaboración propia a partir de los datos de los Estudios sobre la cibercriminalidad en España de los años 2014, 2015 y 2016 (Ministerio del Interior).

Si se analizan estas mismas cifras en función de la edad de las víctimas y, más concretamente, diferenciando entre menores y adultos, tal y como se muestra en la tabla 1, se observa que, aparentemente, las victimizaciones han aumentado tanto en el grupo de adultos como en el de menores. Sin embargo, es importante volver a interpretar con cautela los datos.

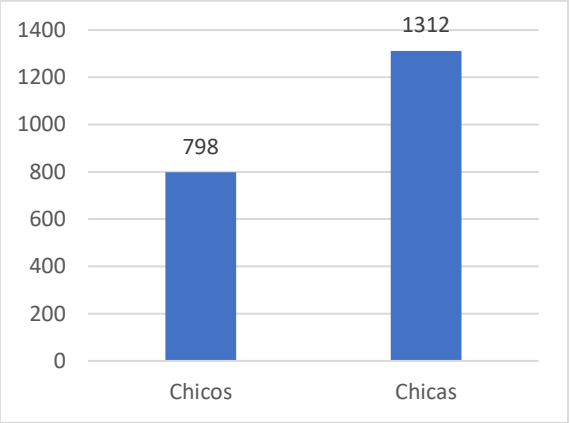
Tabla 1. *Evolución de las victimizaciones registradas en España entre 2014 y 2016 según edad*

Grupo de edad	2014	2015	2016
Adultos	38.811	44.703	51.768
Menores	1.833	2.004	2.110
Edad desconocida	146	153	568
TOTAL	40.790	46.860	54.446

*Fuente: Elaboración propia a partir de los datos de los Estudios sobre la cibercriminalidad en España de los años 2014, 2015 y 2016 (Ministerio del Interior).

Concretando en las cifras relacionadas con los menores, se observa que en el año 2016, de los 2.110 menores cibervictimizados, un 37’82% (n = 798) fueron chicos, mientras que un 62’18% (n = 1312) fueron chicas. Es decir, en el año 2016 hubo más chicas víctimas por cibercriminalidad que chicos.

Gráfico 5. *Prevalencia de la cibervictimización por sexos en menores en el año 2016 en España*



*Fuente: Elaboración propia a partir de los datos del Estudio sobre la cibercriminalidad en España del año 2016 (Ministerio del Interior).

En cuanto a la tipología delictiva, se observa que en el año 2016 la más común entre los menores fue la de amenazas y coacciones, seguida por la de los delitos sexuales.

Tabla 2. *Prevalencia de la cibervictimización por tipología penal en menores en el año 2016 en España*

Tipología penal	Número de menores (F_i)	Porcentajes
Acceso e interceptación ilícita	251	11,9%
Amenazas y coacciones	799	37,87%
Contra el honor	122	5,78%
Contra propiedad industrial/intelectual	0	-
Delitos sexuales	666	31,56%
Falsificación informática	100	4,74%
Fraude informático	163	7,73%
Interferencia en datos y en sistema	9	0,43%

*Fuente: Elaboración propia a partir de los datos del Estudio sobre la cibercriminalidad en España del año 2016 (Ministerio del Interior).

*Porcentajes calculados sobre el total de menores cibervictimizados en el año 2016.

En general, las chicas son más victimizadas en el ciberespacio que los chicos en todas las tipologías penales a excepción del fraude informático, donde son ellos

los que despuntan. Además, la tipología penal en la que existe una mayor diferencia entre unos y otras es la correspondiente a los delitos sexuales, siendo las chicas más víctimas que los chicos.

Tabla 3. *Prevalencia de la cibervictimización por tipología penal y sexo en menores en el año 2016 en España*

Tipología penal	Chicos	Chicas	TOTAL
Acceso e interceptación ilícita	99	152	251
Amenazas y coacciones	309	490	799
Contra el honor	20	102	122
Conta propiedad industrial/intelectual	0	0	0
Delitos sexuales	240	426	666
Falsificación informática	25	75	100
Fraude informático	101	62	163
Interferencia en datos y en sistema	4	5	9
TOTAL	798	1.312	2.110

*Fuente: Elaboración propia a partir de los datos del Estudio sobre la cibercriminalidad en España del año 2016 (Ministerio del Interior).

Como se deduce de todos los datos propuestos sobre cibercriminalidad y cibervictimización, los cuales son escasos y relativamente nuevos, existe una necesidad de investigar más sobre el fenómeno, conocerlo en profundidad y, así, poder realizar actuaciones preventivas en consecuencia.

III. SAF_e: PROTOCOLO DE ACTUACIÓN SOBRE USO SEGURO DE LAS TIC, CONVIVENCIA ESCOLAR Y RIESGOS DE INTERNET EN CASTILLA Y LEÓN

Los nativos digitales, como bien se ha comentado anteriormente, vienen utilizando Internet y las nuevas tecnologías desde su niñez, lo que conlleva que el ciberespacio sea un medio de interacción natural para ellos. Además, hoy día el crecimiento y desarrollo de los más jóvenes está inevitablemente ligado a la comprensión del ciberespacio y su funcionamiento, ya que éste es una fuente de

oportunidades que les permite comunicarse, relacionarse, aprender y desarrollarse.

Sin embargo, esto no es así para las generaciones que les preceden, es decir, sus padres y docentes, ya que ellos no han crecido teniendo el ciberespacio a su alcance. Al contrario, han tenido que adaptarse una vez ya eran adultos, con las dudas y temores propios de quien no ha crecido considerando Internet y las TIC como un medio de relación natural. Esto hace que no estén debidamente informados sobre cómo funciona realmente el ciberespacio y que, por ende, tengan prejuicios y desconfianza a la hora de usarlo. Además, también conlleva que no conozcan cuál es la manera adecuada de actuar en este ámbito, cuáles son los riesgos reales que tiene y la manera de prevenirlos.

Para intentar dar una solución a esta problemática, el gobierno español, más concretamente el Instituto Nacional de Ciberseguridad de España (INCIBE), ha puesto a disposición de los menores recientemente un teléfono cuya utilidad es ayudarlos y aconsejarlos sobre los riesgos de Internet. De forma similar, la comunidad autónoma de Castilla y León ha manifestado estar implicada en la prevención de los riesgos que tienen el ciberespacio y las nuevas TIC, ya que a lo largo de los últimos años ha ido creando distintas guías relacionadas con la prevención de este fenómeno, como por ejemplo la "*Guía de buenas prácticas TIC para las familias*", la "*Guía de actuación contra el ciberacoso*" para padres y educadores, la "*Guía de Buenas Prácticas Ambientales para el usuario de las TIC*" y la "*Guía de Seguridad y Privacidad*". Todas estas guías se centran, cada una en su ámbito de actuación concreto, en fomentar la participación de familias y educadores y en informar sobre cómo hacer un correcto uso de las TIC y, así, conseguir una mayor prevención de la cibervictimización de los menores.

Asimismo, Castilla y León también ha realizado distintos proyectos e iniciativas relacionados con el fenómeno de estudio que nos ocupa, como son la "*Red de*

Centros Piloto de la Junta de Castilla y León" o el "*Proyecto Internet sin riesgos*". La primera tiene como función formar al profesorado sobre cómo aplicar las TIC en el aula de una forma correcta. El segundo persigue el principal objetivo de sensibilizar a los menores sobre los riesgos de Internet.

A su vez, el Centro Crímina para el estudio y prevención de la delincuencia cuenta con experiencia en el ámbito de la cibervictimización, ya que con anterioridad al presente estudio realizó otros dos similares en Alicante[6] y Extremadura[7], siendo el de Alicante el primer estudio en toda España con estas características. Además, antes de realizar estos dos proyectos, llevó a cabo la primera investigación a nivel nacional sobre cibercriminalidad en población adulta en el año 2012.[8]

Por tanto, queda ampliamente demostrada la implicación de Castilla y León en la búsqueda de soluciones para una problemática que preocupa a la comunidad. Con la intención de conocer en profundidad la realidad de este territorio y seguir desarrollando estrategias preventivas en este ámbito, nace Saf_*e*, un protocolo que, a través del análisis de los datos obtenidos a partir de la información transmitida por los menores y los docentes de esta comunidad autónoma,

[6] El proyecto realizado en Alicante tiene como nombre "CIBERAPP: Aprender, prevenir y proteger. Estudio sobre el alcance de la cibercriminalidad contra menores de la provincia de Alicante" (2014). Proyecto financiado por la Excelentísima Diputación de Alicante.

[7] El proyecto realizado en Extremadura tiene como nombre "CiberEduca2.0. Uso seguro de Internet en la Comunidad Autónoma de Extremadura. Análisis inicial de los hábitos en Internet, riesgos de uso y factores de victimización de los menores extremeños" (2016). Proyecto financiado por la Junta de Extremadura.

[8] El proyecto tiene como nombre "Cibercriminalidad, detección de déficits en su prevención jurídica y determinación de los riesgos de victimización para una mejor prevención situacional criminológica" (2012). Proyecto financiado por el Ministerio de Ciencia e Innovación.

pretende ser una herramienta de prevención, actuación e intervención en el ámbito de la cibercriminalidad que afecta a los más jóvenes. Saf_*e* permitirá conocer el alcance de la cibervictimización de los alumnos de enseñanza no universitaria en esta comunidad, así como sus hábitos en el ciberespacio, para poder incidir en estrategias preventivas basadas en la evidencia empírica.

El proyecto Saf_*e* está dividido en dos fases. En la primera de ellas, que es la que motiva la realización del presente informe, se realiza un análisis sobre las principales cifras de cibervictimización y los hábitos de uso de las TIC e Internet de los alumnos de enseñanza no universitaria de Castilla y León, con edades comprendidas entre los 9 y los 21 años. Asimismo, se presentan las estrategias de prevención e intervención llevadas a cabo por los centros educativos. En la segunda fase, se realizará una detección de los factores de riesgo y de protección y se elaborará un plan general de actuación sobre el uso seguro de las TIC, la convivencia escolar y los riesgos de Internet.

Los objetivos concretos del proyecto Saf_*e* que se pretenden alcanzar son los siguientes:

- Analizar los hábitos del alumnado de Castilla y León en el uso de Internet y riesgos derivados.
- Concretar los hábitos de los alumnos en ciberseguridad, y en los dispositivos que utilizan dentro y fuera del ámbito escolar.
- Determinar los factores de protección y de riesgo para la prevención de la ciberdelincuencia.
- Conocer las dinámicas de respuesta de los centros ante el fenómeno, obteniendo información sobre cómo se previene y se actúa ante la cibercriminalidad.

- Desarrollar una herramienta integral de prevención del ciberacoso y la ciberdelincuencia para los alumnos de enseñanza no universitaria de Castilla y León.

Más concretamente, los objetivos de cada fase son los siguientes:

- Fase 1.
  - Establecer la prevalencia de la cibervictimización sufrida por los jóvenes.
  - Conocer los hábitos del uso de las TIC e Internet de los jóvenes.
  - Conocer la actuación de los centros ante los casos que afectan a la convivencia escolar mediante una fuente doble: alumnos y docentes.
- Fase 2.
  - Describir cuáles son los factores de riesgo y de protección relacionados con la cibervictimización.
  - Definir herramientas específicas para la prevención de los riesgos en el uso de las TIC por parte de los menores a partir de la información obtenida sobre la actuación de los centros docentes en los cuestionarios de la Fase 1.
  - Dotar a los centros docentes de la comunidad autónoma de Castilla y León de un protocolo de actuación que contenga una secuencia detallada de indicaciones orientadas a actuar adecuadamente ante las consecuencias del mal uso de las TIC.

En definitiva, Saf_*e* permitirá conocer la realidad de Castilla y León para poder prevenir la cibervictimización de la población más joven de esta comunidad autónoma y minimizar los riesgos existentes en el ciberespacio que afectan a este colectivo. Asimismo, proporcionará herramientas a los docentes que les permitirán actuar debidamente ante casos de cibervictimización.

IV. RESULTADOS

Tras haber contextualizado en los anteriores capítulos qué es, por un lado, el ciberespacio y la cibervictimización en menores y, por el otro, en qué consiste el proyecto Saf_*e*, a lo largo de todo este apartado se presentan los principales resultados acerca de todos aquellos aspectos relacionados con la cibervictimización y el uso de las TIC e Internet de los alumnos de enseñanza no universitaria de la comunidad autónoma de Castilla y León.

Más concretamente, en este capítulo se presentan siete bloques de información distintos. El primero de ellos (apartado "*4.1 Ciberataques sociales autoinformados por los* alumnos") está destinado a aportar conocimiento sobre los ciberataques que realizan los propios alumnos contra otras personas cuando hacen uso de Internet. Más concretamente, se analizan tres tipos de ciberataques sociales: el ciberacoso, el ciberacoso sexual y el control de pareja.

A continuación, se detallan los diferentes tipos de ciberataques que afectan a los jóvenes de Castilla y León, diferenciando entre aquellos que son económicos y aquellos que son sociales (apartado "*4.2. Ciberataques que afectan a los jóvenes de Castilla y León"*).

Seguidamente, tras ver las principales cifras de cibervictimización y ciberataques reportados por los alumnos, se presentan los datos relacionados con el abuso de Internet de los mismos (apartado "*4.3 Conductas de uso desviado de Internet y*

las TIC de los jóvenes de Castilla y León"). En otras palabras, se presenta la prevalencia de alumnos encuestados que abusa de Internet, así como la distribución de los mismos en función de variables como el sexo o la edad.

Tras la introducción de estos tres primeros apartados, se presenta el cuarto (apartado "*4.4 Percepción y conocimiento de los docentes sobre los ciberataques y uso desviado de Internet que afectan a los jóvenes de Castilla y León"*), en el que se exponen las cifras de cibervictimización de los alumnos desde el punto de vista de los docentes. Es decir, en este bloque se detalla lo que los profesores perciben que sucede en sus centros escolares, al mismo tiempo que se incluye información sobre casos reales de cibervictimización y abuso de Internet que los docentes se han encontrado a lo largo de sus carreras profesionales.

En el quinto bloque (apartado "*4.5 Hábitos en el uso de las TIC de los jóvenes de Castilla y León*") se deja de proporcionar datos sobre cibervictimización y, en su lugar, se realiza un estudio sobre los hábitos que tienen los jóvenes de Castilla y León a la hora de usar las TIC e Internet. Más concretamente, se profundiza en el uso de las principales tecnologías utilizadas por los alumnos (ordenador, móvil y tablet), en las herramientas de comunicación más comunes en este colectivo, entre las cuales se incluyen las redes sociales o los blogs, entre otras, y en las actividades que los jóvenes realizan cuando navegan por Internet (comprar, jugar, facilitar datos personales, etc.).

Los últimos dos bloques se reservan para el análisis de los actos llevados a cabo por los padres y otros familiares (apartado "*4.6 Supervisión parental del uso de las TIC*"), así como por los propios centros educativos (apartado *"4.7 Mecanismos de prevención e intervención de los centros educativos ante casos de cibervictimización y uso desviado de Internet*") para prevenir e intervenir ante casos en los que los jóvenes están siendo víctimas de algún tipo de ciberataque o están realizando un mal uso de Internet y las TIC.

4.1 CIBERATAQUES SOCIALES AUTOINFORMADOS POR LOS ALUMNOS

A lo largo de todo este primer apartado se presentan los resultados obtenidos tras el análisis de los ciberataques sociales realizados por los propios alumnos contra otras personas. Más concretamente, se les ha preguntado si realizan conductas de ciberacoso, ciberacoso sexual y control de pareja.

4.1.1 Ciberacoso

Un 13% de los alumnos encuestados (n = 954) afirma haber realizado conductas de ciberacoso alguna vez en su vida. Más concretamente, el tipo más frecuente, realizado por más de la mayoría de los alumnos (un 52%), corresponde al hecho de acceder a las cuentas personales de alguien sin su consentimiento. Los siguientes dos tipos de ciberacoso más realizados son, en primer lugar, insultar (un 37% de alumnos) y, en segundo lugar, marginar o excluir socialmente a alguien (un 25%).

Gráfico 6. *Prevalencia de alumnos que han realizado conductas de ciberacoso*

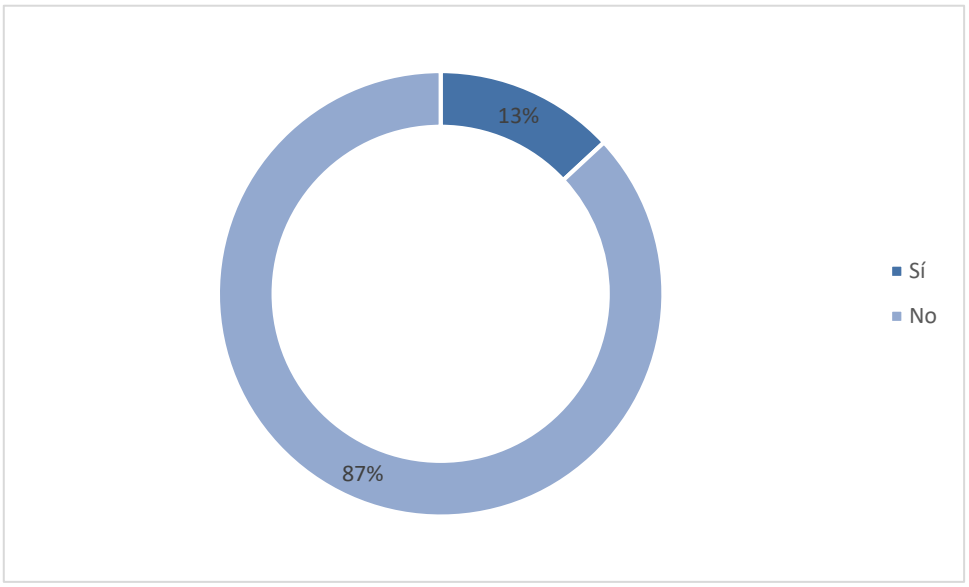
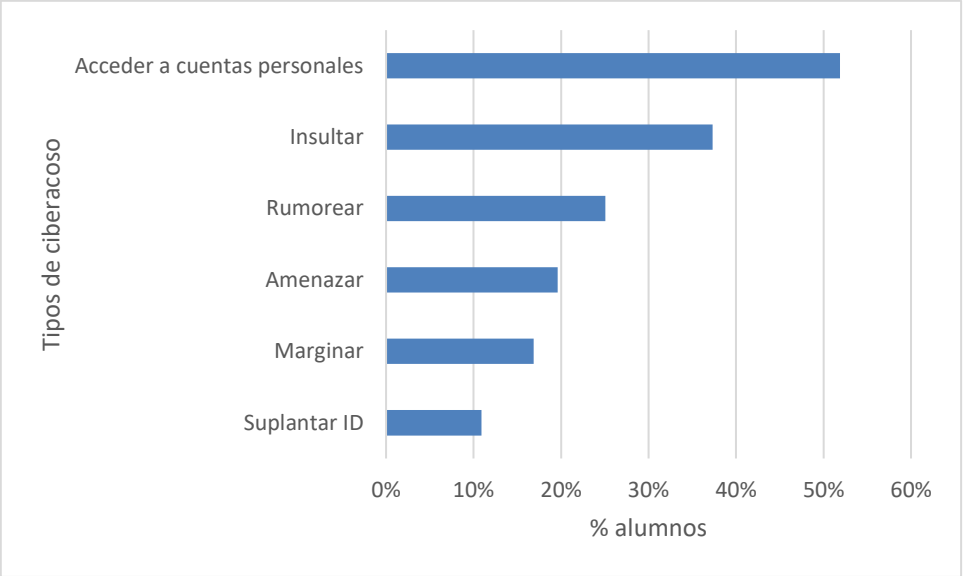


Gráfico 7. *Tipos de ciberacoso autoinformados por los alumnos*



4.1.2 Ciberacoso sexual

Un 7% de los alumnos encuestados (n = 302)[9] afirma haber realizado conductas de ciberacoso sexual alguna vez en su vida. Más concretamente, el tipo más frecuente, realizado por más de la mayoría de los alumnos (un 61%), corresponde al hecho de publicar fotos, vídeos o conversaciones provocativas de otras personas sin su consentimiento. Tras esta conducta, las dos más frecuentes consisten en enviar mensajes obscenos (un 36%) e imágenes provocativas (un 32%).

[9] El ciberacoso sexual autoinformado solo ha sido preguntado entre los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, por lo que los alumnos de 5º y 6º de primaria y 1º de ESO quedan excluidos de este análisis.

Gráfico 8. *Prevalencia de alumnos que han realizado conductas de ciberacoso sexual*

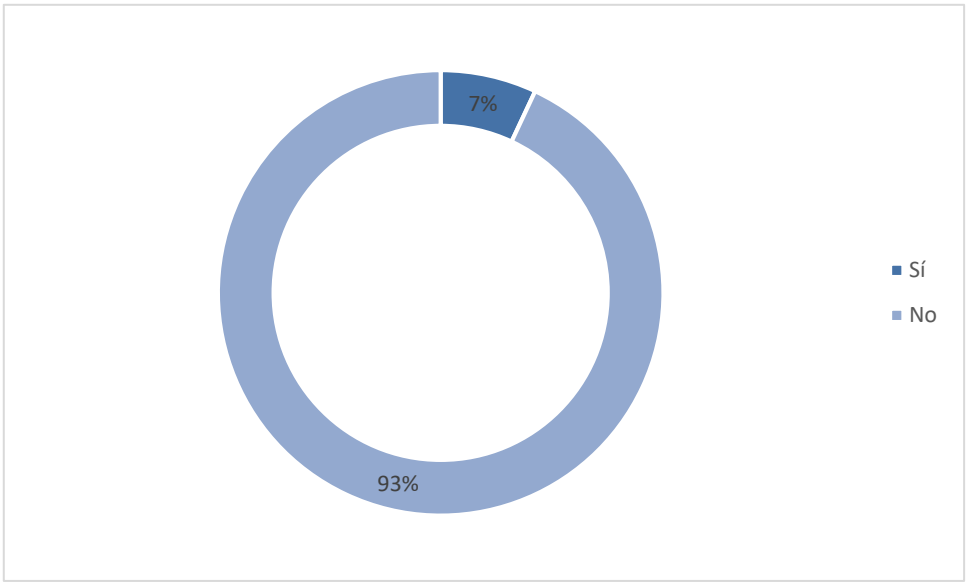
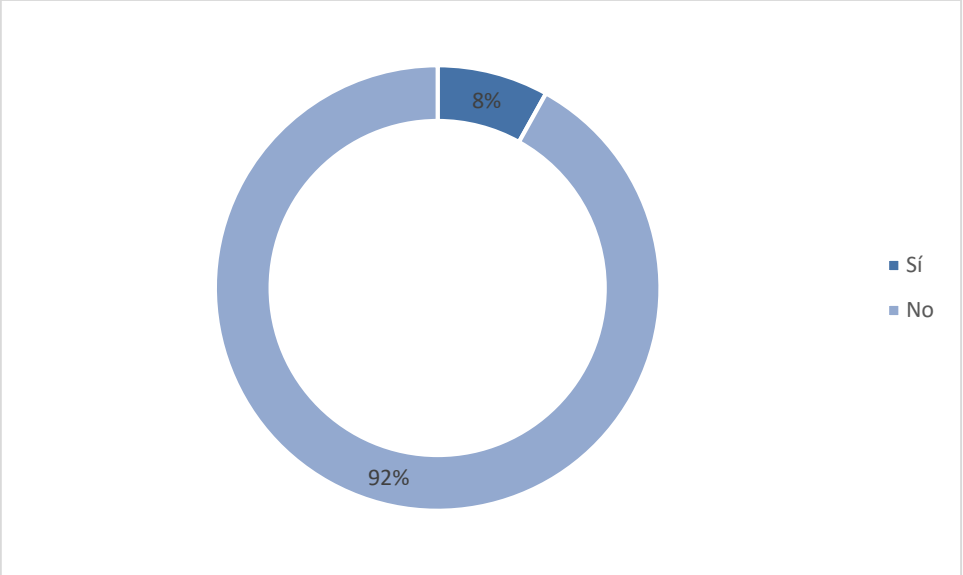


Gráfico 9. *Tipos de ciberacoso sexual autoinformados por los alumnos*

4.1.3 Control de pareja

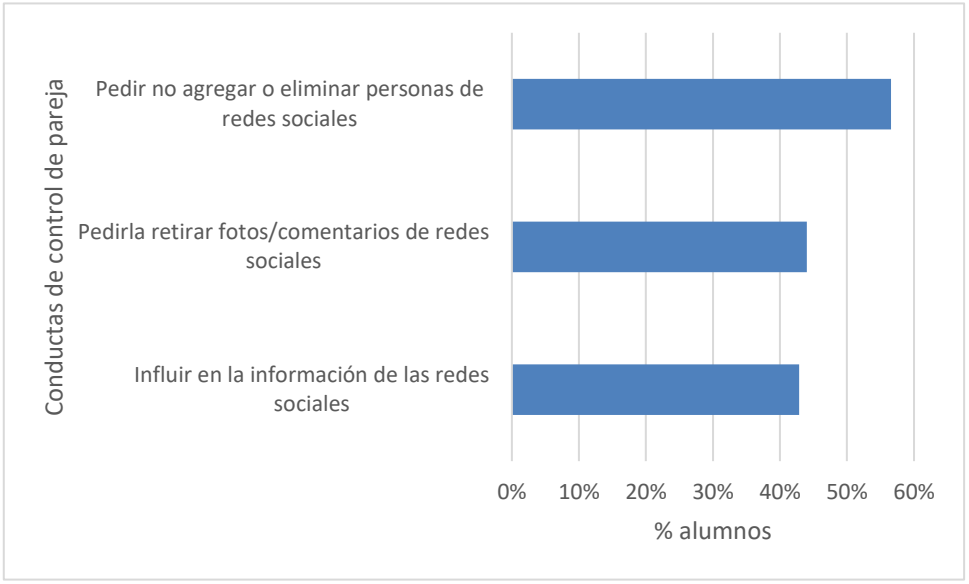
Un 8% de los alumnos encuestados (n = 350)[10] afirma haber realizado conductas de control de pareja a través de Internet alguna vez en su vida. Más concretamente, el tipo más frecuente, realizado por más de la mayoría de los alumnos (un 57%), corresponde al hecho de pedirle a su pareja que no agregase o eliminase a personas de sus redes sociales. Las otras dos conductas realizadas, con prevalencias muy similares, consisten en pedir a su pareja que retire fotos o comentarios de las redes sociales (un 44%) e intentar influir en la información de las redes sociales de su pareja (un 43%).

Gráfico 10. *Prevalencia de alumnos que han realizado conductas de control de pareja a través de las TIC*



[10] El control de pareja a través de las TIC autoinformado solo ha sido preguntado entre los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, por lo que los alumnos de 5º y 6º de primaria y 1º de ESO quedan excluidos de este análisis.

Gráfico 11. *Tipos de control de pareja autoinformados por los alumnos*



4.2 CIBERATAQUES QUE AFECTAN A LOS JÓVENES DE CASTILLA Y LEÓN

En capítulos anteriores se ha profundizado en el importante papel que tienen las TIC e Internet en la vida de las personas, sobre todo en la de aquellas más jóvenes. Asimismo, también se han expuesto datos generales sobre cibercriminalidad y cibervictimización a nivel español tanto en población adulta como en menores, los cuales han permitido saber que cada vez se conocen más casos de cibervictimización en ambos grupos. Sin embargo, sigue habiendo una falta importante de datos y estudios que describan la situación actual sobre la cibervictimización de los más jóvenes.

Por ello, en el marco del proyecto Saf_*e*, y a lo largo de todo el apartado 4.2 de este informe, se presentan las principales cifras de cibervictimización de los alumnos de enseñanza no universitaria de Castilla y León. Más concretamente, se presentan datos sobre cinco tipos de ciberataques económicos (fraude en compra, infección por *malware*, pérdida de archivo por infección por *malware*,

scam y *spam*) y tres tipos de ciberataques sociales (ciberacoso, ciberacoso sexual y control de pareja a través de las TIC).

A su vez, los datos se detallan de tres maneras distintas. Primero, se exponen los resultados sobre la prevalencia global de alumnos encuestados que han sido víctimas de alguno de los distintos tipos de ciberataques. Además, en el caso de los ciberataques sociales también se expone, desde la perspectiva de los jóvenes victimizados, quienes han sido los responsables de realizar estos ataques. Segundo, se profundiza en estos mismos resultados haciendo una diferenciación por sexo con el objetivo de conocer las diferencias de cibervictimización entre chicos y chicas. Por último, se presentan los datos en función del rango de edad de los alumnos que han sido víctimas.

4.2.1 Ciberataques económicos

Los ciberataques económicos engloban todo el conjunto de actos dirigidos a obtener un enriquecimiento ilícito, sea directo o indirecto. En palabras de Miró (2012), es "todo cibercrimen o ciberataque realizado con el propósito final de obtener un lucro económico con el consiguiente perjuicio de uno o varios usuarios. Son cibercrímenes económicos tanto aquellos ciberataques en los que la conducta termina en fraude, como otros que no son más que un acto preparatorio de los ciberataques defraudatorios finales" (p. 301).

En este sentido, se puede hacer una diferenciación entre los ciberataques económicos mediales como, por ejemplo, el *hacking,* las *infecciones por malware*, el *spam* y los *ataques DoS*, y los puros, como son el *phishing,* el *scam* y la *extorsión*.

Para el análisis de este tipo de ciberataques, en este estudio se han tenido en cuenta cinco conductas específicas: 1) fraude en compra, 2) infección por *malware*, 3) pérdida de archivo por infección de *malware*, 4) *scam* y 5) *spam*.

Aunque a lo largo de los siguientes apartados se analizan, uno por uno, cada uno de estos ataques, a continuación, se presentan datos globales del porcentaje total de alumnos de Castilla y León que ha sido víctima de algún ciberataque económico. Más concretamente, se diferencia entre los alumnos más pequeños, que son los que cursan 5º y 6º de Primaria y 1º de ESO, y los más grandes, que son los que cursan 2º, 3º y 4º de ESO, Bachillerato y Ciclos Formativos de Grado Medio (CFGM).

La razón principal por la que se hace esta diferenciación es que a los alumnos más pequeños no se les ha preguntado por el fraude en compra, por lo que los resultados globales de cibervictimización de este grupo se han obtenido a partir del análisis de las cuatro conductas restantes (infección por *malware*, pérdida de archivo por infección por *malware*, *scam* y *spam*). En cambio, en el caso de los más mayores sí que se han incluido los cinco tipos de ciberataques económicos mencionados en el párrafo anterior.

Como se puede observar en los siguientes gráficos, el 68% de alumnos que cursa 5º y 6º de primaria y 1º de ESO (n = 1994) ha sido víctima de algún ciberataque económico, mientras que en el caso del resto de alumnos de ESO, Bachillerato y CFGM la cifra asciende al 84% (n = 3646).

Gráfico 12. *Prevalencia de alumnos de 5º y 6º de primaria y 1º de ESO que han sido víctimas de algún ataque cibereconómico*

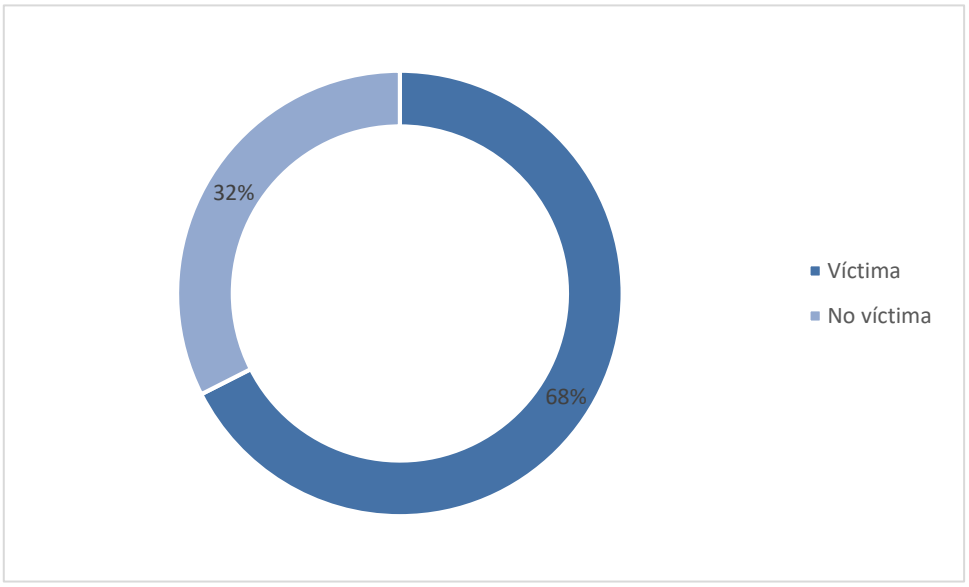
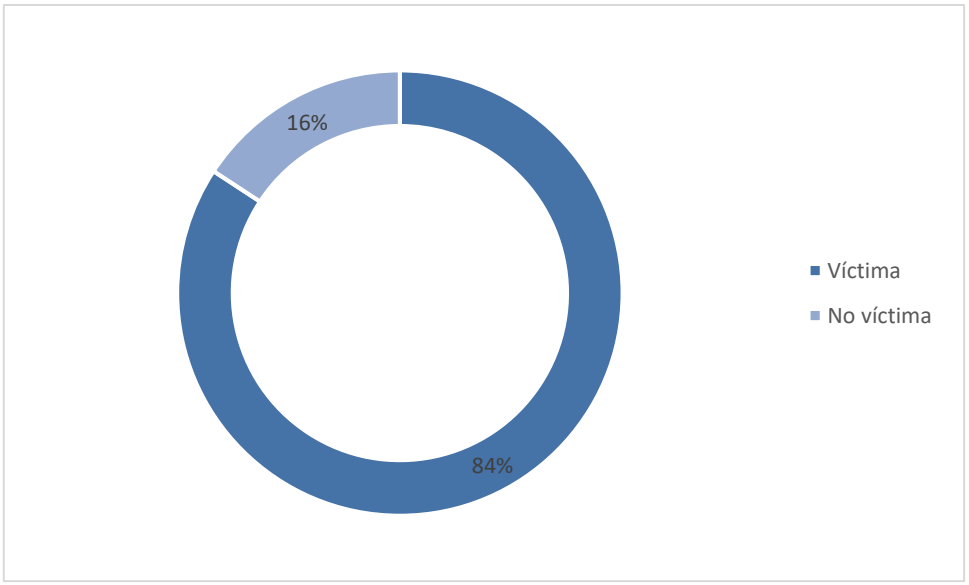


Gráfico 13. *Prevalencia de alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM que han sido víctimas de algún ataque cibereconómico*

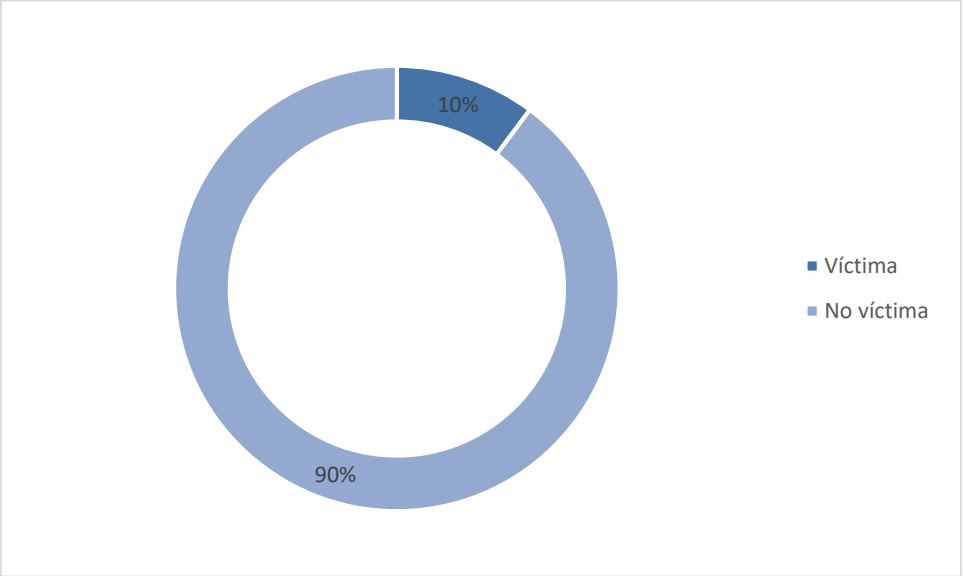


a) Fraude en compra

El fraude en compra es un tipo de ciberataque económico que incluye distintas

tipologías de fraude como, por ejemplo, que el producto comprado nunca llegue a su comprador, que llegue en malas condiciones (roto, defectuoso o de peor calidad) o que directamente sea distinto a lo que la persona compró. En la muestra de jóvenes de Castilla y León analizada se observa que, entre aquellos que han realizado compras por Internet alguna vez en su vida, un 10% ha sido estafado en el último año.[11]

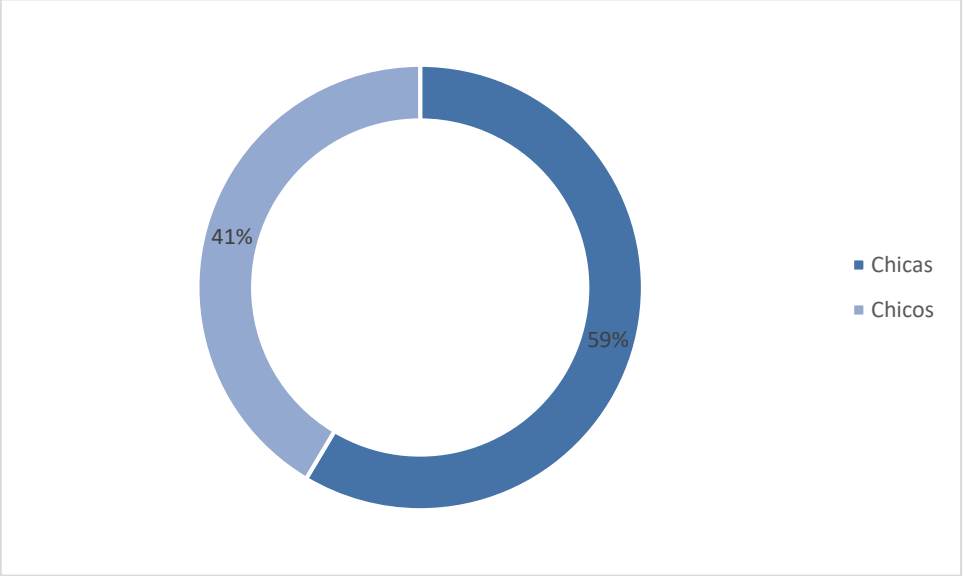
Gráfico 14. *Prevalencia de jóvenes víctimas de fraude en compra en el último año*



Analizando estos mismos datos en función del sexo de los alumnos se observa que, dentro del 10% de jóvenes que ha afirmado ser víctima de estafas a la hora de comprar por Internet, el 41% son chicos (n = 138) y el 59% son chicas (n = 195).

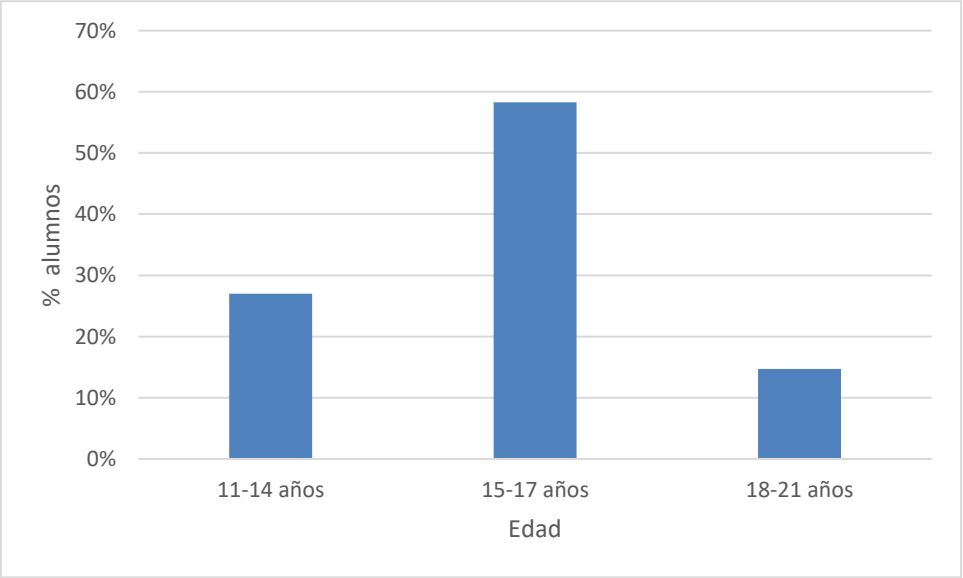
[11] Como bien se ha mencionado al inicio del apartado, el análisis del fraude en compra solo se realiza teniendo en cuenta a los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, ya que se eliminó esta conducta del cuestionario adaptado a los alumnos de 5º y 6º de Primaria y 1º de ESO.

Gráfico 15. *Prevalencia de jóvenes víctimas de fraude en compra en el último año según sexo*



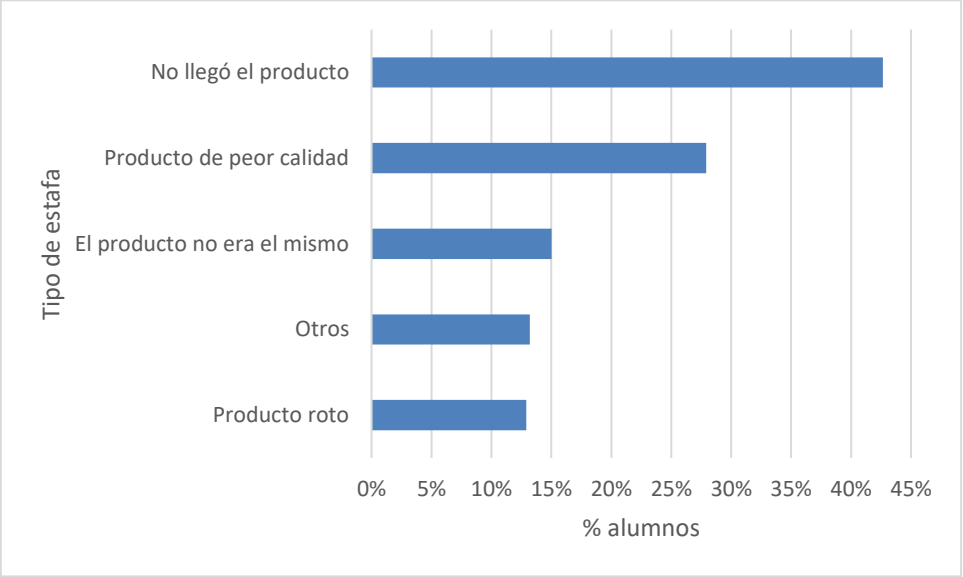
Analizando nuevamente estos mismos datos, aunque ahora en función de la edad, se observa que un 27% de alumnos víctimas de fraude en compra tiene entre 11 y 14 años (n = 90), un 58% tiene entre 15 y 17 años (n = 194) y un 15% tiene entre 18 y 21 años (n = 49).

Gráfico 16. *Prevalencia de jóvenes víctimas de fraude en compra en el último año según edad*



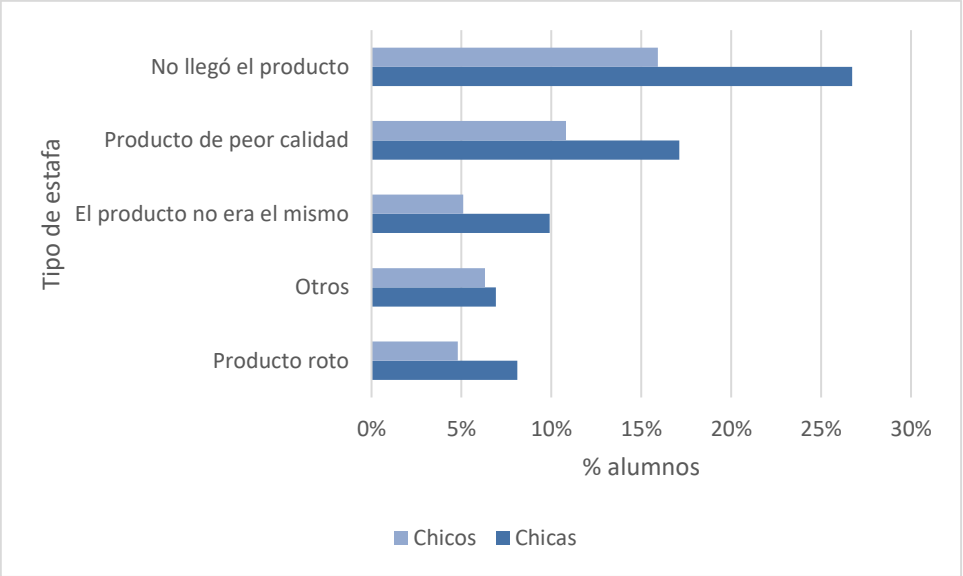
Como bien se ha introducido anteriormente, existen distintos tipos de fraude en compra. En este estudio se han analizado cuatro: 1) el producto estaba roto o averiado, 2) el producto recibido no era el mismo que se compró, 3) el producto era de peor calidad y 4) el producto nunca llegó. Además, se ha dado la opción a los jóvenes de que informen sobre otros tipos de fraude en compra, los cuales se incluyen en la categoría "Otros" del siguiente gráfico. Como se puede observar, el tipo de fraude más frecuente, sufrido por un 43% de los jóvenes, se relaciona con que el producto nunca llegó, seguido de recibir el producto con una calidad inferior a la esperada (un 28% de los jóvenes).

Gráfico 17. *Tipos de fraude en compra sufridos*



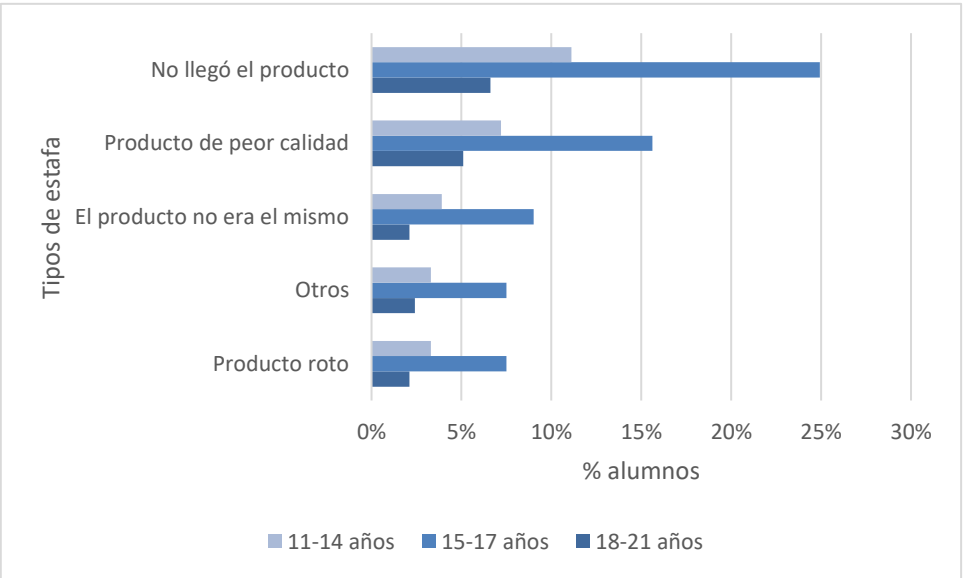
Diferenciando entre chicos y chicas, el tipo de fraude más frecuente, tanto entre unos y otras, consiste en que el producto nunca llegó (un 16% y un 27% de alumnos, respectivamente). De hecho, tanto chicos como chicas coinciden en el resto de tipos de fraude en compra, ya que ambos grupos afirman que el orden de los distintos tipos de estafa sufridos, de más a menos frecuente, es: el producto era de peor calidad, el producto no era el mismo y el producto llegó roto, acabando con la categoría "Otros".

Gráfico 18. *Tipos de fraude en compra sufridos según el sexo de la víctima*



En función del rango de edad, cabe destacar que todos los alumnos, independientemente de la edad, coinciden, al igual que en el caso de las diferencias por sexo, en que la estafa más común es que no les llegó el producto que habían comprado (un 11% de alumnos de entre 11 y 14 años, un 25% de alumnos de entre 15 y 17 años y un 7% de alumnos de entre 18 y 21 años).

Gráfico 19. *Tipos de fraude en compra sufridos según la edad de la víctima*



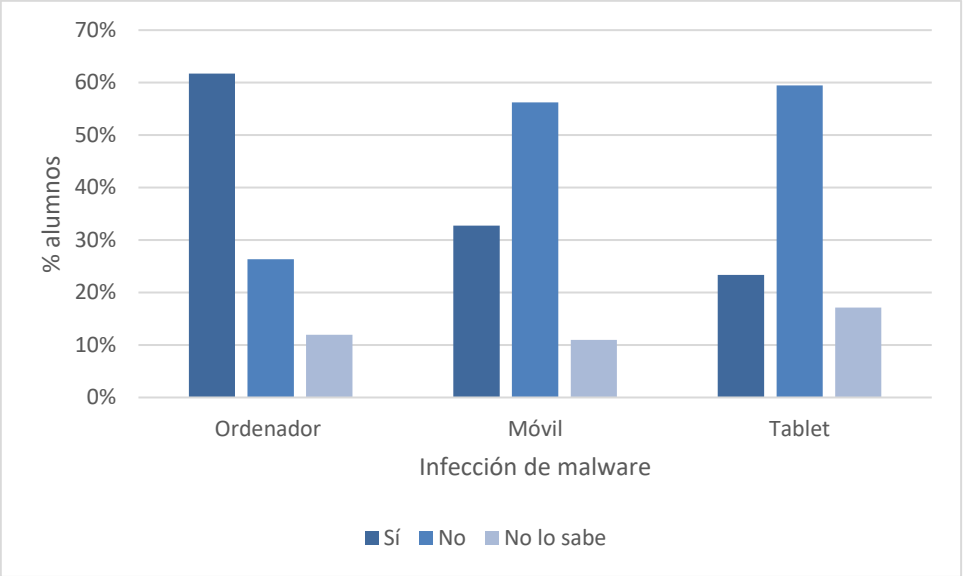
b) Infección por *malware*

Antes de analizar este tipo de estafa, conviene definir a qué hace referencia la palabra *malware*. *Malware* es todo aquel "software malicioso destinado a dañar, controlar o monitorizar un sistema informático" (Miró, 2012, p. 59). En otras palabras, es lo que se conoce comúnmente como virus informático. Existen distintos tipos de software malicioso como, por ejemplo, aquellos que se basan en controlar y capturar información del sistema o aquellos que buscan directamente su destrucción.

En este estudio, se ha preguntado a los alumnos si alguna vez el antivirus les ha avisado, tanto en el ordenador como en el móvil o la tablet, de que tenían un virus en dichos dispositivos. Para calcular los porcentajes de los alumnos que han sido víctimas de una infección por *malware* se ha tenido en cuenta el total de alumnos que tiene ordenador, el total de alumnos que tiene móvil y el total de alumnos que tiene tablet. De este modo, en el siguiente gráfico se muestra que la mayoría de alumnos que tienen ordenador han sido alertados alguna vez de la existencia de un virus (el 62% de los jóvenes), mientras que la cifra se reduce en el caso del móvil (el 33%) y más aún en el caso de la tablet (el 23%).

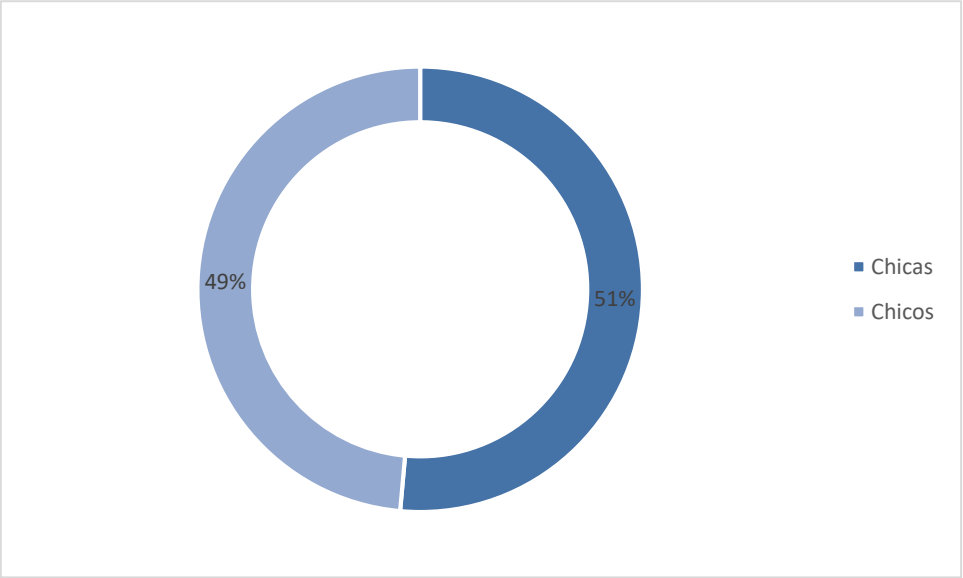
Existe un porcentaje importante de alumnos, en cualquiera de los tres dispositivos, que no sabe si alguna vez el antivirus les ha avisado de la existencia de *malware*. Ello quiere decir que existe la posibilidad de que hayan sido víctimas pero que no lo sepan, por lo que entrarían dentro de la cifra negra, esto es, la cifra de víctimas no conocidas.

Gráfico 20. *Prevalencia de alumnos víctimas de infección de malware según dispositivo*



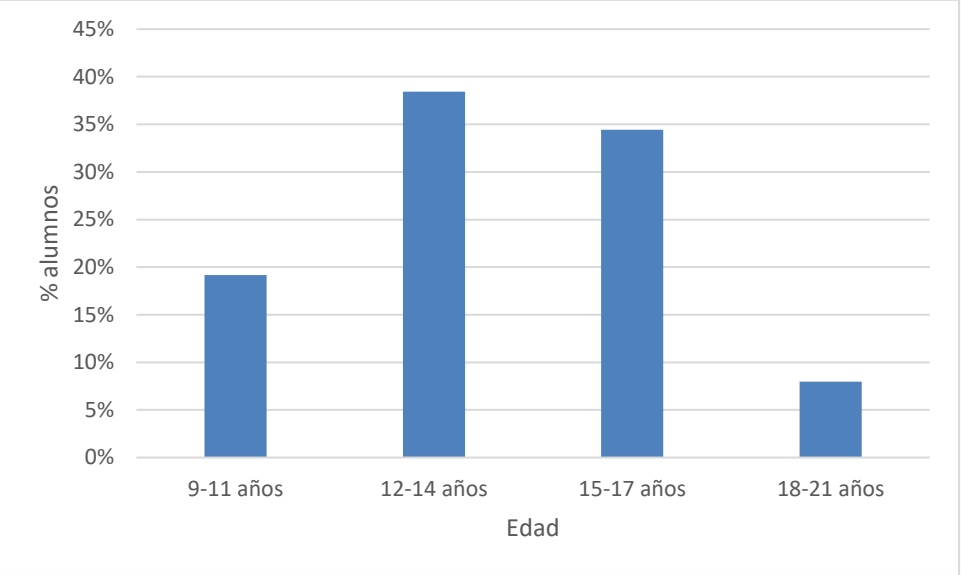
En cuanto al sexo de las víctimas de infección por *malware*, independientemente del dispositivo infectado, la diferencia entre chicos y chicas víctimas es apenas inexistente, ya que el 49% de víctimas viene representado por el sector masculino (n = 2380) y el 51% por el sector femenino (n = 2521).

Gráfico 21. *Prevalencia de alumnos víctimas de infección de malware según sexo*



En cuanto a la edad, en este tipo de ciberataque económico, los alumnos que tienen entre 9 y 11 años representan el 19% de víctimas (n = 939), mientras que los alumnos de 12 a 14 años, los alumnos de 15 a 17 años y los alumnos de 18 a 21 años representan, en este mismo orden, el 38%, el 34% y el 8% de las víctimas, respectivamente.

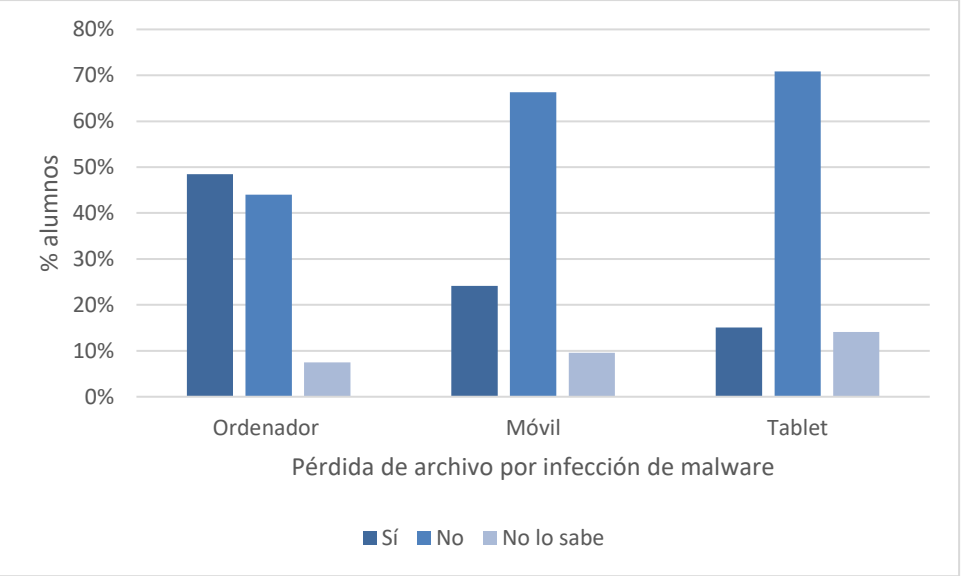
Gráfico 22. *Prevalencia de alumnos víctimas de infección de malware según edad*



c) Pérdida de archivo por infección por *malware*

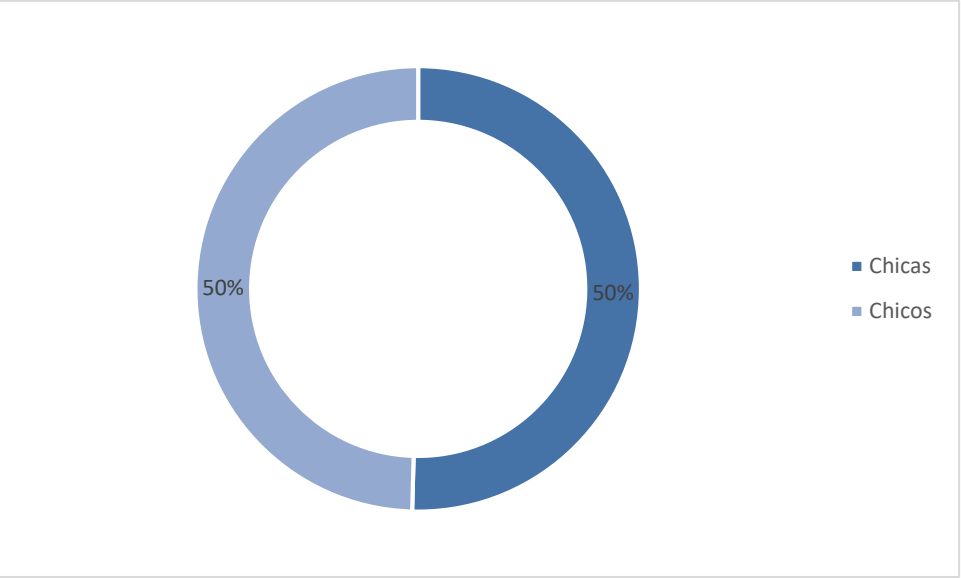
Esta tipología de ciberataque económico se relaciona con la anterior. En este caso, la infección por *malware* ha provocado un daño o pérdida en el dispositivo de la persona. De nuevo, se ha preguntado a los jóvenes si alguna vez han sido víctimas de este ataque tanto en el ordenador como en el móvil y en la tablet. En el siguiente gráfico, se observa que entre aquellos alumnos que tienen ordenador, prácticamente la mayoría (el 48% de los alumnos) afirma haber perdido información o sufrido daños derivados de un virus informático. El porcentaje en el caso del móvil es muy similar (el 44%), mientras que entre los usuarios de la tablet una gran mayoría, más concretamente el 74% de los jóvenes, afirma no haber sufrido este tipo de daño.

Gráfico 23. *Prevalencia de alumnos víctimas de pérdida de información por infección de malware según dispositivo*



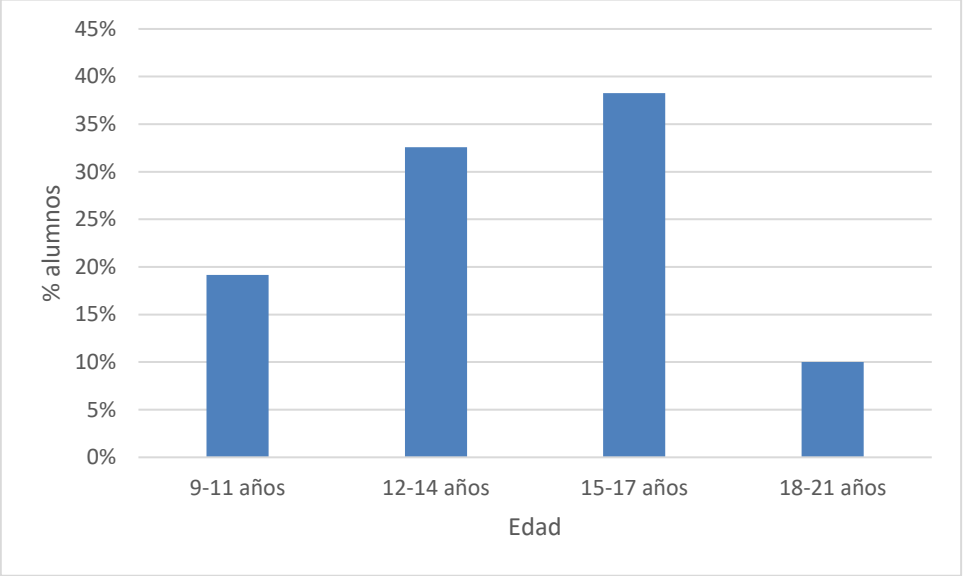
En relación al sexo, en la pérdida de información por infección por *malware* prácticamente no hay diferencias entre chicos y chicas, ya que ambos grupos representan un 50% de las víctimas (hay 700 chicas víctimas y 688 chicos víctimas).

Gráfico 24. *Prevalencia de alumnos víctimas de pérdida de información por infección de malware según sexo*



En cuanto a la edad de las víctimas, cabe destacar que el 19% tiene entre 9 y 11 años (n = 266), el 33% tiene entre 12 y 14 años (n = 452), el 38% tiene entre 15 y 17 años y el 10% restante tiene entre 18 y 21 años.

Gráfico 25. *Prevalencia de alumnos víctimas de pérdida de información por infección de malware según edad*

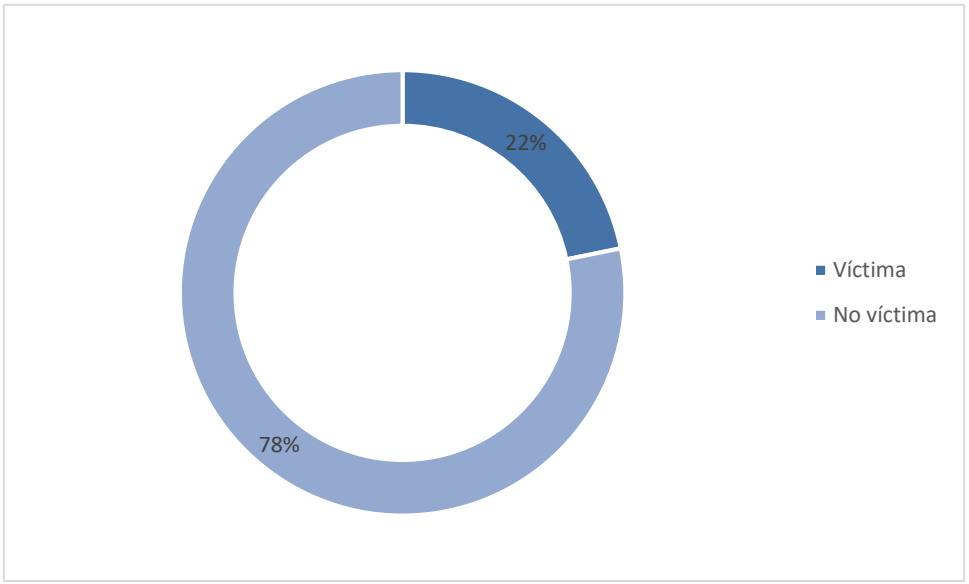


d) *Scam*

El *scam* es un tipo de ciberataque que "podría englobar casi todos los fraudes en el ciberespacio, si bien se suele utilizar como referencia de los más burdos de ellos, aquellos en los que el engaño es poco elaborado y en los que el error de la víctima puede ir más allá de lo común" (Miró, 2012, p. 307).

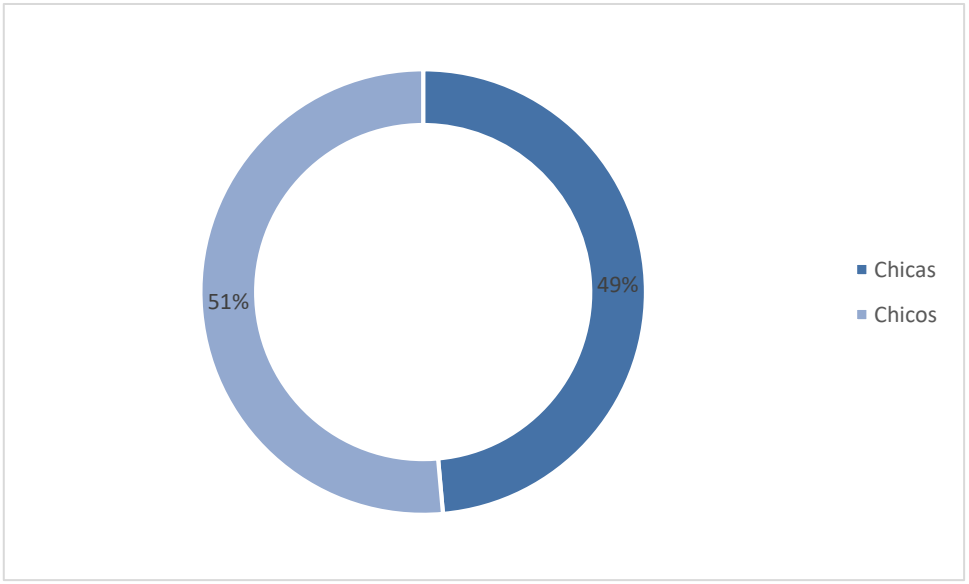
En este estudio, el *scam* se ha medido preguntando si en el último año los alumnos habían recibido algún correo, WhatsApp o mensaje privado informándoles de que habían ganado un premio que sospechaban que era falso. Ante esta pregunta, el 22% (n = 1587) ha contestado afirmativamente, frente al 78% (n = 5695) que no ha recibido ningún correo de estas características.

Gráfico 26. *Prevalencia de alumnos víctimas de scam en el último año*



Del 22% de alumnos que ha afirmado haber sido víctima de *scam*, y sin apenas diferencias entre sexos, el 51% viene representado por los chicos (n = 816) y el 49% restante por las chicas (n = 771).

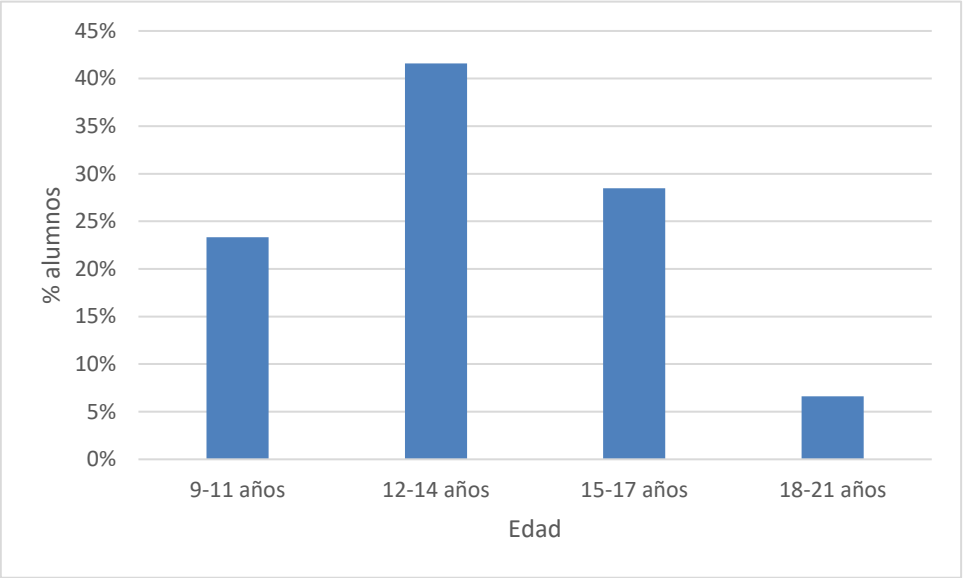
Gráfico 27. *Prevalencia de alumnos víctimas de scam en el último año según sexo*



En cuanto a la distribución de las víctimas en función de su edad, el 23% tiene

entre 9 y 11 años (n = 370), el 42% tiene entre 12 y 14 años (n = 660), el 28% tiene entre 15 y 17 años (n = 452) y el 7% restante tiene entre 18 y 21 años (n = 105).

Gráfico 28. *Prevalencia de alumnos víctimas de scam en el último año según edad*

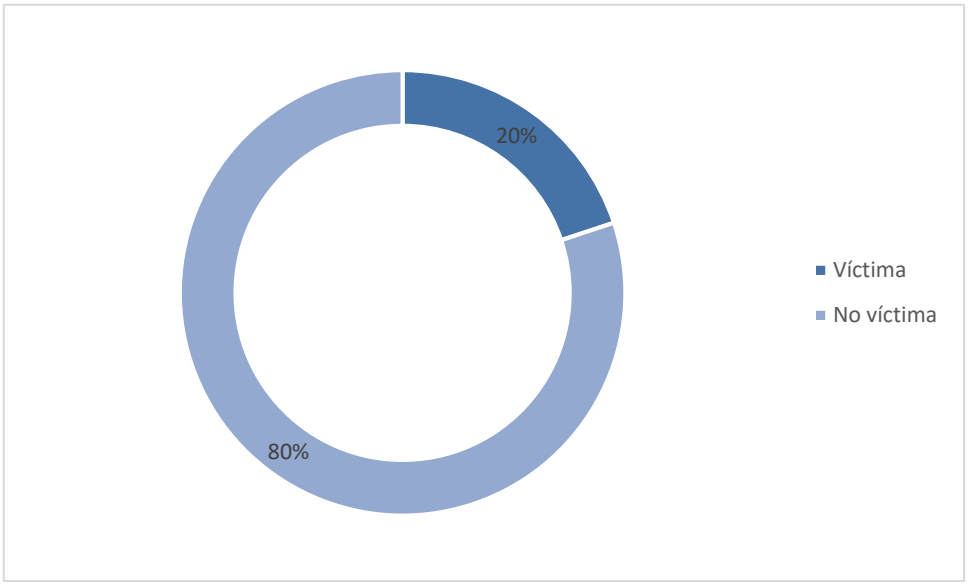


e) *Spam*

El *spam* es, en palabras de Miró (2012), un "e-*mail* no solicitado que suele enviarse a un numeroso número de direcciones electrónicas bien a través de una dirección electrónica (…) o bien a través de un sistema informático infectado" (p. 308).

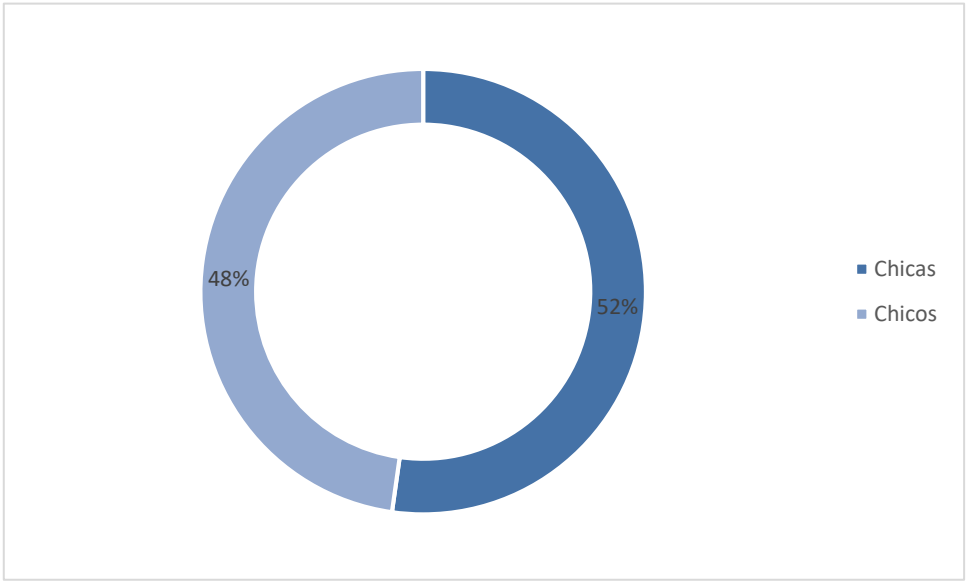
En este estudio el *spam* se ha medido preguntando a los alumnos si en el último año habían recibido algún correo, WhatsApp o mensaje privado de alguien cuya identidad sospechaban que era falsa. Como respuesta, el 20% de ellos (n = 1449) ha contestado afirmativamente, frente al 80% (n = 5833) que no ha recibido ningún correo de estas características. La prevalencia de víctimas es, por tanto, prácticamente igual a la del *scam*, tal y como se puede observar en el siguiente gráfico.

Gráfico 29. *Prevalencia de alumnos víctimas de spam en el último año*



En este último tipo de ciberataque económico tampoco hay apenas diferencias según el sexo de las víctimas, ya que el 48% son chicos (n = 692) y el 52% son chicas (n = 757).

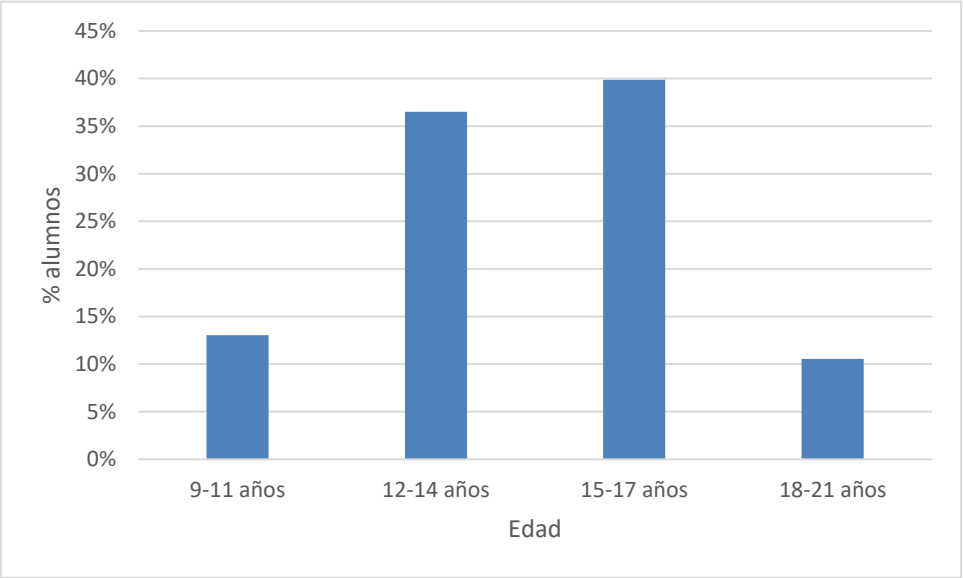
Gráfico 30. *Prevalencia de alumnos víctimas de spam en el último año según sexo*



En cuanto a la edad de las víctimas, cabe mencionar que el 13% está compuesto

por alumnos entre 9 y 11 años (n = 189), el 37% por alumnos de 12 a 14 años (n = 529), el 40% por alumnos de 15 a 17 años (n = 578) y el 11% restante por alumnos entre 18 y 21 años (n = 153).

Gráfico 31. *Prevalencia de alumnos víctimas de spam en el último año según edad*



4.2.2 Ciberataques sociales

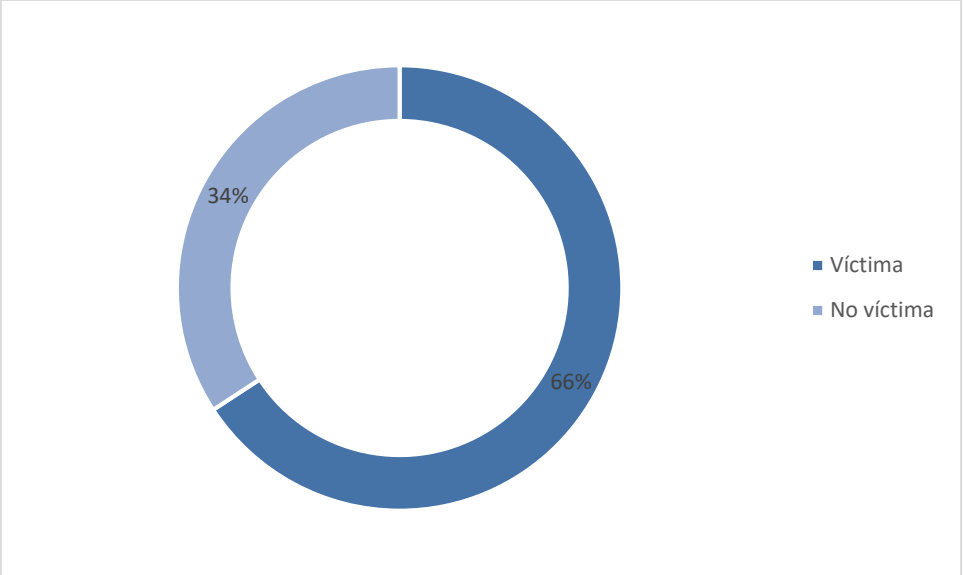
Tomando como referencia, de nuevo, a Miró (2012), el cibercrimen social puede entenderse como aquel "grupo de delitos en Internet que tienen que ver con las relaciones sociales entre las personas y que no son más que trasposición al ciberespacio de los crímenes tradicionales derivados de conflictos entre personas" (p. 301). Para la realización de este estudio se han analizado tres tipos concretos de ciberataques sociales: 1) el ciberacoso, 2) el ciberacoso sexual o *cybergrooming* y 3) el control de pareja a través de las TIC e Internet.

A lo largo de los siguientes apartados se analizarán, específicamente, cada una de las tres conductas que se incluyen dentro del cibercrimen social, incluyendo en cada una de ellas los subtipos que las conforman. Sin embargo, antes se presentan los datos globales de cibervictimización social entre los alumnos de

Castilla y León. Conviene aclarar que, debido a la adaptación del cuestionario a los alumnos de 5º y 6º de primaria y 1º de ESO, la variable global de cibervictimización social solamente se ha creado con la información aportada por los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, ya que a los alumnos más pequeños no se les ha preguntado por el ciberacoso sexual ni por el control de pareja.

Como se puede observar en el siguiente gráfico, el 66% de alumnos (n = 2848) ha sido víctima de algún ataque social, mientras que el 34% restante (n = 1481) niega haber sufrido ciberacoso, ciberacoso sexual o control de pareja.

Gráfico 32. *Prevalencia de alumnos víctimas de algún tipo de ciberataque social*



a) Ciberacoso

A nivel conceptual se puede distinguir entre dos tipos de ciberacoso. El primero de ellos es el *cyberstalking* o ciberacoso propiamente dicho, que consiste en un "ciberacoso continuado a una persona, consistente en el seguimiento, hostigamiento y persecución de la víctima por medio del uso de Internet. También se define como *cyberstalking,* en un sentido más amplio, la utilización

de Internet para realizar uno o más actos de amenazas, insultos, uso indebido de la imagen, solicitud sexual o cualquier otra forma de hostigamiento a una persona" (Miró, 2012, p. 302-303).

El segundo se relaciona con el ámbito escolar y es el conocido como *cyberbullying*, que es aquel "ciberacoso escolar o a menores, esto es, variante del ciberacoso en la que un menor, atormenta, amenaza, hostiga, humilla, o molesta de alguna otra manera a otro, haciendo uso de Internet, teléfono móvil, videoconsola o alguna otra tecnología telemática de comunicación" (Miró, 2012, p. 302). Además, rescatando la definición de Olweus (1978), este tipo de ciberacoso debe ser repetido en el tiempo y realizado por algún compañero de la escuela.

Para este estudio se han analizado ambas tipologías de ciberacoso, aunque conviene hacer algunas aclaraciones al respecto. En primer lugar, el *cyberstalking*, que a lo largo del estudio recibirá el nombre de ciberacoso, se ha medido a partir de diez conductas distintas sufridas por los alumnos de la Comunidad Autónoma de Castilla y León, las cuales se exponen en el siguiente listado:

1. Insultos o ridiculizaciones repetidas en el tiempo a través de Internet
2. Rumores o mentiras repetidas en el tiempo a través de Internet
3. Publicar fotos o vídeos de carácter íntimo o privado (no sexuales) sin consentimiento
4. Difundir información secreta o privada sin consentimiento[12]

[12] Esta tipología solo se ha tenido en cuenta entre los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM. Ello significa que para evaluar el ciberacoso entre los alumnos de 5º y 6º de primaria y 1º

5. Acceder al contenido del correo electrónico, WhatsApp, Instagram, etc. sin consentimiento
6. Utilizar Internet para excluir o marginar de manera continuada
7. Amenazar a través de Internet
8. Obligar al alumno a hacer algo que no quería a través de Internet
9. Hacerse pasar por el alumno a través de Internet para dañarle
10. Contactar repetidamente con el alumno tras haber pedido que no lo hiciera

Por su parte, el *cyberbullying* o ciberacoso escolar se ha medido teniendo en cuenta únicamente tres de las conductas incluidas en el ciberacoso con la condición de que hayan sido realizadas por los compañeros de colegio de los encuestados. Estas tres conductas son: 1) Recibir insultos o ridiculizaciones repetidas en el tiempo a través de Internet, 2) Ser objeto de rumores o mentiras repetidas en el tiempo a través de Internet y 3) Ser excluido o marginado de manera continuada a través de Internet. Se han escogido estas tres conductas porque, en relación a la definición de Olweus (1978) sobre el *bullying* tradicional, son las únicas de las aquí analizadas que se repiten en el tiempo y que pueden haber sido cometidas por compañeros del colegio/instituto.

Cabe destacar que la razón principal por la que no se ha preguntado directamente a los alumnos si han sido víctimas de *cyberbullying* y, en su lugar, se ha decidido extraer esta información a partir de las conductas del ciberacoso general, radica en que existen dificultades a la hora de preguntar directamente

de ESO se han tenido en cuenta 9 tipologías de ciberacoso, mientras que para el resto de alumnos se han tenido en cuenta 10.

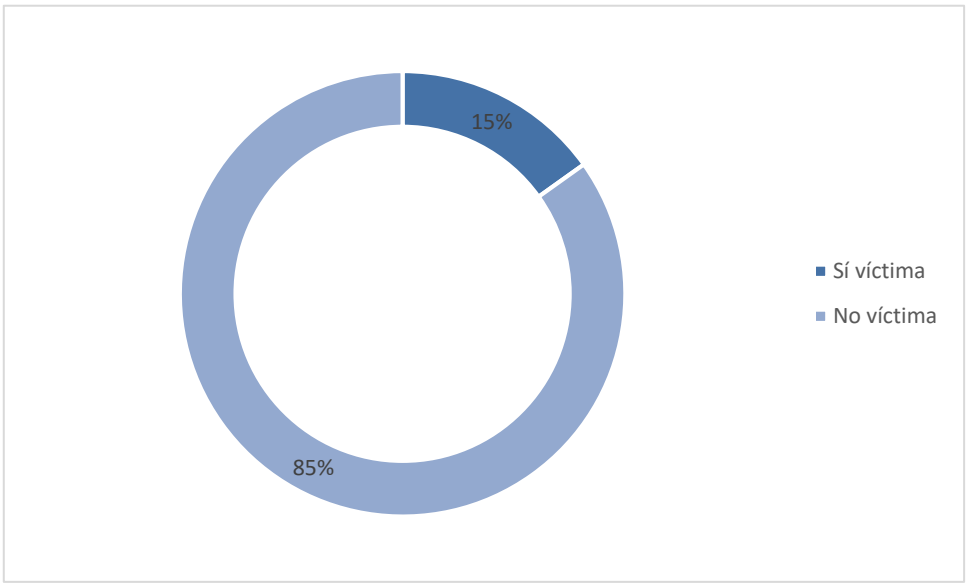
por este fenómeno, ya que muchas veces los propios jóvenes no son conscientes de que están sufriendo este tipo de ataque.

En los siguientes dos apartados se presentan las prevalencias de *cyberbullying* y ciberacoso (o *cyberstalking*) de los alumnos de enseñanza no universitaria de la comunidad Autónoma de Castilla y León que han sido objeto de este estudio.

1. *Cyberbullying*

A modo general, puede afirmarse que 1.102 alumnos de los 7.282 encuestados, es decir, un 15% de los mismos, ha sido víctima de *cyberbullying* en el último año. Concretamente, la prevalencia de este fenómeno entre los alumnos de 5º y 6º de primaria y 1º de ESO es de un 14% (410 alumnos de 1.953), mientras que entre los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM la cifra asciende a un 16% (692 alumnos de 4.329). Como se desprende de los datos, las tres prevalencias son prácticamente idénticas.

Gráfico 33. *Prevalencia total de alumnos víctimas de cyberbullying*

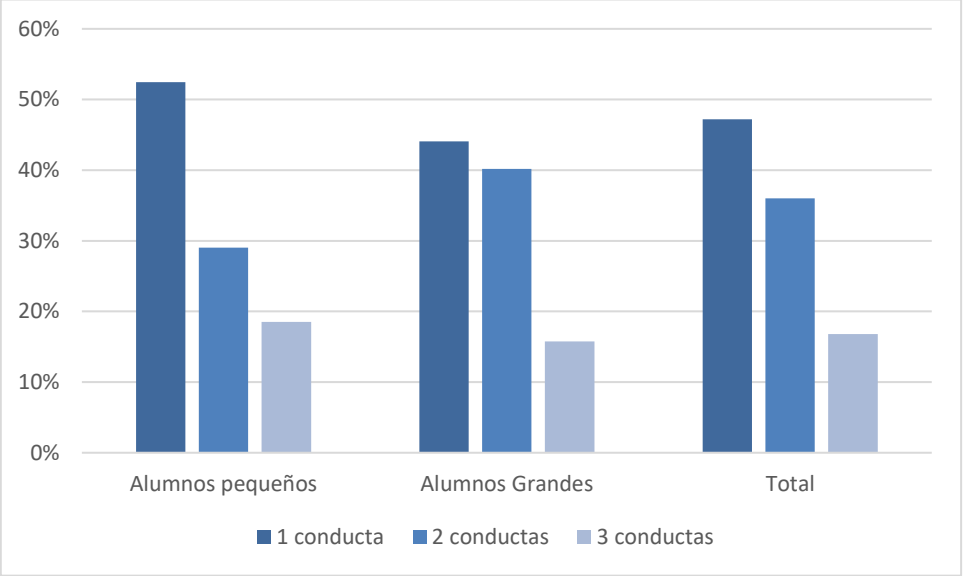


Como bien se ha comentado anteriormente, en este estudio el *cyberbullying* se ha medido a partir de 3 conductas -insultos, rumores y exclusión social-. A

continuación, se presenta la prevalencia de alumnos que ha sufrido únicamente una de estas conductas, el porcentaje de aquellos han sufrido hasta 2 y el porcentaje de aquellos que han sufrido las 3. Como se observa, lo más común es que los alumnos hayan sufrido una única conducta (casi la mitad afirma este dato, esto es, 520 alumnos). Por otro lado, más de un 35% de las víctimas afirma que ha sufrido hasta 2 de estas conductas (n = 397), mientras que 17% afirma haber sufrido las tres (n = 185).

Si se diferencia entre los alumnos de primaria y 1º de ESO y los del resto de la ESO, Bachillerato y CFGM, se observa que entre los más pequeños es más común haber sufrido una única conducta, mientras que entre los más grandes no existe una diferencia muy grande entre haber sufrido una o dos conductas.

Gráfico 34. *Número de conductas de cyberbullying sufridas por los alumnos*



2. *Cyberstalking*

Desde una perspectiva generalizada del ciberacoso, y diferenciando entre aquellos alumnos de menor edad (5º y 6º de Primaria y 1º de ESO) y aquellos de mayor edad (2º, 3º y 4º de ESO, Bachillerato y CFGM), cabe destacar que en el

primero de los grupos el 35% de jóvenes afirma haber sido víctima de ciberacoso (n = 1039), mientras que en el segundo grupo la cifra asciende a un 53% (n = 2313).

Gráfico 35. *Prevalencia de alumnos de 5º y 6º de Primaria y 1º de ESO víctimas de ciberacoso*

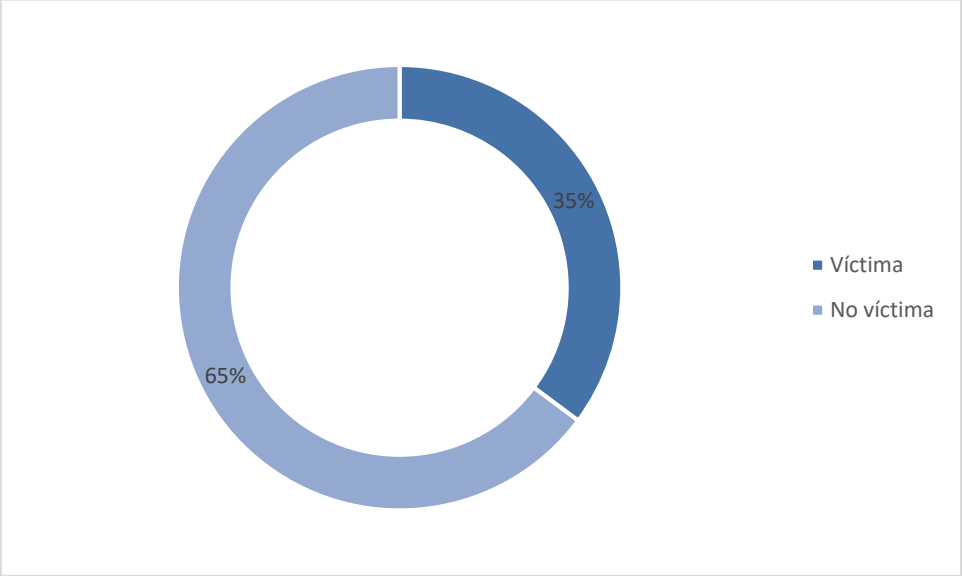
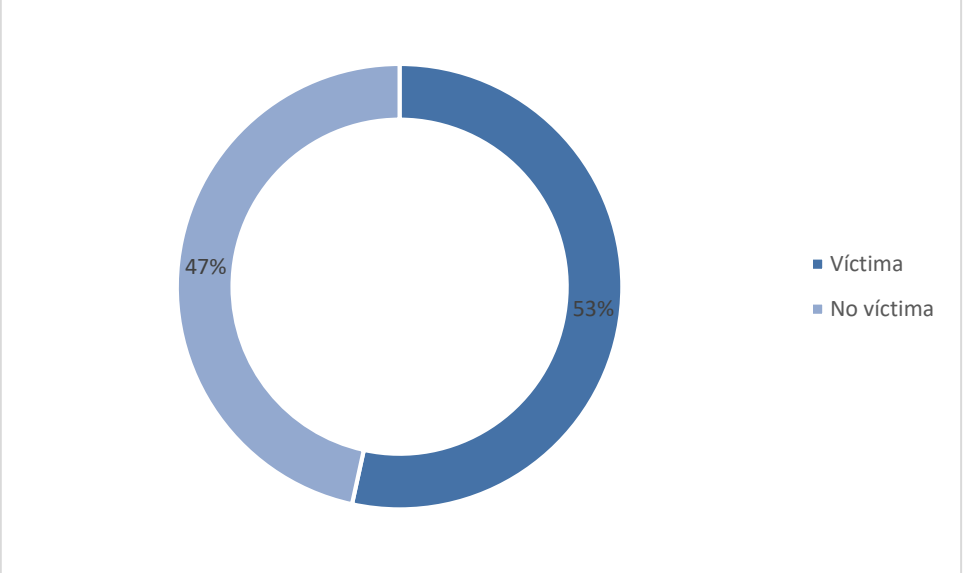


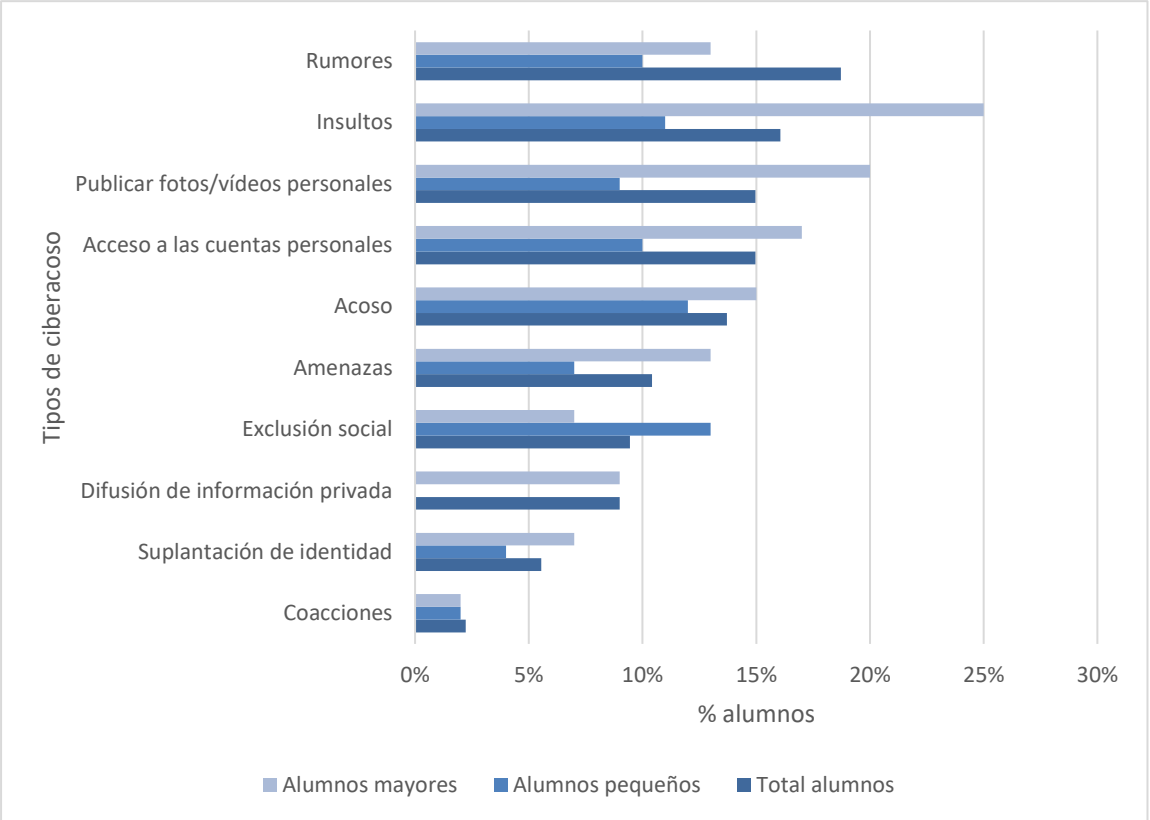
Gráfico 36. *Prevalencia de alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM víctimas de ciberacoso*



En el siguiente gráfico se muestra la prevalencia de los distintos tipos de

ciberacoso sufridos por los alumnos, así como una prevalencia específica entre los alumnos de 5º y 6º de primaria y 1º de ESO y otra para el resto de alumnos de ESO, Bachillerato y CFGM. En el caso del primer grupo, el tipo más frecuente de ciberacoso es la exclusión social (un 13% de los alumnos), es decir, marginar al menor a través de Internet, seguido del acoso (un 12%) y los insultos (un 11%). En el segundo grupo, las prevalencias son algo distintas, ya que la tipología más frecuente son los insultos (un 25% de alumnos), seguida de la publicación de fotos y vídeos personales (un 20%) y el acceso a las cuentas personales sin consentimiento (un 17%).

Gráfico 37. *Prevalencias de las distintas tipologías de ciberacoso*

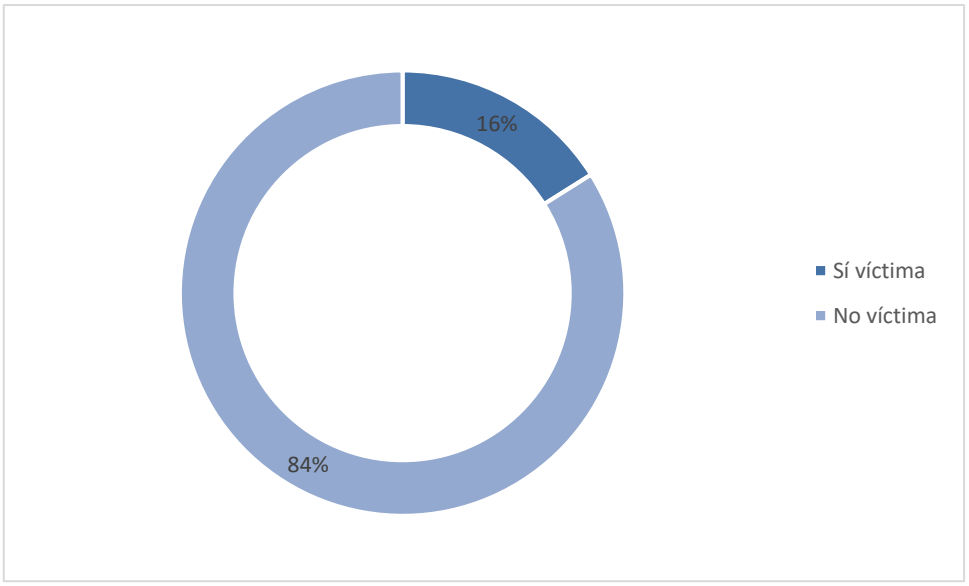


A continuación, se analiza en mayor profundidad cada conducta de ciberacoso para ver cómo afecta cada una de ellas al conjunto de los jóvenes de Castilla y León.

1. Insultos

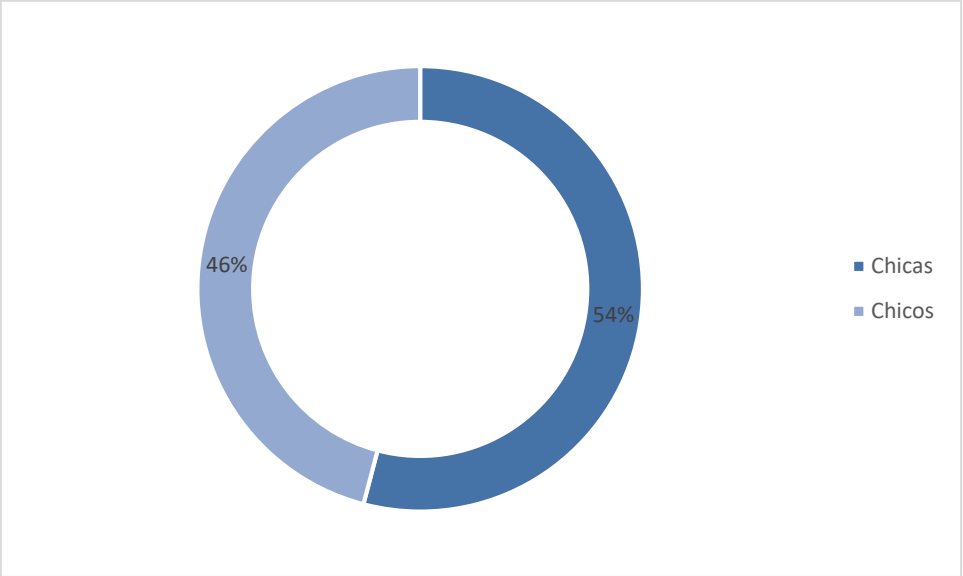
El 16% (n = 1170) de alumnos encuestados afirma haber sido víctima de insultos o ridiculizaciones repetidas a través de Internet o del móvil en algún momento de sus vidas. Más concretamente, la prevalencia de víctimas de insultos o ridiculizaciones entre los alumnos más pequeños (5º y 6º de primaria y 1º de ESO) es del 11% (n = 326), mientras que la cifra asciende al 25% de alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM (n = 844).

Gráfico 38. *Prevalencia de alumnos víctimas de insultos a través de Internet*



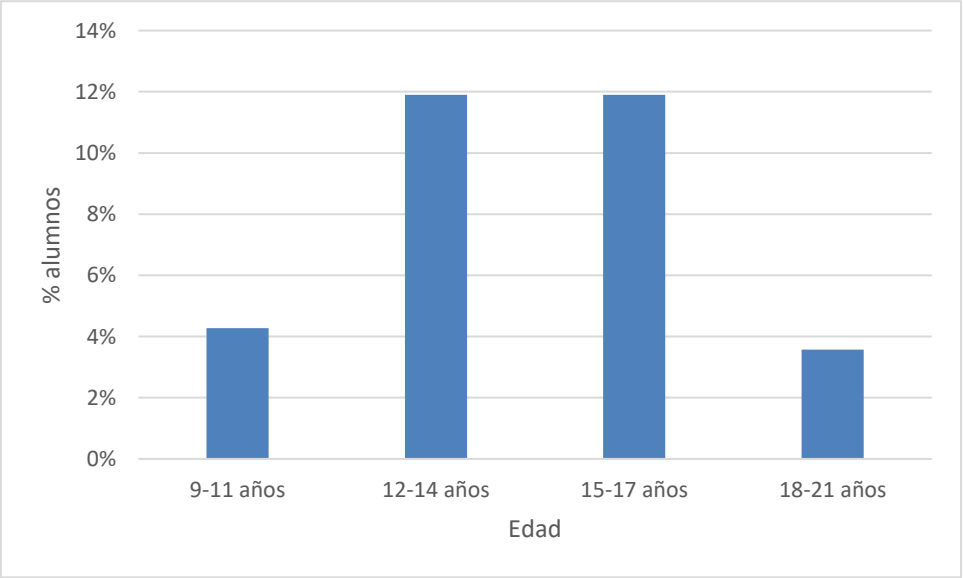
Del 16% de jóvenes que sí ha recibido insultos o ha sido objeto de ridiculizaciones, el 46% son chicos (n = 537), mientras que el 54% son chicas (n = 633). Se observa, por tanto, un mayor porcentaje de chicas víctimas en comparación con los chicos.

Gráfico 39. *Prevalencia de alumnos víctimas de insultos a través de Internet según sexo*



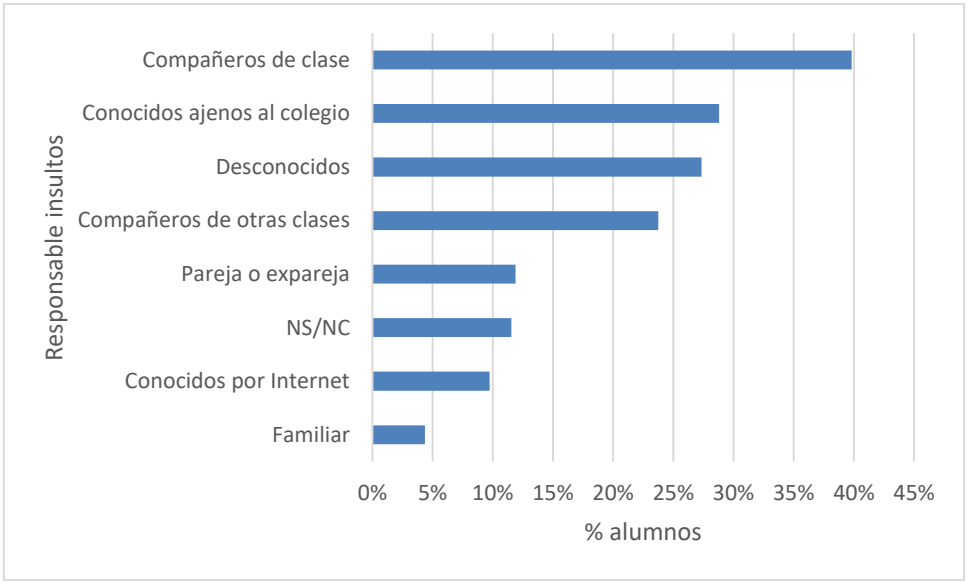
La distribución de las víctimas según su edad es la siguiente: el 4% de los alumnos tiene entre 9 y 11 años (n = 158), el 12% tiene entre 12 y 14 años (n = 440), otro 12% tiene entre 15 y 17 años (n = 440) y el 4% restante tiene entre 18 y 21 años (n = 132).

Gráfico 40. *Prevalencia de alumnos víctimas de insultos a través de Internet según edad*



En cuanto a los responsables de los insultos, y teniendo en cuenta a todos los alumnos en su conjunto, tanto los más pequeños como los más grandes, se observa que observa que un 40% afirma que los responsables fueron compañeros de clase, seguido de un 29% que afirma que los responsables fueron conocidos ajenos al colegio.

Gráfico 41. *Responsables de los insultos según las víctimas*



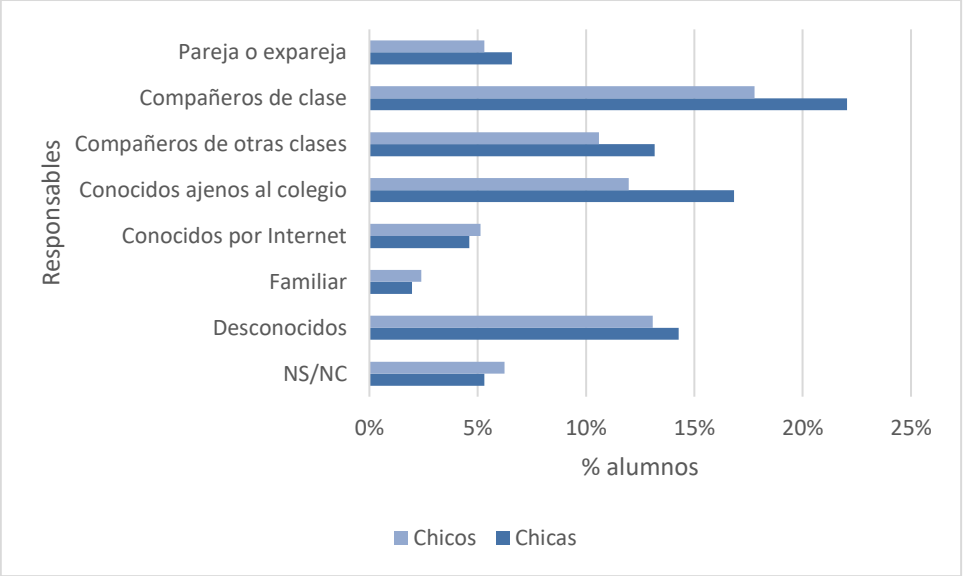
Entre las chicas, el principal responsable de los insultos es uno o varios compañeros de clase (un 22%), al igual que sucede entre los chicos (un 18%). En otras palabras, tanto chicos como chicas coinciden en afirmar que los principales responsables de los insultos fueron uno o varios compañeros de clase.

La segunda categoría con más consenso entre las chicas es la de conocidos ajenos al colegio, ya que un 17% ha afirmado que este tipo de personas fue quien las insultó. Entre los chicos, en cambio, la segunda categoría con mayor consenso es la de personas desconocidas (un 13% de los casos).

Finalmente, tanto chicos como chicas coinciden en afirmar que lo menos común es que un familiar sea el responsable de los insultos, con un 2% de alumnos

haciendo esta afirmación en ambos casos.

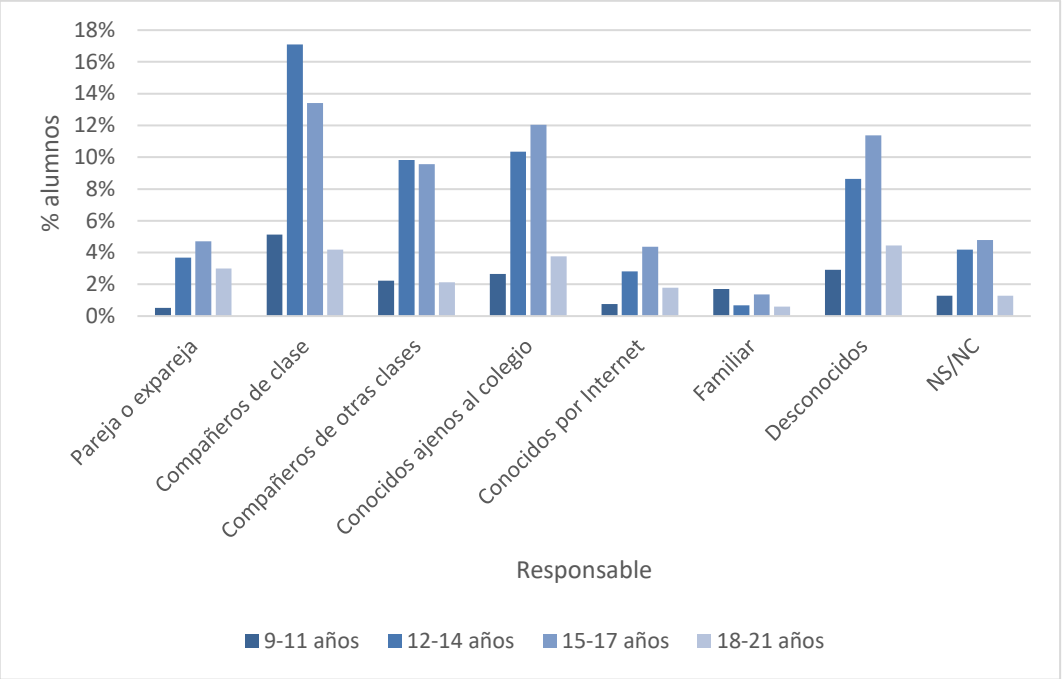
Gráfico 42. *Responsables de los insultos según el sexo de la víctima*



En cuanto a los responsables de los insultos según la edad de las víctimas, cabe destacar que, en todas las franjas de edad, los alumnos afirman que los principales responsables de este tipo de ciberacoso fueron uno o varios compañeros de la propia clase. Más concretamente, un 5% de alumnos entre 9 y 11 años, un 17% de alumnos entre 12 y 14 años, un 13% de alumnos entre 15 y 17 años y un 4% de alumnos de entre 18 y 21 años hacen esta afirmación. Concretando en la franja de edad de 18 a 21 años, cabe destacar que el mismo porcentaje de alumnos (un 4%) ha afirmado que los principales responsables también fueron conocidos ajenos al colegio y personas desconocidas.

Al igual que sucede en el caso del sexo, una de las categorías de responsables que presenta más consenso entre los alumnos, en casi todas las franjas de edad, a la hora de afirmar que es de las personas que menos ha insultado, es la de familiar, tal y como se observa en el siguiente gráfico.

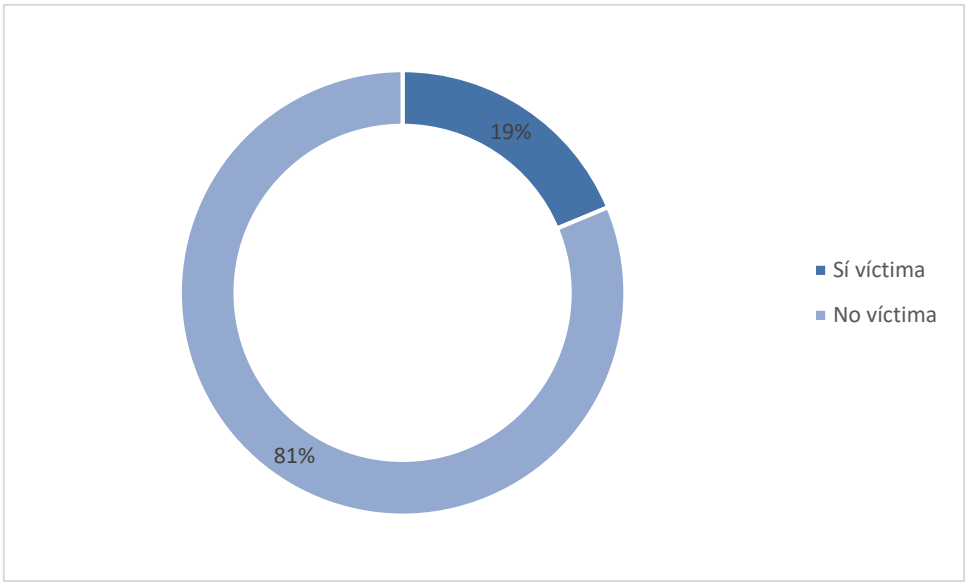
Gráfico 43. *Responsables de los insultos según la edad de la víctima*



2. Rumores

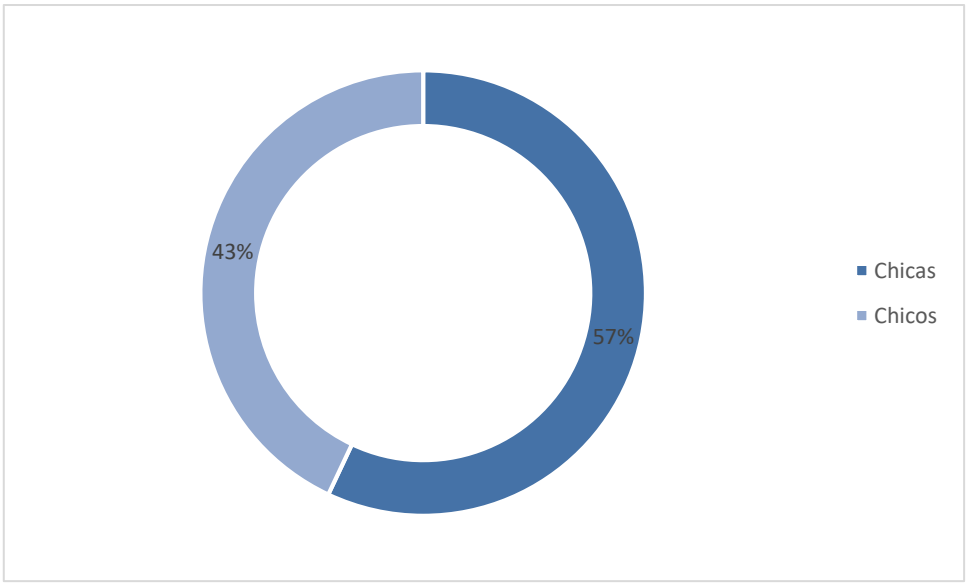
En la tipología de rumores o mentiras la prevalencia de víctimas es ligeramente mayor que en el caso de los insultos, siendo la cifra de alumnos víctimas de un 19% (n = 1363). En el caso de los pequeños, la prevalencia se encuentra en casi un 10% (n = 288), mientras que en el caso de los alumnos de mayor edad la prevalencia asciende a casi un 20% (n = 1075).

Gráfico 44. *Prevalencia de alumnos víctimas de rumores a través de Internet*



Del 19% de los alumnos que ha afirmado haber sido víctima de rumores o mentiras, el 57% son chicas (n = 777) y el 43% son chicos (n = 586).

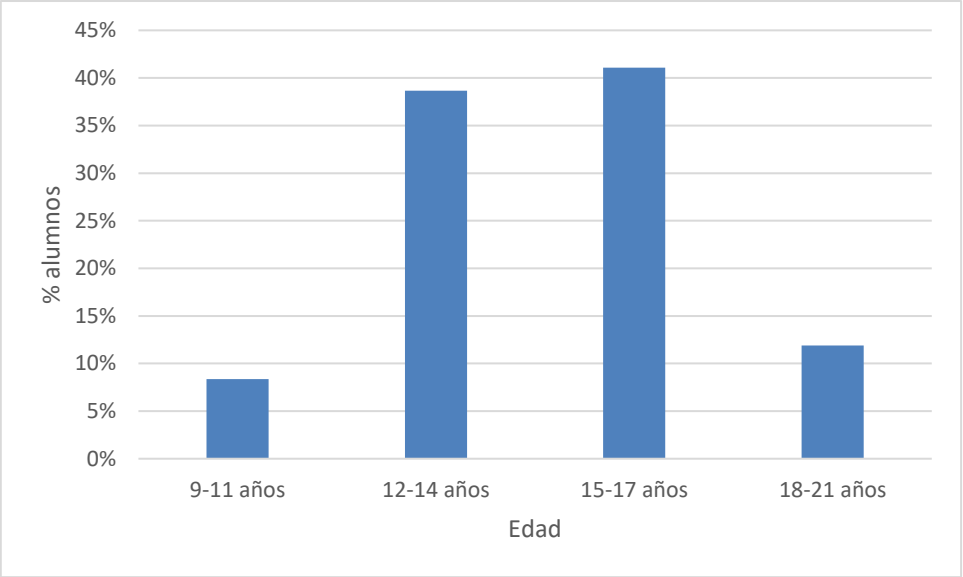
Gráfico 45. *Prevalencia de alumnos víctimas de rumores a través de Internet según sexo*



En cuanto a la distribución de las víctimas de rumores según su edad, se observa que el 8% tiene entre 9 y 11 años (n = 114), el 39% tiene entre 12 y 14 años (n =

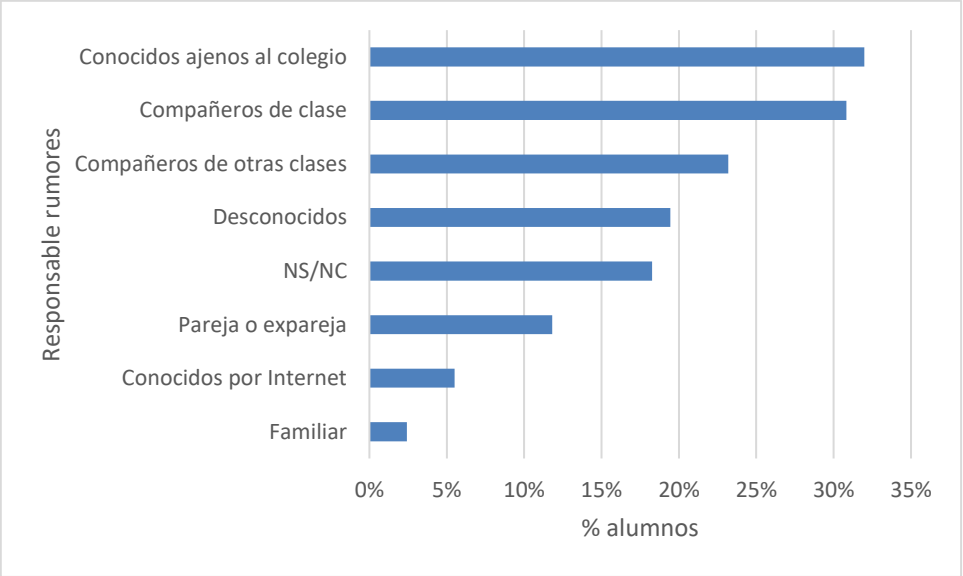
527), el 41% tiene entre 15 y 17 años (n = 560) y el 12% restante tiene entre 18 y 21 años (n = 162).

Gráfico 46. *Prevalencia de alumnos víctimas de rumores a través de Internet según edad*



En cuanto a los responsables de los rumores, un 32% de los alumnos afirma que fueron personas conocidas ajenas al colegio, seguido de un 31% y un 23% que informa de que fueron compañeros de clase y de otras clases, respectivamente. En el caso de los más pequeños las prevalencias de los autores de los rumores son un tanto distintas, ya que un 40% afirma que los responsables fueron compañeros de clase.

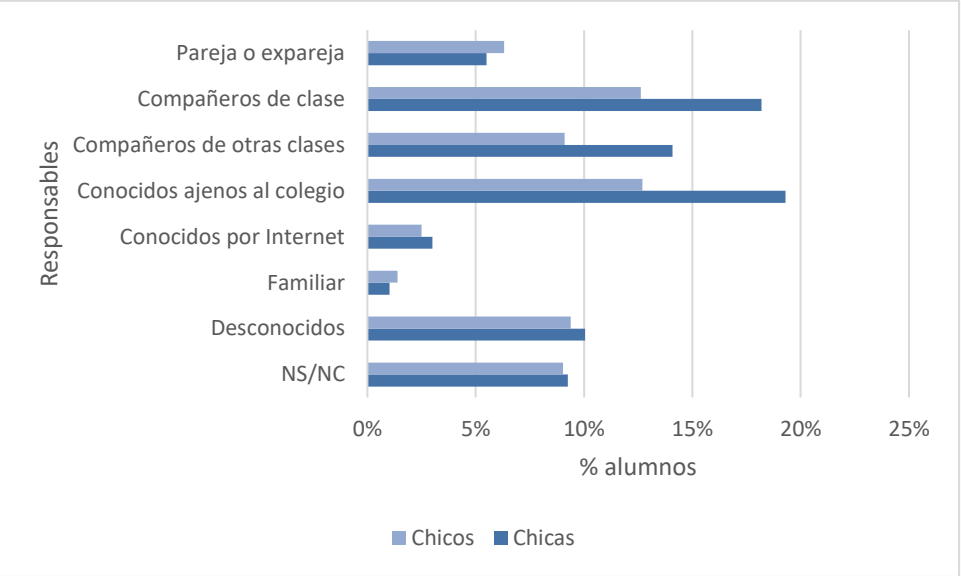
Gráfico 47. *Responsables de los rumores según las víctimas*



En función del sexo, cabe destacar que tanto chicas como chicos consideran que los principales responsables de rumorear son personas conocidas ajenas al colegio, con una prevalencia de un 19% y 13% en cada caso. Asimismo, un 13% de los chicos también considera que los principales responsables son compañeros de clase.

Los compañeros de clase son, para un 18% de las chicas, el segundo tipo de responsables más comunes en este tipo de ciberacoso, porcentaje muy similar al de la categoría de personas conocidas ajenas al colegio. Cabe destacar, también, que tanto chicos como chicas coinciden en que los familiares son los menos responsables, con una prevalencia de un 1% en ambos sexos.

Gráfico 48. *Responsables de los rumores según el sexo de la víctima*

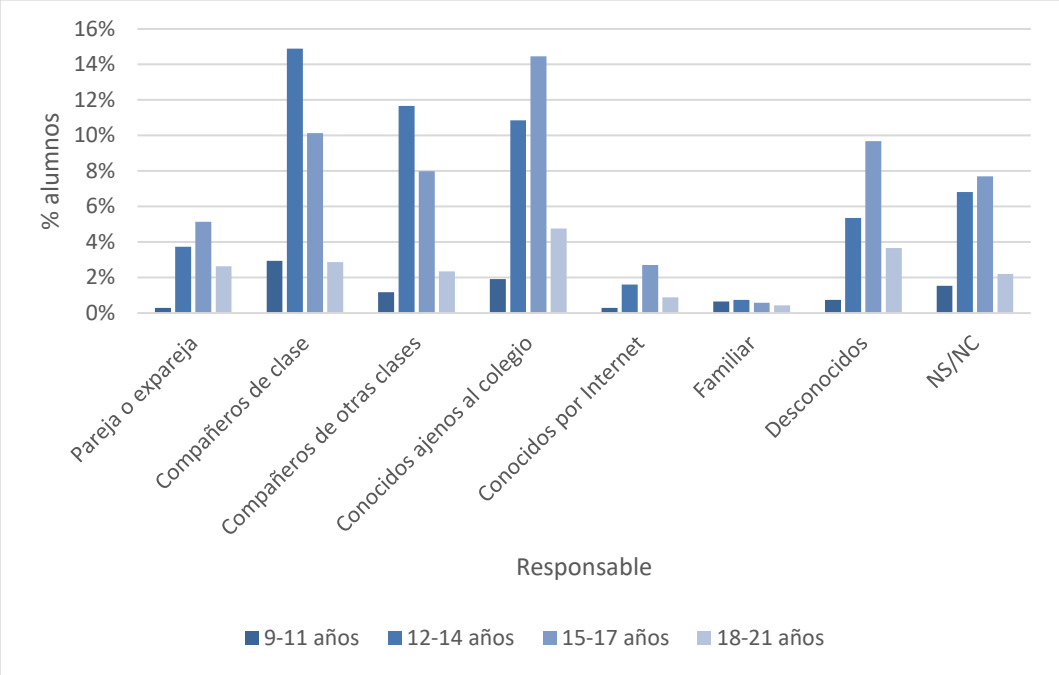


En cuanto a la distribución de los responsables según la edad de las víctimas, se destacan varios puntos. Primero, la franja de edad de entre 9 y 11 años y la franja de edad de entre 12 y 14 años coinciden, en un 3% y un 15% de los casos, respectivamente, en que el principal responsable de los rumores fue uno o varios compañeros de clase. Las otras dos franjas restantes, la de 15 a 17 años y la de 18 a 21 años, coinciden, en un 14% y un 5% de los casos, respectivamente, en que los principales responsables fueron conocidos ajenos al colegio.

Segundo, las siguientes categorías de responsable más comunes entre los alumnos entre 11 y 14 años son la de conocidos ajenos al colegio y la de "No sabe / No contesta" (un 2% de alumnos en ambos casos). Entre los alumnos que tienen entre 12 y 14 años, la siguiente categoría más común es la de compañeros de otras clases (un 12%), mientras que los que tienen entre 15 y 17 años afirman que la segunda categoría más común es la de compañeros de clase, así como la de personas desconocidas (un 10% en ambos casos). Finalmente, entre los alumnos que tienen más de 18 años, la segunda categoría con más consenso es la de personas desconocidas (un 4%).

Por último, cabe destacar que, al igual que en el caso de los insultos, casi todas las franjas de edad coinciden en afirmar que la categoría de responsable menos común corresponde es la de los familiares.

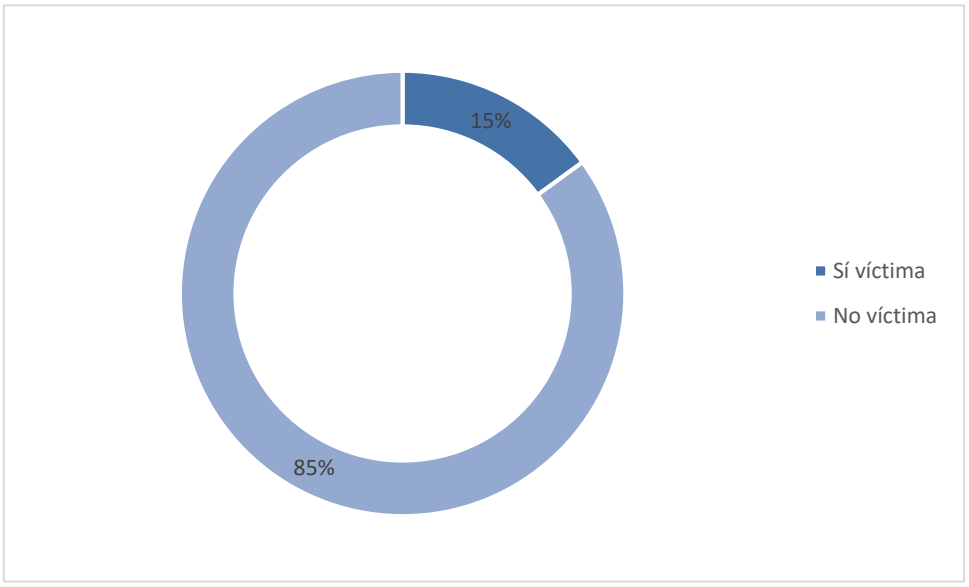
Gráfico 49. *Responsables de los rumores según la edad de la víctima*



3. Publicación de fotos o vídeos sin consentimiento

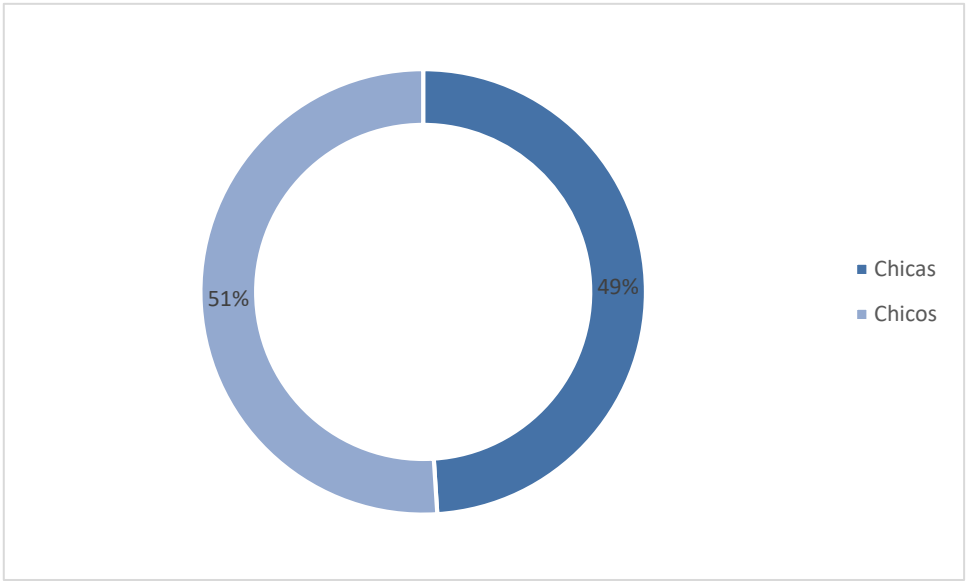
En la línea de las dos tipologías anteriores, la prevalencia global de publicar fotos o vídeos sin consentimiento se encuentra en un 15% (n = 1090). En el caso de los pequeños, la prevalencia se encuentra en un 8,6% (n = 253), mientras que en el caso de los alumnos de mayor edad la prevalencia asciende a un 19,3% (n = 837).

Gráfico 50. *Prevalencia de alumnos víctimas de publicación de fotos o vídeos suyos sin consentimiento a través de Internet*



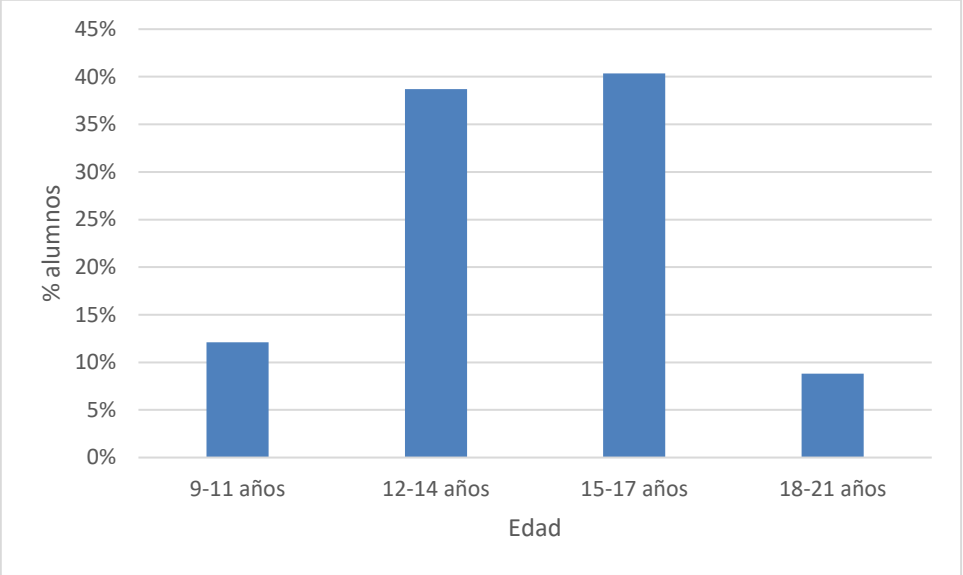
Con apenas diferencias entre chicos y chicas, el 51% de los 1090 alumnos que ha afirmado que alguien ha publicado sus fotos o vídeos privados sin su consentimiento son chicos (n = 556), siendo el 49% chicas (n = 534).

Gráfico 51. *Prevalencia de alumnos víctimas de publicación de fotos o vídeos suyos sin consentimiento a través de Internet según sexo*



En cuanto a la distribución por edad de las víctimas de este tipo de ciberacoso, se observa que el 12% tiene entre 9 y 11 años (n = 132), el 39% tiene entre 12 y 14 años (n = 422), el 40% tiene entre 15 y 17 años (n = 440) y el 9% restante tiene entre 18 y 21 años (n = 96).

Gráfico 52. *Prevalencia de alumnos víctimas de publicación de fotos o vídeos suyos sin consentimiento a través de Internet según edad*

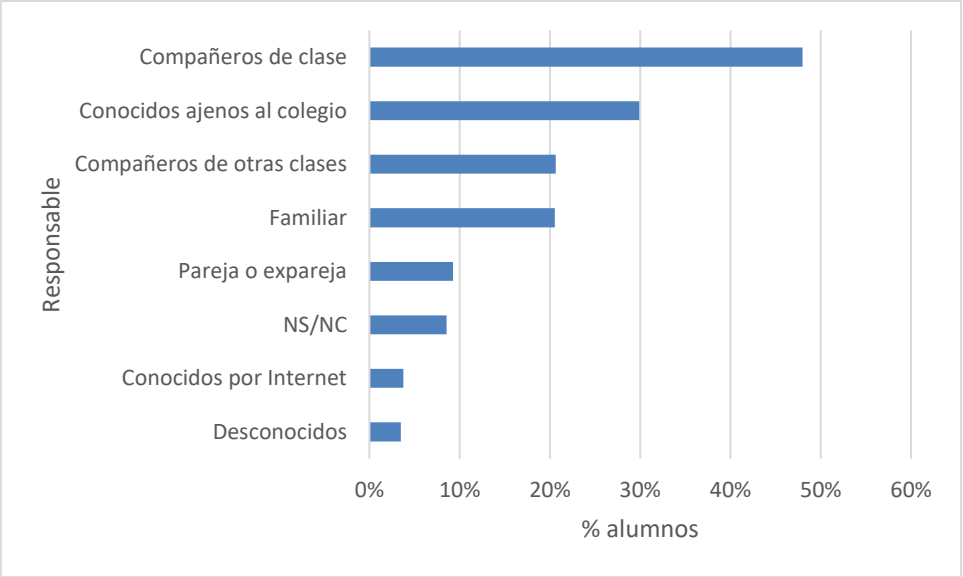


También en la línea de las dos anteriores conductas, la categoría de responsables de difundir o publicar fotos o vídeos sin consentimiento que presenta una mayor prevalencia corresponde a los compañeros de clase, con casi un 50% de alumnos que afirman este dato. Seguidamente, se encuentran las categorías de conocidos ajenos al colegio y compañeros de otras clases, con un 30% y un 21% respectivamente.

En el caso de los más pequeños, las prevalencias sobre los responsables de publicar fotos o vídeos personales sin consentimiento son de un 39% en el caso de la categoría "Compañeros de clase" y de un 28% en el caso de los familiares. En el grupo de alumnos con más edad (2º, 3º y 4º de ESO, Bachillerato y CFGM), la categoría con una prevalencia mayor es la de los compañeros de clase, con un

51% de los alumnos, seguida de la categoría “Conocidos ajenos al colegio”, con un 33%.

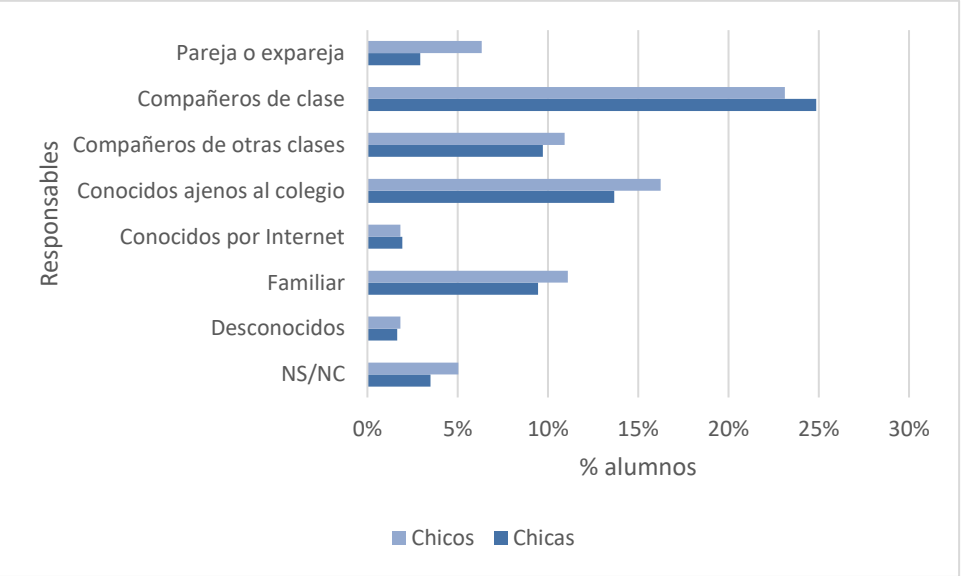
Gráfico 53. *Responsables de la publicación de fotos o vídeos sin consentimiento según las víctimas*



Con apenas diferencias entre sexos, tanto las chicas como los chicos consideran que sus compañeros de clase son los principales responsables de este tipo de ciberacoso, con porcentajes que alcanzan las cifras de 25% y 23%, respectivamente. Además, ambos grupos también coinciden en afirmar que el segundo tipo de responsable más frecuente es el de “Conocidos ajenos al colegio” (14% y 16%, respectivamente).

En cuanto a los responsables con menos representación, tanto chicos y chicas vuelven a coincidir, por tercera vez y con un porcentaje del 2% en ambos casos, que las personas conocidas por Internet y las personas desconocidas son las que menos realizan este tipo de conducta.

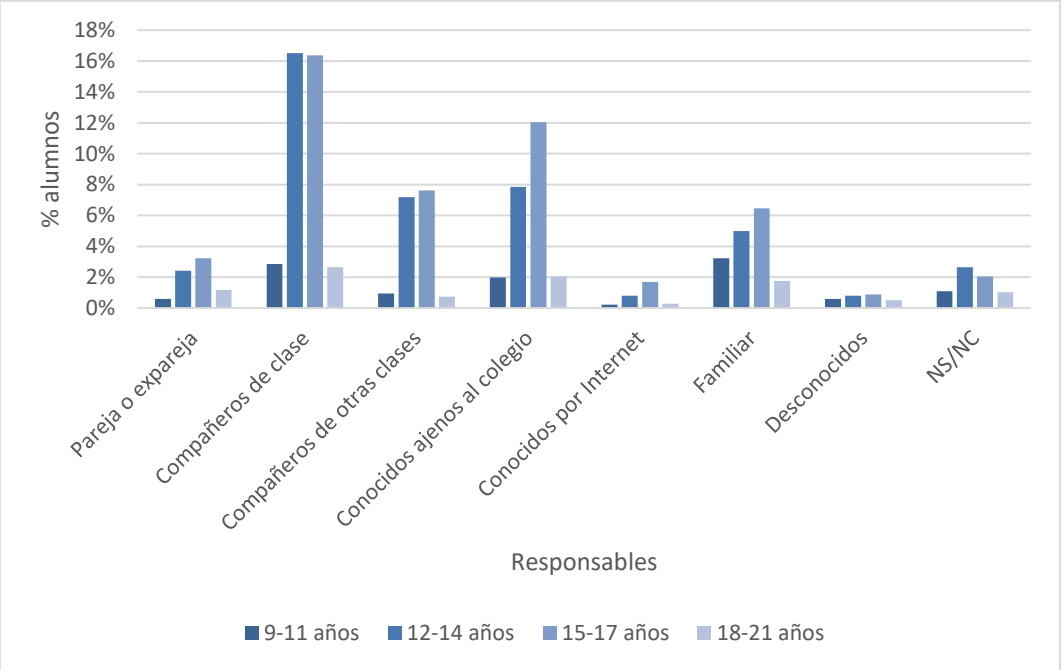
Gráfico 54. *Responsables de la publicación de fotos o vídeos sin consentimiento según el sexo de la víctima*



En cuanto a la distribución de los responsables según la edad de las víctimas, cabe destacar que todas las franjas de edad coinciden en que los principales responsables de este tipo de ciberacoso fueron uno o varios compañeros de clase (un 3% de los alumnos entre 9 y 11 años, un 17% de alumnos entre 12 y 14 años, un 16% de alumnos entre 15 y 17 años y un 3% de alumnos que tiene entre 18 y 21 años). Entre los alumnos que tienen entre 9 y 11 años, también existe un 3% de ellos que ha informado que el principal responsable fue un familiar.

Además, todos los alumnos de las distintas franjas de edad vuelven a coincidir, en un 2% (alumnos entre 9 y 11 años), un 8% (alumnos entre 12 y 14 años), un 12% (alumnos entre 15 y 17 años) y un 2% de los casos (alumnos entre 18 y 21 años), en que la segunda categoría de responsables más frecuente es la de conocidos ajenos al colegio. Entre los alumnos que tienen de 18 a 21 años, también existe un 2% de ellos que ha informado que el segundo responsable más común se trata de un familiar.

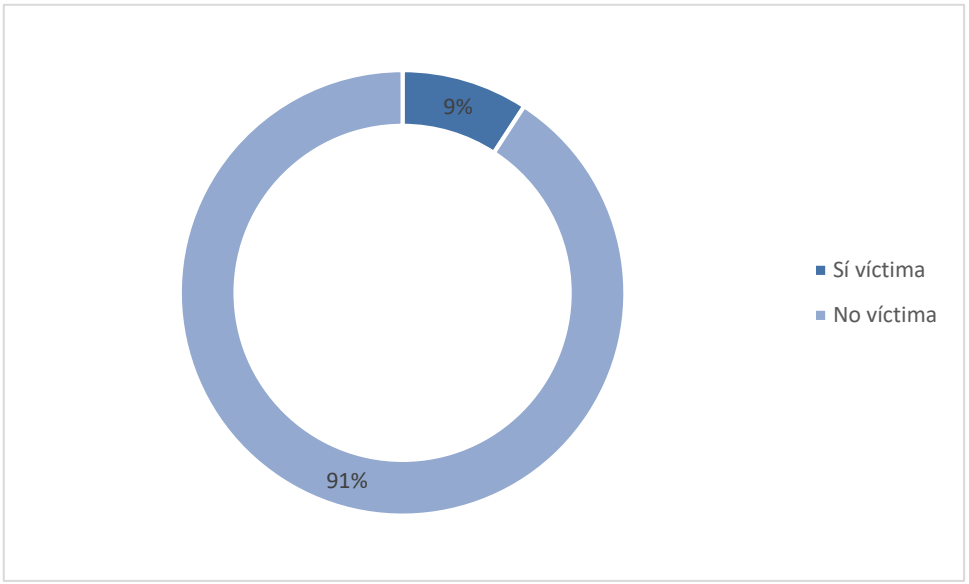
Gráfico 55. *Responsables de la publicación de fotos o vídeos sin consentimiento según la edad de la víctima*



4. Difusión de información íntima

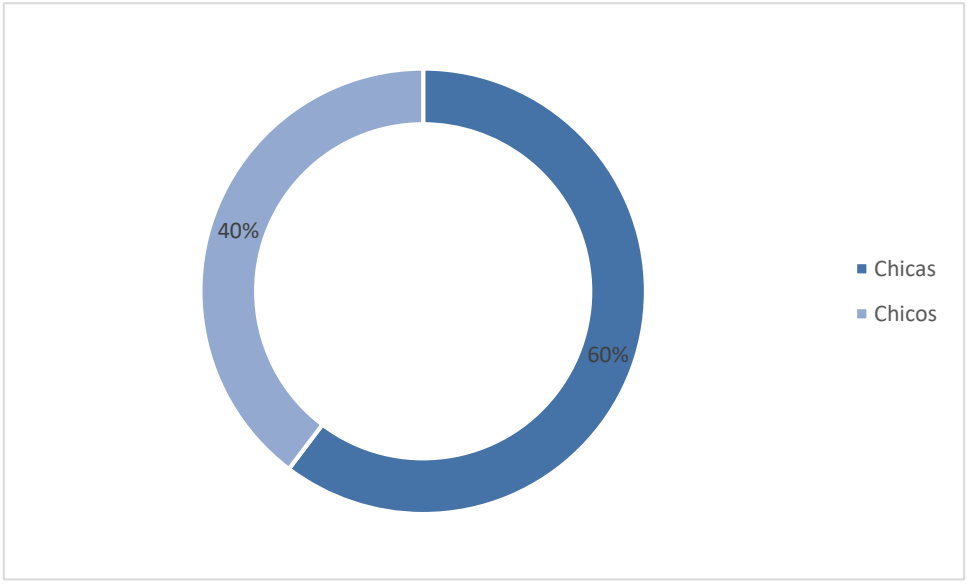
Esta tipología de ciberacoso, que solo ha sido analizada entre los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, presenta una prevalencia de víctimas del 9% (n = 398), cifra inferior al resto de tipologías vistas hasta el momento.

Gráfico 56. *Prevalencia de alumnos víctimas difusión de información íntima a través de Internet*



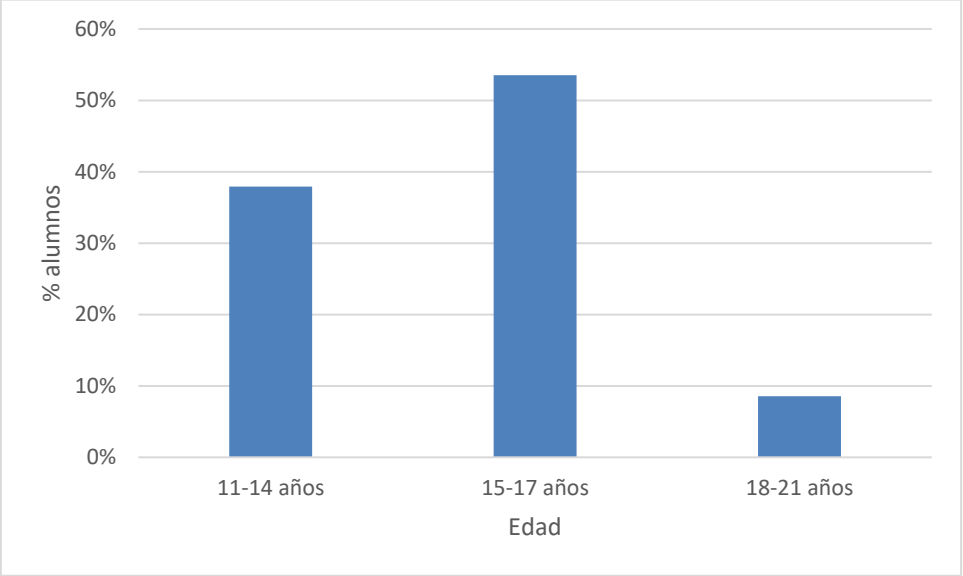
Con una diferencia algo mayor respecto al resto de subtipos de ciberacoso vistos hasta el momento, en este caso el 40% de alumnos que ha sido víctima representa al sector masculino (n = 158), mientras que el 60% son chicas (n = 240).

Gráfico 57. *Prevalencia de alumnos víctimas difusión de información íntima a través de Internet según sexo*



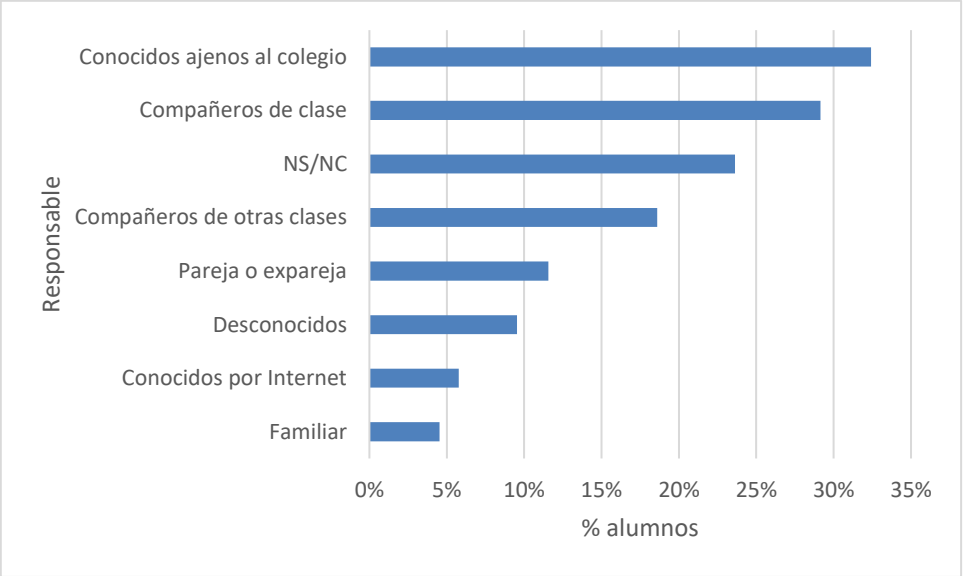
En cuanto a la distribución por edad de las víctimas de este tipo de ciberacoso, se observa que el 38% tiene entre 11 y 14 años (n = 151), el 54% tiene entre 15 y 17 años (n = 213) y el 9% restante tiene entre 18 y 21 años (n = 32).

Gráfico 58. *Prevalencia de alumnos víctimas difusión de información íntima a través de Internet según edad*



De nuevo, los responsables más comunes a la hora de realizar esta conducta son, en un 32,4% y un 29% de los casos, conocidos ajenos al colegio y los propios compañeros de clase, respectivamente. Cabe destacar que, en esta conducta concreta, el porcentaje de alumnos que no sabe o no ha querido responder quien fue el autor asciende a un 23,9%.

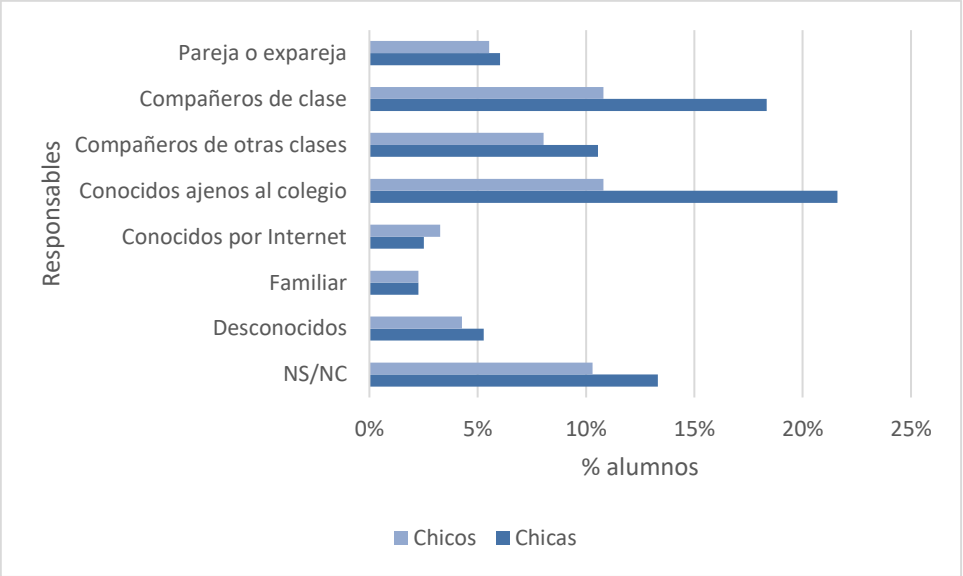
Gráfico 59. *Responsables de la difusión de información íntima según las víctimas*



Tanto las chicas, en un 22% de los casos, como los chicos, en un 11%, consideran que los conocidos ajenos al colegio son los principales responsables de difundir información íntima. Además, un 11% de los chicos también considera a los compañeros de clase como los principales autores de este tipo de ciberacoso.

Según un 2% y un 3% de chicas y un 2% y 3% de chicos, los familiares y conocidos por Internet vuelven a ser las personas que menos realizan este tipo de ciberacoso.

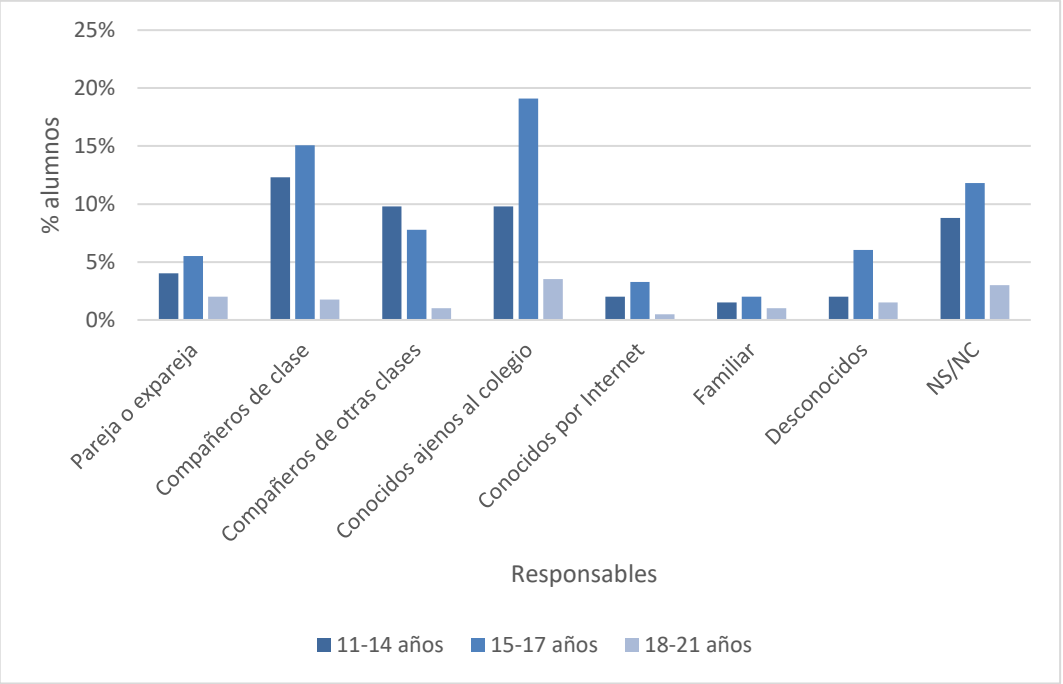
Gráfico 60. *Responsables de la difusión de información íntima según el sexo de la víctima*



En cuanto a los responsables según la edad de las víctimas, los conocidos ajenos al colegio son los considerados como principales responsables por los jóvenes de 15 a 17 años y por los que tienen entre 18 y 21 años (en un 19% y 4% de los casos, respectivamente). Respecto a los alumnos entre 11 y 14 años, los responsables más comunes, según un 12% de los casos, son uno o varios compañeros de clase.

La segunda categoría de responsables más frecuente es, en el caso de los alumnos de 11 a 14 años, la de los compañeros de otras clases y los conocidos ajenos al colegio (un 10% en ambas categorías). En cuanto a los que tienen de 15 a 17 años, la segunda categoría más común es la de compañeros de clase (un 15%), mientras que entre los que tienen de 18 y 21 años, un 3% ha preferido no responder o no ha sabido qué decir ante esta pregunta.

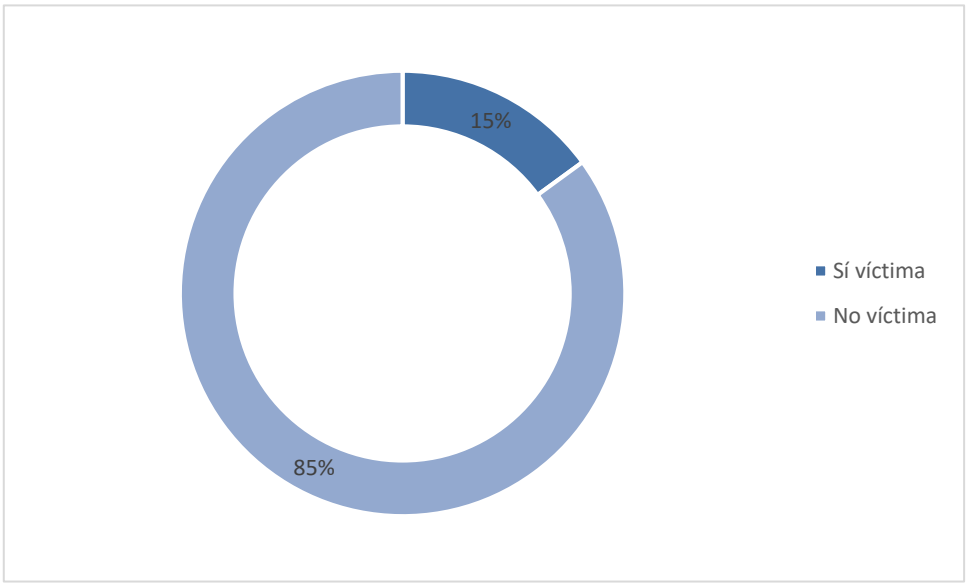
Gráfico 61. *Responsables de la difusión de información íntima según la edad de la víctima*



5. Acceder a las cuentas personales sin autorización

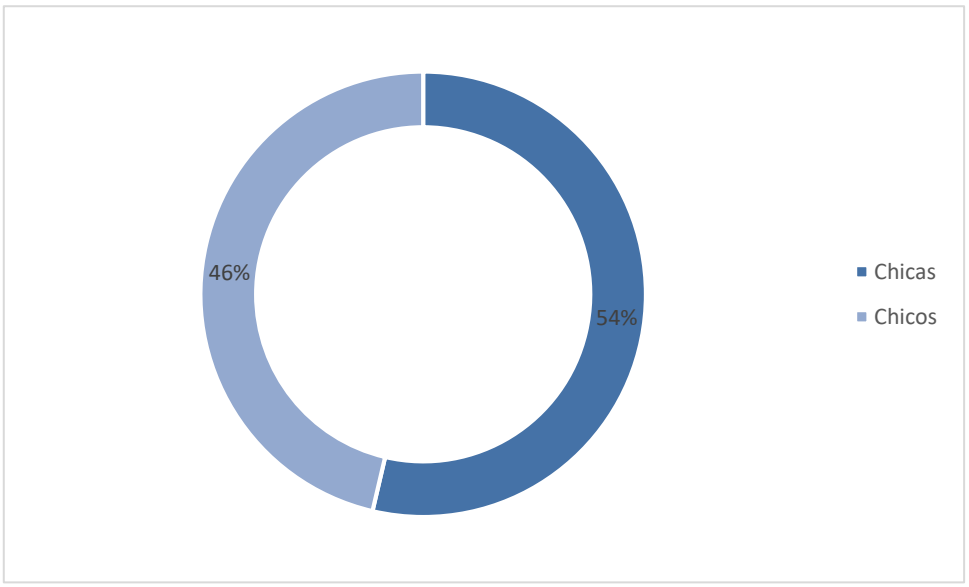
De nuevo, la prevalencia de cibervictimización de esta conducta es similar a las anteriores, con un 15% de alumnos víctimas (n = 848). En el caso de los alumnos pequeños, la prevalencia desciende al 10,3% (n = 304) y en el caso de los grandes al 12,6% (n = 544).

Gráfico 62. *Prevalencia de alumnos víctimas de acceder a sus cuentas personales sin autorización a través de Internet*



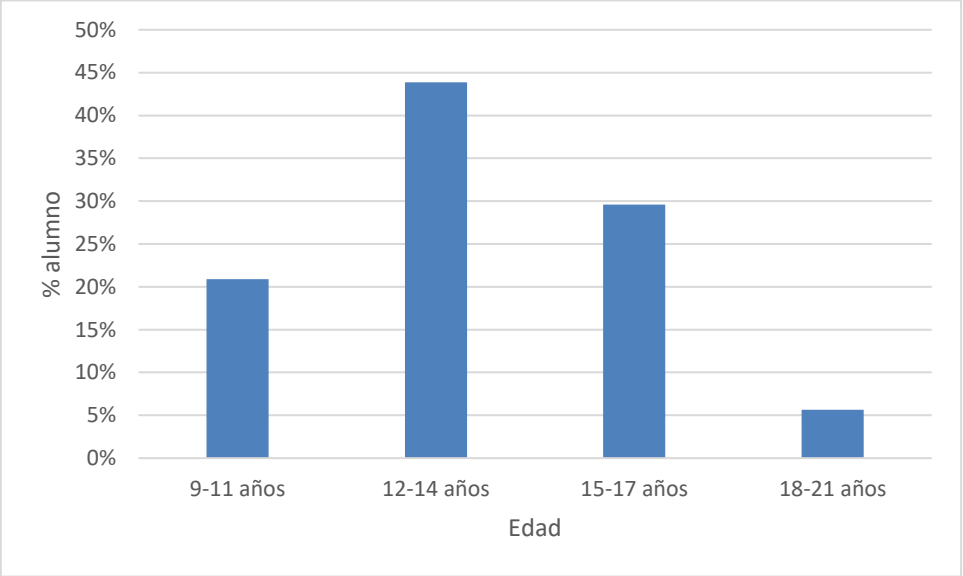
Entre el 15% de alumnos que afirman que han accedido a sus cuentas personales sin su autorización, el 54% son chicas (n = 455) y el 46% son chicos (n = 393).

Gráfico 63. *Prevalencia de alumnos víctimas de acceder a sus cuentas personales sin autorización a través de Internet según sexo*



La edad de los alumnos que han afirmado que alguien ha accedido a sus cuentas personales sin autorización se encuentra, en el 21% de los casos, entre los 9 y los 11 años (n = 177). En el 44% de los casos los alumnos tienen entre 12 y 14 años (n = 372) y en el 30% tienen entre 15 y 17 años (n = 251). Finalmente, los alumnos que tienen entre 18 y 21 años suponen el 6% de víctimas (n = 48).

Gráfico 64. *Prevalencia de alumnos víctimas de acceder a sus cuentas personales sin autorización a través de Internet según edad*

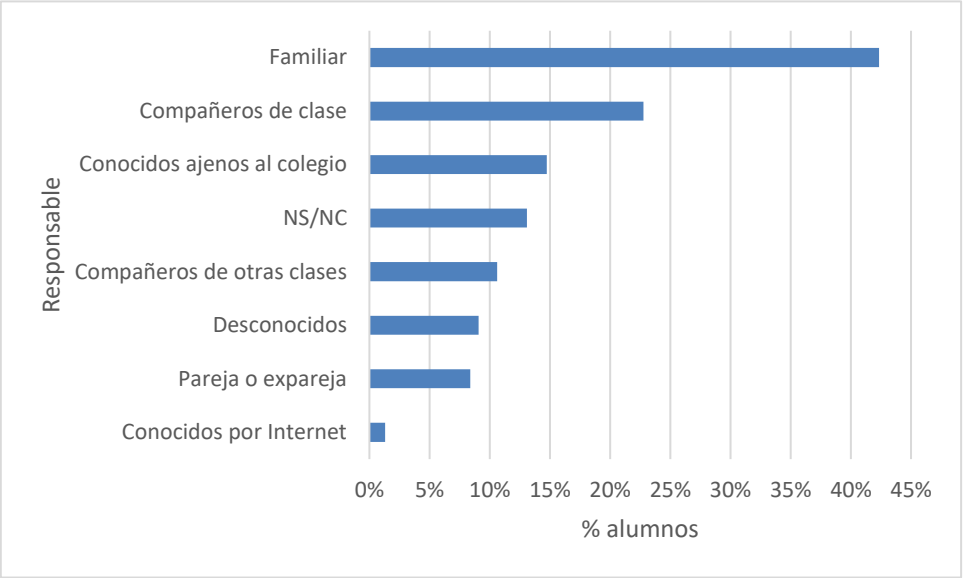


A diferencia del resto de tipologías de ciberacoso, en el caso de acceder a las cuentas personales sin autorización, un elevado número de alumnos afirma que el responsable fue un familiar, alcanzando una cifra del 42%. Las diferencias son aún mayores si se analiza específicamente según el grupo de alumnos (pequeños y grandes). En el caso de los pequeños, un 60% ha afirmado que el responsable fue un familiar, mientras que el caso de los mayores la cifra desciende a un 33,6%. Estos resultados parecen indicar que, cuanto menor es la edad, mayor es el acceso a las cuentas personales sin consentimiento por parte de un familiar.

En cuanto al resto de categorías, se observa que vuelve a ser frecuente que los responsables sean los compañeros de clase (un 23%) o conocidos ajenos al

colegio (un 15%).

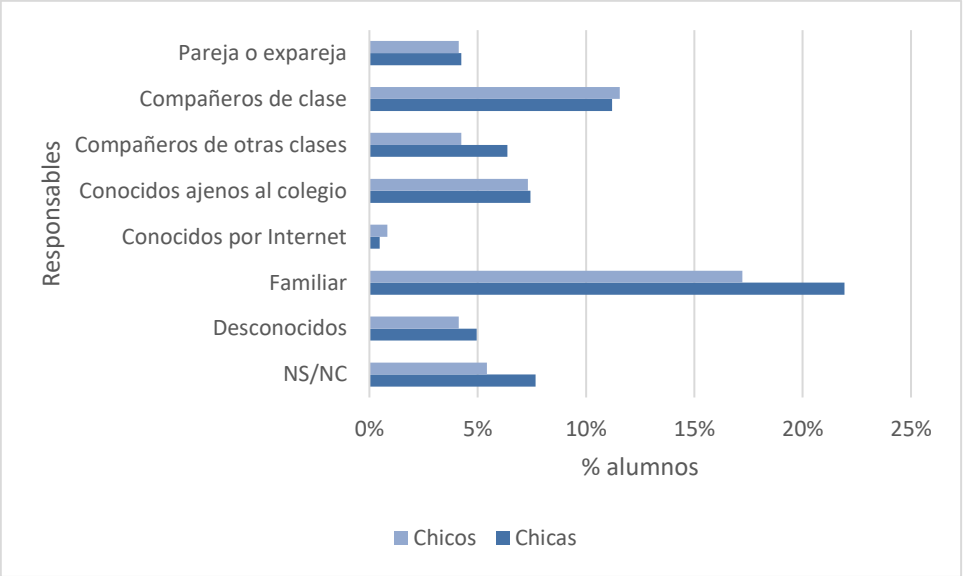
Gráfico 65. *Responsables del acceso a las cuentas personales sin autorización según las víctimas*



Respecto a los responsables del acceso a las cuentas personales sin autorización según el sexo de las víctimas, cabe destacar que en este caso los chicos y las chicas coinciden a la hora de afirmar quiénes son los principales responsables y aquellas personas que menos realizan esta conducta. Un 22% de las chicas y un 17% de los chicos considera que el principal responsable es un familiar, seguido de un 11% de chicas y un 12% de chicos que considera que son los compañeros de clase los que acceden a las cuentas sin permiso.

Entre las personas que apenas tienen responsabilidad sobre estos actos se encuentran, según un 0,5% de chicas y un 0,8% de chicos, los conocidos a través de Internet.

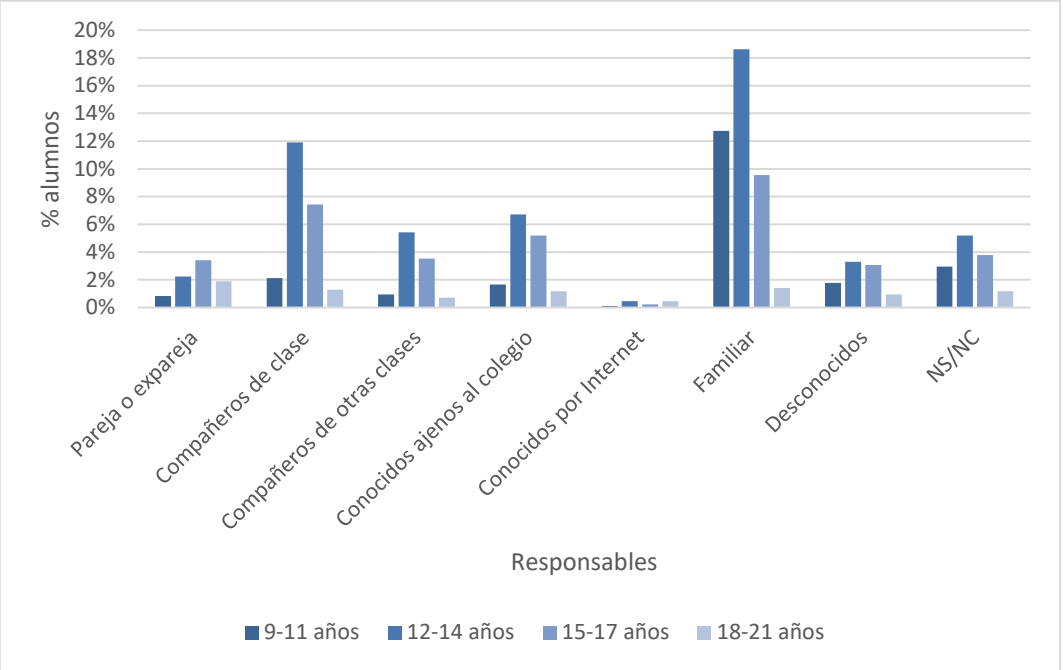
Gráfico 66. *Responsables del acceso a las cuentas personales sin autorización según el sexo de la víctima*



Todos los alumnos que se encuentran en las franjas de edad de 9 a 11 años, de 12 a 14 años y de 15 a 17 años coinciden en que los familiares son los principales responsables de acceder a las cuentas personales sin autorización, con una prevalencia de un 13%, un 19% y un 10% en cada caso. Entre los jóvenes de mayor edad (de 18 a 21 años), el principal autor de este tipo de ciberacoso es la pareja o expareja (un 2% de los alumnos).

Cabe destacar que los responsables menos frecuentes, en todas las franjas de edad, son los conocidos por Internet, ya que ni un 1% de los alumnos ha afirmado, en ninguno de los casos, que el responsable de este tipo de ciberacoso fuese alguien conocido a través de Internet.

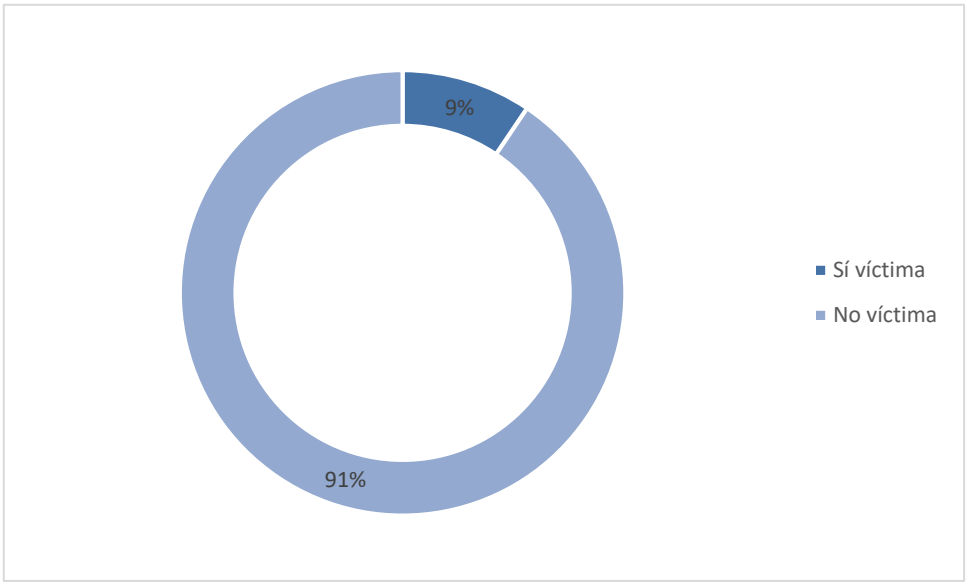
Gráfico 67. *Responsables del acceso a las cuentas personales sin autorización según la edad de la víctima*



6. Exclusión social

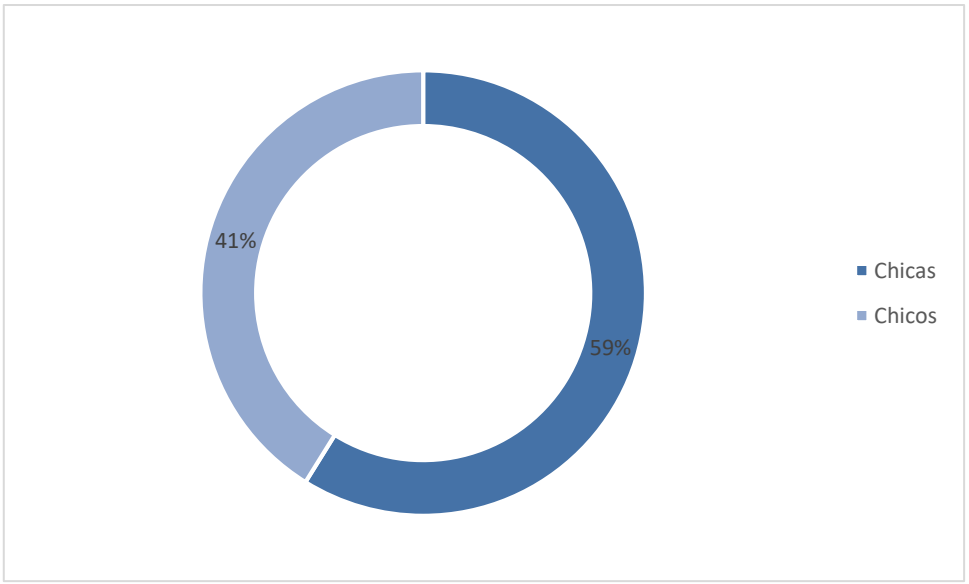
Esta es otra de las tipologías de ciberacoso con una de las prevalencias de cibervictimización más bajas, siendo ésta de un 9% (n = 688). En el caso de los más pequeños, la prevalencia es de casi un 13% (n = 374) y en el caso de los grandes de un 7,3% (n = 314).

Gráfico 68. *Prevalencia de alumnos víctimas de exclusión social a través de Internet*



Con una diferencia ligeramente mayor según el sexo de las víctimas, en este caso el 41% de las víctimas son chicos (n = 283) y el 59% son chicas (n = 405).

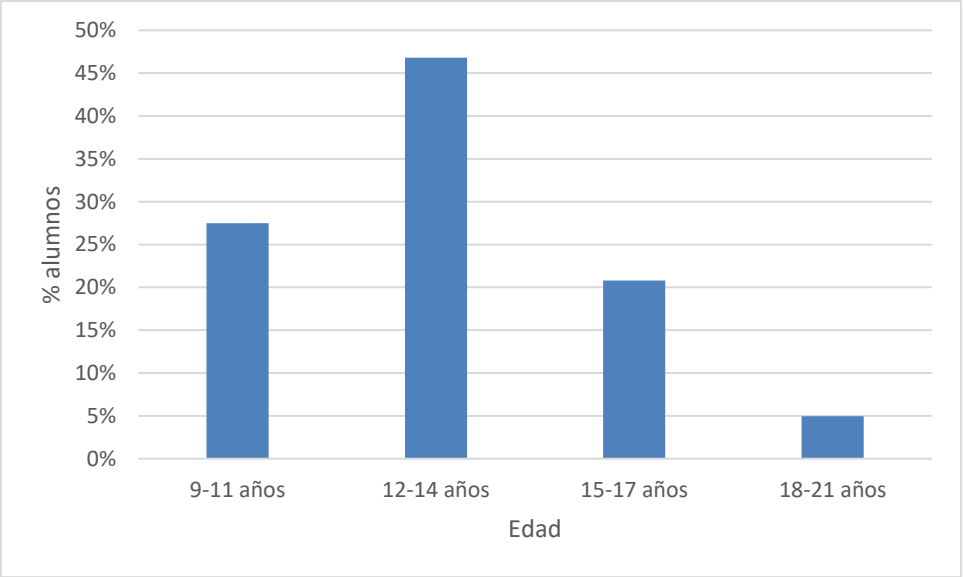
Gráfico 69. *Prevalencia de alumnos víctimas de exclusión social a través de Internet según sexo*



En cuanto a la distribución por edad de las víctimas de este tipo de ciberacoso, se observa que el 27% tiene entre 9 y 11 años (n = 189), el 47% tiene entre 12 y 14

años (n = 322), el 21% tiene entre 15 y 17 años (n = 143) y el 5% restante tiene entre 18 y 21 años (n = 34).

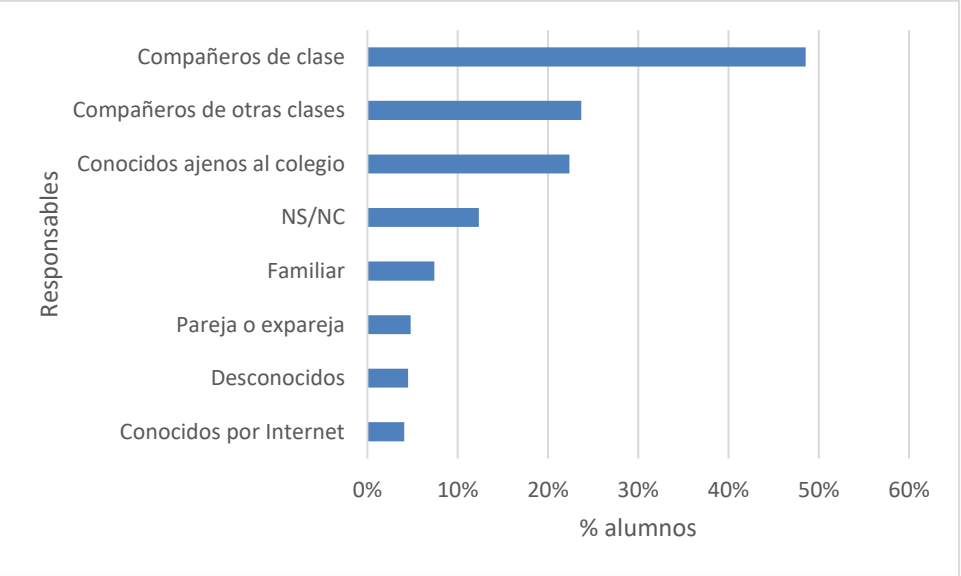
Gráfico 70. *Prevalencia de alumnos víctimas de exclusión social a través de Internet según edad*



Aunque es una de las tipologías de ciberacoso con menor prevalencia, es la que más realizan los propios compañeros de clase. Como se observa en el gráfico 69, casi un 50% de los alumnos afirma que los responsables de la exclusión social fueron los propios compañeros de clase, seguido de un 24% de alumnos que afirma que fueron compañeros de otras clases.

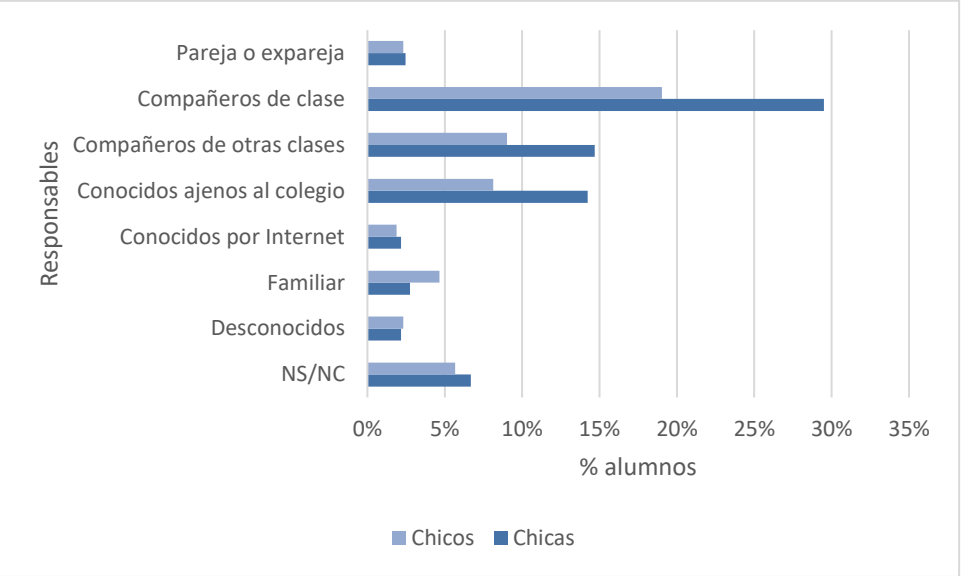
Analizando las cifras de manera más específica, se encuentra que, entre los pequeños, la mayoría (un 51,1%) afirma que los responsables fueron compañeros de clase, seguido de un 23,3% que afirma que fueron compañeros de otras clases. Los alumnos más grandes, por su parte, sostienen que la mayor parte de responsables son compañeros de clase (un 45,5%), seguido de conocidos ajenos al colegio (un 26%).

Gráfico 71. *Responsables de la exclusión social según las víctimas*



En relación al sexo de las víctimas, un 30% de las chicas ha afirmado que el principal responsable de excluirlas socialmente ha sido un compañero de clase, seguido de un compañero de otras clases (un 15%) y conocidos ajenos al colegio (un 14%). En cuanto a los chicos, la situación es prácticamente idéntica, ya que un 19% de los mismos afirma que el principal responsable es un compañero de clase, seguido de un 9% y un 8% que afirman que la responsabilidad recae sobre compañeros de otras clases y sobre conocidos ajenos al colegio, respectivamente.

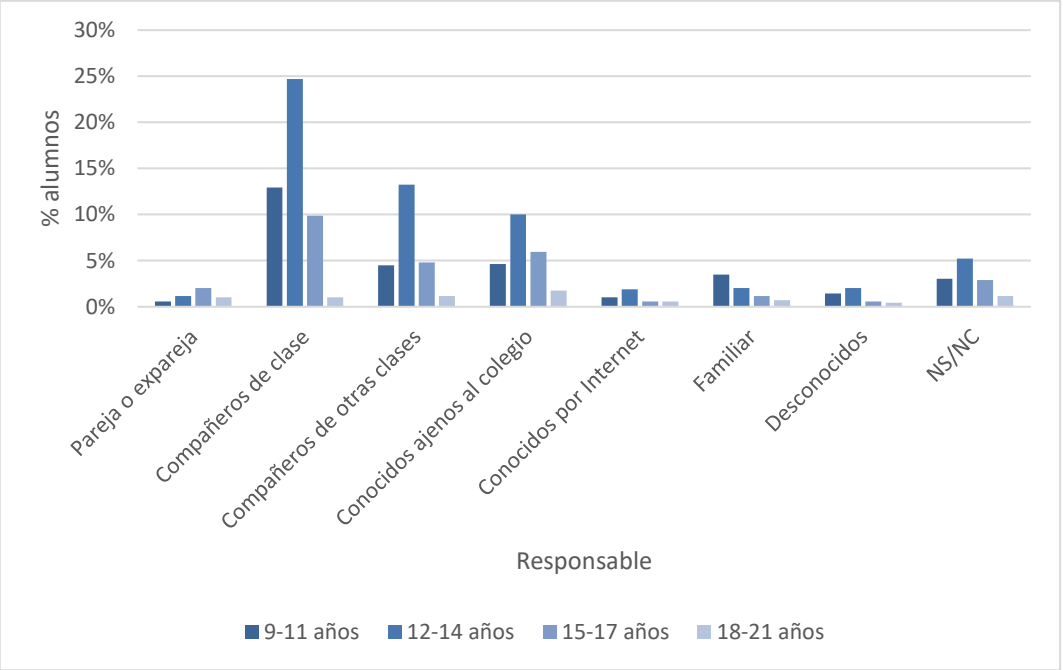
Gráfico 72. *Responsables de la exclusión social según el sexo de la víctima*



De nuevo, tanto los jóvenes de entre 9 y 11 años, de 12 a 14 y de 15 a 17 coinciden, en un 13%, un 25% y un 10% de los casos, respectivamente, en que el principal responsable de la exclusión fue uno o varios compañeros de clase. En cambio, los jóvenes de entre 18 y 21 años consideran que los principales responsables fueron conocidos ajenos al colegio (un 2%).

Concretando más en cada franja de edad, los alumnos que tienen entre 9 y 11 años consideran, en un 5% de los casos, que los compañeros de otras clases y los conocidos ajenos al colegio representan el segundo tipo de responsables más frecuente en este tipo de ciberacoso. Los alumnos entre 12 y 14 años coinciden con los alumnos de la primera franja de edad en afirmar que el segundo tipo de responsable más frecuente corresponde a los compañeros de otras clases (un 13%). Por su parte, los alumnos que tienen entre 15 y 17 años se decantan, en un 6% de los casos, por la categoría de conocidos ajenos al colegio. Finalmente, no hay diferencias entre las distintas categorías de responsables entre los alumnos de 18 a 21 años.

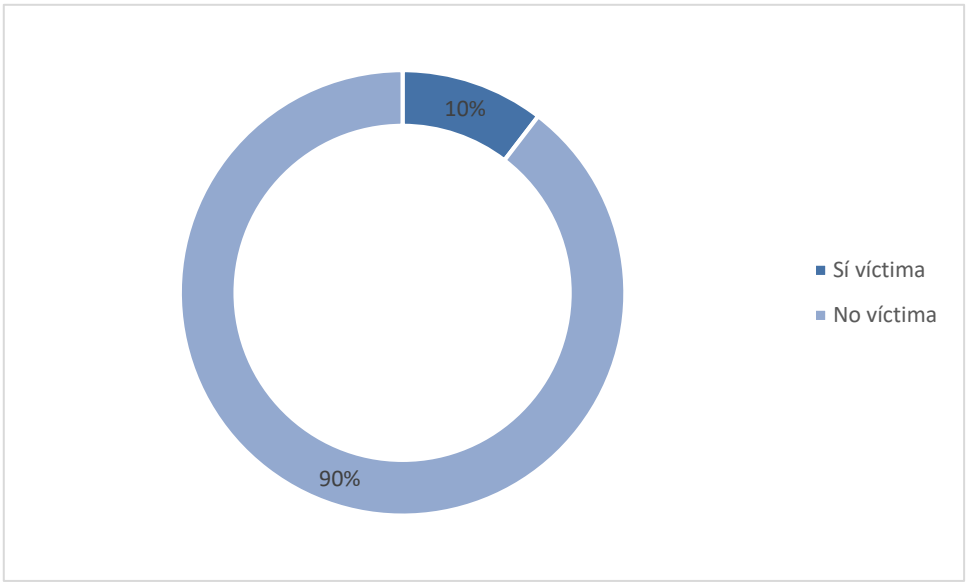
Gráfico 73. *Responsables de la exclusión social según la edad de la víctima*



7. Amenazas

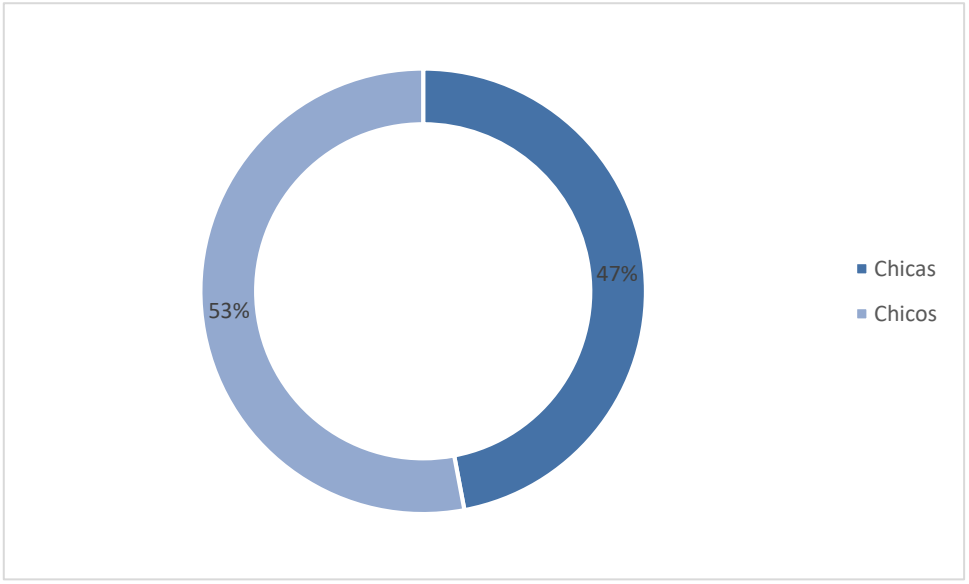
El 10% de los alumnos (n = 759) afirma haber sufrido amenazas a través de Internet en el último año. Más concretamente, en el grupo de los alumnos más pequeños la prevalencia es del 6,7% y, en el caso de los más grandes, del 13%.

Gráfico 74. *Prevalencia de alumnos víctimas de amenazas a través de Internet*



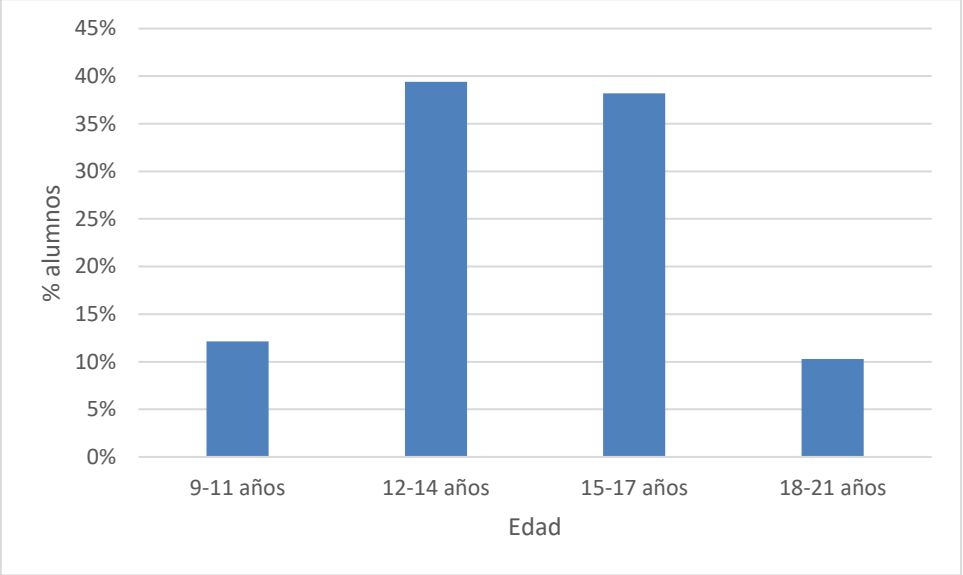
Entre los alumnos que han afirmado haber recibido amenazas a través de Internet, el 53% son chicos (n = 402) y el 47% son chicas (n = 357). Se observa que, a diferencia del resto de tipos de ciberacoso analizados hasta el momento, en este caso los chicos son más victimizados que las chicas.

Gráfico 75. *Prevalencia de alumnos víctimas de amenazas a través de Internet según sexo*



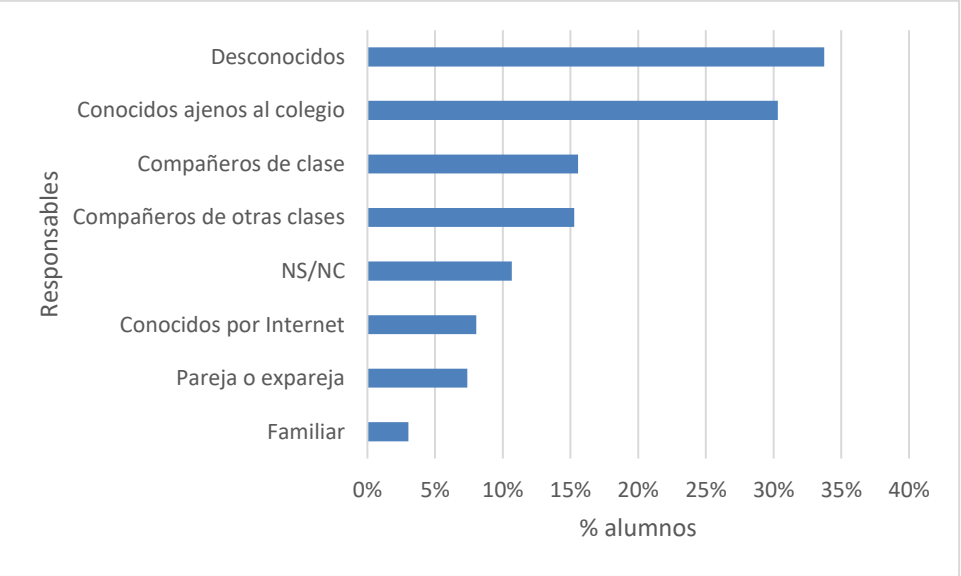
En cuanto a la distribución de las víctimas de haber recibido amenazas, se observa que el 12% tiene entre 9 y 11 años (n = 92), el 39% tiene entre 12 y 14 años (n = 299), el 38% tiene entre 15 y 17 años (n = 290) y el 10% restante tiene entre 18 y 21 años (n = 78).

Gráfico 76. *Prevalencia de alumnos víctimas de amenazas a través de Internet según edad*



En cuanto a los responsables de estas amenazas, casi un 35% de alumnos afirma que los responsables fueron personas desconocidas, seguido de un 30% y un 16% que afirman que eran compañeros de clase y de otras clases, respectivamente. De forma más específica, los alumnos más pequeños indican que la categoría de responsables con una mayor prevalencia es la de "Compañeros de clase" (casi un 27%), seguida de la de "Conocidos ajenos al colegio" (un 26%). En el caso de los alumnos de mayor edad, la categoría con una mayor prevalencia coincide con la que aparece en primer lugar en los análisis globales, que es la de "Desconocidos" (un 38% de los alumnos), seguida de la de conocidos ajenos al colegio, con un 31,7%.

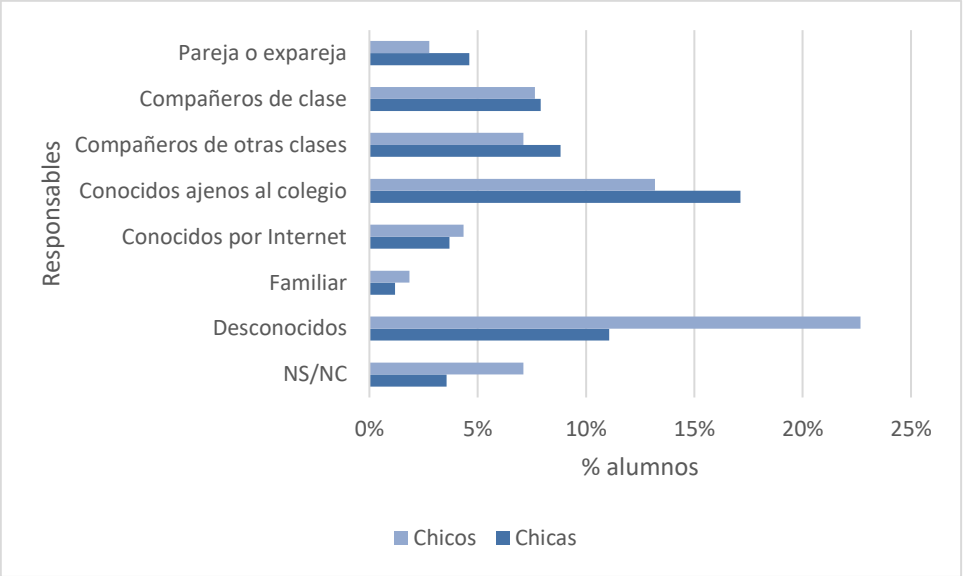
Gráfico 77. *Responsables de las amenazas según las víctimas*



A la hora de admitir quien es el responsable de las amenazas a través de Internet, chicos y chicas tienen opiniones un tanto distintas. En cuanto a las chicas, un 17% afirma que los principales responsables son conocidos ajenos al colegio, seguido de un 11% que considera que el responsable fue alguien conocido externo al colegio. En el caso de los chicos, en cambio, el principal responsable se trata de alguien desconocido (un 23% de los chicos), seguido de alguien conocido ajeno a la escuela (un 13%).

Donde sí coinciden chicos y chicas es a la hora de afirmar que los familiares son los que menos han realizado amenazas a través de Internet (un 2% y un 1% de los casos, respectivamente).

Gráfico 78. *Responsables de las amenazas según el sexo de la víctima*

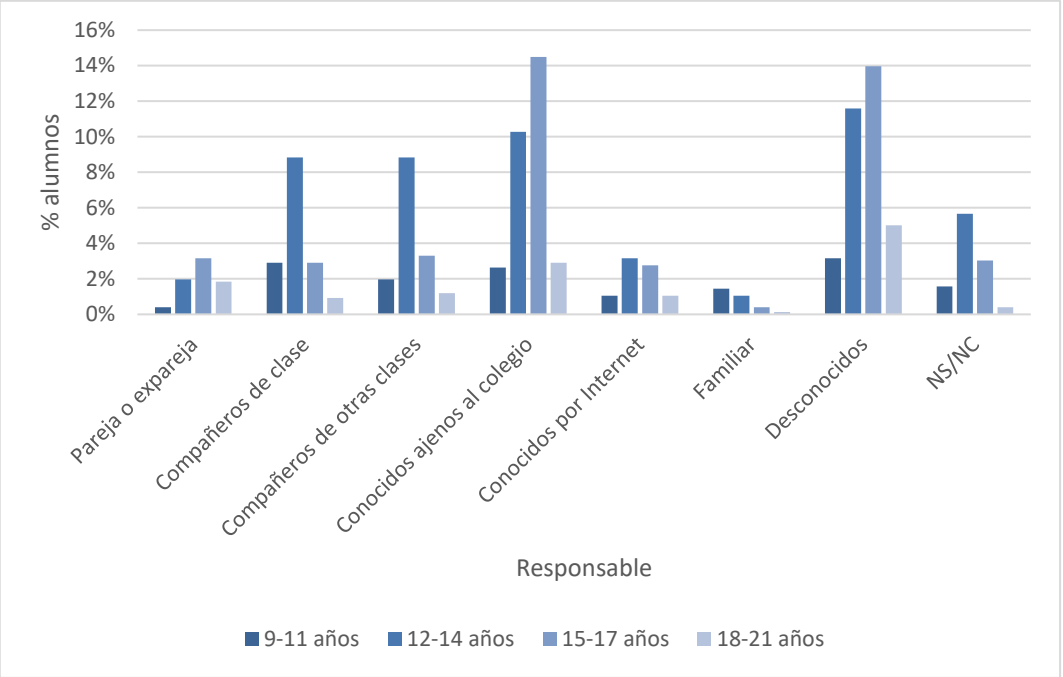


Todos los alumnos, independientemente de su edad, coinciden en que el principal responsable de las amenazas fue una persona desconocida (un 3% de alumnos entre 9 y 11 años, un 12% entre 12 y 14 años, un 14% entre 15 y 17 años y un 5% entre 18 y 21 años). Sin embargo, en las franjas de edad de 9 a 11 años y de 15 a 17 años hay algunos detalles a destacar.

Respecto a los alumnos de 9 a 11 años, también se ha afirmado, en un 3% de los casos, que los principales responsables fueron compañeros de clase y conocidos por Internet. En cuanto a los que tienen entre 15 y 17 años, un 14% también ha afirmado que los responsables más frecuentes a la hora de amenazar fueron personas conocidas a través de Internet.

Finalmente, en general, la categoría de responsables que presenta un mayor consenso a la hora de afirmar que es la menos frecuente, es la de los familiares, tal y como se observa en el siguiente gráfico.

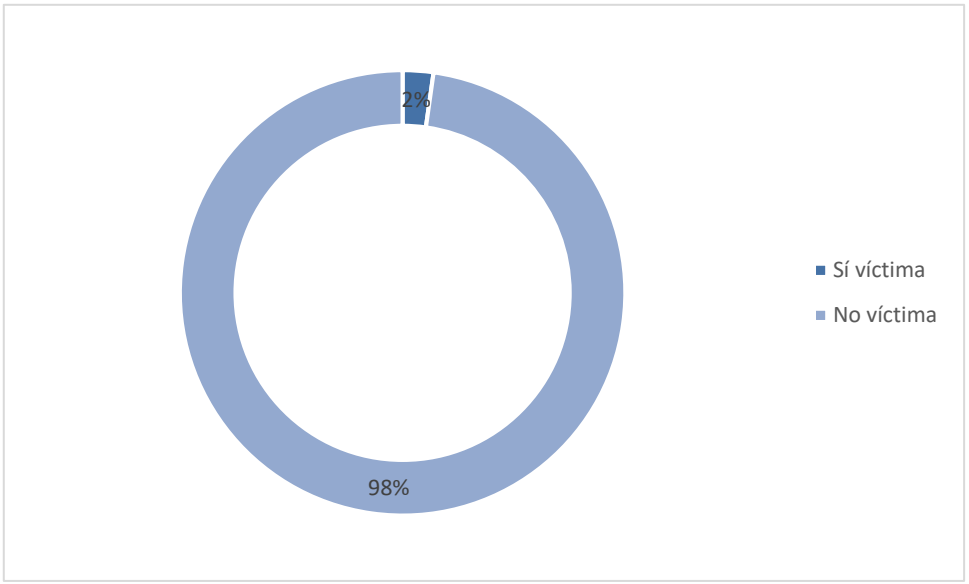
Gráfico 79. *Responsables de las amenazas según la edad de la víctima*



8. Coacciones

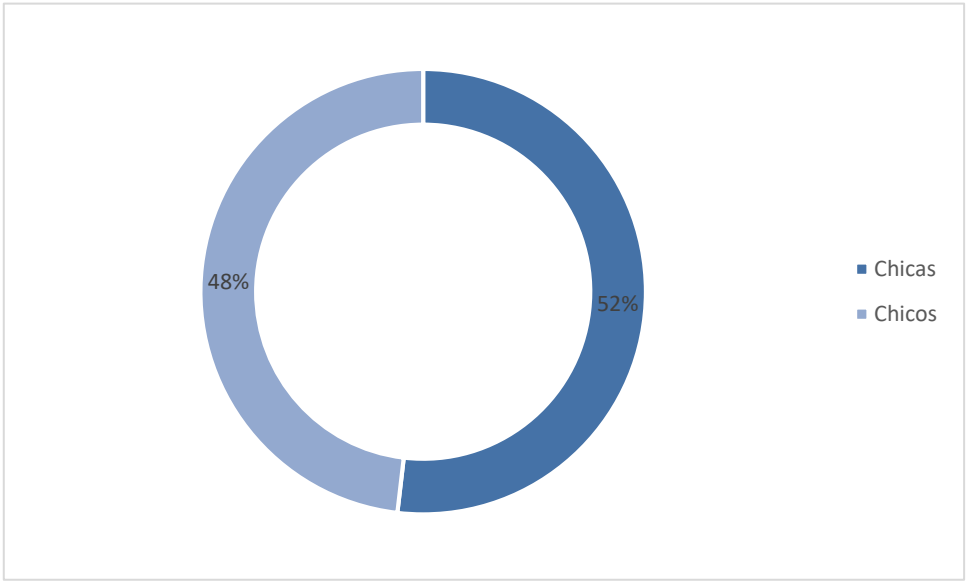
Este es el tipo de ciberacoso menos frecuente entre los alumnos, ya que solo el 2% (n = 162) afirma haber sufrido coacciones en el último año. En el caso de los alumnos pequeños, la prevalencia es del 2,3%, y en el de los más mayores, del 2,1%. Es decir, las tres prevalencias (la global y las dos específicas según etapa educativa) coinciden prácticamente en la misma cifra.

Gráfico 80. *Prevalencia de alumnos víctimas de coacciones a través de Internet*



De los 162 alumnos que parecen haber sido víctimas de coacciones, 78 de ellos son chicos (el 48%) y 84 chicas (el 52%). Aunque la diferencia no es muy elevada, las chicas vuelven a ser más victimizadas que los chicos.

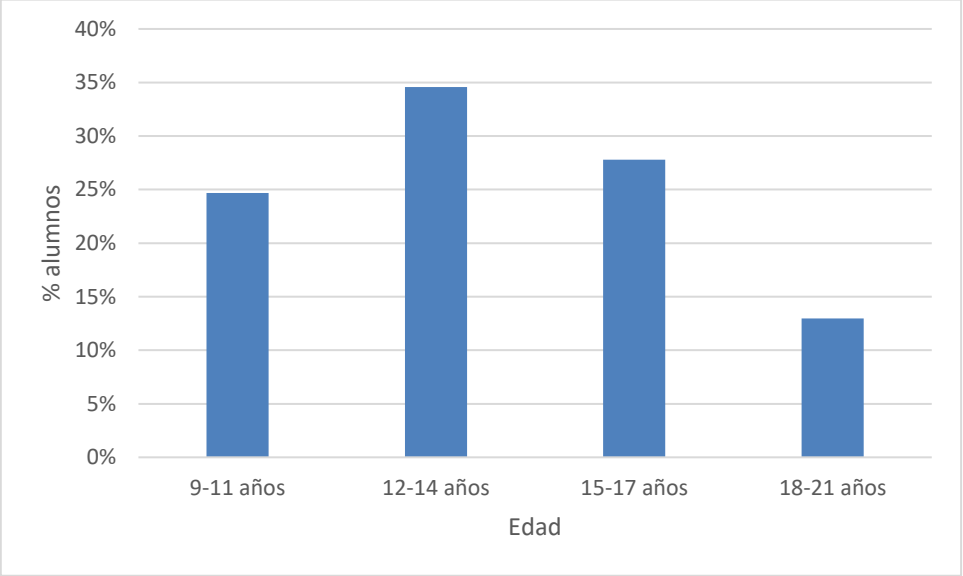
Gráfico 81. *Prevalencia de alumnos víctimas de coacciones a través de Internet según sexo*



En cuanto a la edad de las víctimas, el 25% tiene entre 9 y 11 años (n = 40), el

35% tiene entre 12 y 14 años (n = 56), el 28% tiene entre 15 y 17 años (n = 45) y el 13% restante tiene entre 18 y 21 años (n = 21), tal y como se observa en el siguiente gráfico.

Gráfico 82. *Prevalencia de alumnos víctimas de coacciones a través de Internet según edad*

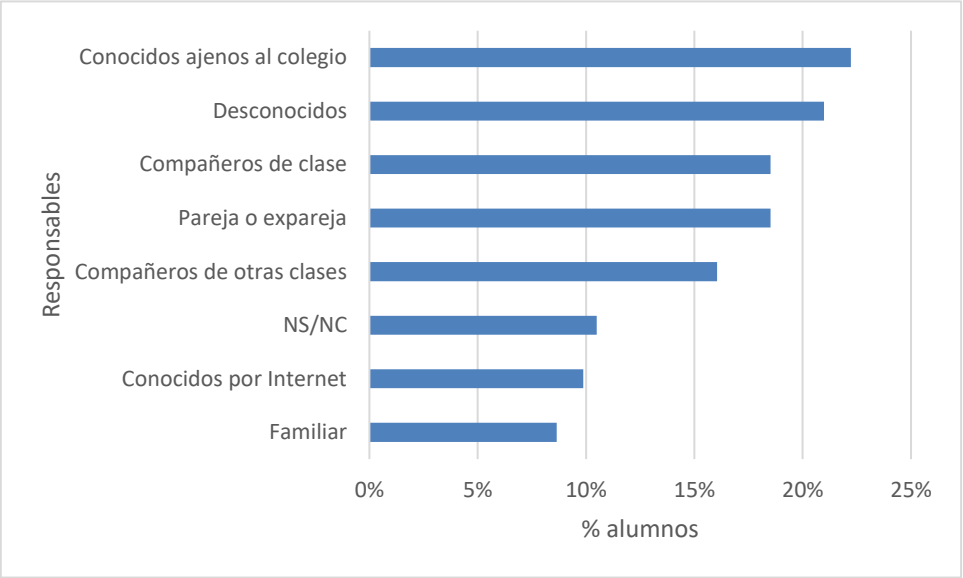


La mayor parte de responsables son conocidos ajenos al colegio (un 22% de los alumnos ha afirmado este dato), seguido de desconocidos (un 21%) y compañeros de clase (un 19%). Asimismo, la categoría "Pareja o expareja" también tiene una prevalencia del 19%, que es la cifra más elevada obtenida hasta el momento en esta categoría de todas las conductas de ciberacoso analizadas hasta ahora.

De hecho, las diferencias entre los alumnos de las distintas etapas educativas son bastante grandes. En el caso de los más pequeños, la mayoría de las coacciones provienen de compañeros de clase o de otras clases (un 29% y un 20% de alumnos, respectivamente). En el caso de los más grandes, la categoría de responsables con una mayor prevalencia es la de la "Pareja o expareja", con un 30% de alumnos. Las dos siguientes categorías con una mayor prevalencia son la de "Conocidos ajenos al colegio", con casi un 26%, y "Desconocidos", con casi un

23%.

Gráfico 83. *Responsables de las coacciones según las víctimas*

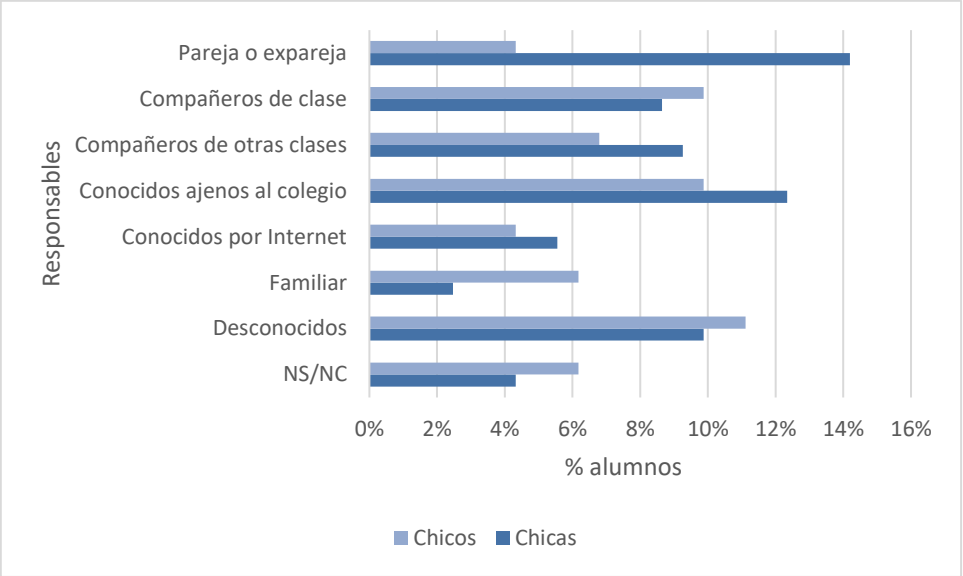


En relación al sexo de las víctimas, cabe destacar que un 14% de las chicas afirma que el principal responsable de las coacciones es su pareja o expareja, mientras que en el caso de los chicos esta es una de las categorías con una prevalencia más baja (un 4%). La siguiente categoría más común de responsables, según las chicas, es la de conocidos ajenos al colegio (un 12%) y la de personas desconocidas (un 10%).

En cuanto a los chicos, la categoría de responsables con mayor consenso, con un 11% de los casos, es la de personas desconocidas. De cerca le siguen las categorías de conocidos ajenos al colegio y compañeros de clase, con un porcentaje del 10% en ambos casos.

En cuanto a los responsables con una prevalencia más baja se encuentran, en el caso de las chicas, los familiares (un 2%) y, en el caso de los chicos, los conocidos por Internet y la pareja o expareja (un 4%), tal y como se ha comentado anteriormente.

Gráfico 84. *Responsables de las coacciones según el sexo de la víctima*



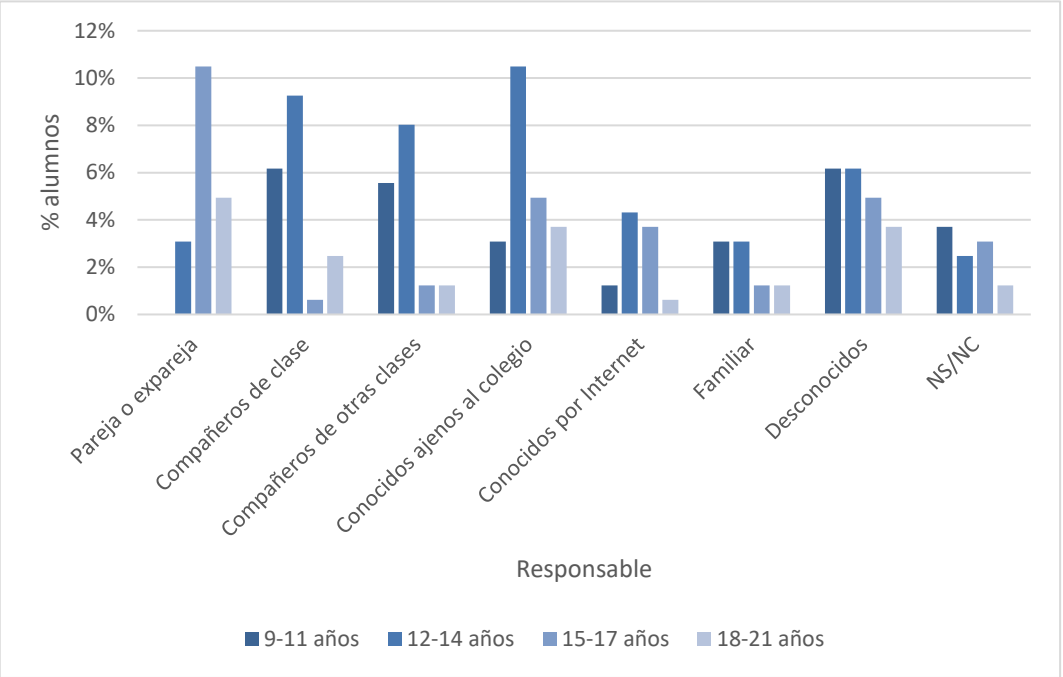
En este tipo de ciberacoso, los alumnos de las distintas franjas de edad tienen opiniones bastante diferentes en comparación con el resto de subtipos analizados hasta el momento. Comenzando por los alumnos que tienen entre 9 y 11 años, cabe destacar que un 6% de ellos coincide en que los principales responsables de las coacciones fueron compañeros de clase, compañeros de otras clases y personas desconocidas.

En cuanto a los alumnos entre 12 y 14 años, un 10% informa que el principal responsable fue un conocido ajeno al colegio, mientras que en las otras dos franjas de edad, la de alumnos entre 15 y 17 años y entre 18 y 21 años, el principal responsable fue la pareja o la expareja (en un 10% y 5% de los casos, respectivamente).

Si se observa el porcentaje de alumnos entre 9 y 11 años y entre 12 y 14 años que ha afirmado que el responsable fue la pareja o expareja, sorprende que en el primero de los casos la cifra sea de 0%, mientras que en el segundo se queda en un 3%. Es decir, mientras que para los alumnos de las dos franjas de edad más elevadas el principal responsable fue la pareja o expareja, para los alumnos de

menor edad esta categoría es una de las que presenta una menor prevalencia.

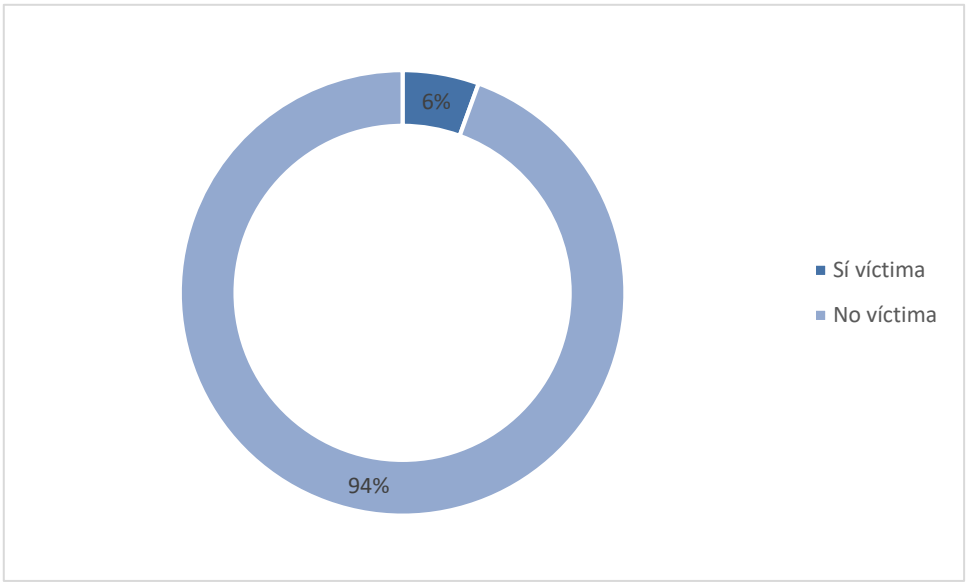
Gráfico 85. *Responsables de las coacciones según la edad de la víctima*



9. Suplantación de identidad

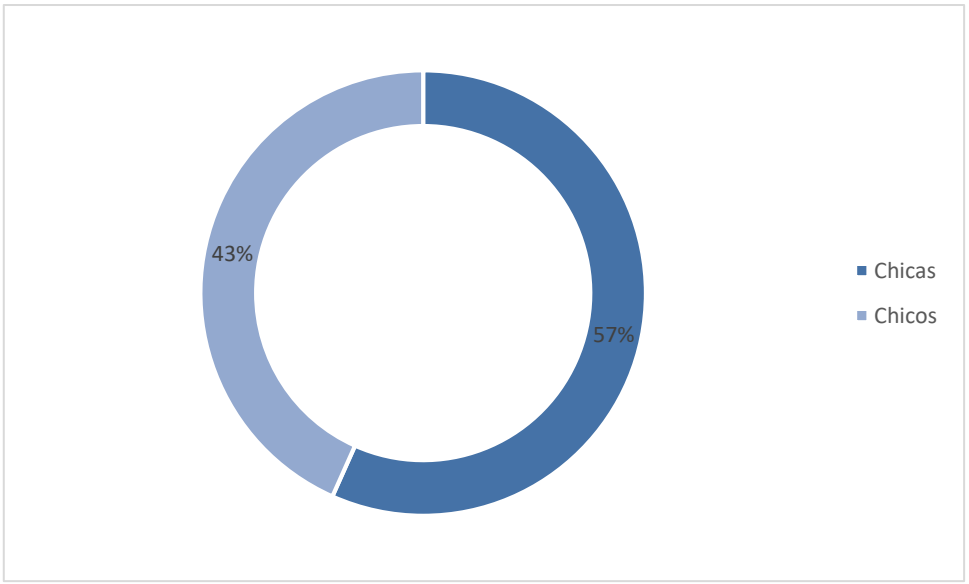
Esta tipología de ciberacoso también presenta una prevalencia baja en comparación con el resto de tipos de ciberacoso, siendo de un 6% (n = 404) el porcentaje de alumnos que ha afirmado haber sido víctima de suplantación de identidad en el último año. En el caso de los pequeños, la prevalencia es de casi un 4%, mientras que en el grupo de alumnos de mayor edad la cifra asciende a casi un 7%.

Gráfico 86. *Prevalencia de alumnos víctimas de suplantación de identidad a través de Internet*



Del 6% de alumnos cuya identidad ha sido suplantada a través de Internet, el 43% son chicos (n = 175) y el 57% son chicas (n = 229).

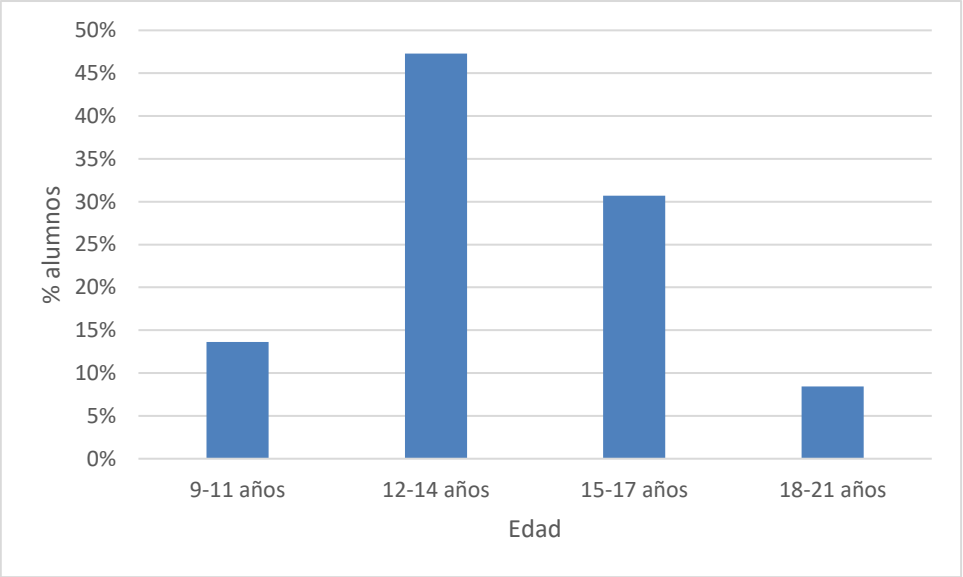
Gráfico 87. *Prevalencia de alumnos víctimas de suplantación de identidad a través de Internet según sexo*



En cuanto a la distribución de las víctimas de este tipo de ciberacoso, se observa que el 14% tiene entre 9 y 11 años (n = 55), el 47% tiene entre 12 y 14 años (n =

191), el 31% tiene entre 15 y 17 años (n = 124) y el 8% restante tiene entre 18 y 21 años (n = 34).

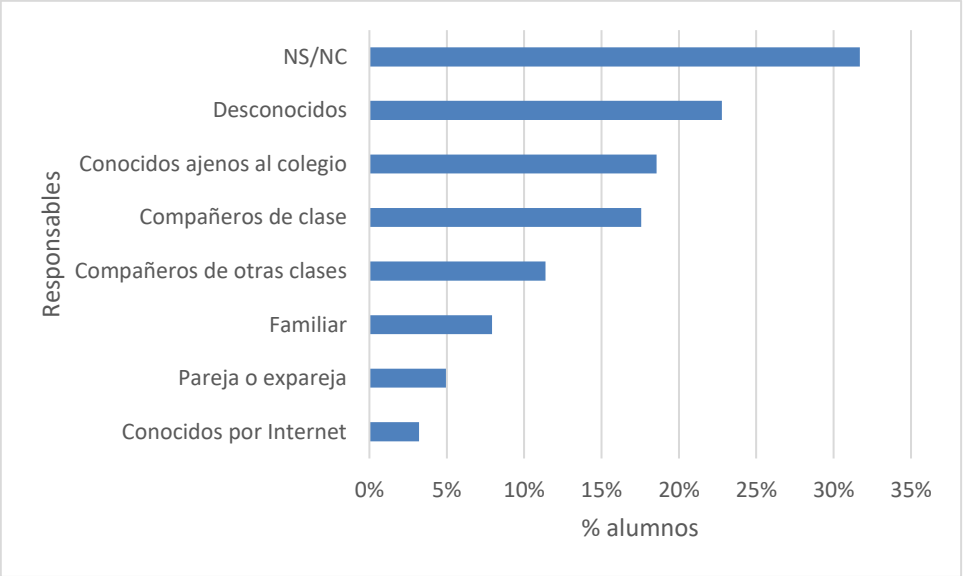
Gráfico 88. *Prevalencia de alumnos víctimas de suplantación de identidad a través de Internet según edad*



Esta es la tipología de ciberacoso donde más alumnos coinciden en afirmar que no saben quién fue el responsable de este ataque, alcanzado una prevalencia global del 32% la categoría "NS/NC", seguida de la categoría "Desconocidos" con un 23% de los alumnos. Entre los más jóvenes, cabe destacar que un 22% y un 18% afirma no saber quién fue el responsable o que éste era desconocido, respectivamente. Asimismo, cabe destacar que casi un 19% afirma que los responsables fueron compañeros de clase.

Entre los más grandes, la situación se repite. Un 35,4% de alumnos afirma que no sabe quién fue el responsable, seguido de un 24,7% que afirma que el responsable era una persona desconocida. La tercera categoría con una mayor prevalencia es la de "Conocidos ajenos al colegio" (un 19,6% de los alumnos).

Gráfico 89. *Responsables de la suplantación de identidad según las víctimas*

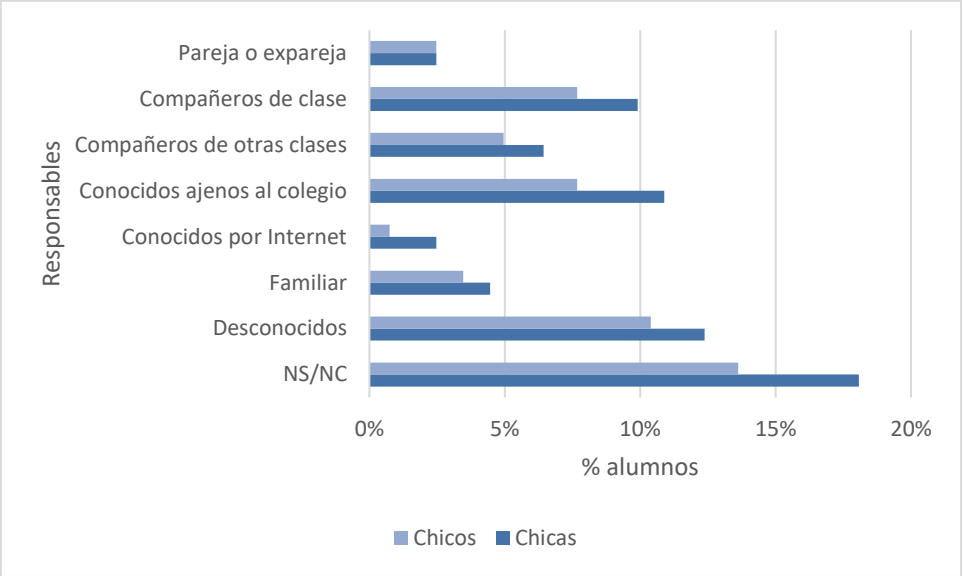


De los alumnos que han respondido "NS/NC", un 18% (n = 73) han sido chicas y un 14% (n = 55) chicos. Ambos coinciden, con apenas diferencia de porcentaje, en que los conocidos por internet o la pareja o expareja son los menos responsables.

Tanto chicos como chicas, en un 14% y un 18% de los casos, respectivamente, han informado que no saben o que prefieren no responder quién es el responsable de la suplantación de identidad. Muy de cerca, un 12% de chicas y un 10% de chicos han comunicado que los responsables fueron personas desconocidas.

En cuanto a las categorías con menos representación se encuentran, con un 2% de chicas y un 1% de chicos, los conocidos por Internet, seguidas de la pareja o expareja (un 2% tanto de chicos como de chicas).

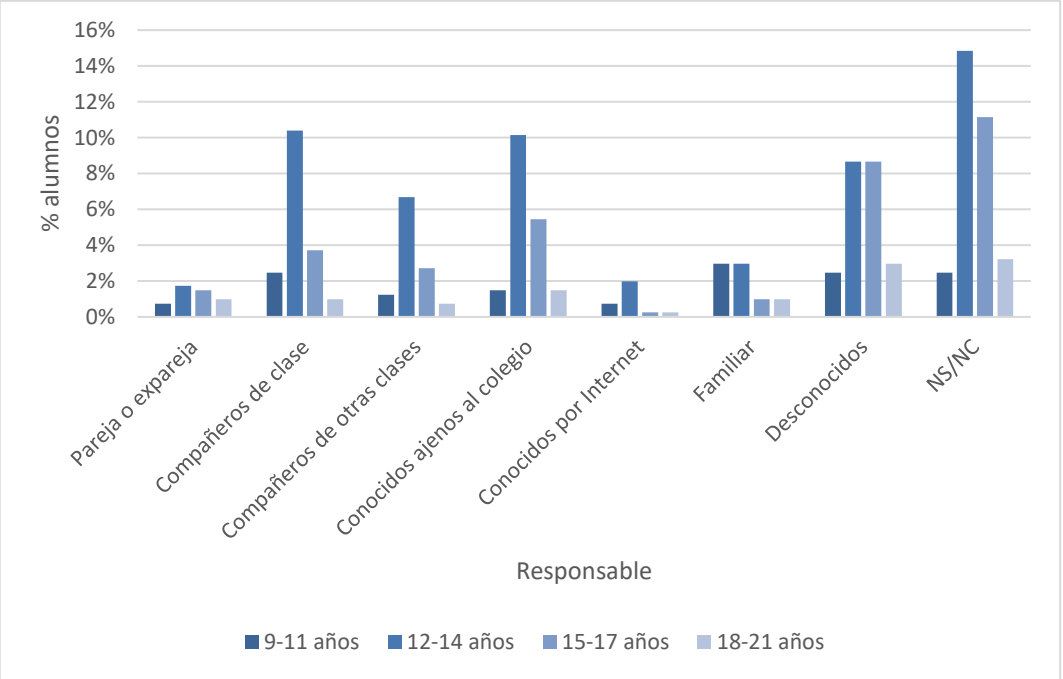
Gráfico 90. *Responsables de la suplantación de identidad según el sexo de la víctima*



Tanto los jóvenes que tienen entre 12 y 14 años, como lo que tienen entre 15 y 17 o entre 18 y 21 años han optado por la opción de "no sabe/no contesta" para hacer mención a los principales responsables de suplantar la identidad, con una prevalencia de un 15%, un 11% y un 3%, respectivamente. Por su parte, los jóvenes con edades entre los 9 y los 11 años consideran, en un 3% de los casos, que los principales responsables de este tipo de ciberacoso fueron familiares.

Por el contrario, la categoría de responsables menos frecuente en prácticamente todas las franjas de edad es la que hace referencia a las personas conocidas a través de Internet.

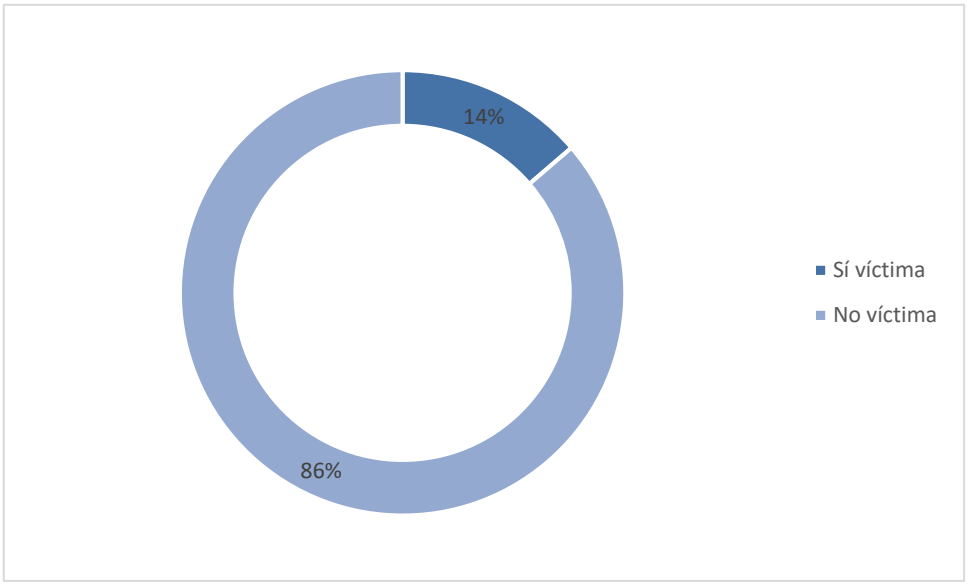
Gráfico 91. *Responsables de la suplantación de identidad según la edad de la víctima*



10. Contacto repetido no deseado

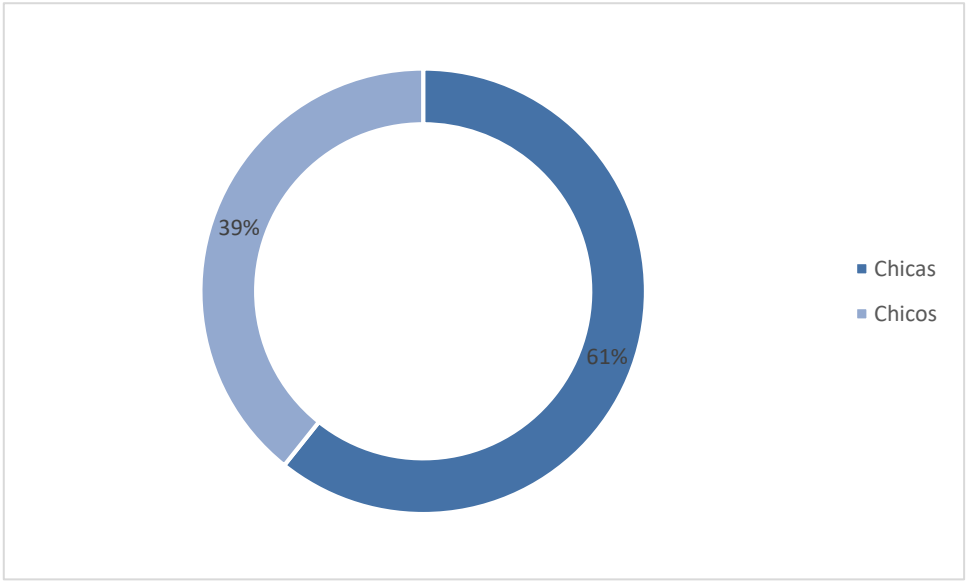
Finalmente, esta es una de las tipologías, junto con los rumores, los insultos, el acceso a las cuentas personales y la publicación de fotos o vídeos privados, que presenta una mayor prevalencia de víctimas. Más concretamente, el 14% (n = 998) de los alumnos afirma haber sido víctimas de contacto repetido no deseado en el último año. Entre los más pequeños, la prevalencia es de prácticamente el 12% de los alumnos, mientras que, en el caso de los más grandes, la cifra asciende al 15%.

Gráfico 92. *Prevalencia de alumnos víctimas de contacto repetido no deseado a través de Internet*



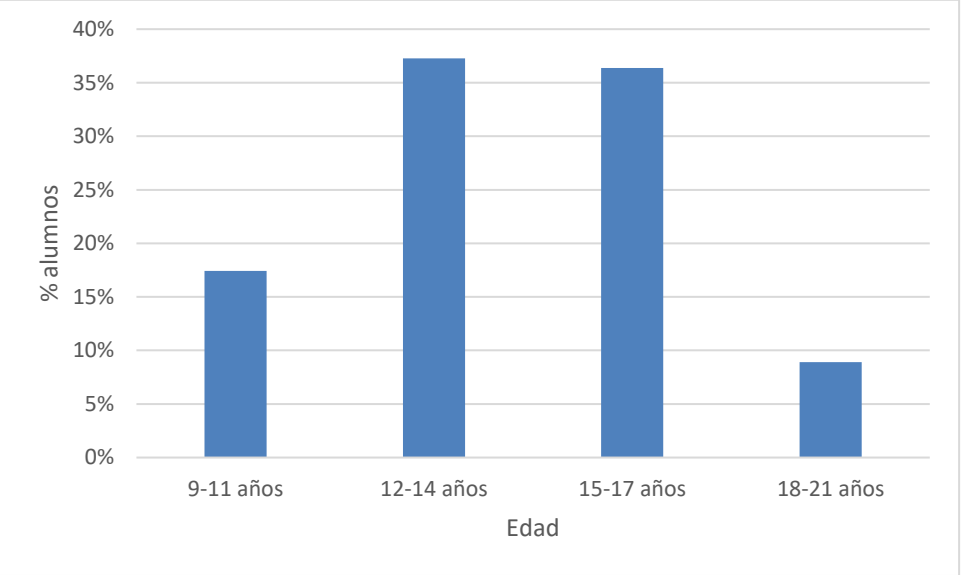
Con una diferencia de sexo mayor al resto de tipos de ciberacoso, el 61% de víctimas de contacto repetido no deseado a través de Internet son chicas (n = 606), mientras que el 39% restante son chicos (n = 392).

Gráfico 93. *Prevalencia de alumnos víctimas de contacto repetido no deseado a través de Internet según sexo*



Respecto a la distribución de las víctimas de este tipo de ciberacoso, se observa que el 14% tiene entre 9 y 11 años (n = 55), el 47% tiene entre 12 y 14 años (n = 191), el 31% tiene entre 15 y 17 años (n = 124) y el 8% restante tiene entre 18 y 21 años (n = 34).

Gráfico 94. *Prevalencia de alumnos víctimas de contacto repetido no deseado a través de Internet según edad*

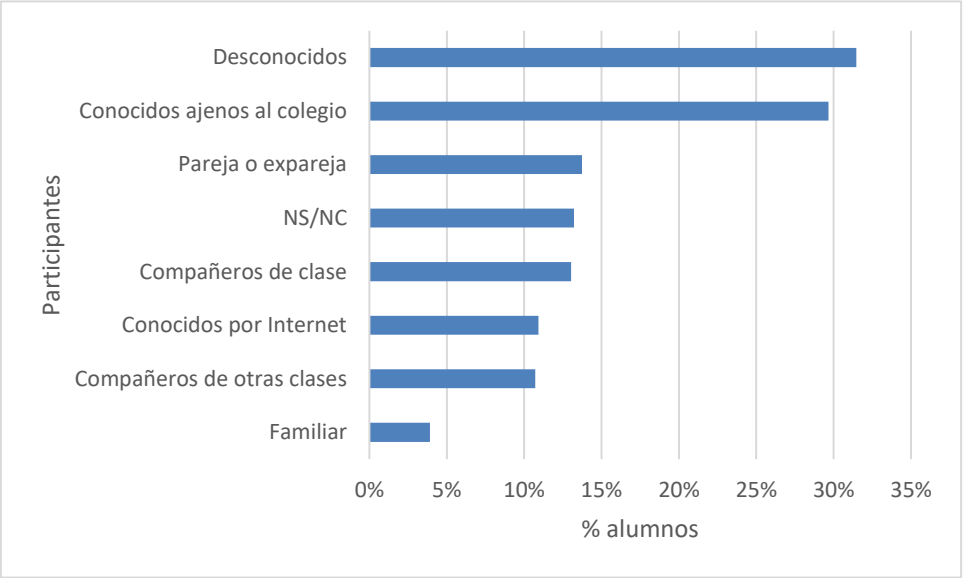


En este caso, las categorías de "Desconocidos" y "Pareja o expareja" vuelven a tener prevalencias elevadas en comparación con el resto de tipologías de ciberacoso (un 31% y un 14%, respectivamente). Asimismo, también es bastante frecuente que los responsables del acoso sean conocidos ajenos al colegio (un 30% de los alumnos).

De forma más concreta, entre los alumnos pequeños la mayor parte de responsables son desconocidos (un 26,6%), conocidos ajenos al colegio (un 23,1%) y compañeros de clase (un 20,9%). Entre los más grandes, las dos primeras categorías más frecuentes coinciden con la de los alumnos más pequeños, con un 34% y un 33% de alumnos, respectivamente, mientras que la tercera categoría de responsables más frecuente es la de la Pareja o expareja,

con un 17%.

Gráfico 95. *Responsables del contacto repetido no deseado según las víctimas*

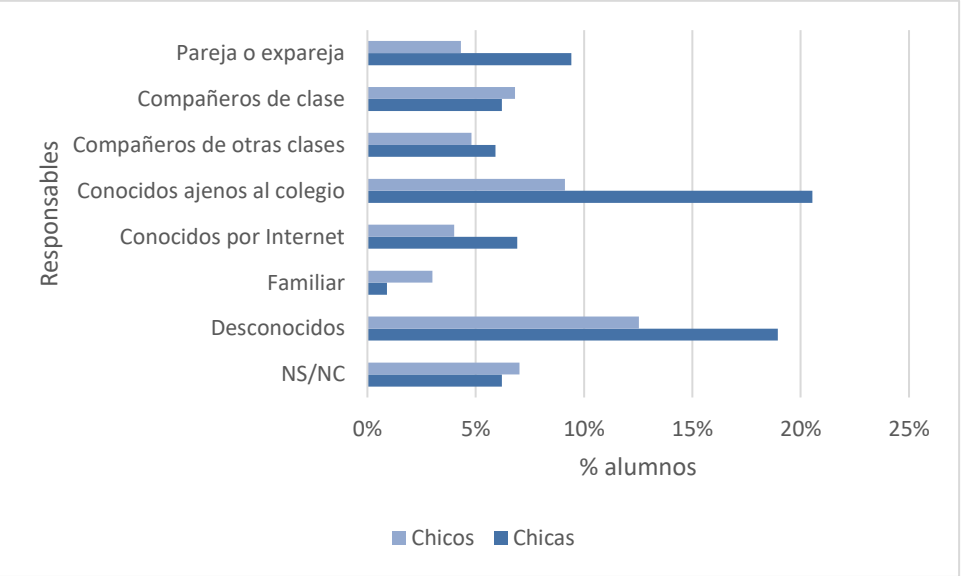


En relación al sexo de las víctimas, cabe destacar que un 21% de las chicas considera que el principal responsable del contacto repetido no deseado es un conocido ajeno al colegio, seguido de un 19% que considera que el principal responsable es alguien desconocido.

En cuanto a los chicos, la información se invierte. Un mayor porcentaje de chicos (un 13%) considera que el responsable es alguien desconocido, seguido de un 9% que afirma que el responsable es un conocido ajeno al colegio.

Tanto chicos como chicas coinciden a la hora de afirmar que los familiares son las personas que menos han realizado este tipo de ciberacoso, con un 3% en el caso de los chicos y un 1% en el caso de las chicas.

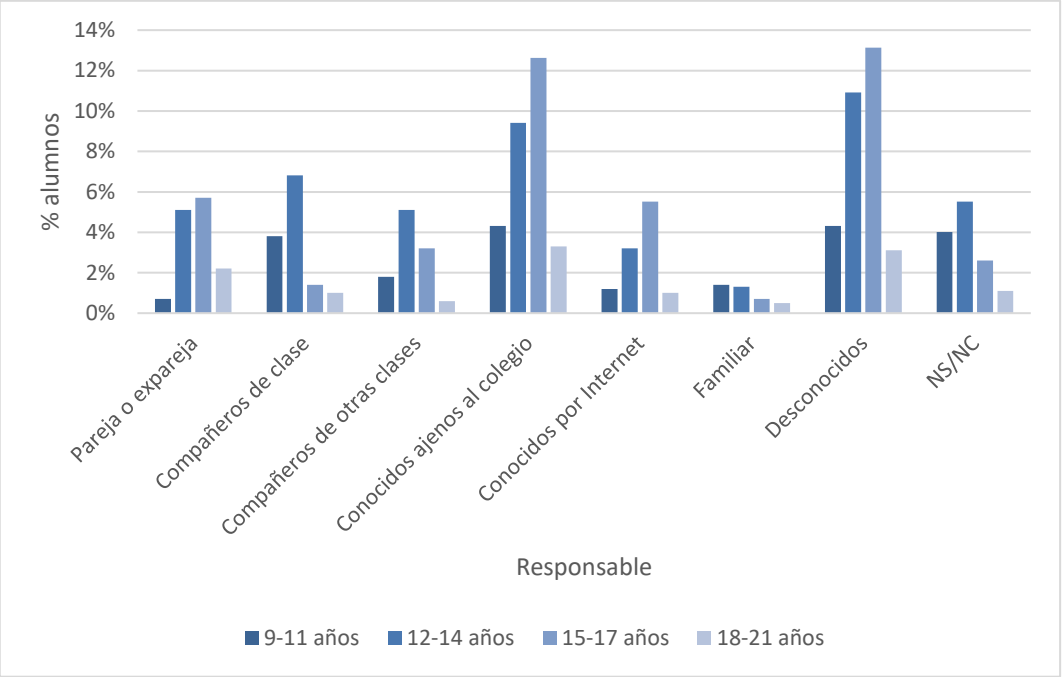
Gráfico 96. *Responsables del contacto repetido no deseado según el sexo de la víctima*



En este último tipo de ciberacoso existen bastantes coincidencias entre los alumnos de una misma franja de edad a la hora de afirmar quien fue el responsable principal del contacto repetido no deseado. Más concretamente, los alumnos que tienen entre 9 y 11 años coinciden, en un 4% de los casos, que los principales responsables fueron compañeros de clase, conocidos ajenos al colegio, personas desconocidas o directamente han preferido no responder.

Los alumnos de 12 a 14 años afirman, en un 11% de los casos, que el principal responsable fue una persona desconocida. Los que tienen entre 15 y 17 años coinciden con los compañeros de las dos franjas de edad anteriores al afirmar que los principales responsables fueron personas desconocidas (un 13%). Sin embargo, también es un 13% de alumnos de esta tercera franja de edad quien afirma que el principal responsable fue una persona conocida ajena al colegio. Finalmente, los alumnos de 18 a 21 años afirman, en un 3% de los casos, que los principales responsables fueron conocidos ajenos al colegio y personas desconocidas.

Gráfico 97. *Responsables del contacto repetido no deseado según la edad de la víctima*



b) Ciberacoso sexual

El ciberacoso sexual es un tipo de ciberacoso en el que se engloban distintas conductas que menoscaban la integridad sexual o la libre formación de la sexualidad de las víctimas. En este estudio se han decidido analizar siete conductas distintas de ciberacoso sexual, las cuales son:

1. Enviar imágenes sexuales creando incomodidad
2. Enviar mensajes obscenos o peticiones sexuales creando incomodidad
3. Obligar con violencia o intimidación o insistiendo repetidamente a enviar fotos o vídeos con contenido sexual o erótico
4. Obligar con violencia o intimidación o insistiendo repetidamente a realizar comportamientos sexuales online
5. Amenazar con publicar o difundir imágenes o vídeos personales de

carácter sexual si no se lleva a cabo una determinada conducta

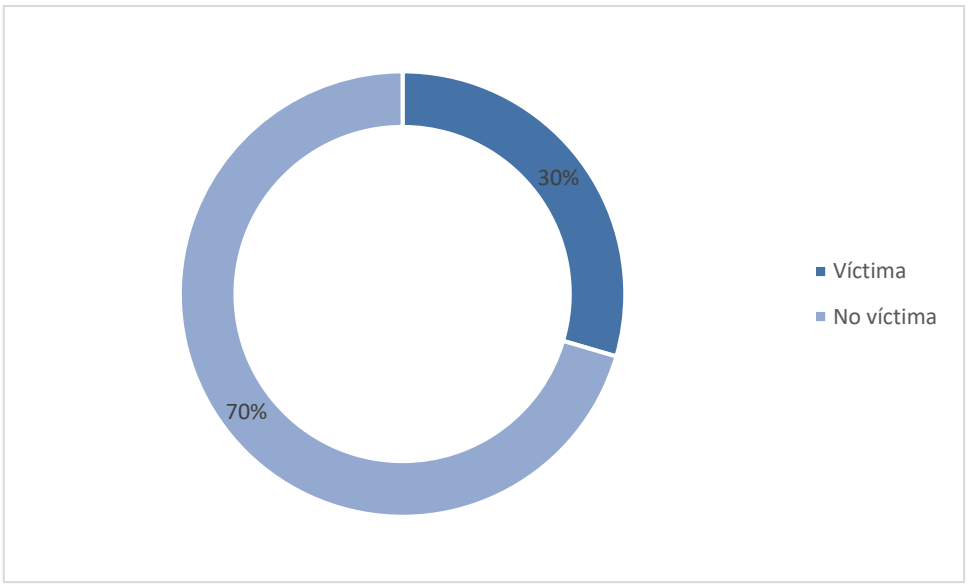
6. Publicar o difundir fotos o vídeos de carácter sexual o erótico sin consentimiento

7. Presionar, insistiendo repetidamente, para quedar en persona

En ese estudio, el ciberacoso sexual solo ha sido preguntado a los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM por considerar que el contenido no era adecuado para los alumnos más jóvenes, es decir, los de 5º y 6º de primaria y 1º de ESO. Es por ello que los datos presentados a lo largo de este apartado no serán sobre el total de alumnos de todo el estudio (n = 7282), sino sobre el número de alumnos que forman parte de los cursos anteriormente citados (n = 4329).

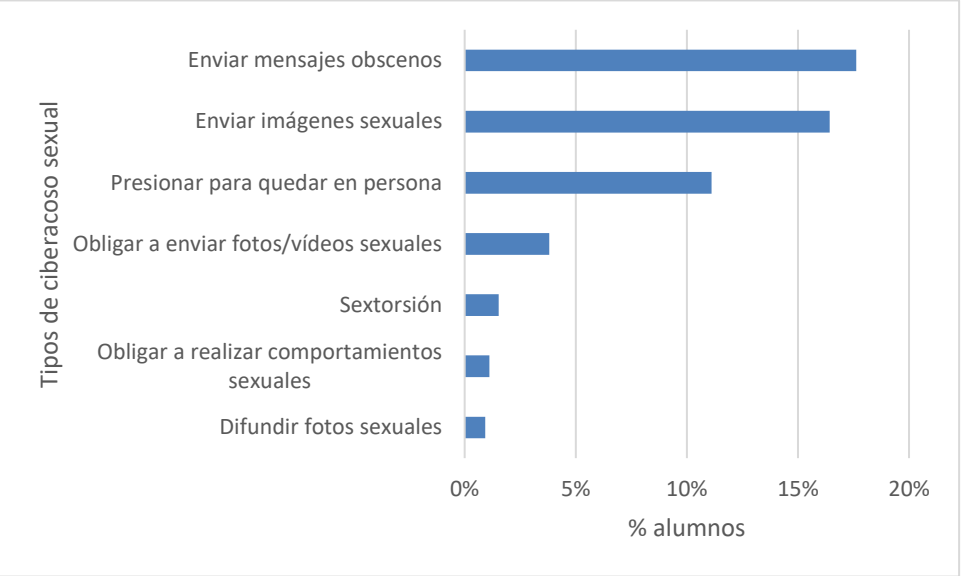
Desde un punto de vista global del ciberacoso sexual, cabe destacar que el 30% de jóvenes encuestados (n = 1278) afirma haber sido víctima de este tipo de ciberacoso, mientras que el 70% no ha sido víctima (n = 3051), tal y como se observa en el siguiente gráfico.

Gráfico 98. *Prevalencia de alumnos que han sido víctimas de ciberacoso sexual*



En cuanto a los distintos tipos de ciberacoso sexual mencionados anteriormente, el más frecuente al que se han visto expuestos los alumnos es el de recibir mensajes obscenos (un 18% de los alumnos han sido víctimas). Después de este tipo, los dos siguientes más frecuentes son enviar imágenes sexuales y presionar al alumno para quedar en persona, con un 16% y un 11% de alumnos víctimas, respectivamente.

Gráfico 99. *Prevalencia de los distintos tipos de ciberacoso sexual*



A continuación, se analiza en mayor profundidad cada conducta de ciberacoso sexual. Para una mejor lectura y comprensión del fenómeno, las 7 tipologías de ciberacoso sexual expuestas anteriormente se agruparán en los siguientes cinco apartados: 1) Exposición involuntaria a contenido sexual, 2) Coacciones sexuales, 3) Sextorsión, 4) Publicación o difusión de imágenes o vídeos sexuales sin consentimiento, 5) Presionar para quedar en persona.

1. Exposición involuntaria a contenido sexual

La exposición involuntaria a contenido sexual incluye dos tipos de conductas: 1) recibir imágenes sexuales y 2) recibir mensajes obscenos. En cuanto al primer

grupo, se observa una prevalencia del 16% de alumnos (n = 711), mientras que en el segundo grupo esta prevalencia aumenta dos puntos hasta el 18% (n = 763).

Gráfico 100. *Prevalencia de alumnos víctimas de haber recibido imágenes sexuales en el último año*

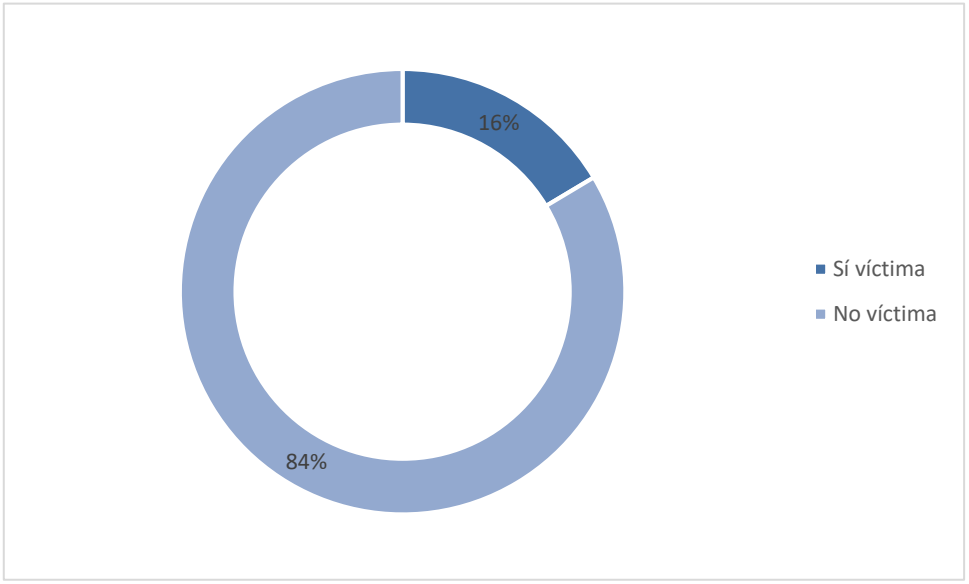
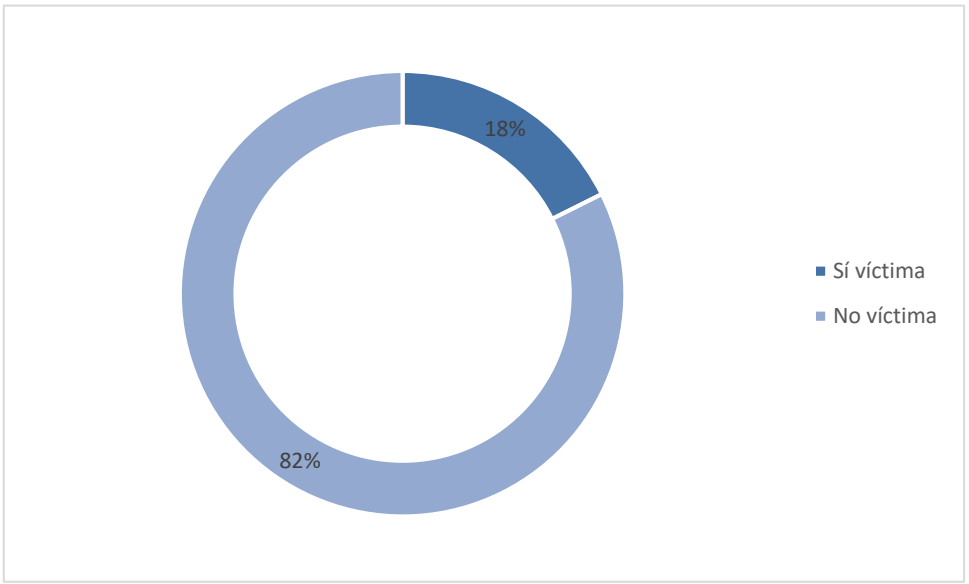


Gráfico 101. *Prevalencia de alumnos víctimas de haber recibido comentarios obscenos en el último año*



Del 16% de alumnos que ha afirmado haber sido víctima de recibir imágenes

sexuales que le han hecho sentir incómodo, un 44% son chicos (n = 313) y un 56% son chicas (n = 398). En el caso de haber recibido comentarios obscenos, la diferencia entre chicos y chicas es mayor, ya que casi un 70% de las víctimas son chicas (n = 521) y un 32% son chicos (n = 242).

Gráfico 102. *Prevalencia de alumnos víctimas de haber recibido imágenes sexuales en el último año según sexo*

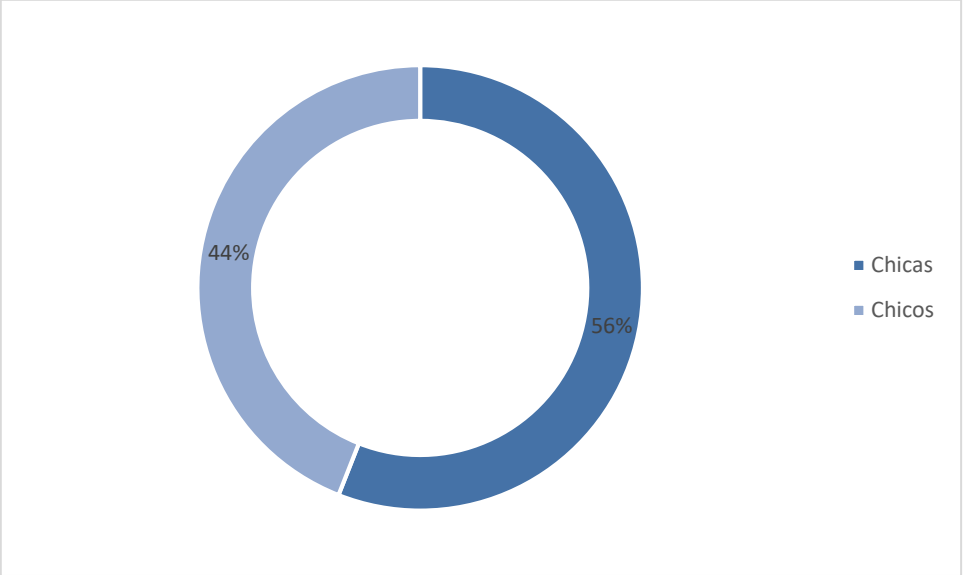
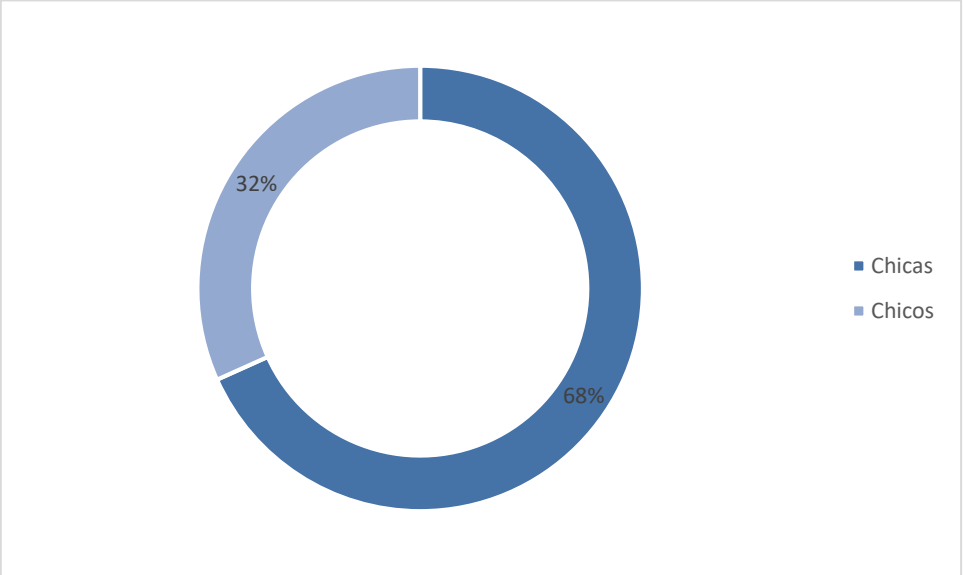


Gráfico 103. *Prevalencia de alumnos víctimas de haber recibido comentarios obscenos en el último año según sexo*



Si se analizan los datos de victimización según la edad de los alumnos, se observa que del 16% de víctimas de haber recibido imágenes sexuales, el 30% tiene entre 11 y 14 años (n = 213), el 58% tiene entre 15 y 17 años (n = 410) y el 12% entre 18 y 21 años (n = 88). En cuanto a la conducta de recibir mensajes obscenos, los porcentajes son idénticos: el 30% tiene entre 11 y 14 años (n = 228), el 58% tiene entre 15 y 17 años (n = 444) y el 12% entre 18 y 21 años (n = 91).

Gráfico 104. *Prevalencia de alumnos víctimas de haber recibido imágenes sexuales en el último año según edad*

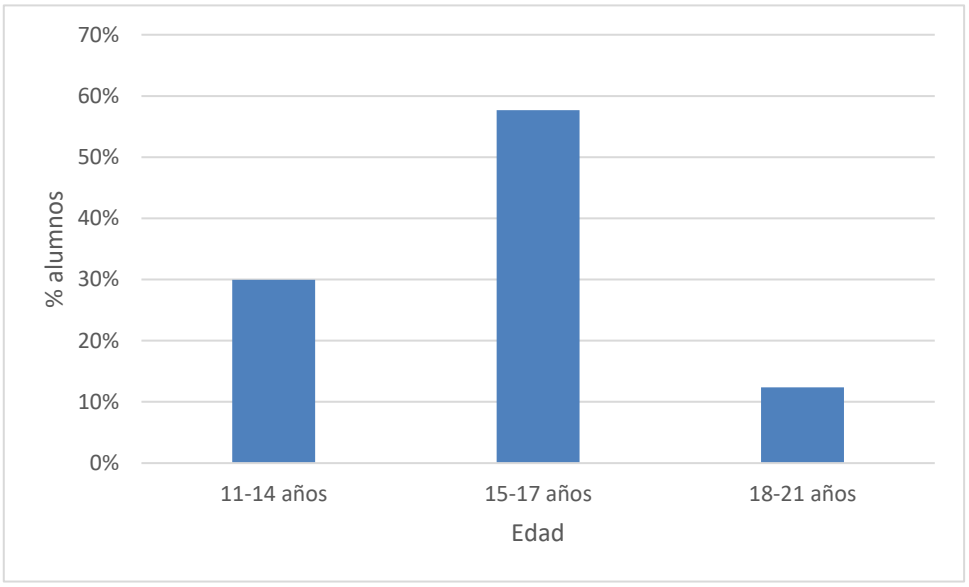
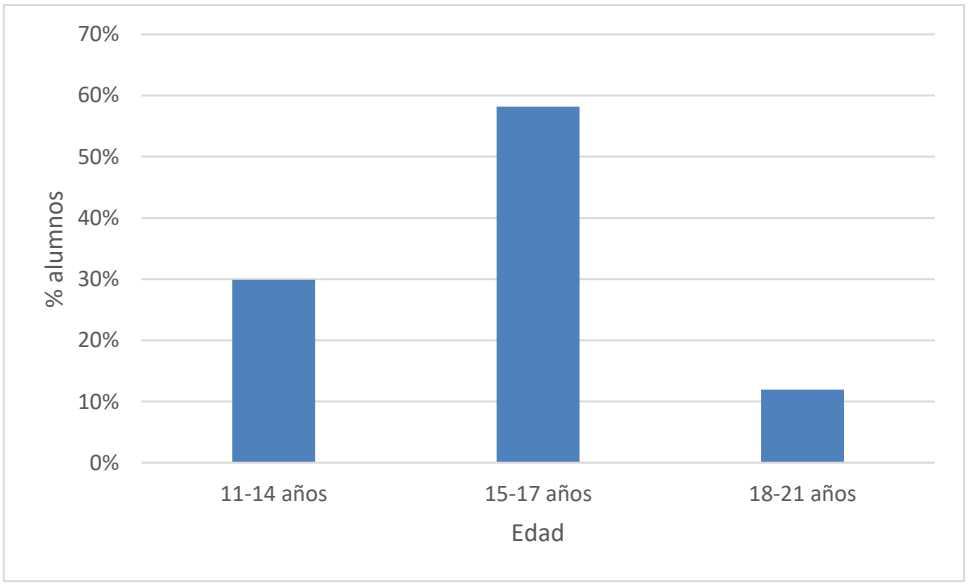


Gráfico 105. *Prevalencia de alumnos víctimas de haber recibido comentarios obscenos en el último año según edad*



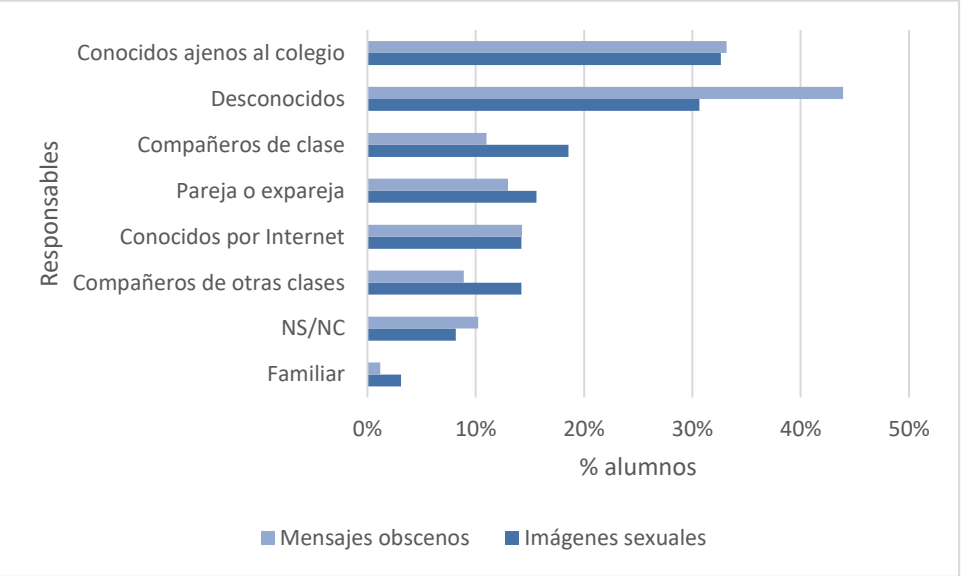
Existen diferencias entre los responsables de enviar fotos y comentarios sexuales a los alumnos haciéndoles sentir incómodos o molestos. En cuanto al envío de imágenes sexuales, los alumnos afirman, en un 33% de los casos, que los

responsables fueron conocidos ajenos del colegio, seguido de un 31% que afirma que los responsables fueron desconocidos y un 19% que afirma que eran compañeros de clase.

Respecto a los comentarios obscenos, cabe destacar que la categoría más frecuente es la de "Desconocidos", con un 44% de alumnos que afirma que no conocía a los responsables de esta conducta. Seguidamente, los alumnos afirman, en un 33% y 14% de los casos, que los responsables más frecuentes son conocidos ajenos al colegio y personas conocidas por Internet, respectivamente.

Los datos parecen indicar que la exposición involuntaria a contenido sexual no viene provocada por compañeros del colegio, sino que es algo externo. Sin embargo, ello no quiere decir que no afecte al rendimiento escolar ni a la convivencia, por lo que los resultados aquí arrojados deben tenerse en cuenta a la hora de diseñar acciones preventivas.

Gráfico 106. *Responsables de enviar imágenes sexuales y mensajes obscenos*



Tanto en la conducta de enviar imágenes sexuales como en la de enviar mensajes obscenos, las chicas consideran, en un 24% y 34% de los casos, respectivamente,

que los principales responsables son personas desconocidas. En cuanto a los chicos, la situación es un tanto distinta, ya que un 16% de los chicos considera que el principal responsable de enviar imágenes sexuales es un conocido ajeno al colegio, mientras que un 10% considera que el principal responsable de enviar mensajes obscenos fue una persona desconocida.

En lo que sí coinciden chicos y chicas es en afirmar que, de nuevo, los familiares son las personas que menos realizan conductas de ciberacoso y, en este caso concreto, de estos dos subtipos de ciberacoso sexual.

Gráfico 107. *Responsables de enviar imágenes sexuales según el sexo de la víctima*

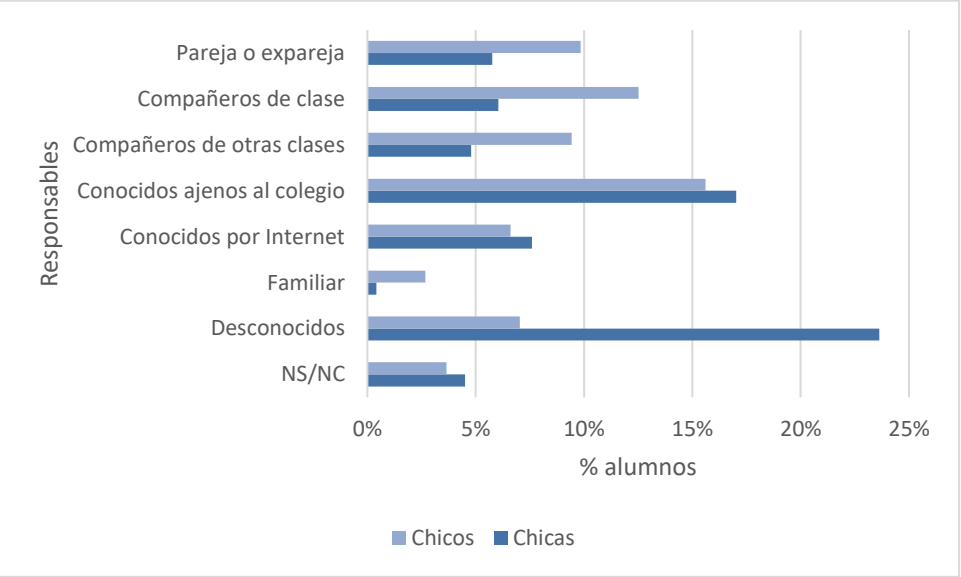
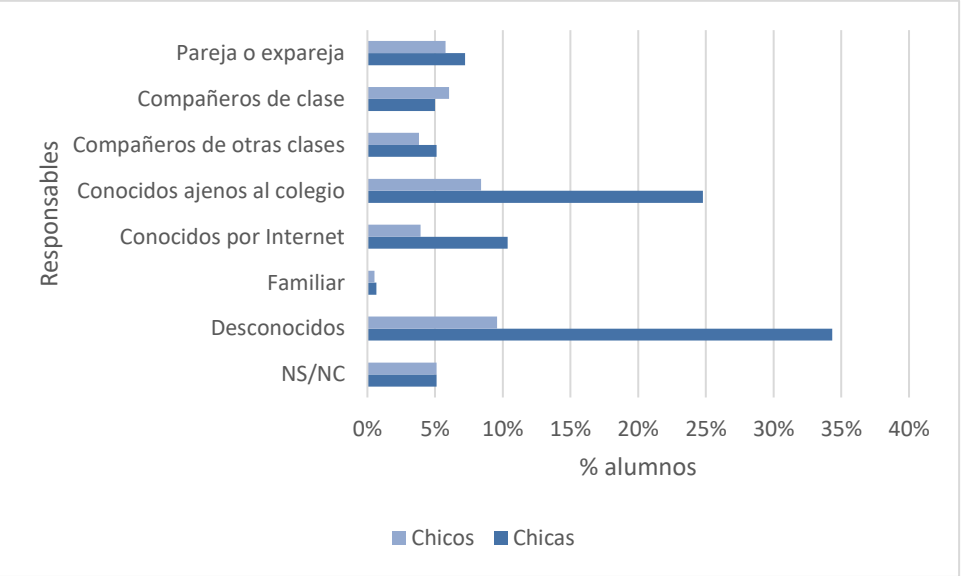


Gráfico 108. *Responsables de enviar mensajes obscenos según el sexo de la víctima*



En cuanto a los responsables de estos dos tipos de ciberacoso sexual según la edad de las víctimas, es interesante destacar los siguientes datos. En primer lugar, en cuanto al tipo de ciberacoso sexual consistente en enviar imágenes sexuales, los alumnos entre 11 y 14 años informan que los principales responsables fueron compañeros de clase y conocidos ajenos al colegio (un 8% de los casos en ambas categorías). En la franja de edad de 15 a 17 años, los principales responsables fueron conocidos ajenos al colegio y desconocidos (un 20% de alumnos en ambos casos). Finalmente, en la franja de edad de 18 a 21 años, con un 5% de alumnos que hacen esta afirmación, se observa que los responsables más comunes fueron conocidos ajenos al colegio, seguido de conocidos por Internet y desconocidos (un 3% en ambas categorías).

En segundo lugar, en relación al otro tipo de ciberacoso sexual analizado en este apartado (enviar mensajes obscenos), cabe destacar que los alumnos de 11 a 14 años informan que los principales responsables fueron conocidos ajenos al colegio y desconocidos (un 9% de alumnos en ambas categorías). En la franja de edad de 15 a 17 años, la categoría de responsable que presenta un mayor

consenso entre los alumnos, en un 29% de los casos, corresponde a personas desconocidas. Por último, los alumnos entre 18 y 21 años coinciden con el resto de franjas de edad a la hora de afirmar que el responsable más común fue una persona desconocida.

En conclusión, los jóvenes entre 15 y 17 años coinciden en ambos subtipos de ciberacoso sexual que los principales responsables fueron desconocidos, mientras que en los otros dos rangos de edad existen diferencias en cuanto a los responsables de enviar imágenes sexuales y mensajes obscenos.

Gráfico 109. *Responsables de enviar imágenes sexuales según la edad de la víctima*

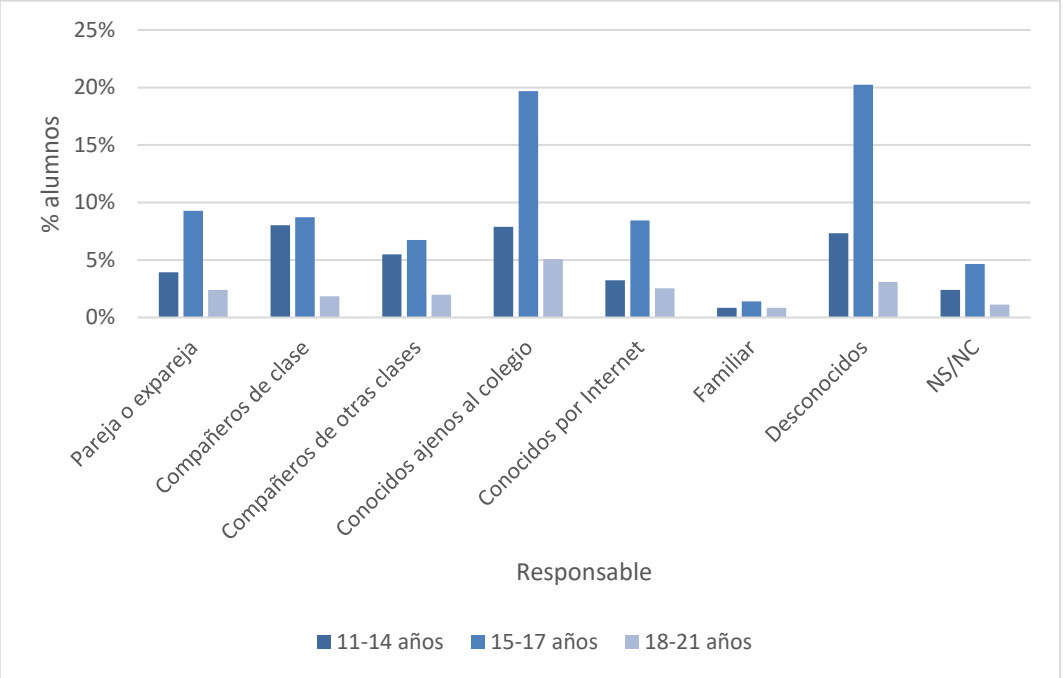
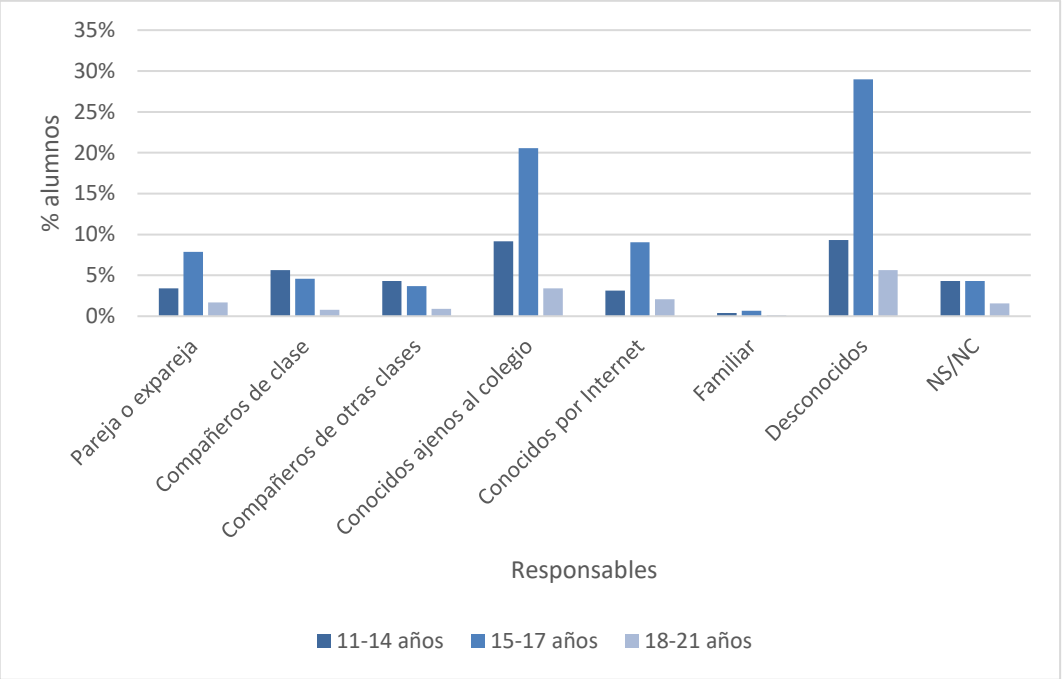
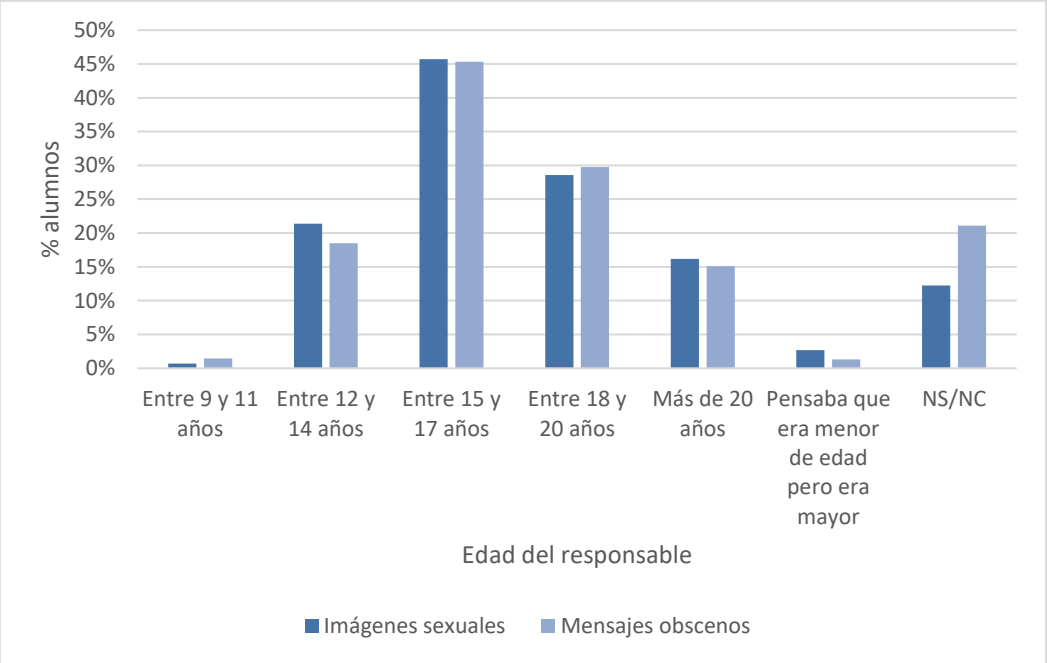


Gráfico 110. *Responsables de enviar mensajes obscenos según la edad de la víctima*



Finalmente, en cuanto a la edad de los responsables, tanto en el caso de recibir imágenes sexuales como mensajes obscenos, los gráficos indican que las edades son bastantes similares. La mayor parte de responsables, en ambos casos, se encuentra entre los 12 y los 20 años y, más concretamente, entre los 15 y los 17.

Gráfico 111. *Edad de los responsables de enviar imágenes sexuales y mensajes obscenos*



2. Coacciones sexuales

Las coacciones sexuales incluyen dos tipos de conductas llevadas a cabo con violencia o intimidación: 1) obligar a enviar imágenes o vídeos sexuales y 2) obligar a realizar comportamientos sexuales. En cuanto al primer grupo, se observa una prevalencia del 4% de alumnos (n = 165), mientras que en el segundo grupo esta prevalencia disminuye tres puntos hasta el 1% (n = 48). Como se observa, la prevalencia de víctimas en ambos tipos de coacciones sexuales es muy baja en comparación con otros tipos de ciberacoso sexual.

Gráfico 112. *Prevalencia de alumnos víctimas de haber sido obligados a enviar fotos/vídeos sexuales propios*

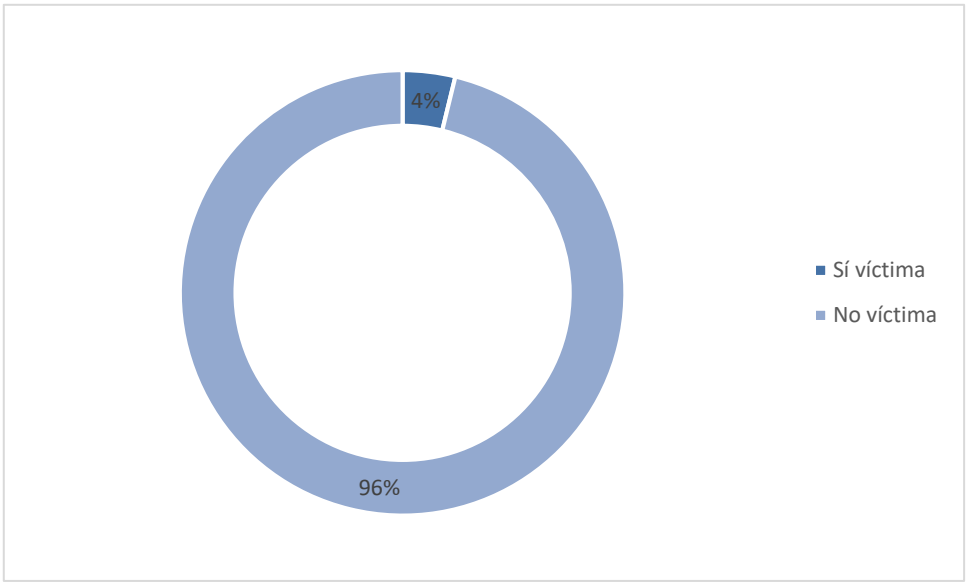
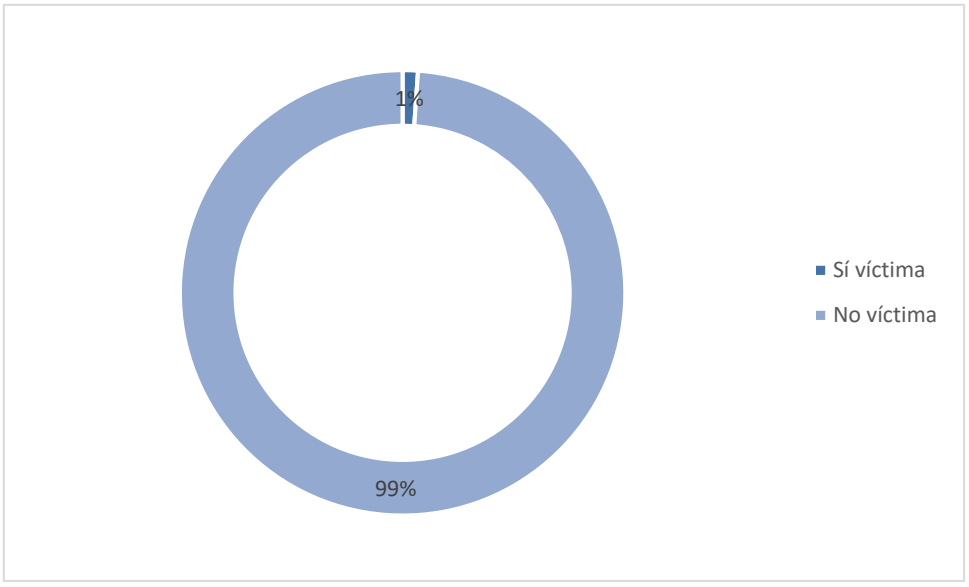


Gráfico 113. *Prevalencia de alumnos víctimas de haber sido obligados a realizar comportamientos sexuales*



Del 4% de los alumnos víctimas de haber sido obligados a enviar imágenes o vídeos sexuales, el 22% viene representado por los chicos (n = 36) y el 78% por las chicas (n = 129). Con una diferencia de sexo similar, en el caso de haber sido obligados a realizar comportamientos sexuales los chicos constituyen el 27% (n = 13) y las chicas el 73% (n = 35).

Gráfico 114. *Prevalencia de alumnos víctimas de haber sido obligados a enviar fotos o vídeos sexuales propios según sexo*

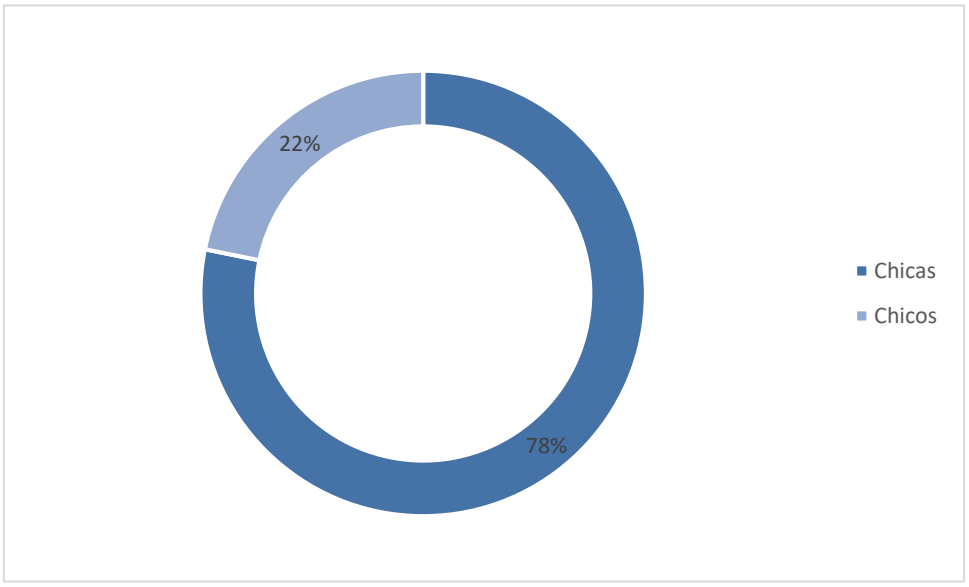
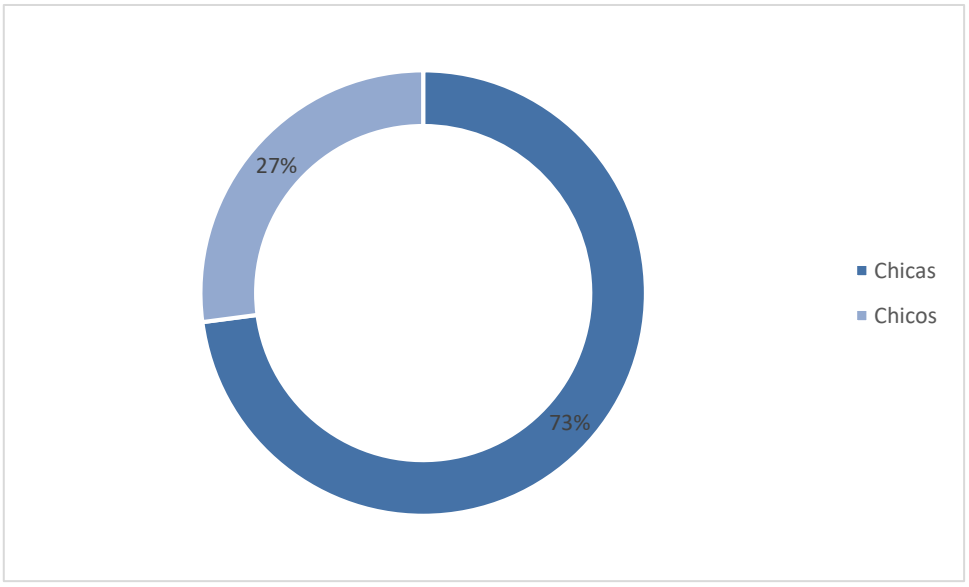


Gráfico 115. *Prevalencia de alumnos víctimas de haber sido obligados a realizar comportamientos sexuales según sexo*



En función de la edad, del 4% de alumnos víctimas de haber sido obligados a enviar imágenes sexuales, el 23% tiene entre 11 y 14 años (n = 38), el 63% tiene entre 15 y 17 años (n = 104) y el 14% tiene entre 18 y 21 (n = 23). Del 1% que ha

reportado que le obligaron a realizar comportamientos sexuales a través de Internet, el 29% tiene entre 11 y 14 años (n = 14), el 54% tiene entre 15 y 17 años (n = 26) y el 17% tiene entre 18 y 21 años (n = 8).

Gráfico 116. *Prevalencia de alumnos víctimas de haber sido obligados a enviar fotos o vídeos sexuales propios según edad*

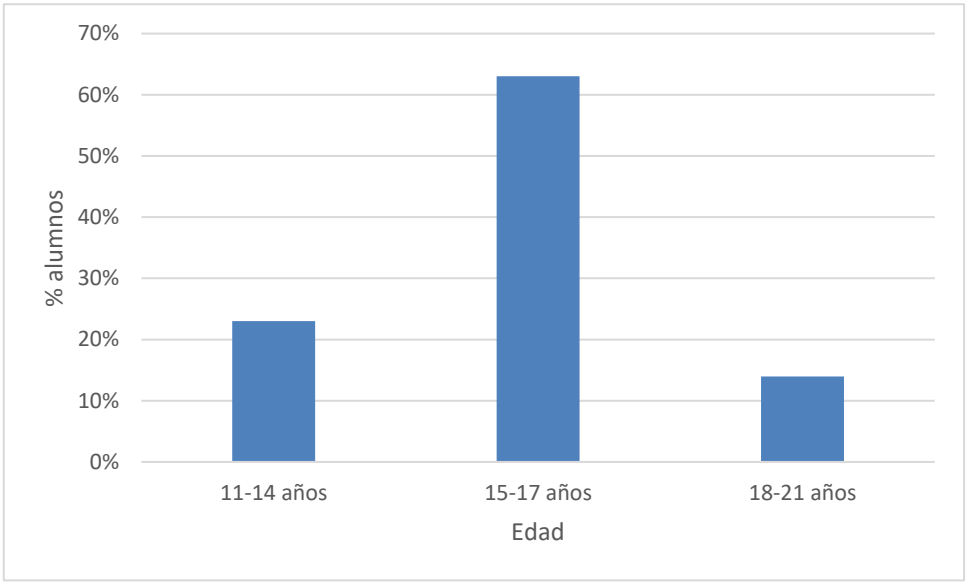
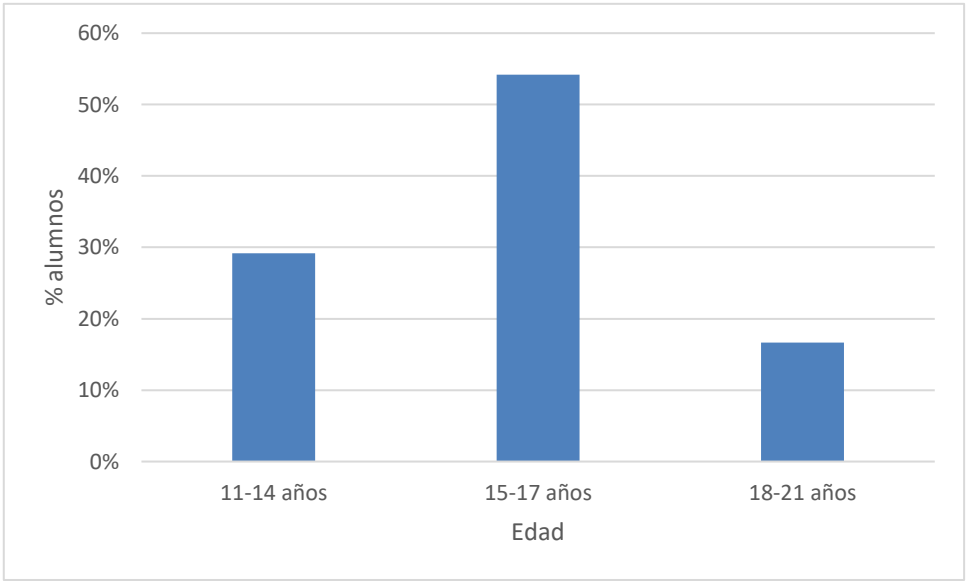


Gráfico 117. *Prevalencia de alumnos víctimas de haber sido obligados a realizar comportamientos sexuales según edad*

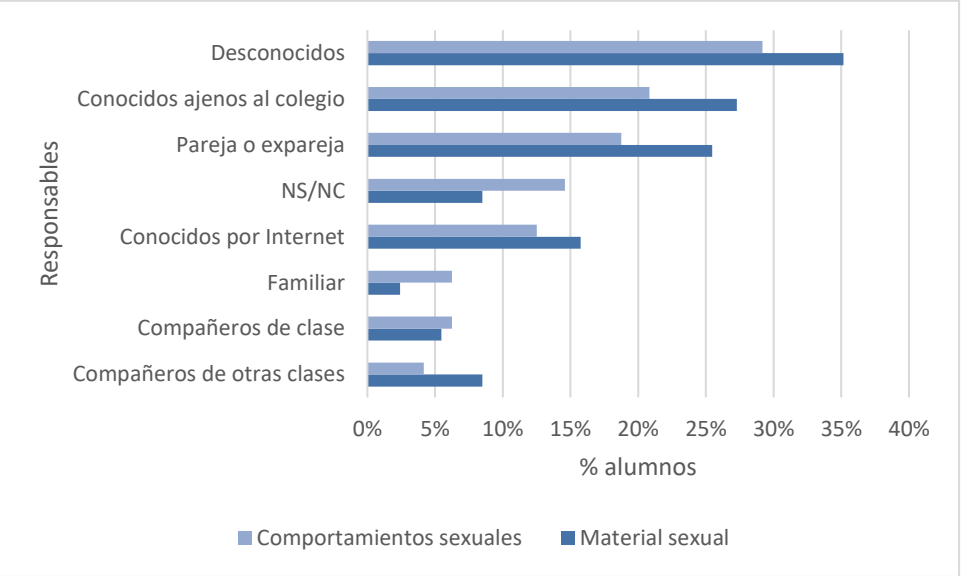


Existen diferencias entre los responsables de ambos tipos de coacción. En cuanto al tipo relacionado con obligar a enviar material sexual propio, los alumnos afirman, en un 35% de los casos, que los responsables fueron personas desconocidas, seguido de un 27% que afirma que los responsables fueron conocidos ajenos al colegio y un 25% que afirma que fue su pareja o expareja.

Respecto al segundo tipo de coacción, que se basa en obligar a realizar comportamientos sexuales, cabe destacar que la categoría más frecuente de responsables es la de desconocidos, con un 29% de los alumnos que afirma que no conocía a los responsables de esta conducta. A continuación, los alumnos afirman, en un 21% y 19% de los casos, que los responsables más frecuentes son conocidos ajenos al colegio y la pareja o expareja, respectivamente.

Los datos indican, a diferencia de la exposición involuntaria a contenido sexual, que en las coacciones sexuales el papel de la pareja o expareja del alumno tiene un papel relevante, sobre todo a la hora exigir material sexual. Además, en estos casos, dos de las categorías de responsables menos frecuentes son la de los "Compañeros de clase" y los "Compañeros de otras clases", lo que podría indicar, de nuevo, que no es un problema que proviene del ámbito escolar, pero que puede afectar de todos modos a los alumnos en ese contexto.

Gráfico 118. *Responsables de los dos tipos de coacciones sexuales*



En cuanto a las diferencias entre chicos y chicas, cabe destacar que un 25% de chicas afirma que tanto en la conducta de obligar a enviar material sexual como en la de obligar a realizar comportamientos sexuales, los principales responsables son personas desconocidas. En los chicos, en cambio, el principal responsable de obligar a enviar material sexual es una persona desconocida (un 10% de los chicos), mientras que en el segundo tipo de coacción los principales responsables son los familiares (un 6%).

En relación a los responsables con menor representación, y partiendo del primer tipo de coacción, un 1% de chicas y un 2% de chicos afirma que la categoría menos frecuente es la de los familiares. En cuanto al segundo tipo de coacción, ninguna chica afirma que alguno de los responsables sea un familiar, mientras que solo un 2% de chicos afirma que los responsables son compañeros de clase o de otras clases.

Gráfico 119. *Responsables de obligar a enviar fotos o vídeos sexuales propios según el sexo de la víctima*

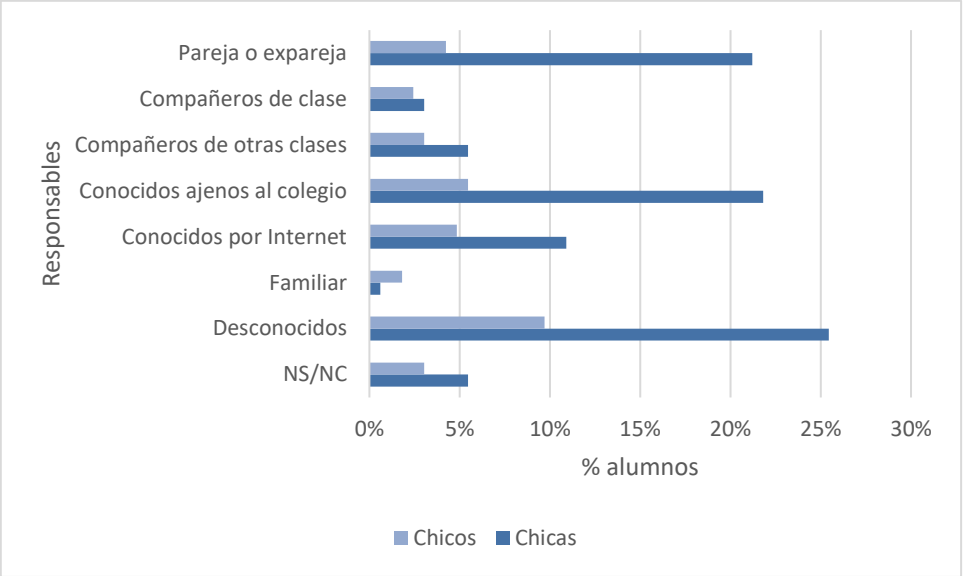
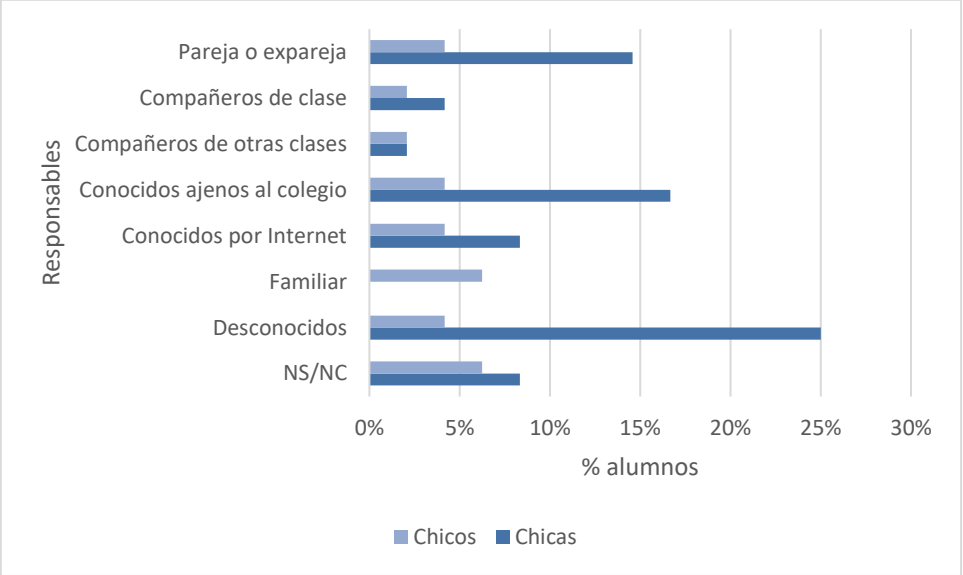


Gráfico 120. *Responsables de obligar a realizar comportamientos sexuales según el sexo de la víctima*



Respecto a las coacciones sexuales consistentes en obligar a enviar imágenes sexuales, los alumnos entre 11 y 14 años informan de que los principales responsables fueron, por un lado, personas desconocidas y, por el otro, la pareja o expareja (un 7% de alumnos en ambos casos). Tanto los alumnos de 15 a 17 años como los que tienen entre 18 y 21 años coinciden, en un 23% y 5% de los

casos, respectivamente, en que los responsables de este tipo de coacción sexual fueron personas desconocidas.

En cuanto al otro tipo de coacción sexual, consistente en obligar al alumno a realizar comportamientos sexuales a través de Internet, cabe destacar que en la franja de edad de 11 a 14 años los alumnos afirman, en un 13% de los casos, que el responsable fue una persona desconocida. En cambio, en la franja de edad de 15 a 17 años los alumnos informan, en un 17% de los casos, que el principal responsable fue una persona conocida ajena al colegio. Finalmente, en la franja de edad de 18 a 21 años el mayor porcentaje de alumnos coincide en que el responsable fue una persona desconocida (un 6% de alumnos). Asimismo, también un 6% de alumnos entre 18 y 21 años ha preferido no responder quien fue el responsable.

Gráfico 121. *Responsables de obligar a enviar fotos o vídeos sexuales propios según la edad de la víctima*

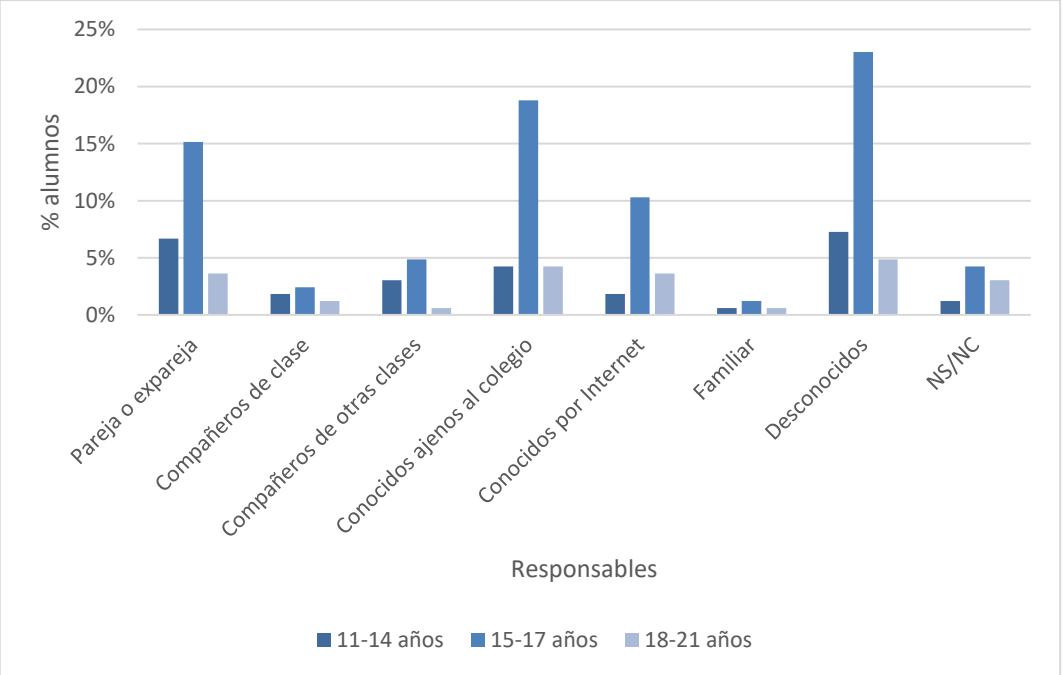
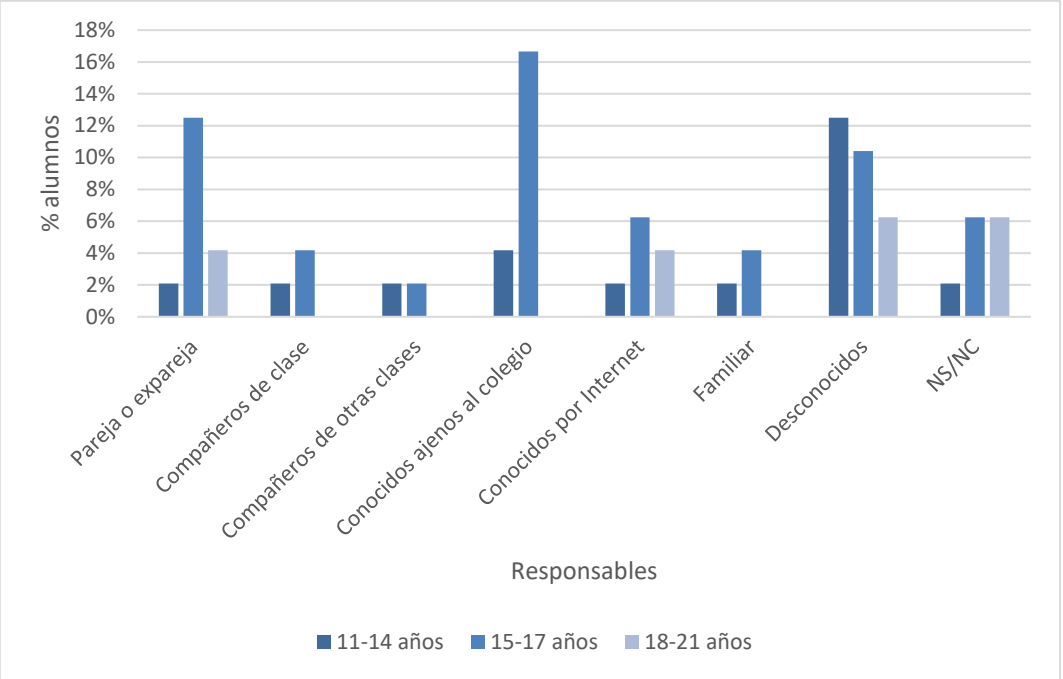
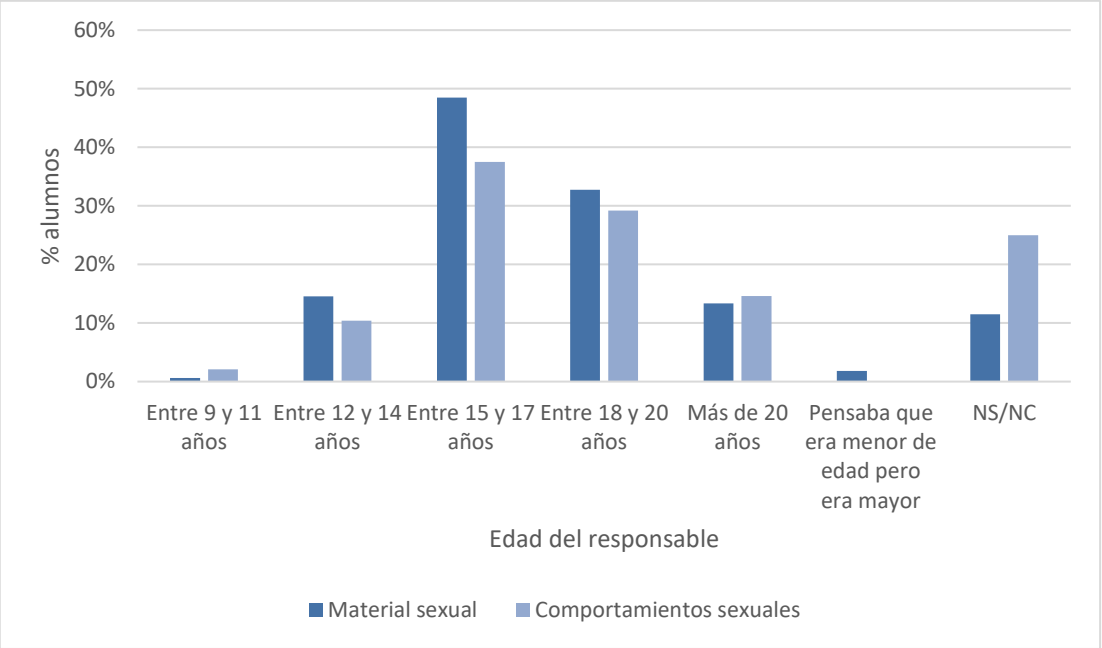


Gráfico 122. *Responsables de obligar a realizar comportamientos sexuales según la edad de la víctima*



Finalmente, en cuanto a la edad de los responsables de ambos tipos de coacciones, y de manera similar a la exposición involuntaria de contenido sexual, la mayor parte de responsables tiene entre 12 y 18 años y, más concretamente, entre 15 y 17 años. Especial mención requiere el hecho de que en las coacciones en las que se exige realizar comportamientos sexuales, existe un 25% de alumnos que afirma que desconoce la edad de la persona que le obligó a realizar dichos comportamientos.

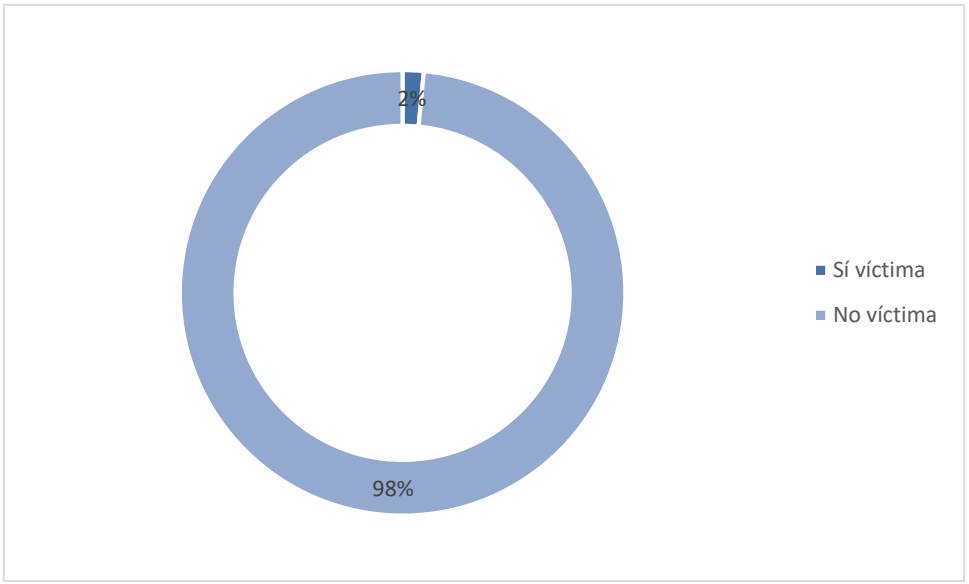
Gráfico 123. *Edad de la persona responsable de ambos tipos de coacciones sexuales*



3. Sextorsión

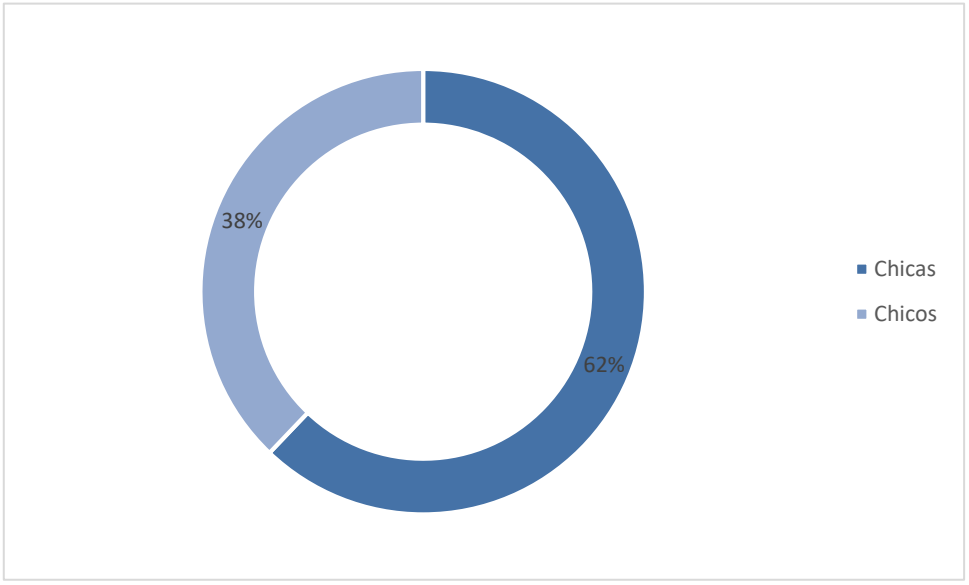
Las sextorsión consiste en chantajear y amenazar a alguien diciéndole que si no realiza una determinada conducta hará públicos vídeos o fotos sexuales suyos. En este sentido, la prevalencia de alumnos víctimas de este tipo de ciberacoso sexual es muy baja, llegando a un 2% (n = 66).

Gráfico 124. *Prevalencia de alumnos víctimas de sextorsión*



Del 2% de alumnos que afirma haber sido víctima de sextorsión, el 62% son chicas (n = 41) y el 38% son chicos (n = 25). Se observa, por tanto, un mayor porcentaje de chicas que chicos víctimas en una conducta de ciberacoso sexual.

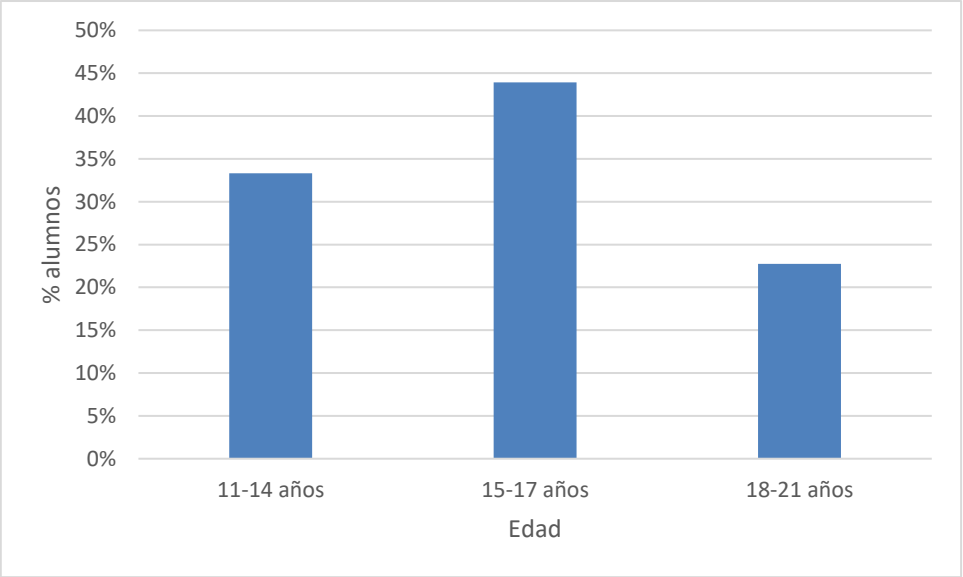
Gráfico 125. *Prevalencia de alumnos víctimas de sextorsión según sexo*



En cuanto a la edad de las víctimas, el 33% tiene entre 11 y 14 años (n = 22), el

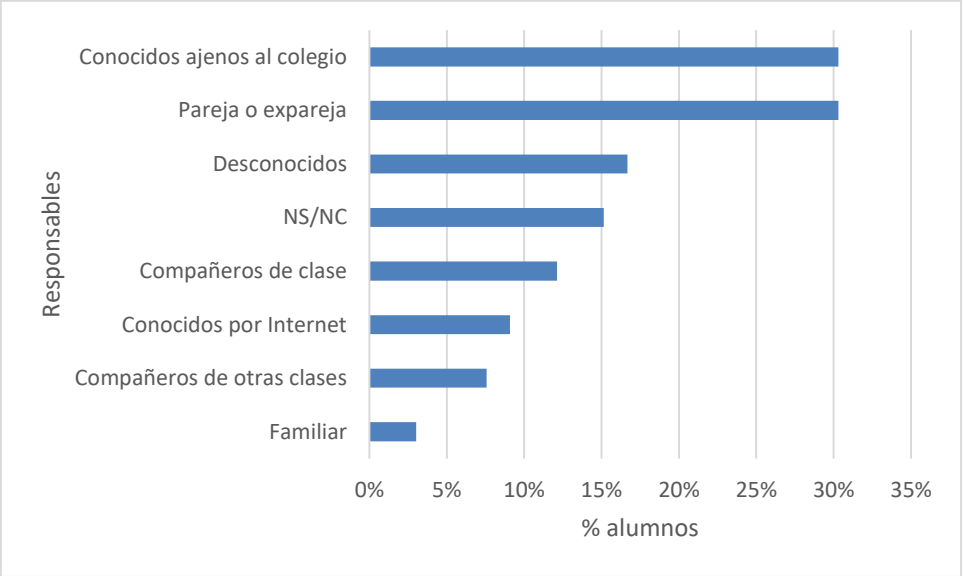
44% tiene entre 15 y 17 años (n = 29) y el 23% restante tiene entre 18 y 21 años (n = 15).

Gráfico 126. *Prevalencia de alumnos víctimas de sextorsión según edad*



En cuanto a los responsables de sextorsión, cabe destacar que los más frecuentes son personas conocidas ajenas al colegio y la pareja o expareja, ambas categorías con una prevalencia del 30%. También existe un alto porcentaje de alumnos que desconocen a los responsables o que no saben o no quieren responder, con porcentajes del 17% y 15%, respectivamente.

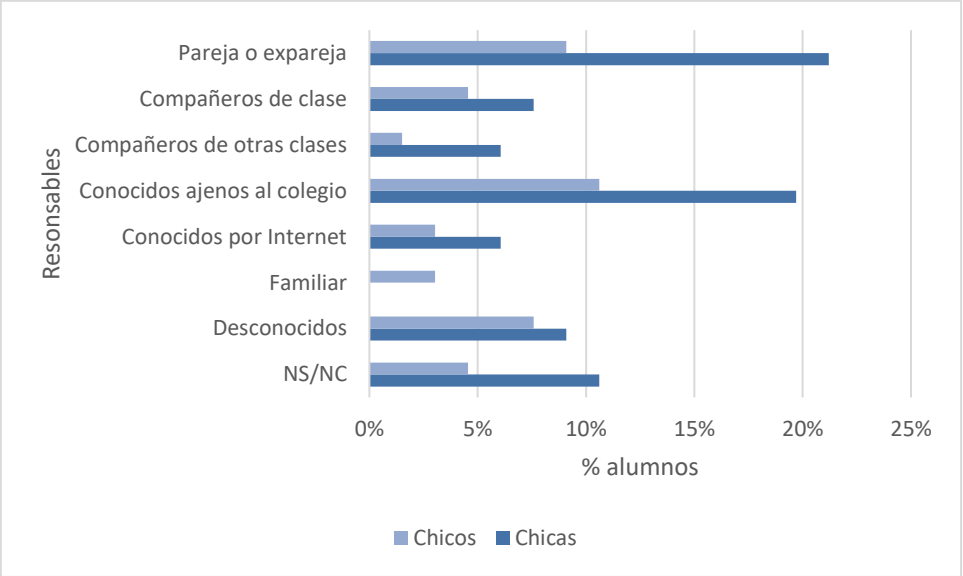
Gráfico 127. *Persona responsable de la sextorsión*



Un 21% de chicas considera que el principal responsable de la sextorsión es su pareja o expareja, seguido de un 20% que considera que el responsable es un conocido ajeno al colegio. Respecto a los chicos, la situación es un tanto similar, ya que el mayor porcentaje de chicos ha afirmado que el responsable es un conocido ajeno al colegio (un 11%).

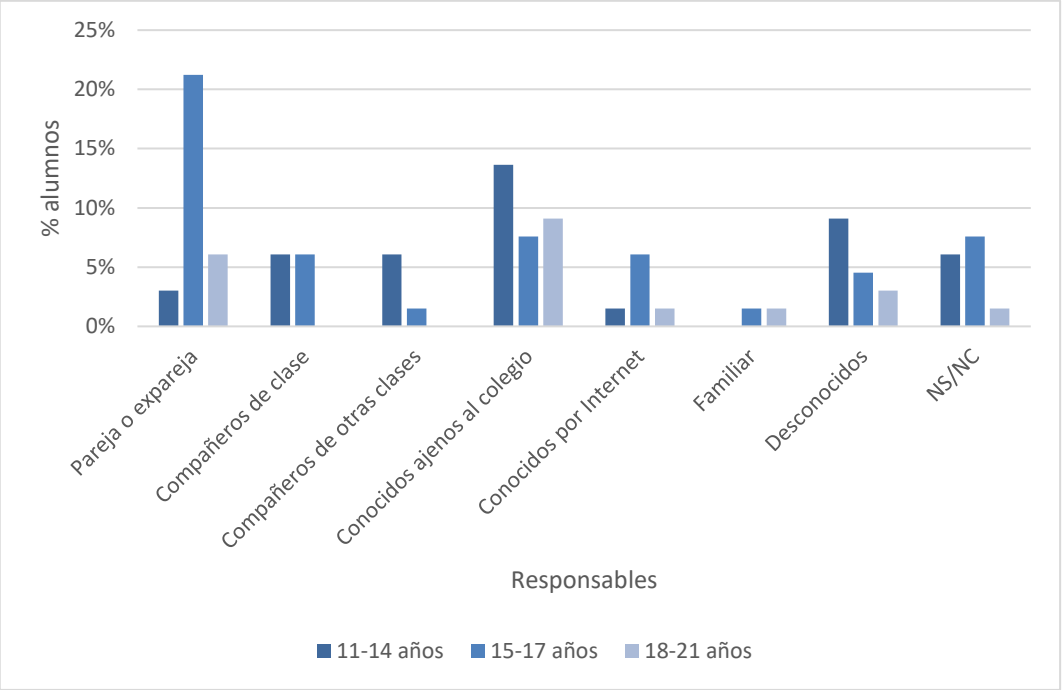
En cuanto a las categorías con menos prevalencia, las chicas afirman que los familiares nunca han realizado este tipo de ciberacoso sexual, mientras que los chicos sitúan en última posición, en un 3% de los casos, a las personas conocidas por Internet y a los propios familiares.

Gráfico 128. *Persona responsable de la sextorsión según el sexo de la víctima*



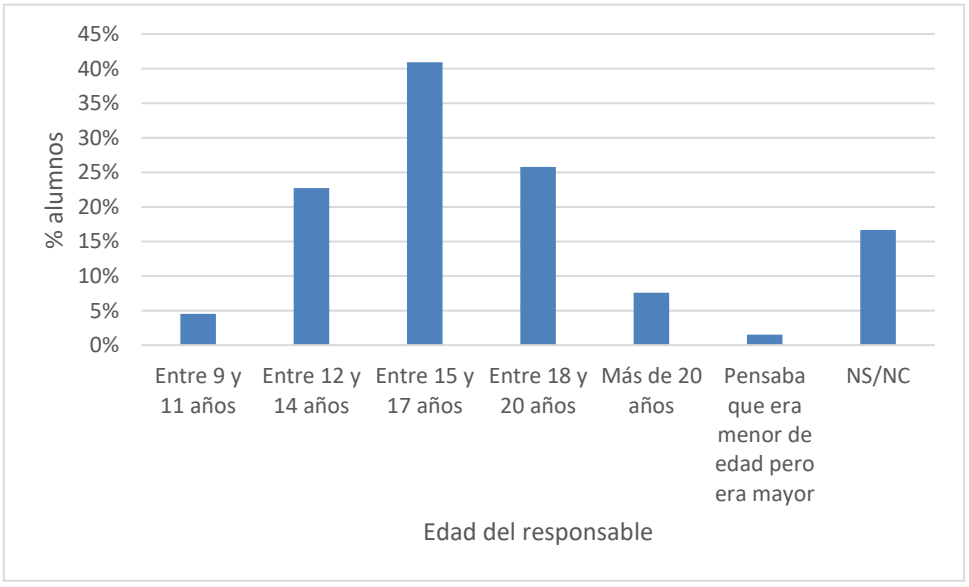
En cuanto a los responsables de realizar la conducta de sextorsión según la edad de las víctimas, cabe destacar que, en la franja de edad de 11 a 14 años, la categoría de persona responsable que más consenso presenta entre los alumnos es la de conocidos ajenos al colegio, con un 14% de los alumnos haciendo esta afirmación. Respecto a las otras dos franjas de edad, los alumnos entre 15 y 17 años afirman, en un 21% de los casos, que el responsable fue la pareja o expareja, mientras que en la franja de edad de 18 a 21 años, y coincidiendo con los alumnos más pequeños, la categoría de persona responsable que más consenso presenta entre los alumnos es la de conocidos ajenos al colegio, con un 9% de los alumnos.

Gráfico 129. *Persona responsable de la sextorsión según la edad de la víctima*



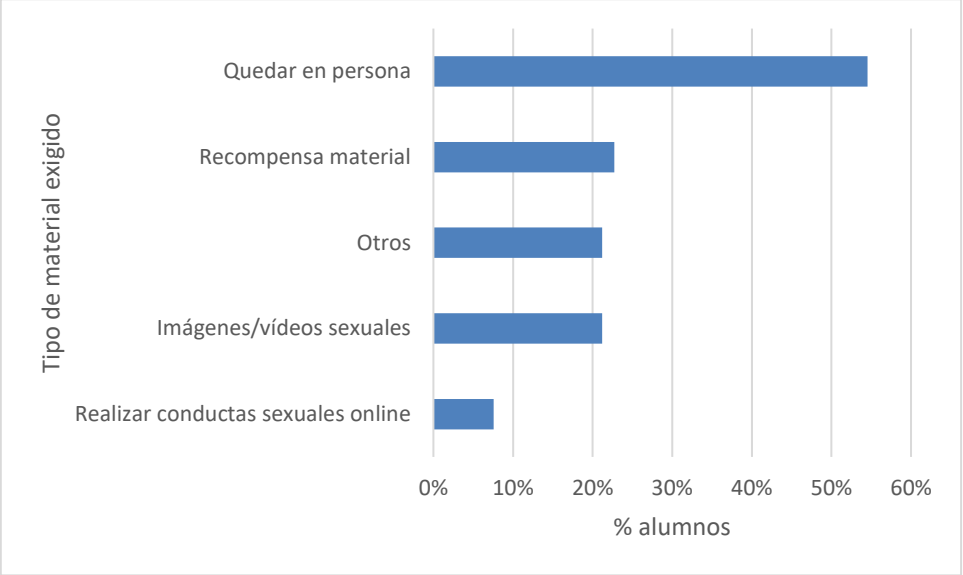
La franja de edad de los responsables que vuelve a ser más frecuente es la de 15 a 17 años pero, en este caso, como en el de las coacciones sexuales, existe un elevado número de alumnos que no sabe la edad del responsable (un 17%).

Gráfico 130. *Edad de la persona responsable de la sextorsión*



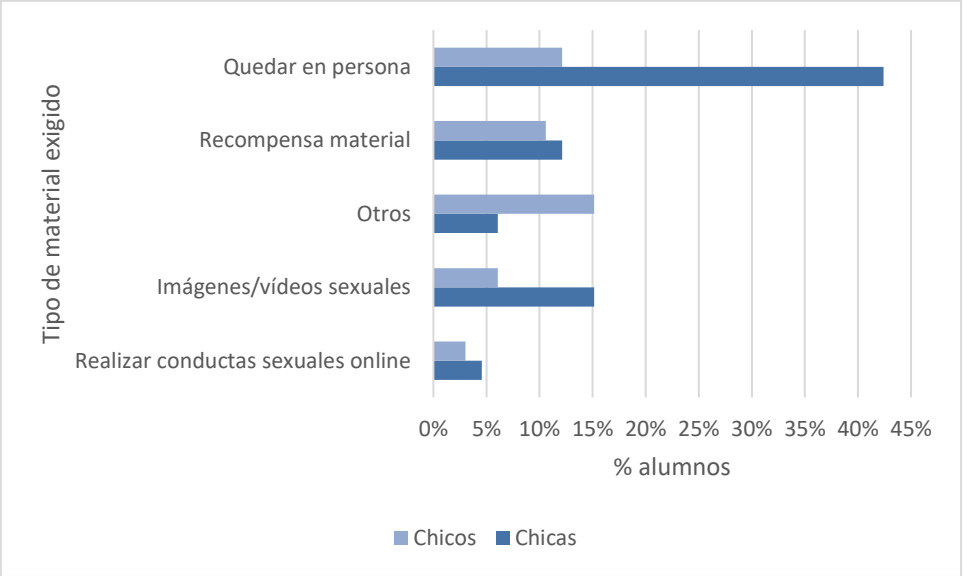
En la mayoría de los casos (un 55%) lo que se exigía al alumno a cambio de no publicar material sexual suyo era quedar en persona. Este hecho podría indicar una voluntad del acosador por conseguir algún tipo de acercamiento físico con el menor.

Gráfico 131. *Tipo de material exigido en la sextorsión*



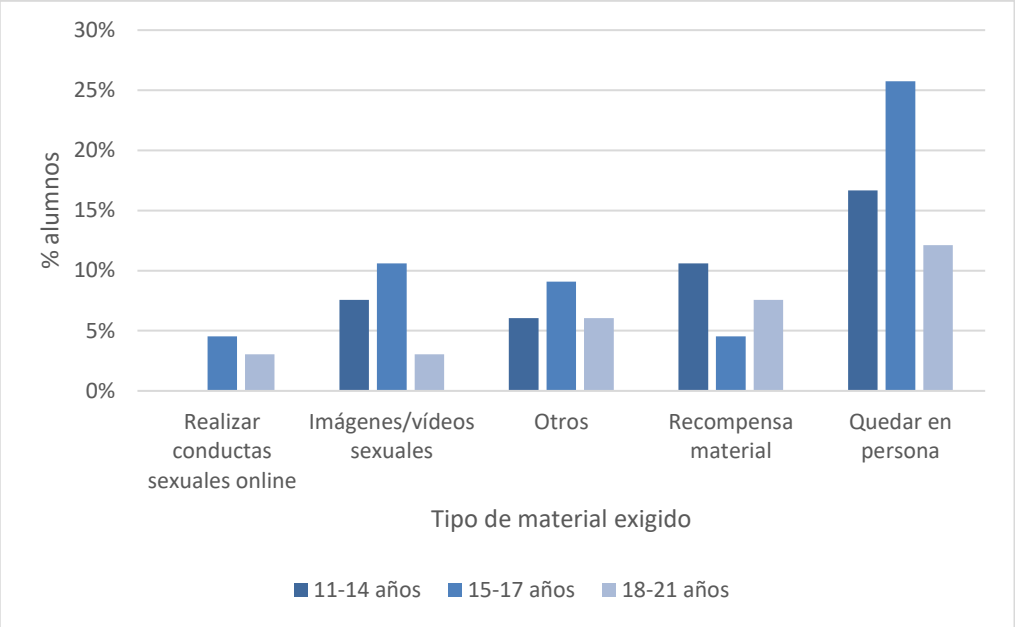
Las chicas informan de que la condición más exigida a cambio de no publicar material sexual relacionado con ellas es quedar en persona (un 42% de las chicas), seguido de enviar imágenes o vídeos sexuales propios (un 15%). Del mismo modo, los chicos informan, en un 12% de los casos, que quedar en persona es la principal condición exigida. Además, un 15% de chicos informa que se le pidió otro tipo de material.

Gráfico 132. *Tipo de material exigido en la sextorsión según el sexo de la víctima*



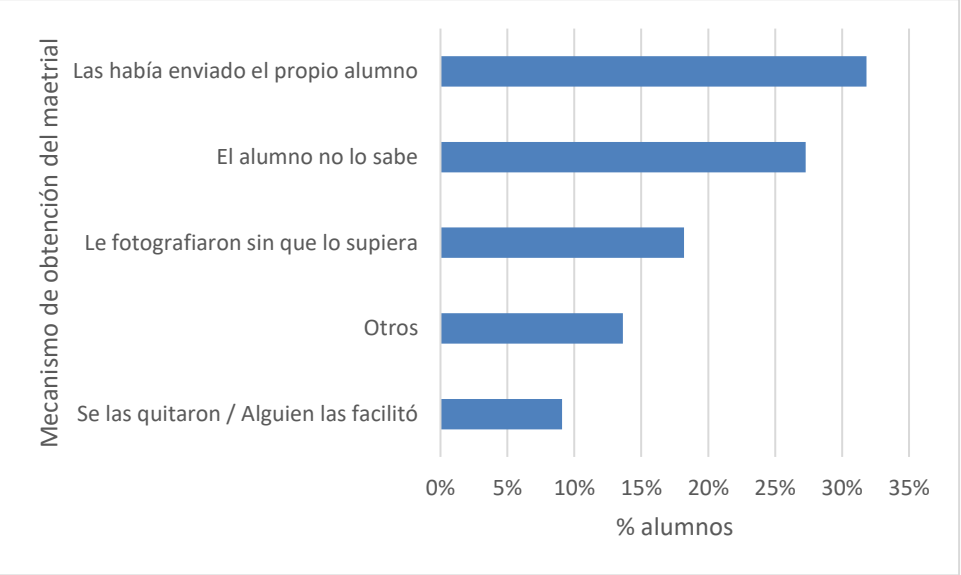
Para las tres franjas de edad, quedar en persona es la condición más común exigida si las víctimas no querían que su material sexual fuese publicado. Más concretamente, los porcentajes de víctimas que han afirmado esta información son de un 17% entre los alumnos de 11 a 14 años, de un 26% entre los alumnos de 15 a 17 años y de un 12% en el caso de los alumnos entre 18 y 21 años.

Gráfico 133. *Tipo de material exigido en la sextorsión según la edad de la víctima*



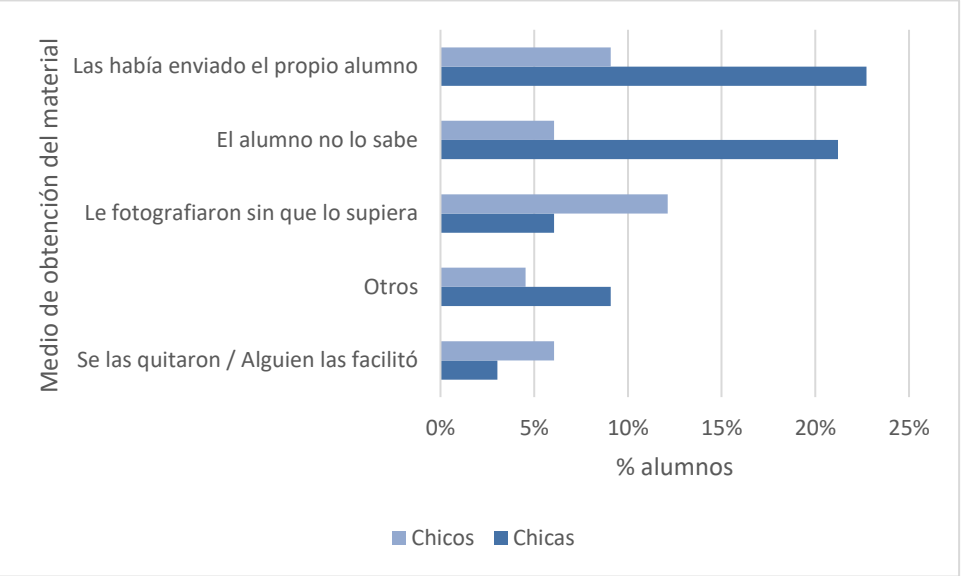
Finalmente, cabe destacar que en un elevado número de ocasiones (un 32% de los alumnos lo afirma), había sido el propio alumno quien había proporcionado el material sexual propio al acosador. Seguidamente, un 27% de los alumnos indica que no sabe cómo el acosador consiguió el material sexual

Gráfico 134. *Mecanismo por el cual el responsable de la sextorsión obtuvo el material*



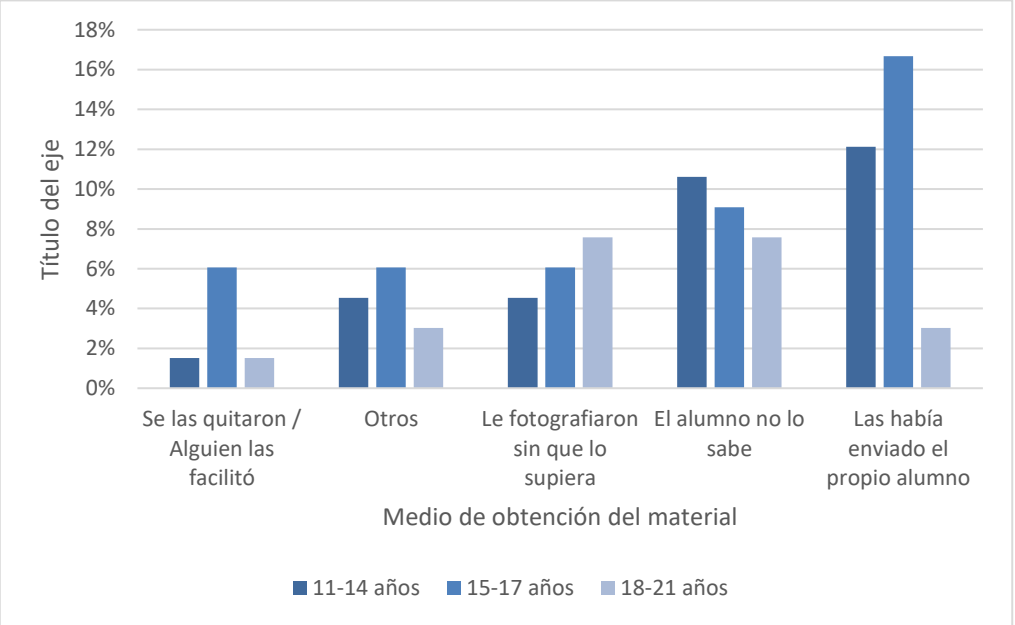
Los mecanismos más comunes de obtención de material expuestos por las chicas son que ellas mismas enviaron las fotos (un 23%) y que no saben cómo obtuvieron dicho material (un 21%). En el caso de los chicos, en cambio, lo más frecuente, en un 12% de los casos, es que les fotografiaran sin que ellos lo supieran.

Gráfico 135. *Mecanismo por el cual el responsable de la sextorsión obtuvo el material según el sexo de la víctima*



Tanto para los alumnos de 11 a 14 años, como para los que se encuentran en la franja de edad de 15 a 17 años, el principal mecanismo a partir del cual el responsable de la sextorsión obtuvo el material sexual consiste en que fue el propio alumno quien envió ese material (un 12% y un 17% de alumnos, respectivamente). Entre los jóvenes de 18 a 21 alumnos, un 8% coincide en que le fotografiaron sin que lo supiera. Asimismo, un 8% de alumnos de esta misma franja de edad afirma que no sabe cómo pudieron hacerse con ese material.

Gráfico 136. *Mecanismo por el cual el responsable de la sextorsión obtuvo el material según la edad de la víctima*



4. Publicación o difusión de imágenes o vídeos sexuales sin consentimiento

La prevalencia de alumnos que ha sufrido este tipo de ciberacoso sexual es de un 1% (n = 40), cifra muy inferior al resto de tipos de ciberacoso sexual. De ese 1%, prácticamente la mitad son chicos y la otra mitad son chicas. Más concretamente, el 48% son chicos (n = 19) y el 53% son chicas (n = 21).

Gráfico 137. *Prevalencia de alumnos víctimas de publicación o difusión de imágenes o vídeos sexuales sin consentimiento*

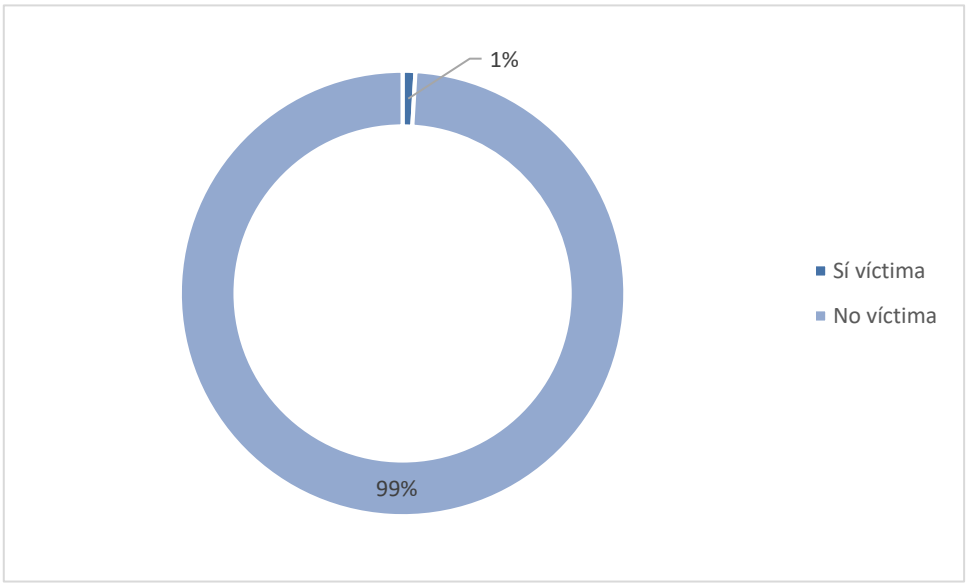
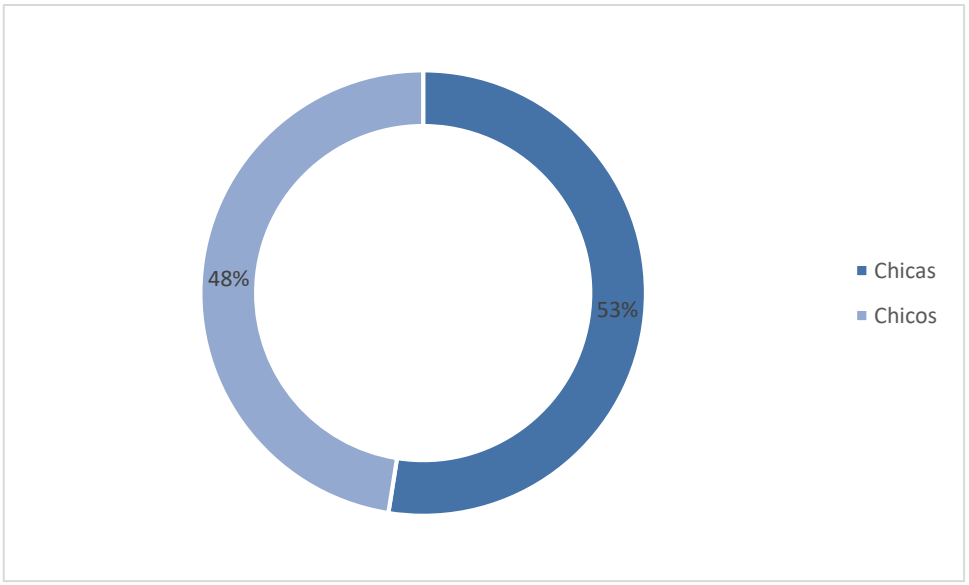
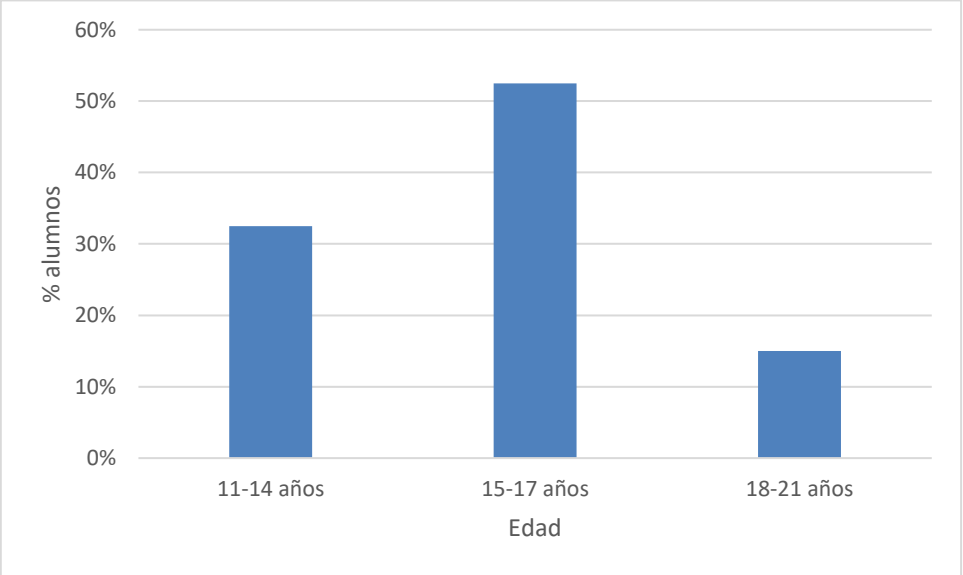


Gráfico 138. *Prevalencia de alumnos víctimas de publicación o difusión de imágenes o vídeos sexuales sin consentimiento según sexo*



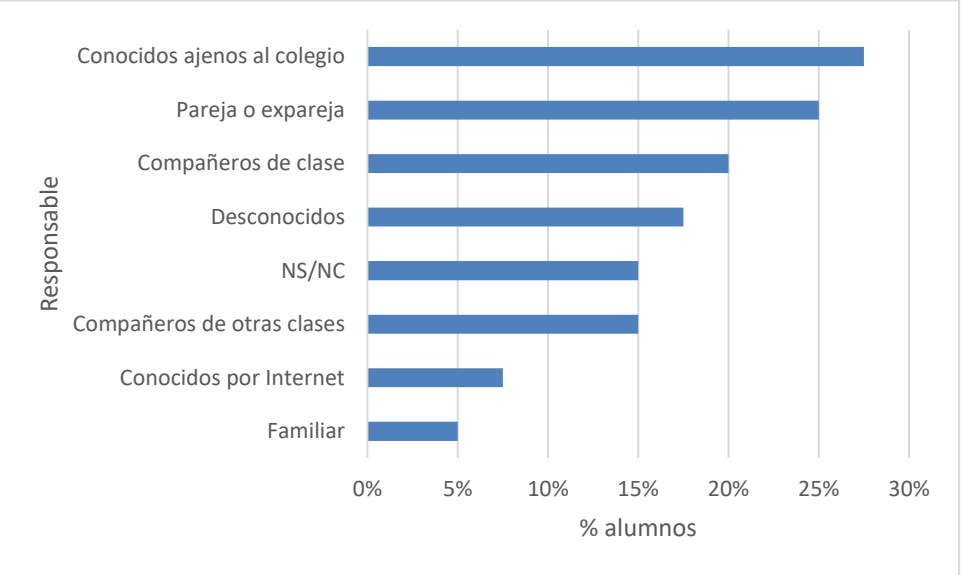
En cuanto al rango de edad de las víctimas, un 33% son alumnos entre 11 y 14 años (n = 13), un 53% son alumnos entre 15 y 17 años (n = 21) y un 15% son alumnos de 18 a 21 años (n = 6).

Gráfico 139. *Prevalencia de alumnos víctimas de publicación o difusión de imágenes o vídeos sexuales sin consentimiento según edad*



En esta conducta, la mayor parte de responsables eran conocidos de los alumnos. Más concretamente, la mayor parte de responsables eran conocidos ajenos al colegio (un 28%), seguido de la pareja o expareja (un 25%) y los compañeros de clase (un 20%). Estos resultados parecen indicar que en muchas ocasiones los jóvenes conocen a las personas que les han producido este daño, las cuales estaban en posesión de dicho material.

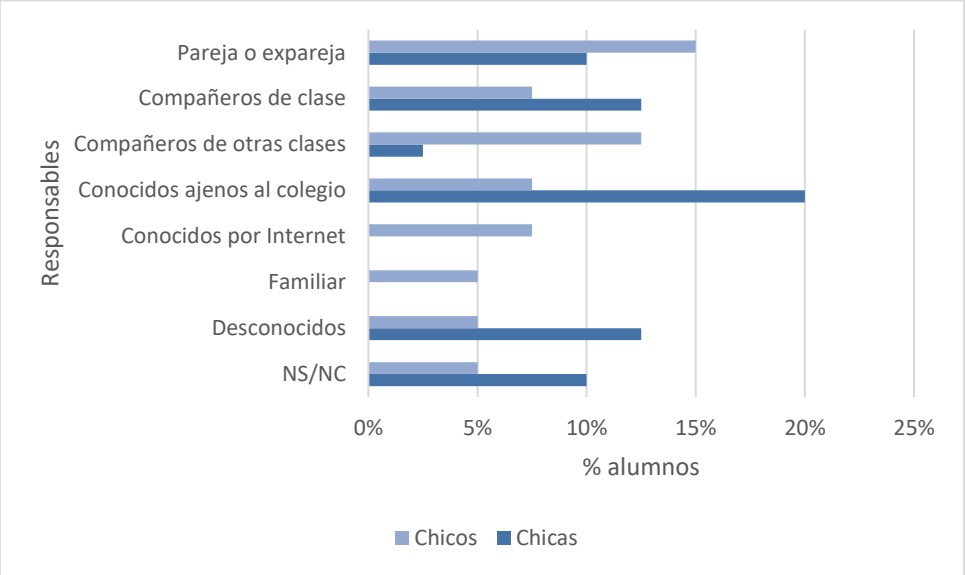
Gráfico 140. *Persona responsable de la publicación o difusión de imágenes o vídeos sexuales sin consentimiento*



En este tipo de ciberacoso, las chicas afirman, en un 20% de los casos, que los principales responsables son conocidos ajenos al colegio, seguidos de personas desconocidas y compañeros de clase (un 13% en ambos casos). Los chicos, por su parte, se inclinan más en afirmar que el principal responsable fue la pareja o expareja (un 15%), seguido de compañeros de otras clases (un 13%).

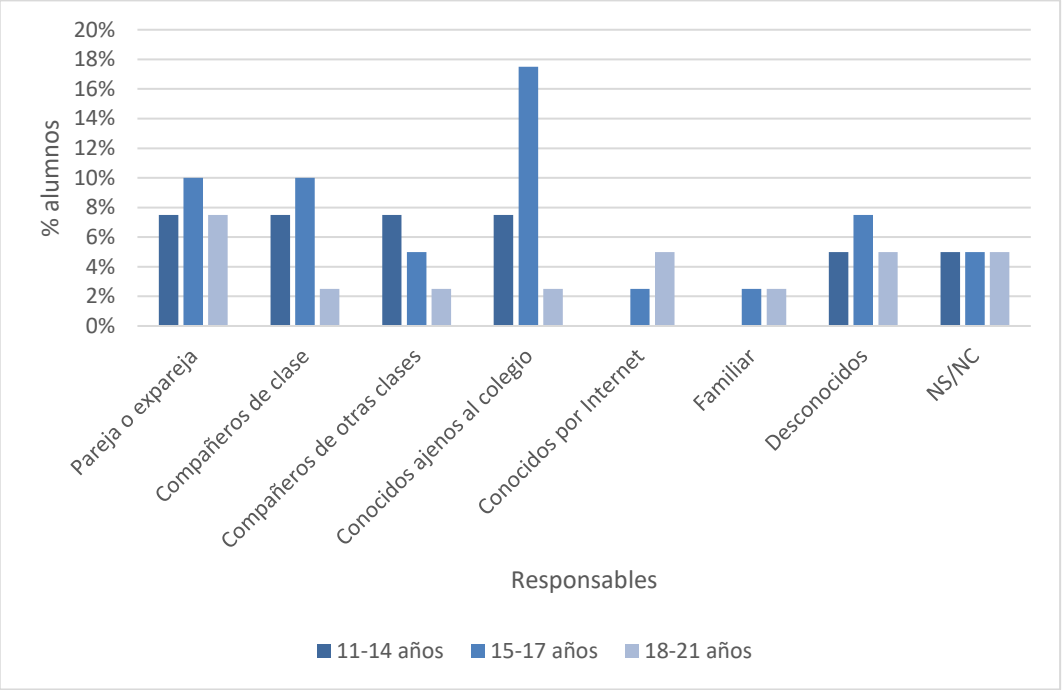
Resulta interesante destacar que ninguna chica ha afirmado que los responsables fueran familiares o personas conocidas a través de Internet.

Gráfico 141. *Persona responsable de la publicación o difusión de imágenes o vídeos sexuales sin consentimiento según el sexo de la víctima*



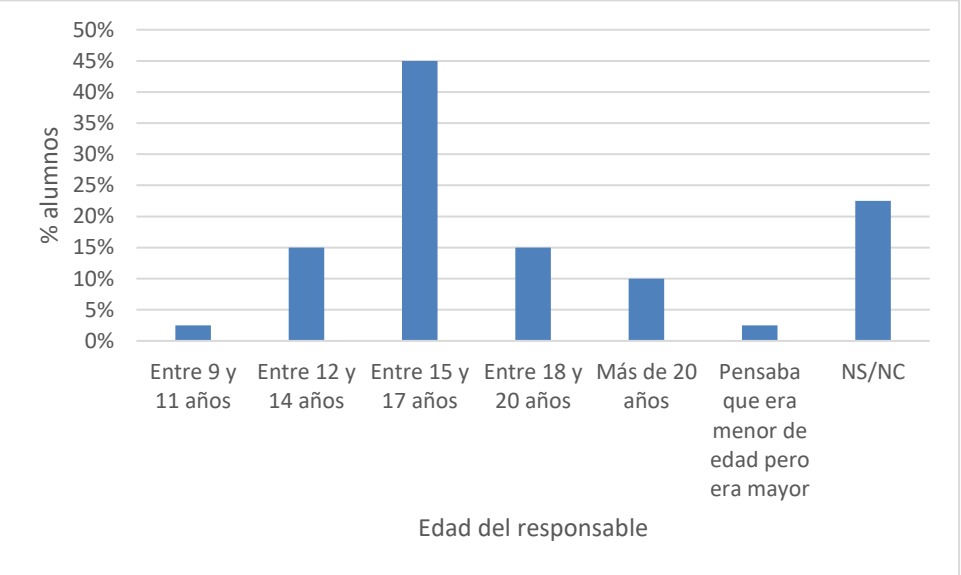
Entre los alumnos que tienen de 11 a 14 años, un 8% coincide en que las personas responsables de la publicación de este material sexual privado fueron la pareja o expareja, compañeros de clase, compañeros de otras clases y conocidos ajenos al colegio (todas las categorías presentan el mismo porcentaje de alumnos). En la franja de edad entre 15 y 17 años, el mayor porcentaje de alumnos que coincide a la hora de decir quien fue el responsable de la publicación del material sexual es de un 18%, afirmando que el responsable fue una persona conocida ajena al colegio. Finalmente, en cuanto a los alumnos entre 18 y 21 años, un 8% considera que el principal responsable fue la pareja o expareja.

Gráfico 142. *Persona responsable de la publicación o difusión de imágenes o vídeos sexuales sin consentimiento según la edad de la víctima*



Siguiendo el mismo patrón que en el resto de tipologías de ciberacoso sexual analizadas en apartados anteriores, la mayor parte de responsables (casi un 45%) tiene entre 15 y 17 años. Sin embargo, continúa habiendo un alto porcentaje de alumnos que no saben la edad de la persona que publicó material sexual suyo (en este caso es de un 23%).

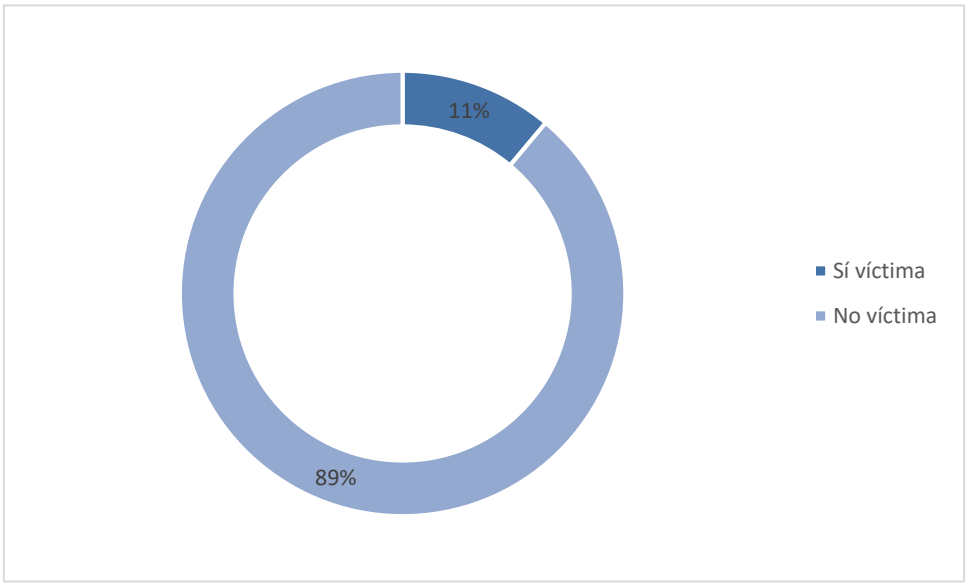
Gráfico 143. *Edad de la persona responsable de publicar o difundir imágenes o vídeos sexuales sin consentimiento*



5. Presionar para quedar en persona

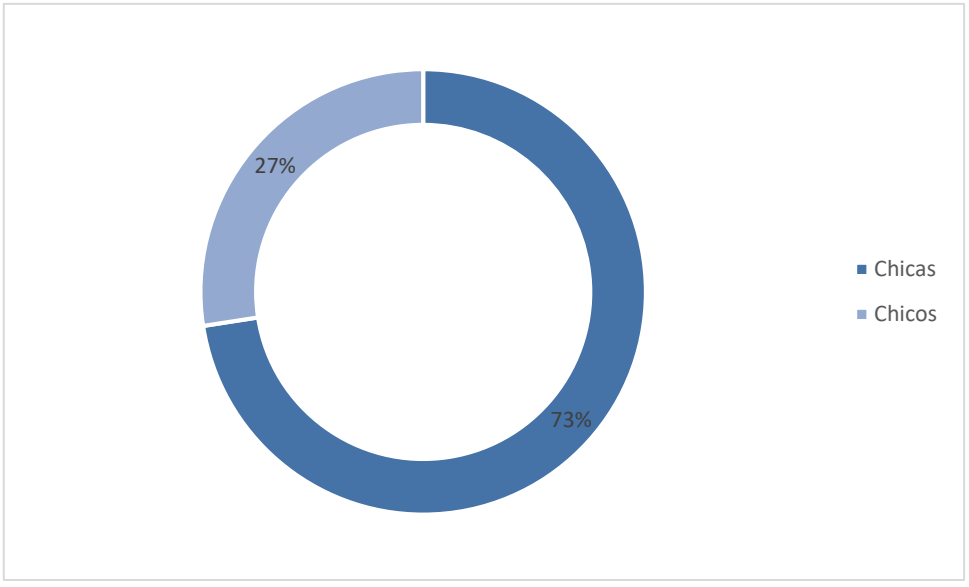
En este tipo de ciberacoso sexual se preguntó a los alumnos si en el último año alguien a quien solo conocían por Internet les había presionado, insistiendo repetidamente, para quedar en persona. Como respuesta, se ha obtenido que el 11% (n = 481) de los alumnos ha sido víctima de dicho comportamiento, frente al 89% que no.

Gráfico 144. *Prevalencia de alumnos víctimas de haber sido presionados para quedar en persona por un desconocido*



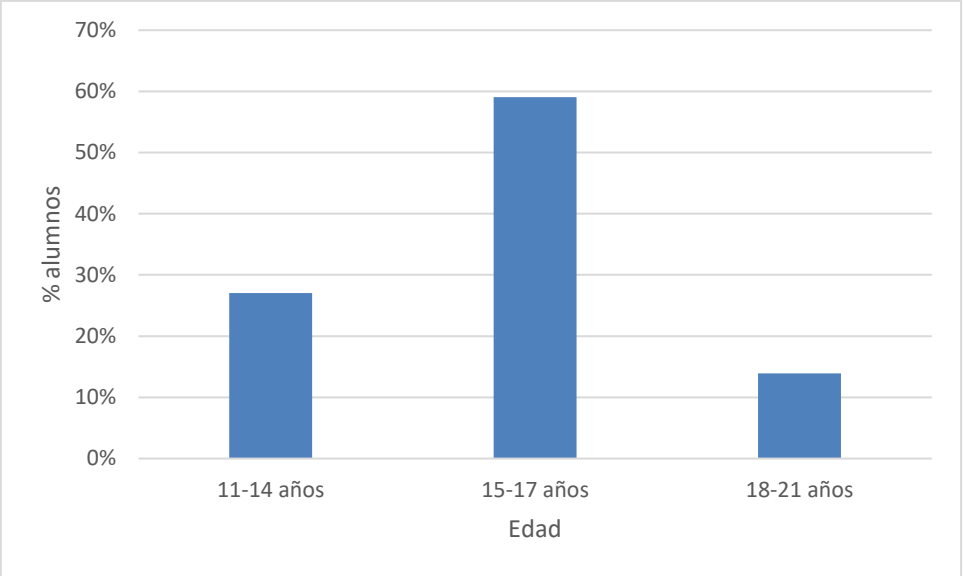
Con una diferencia bastante mayor que en los tipos de ciberacoso anteriormente analizados, en este caso el 73% de las chicas confiesa haber sido víctima de este tipo de ciberacoso sexual (n = 349) frente al 27% de los chicos (n = 132).

Gráfico 145. *Prevalencia de alumnos víctimas de haber sido presionados para quedar en persona por un desconocido según sexo*



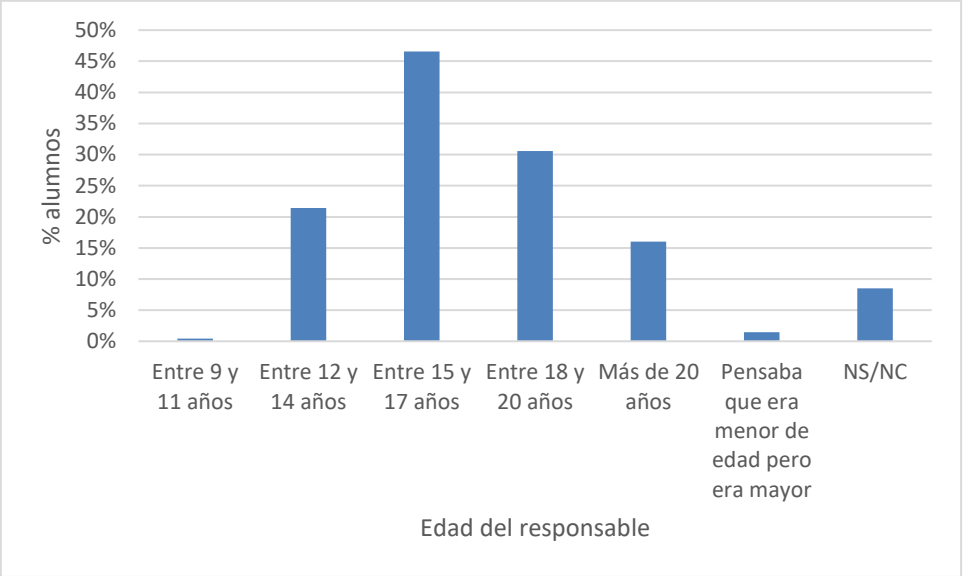
La distribución de las víctimas según su edad se estructura de la siguiente manera: un 27% son alumnos entre 11 y 14 años (n = 130), un 59% tiene entre 15 y 17 años (n = 284) y un 14% tiene entre 18 y 21 años (n = 67).

Gráfico 146. *Prevalencia de alumnos víctimas de haber sido presionados para quedar en persona por un desconocido según edad*



En cuanto a la edad de los responsables de dichas presiones, cabe destacar, de nuevo, que existe un alto porcentaje de responsables que tienen entre 15 y 17 años (casi un 50% afirman que los responsables tenían esta edad). En esta tipología, la cantidad de alumnos que afirma que los responsables tenían de 18 a 20 años es ligeramente superior que en el resto de tipos de ciberacoso sexual, alcanzando una cifra del 31%.

Gráfico 147. *Edad de la persona responsable de presionar para quedar en persona*



c) Control de pareja a través de las TIC

El control de pareja a través de las TIC hace referencia a todos aquellos comportamientos que un miembro de la pareja realiza para controlar y/o manipular al otro con el objetivo de que se comporte de una determinada manera utilizando, para ello, las nuevas tecnologías e Internet.

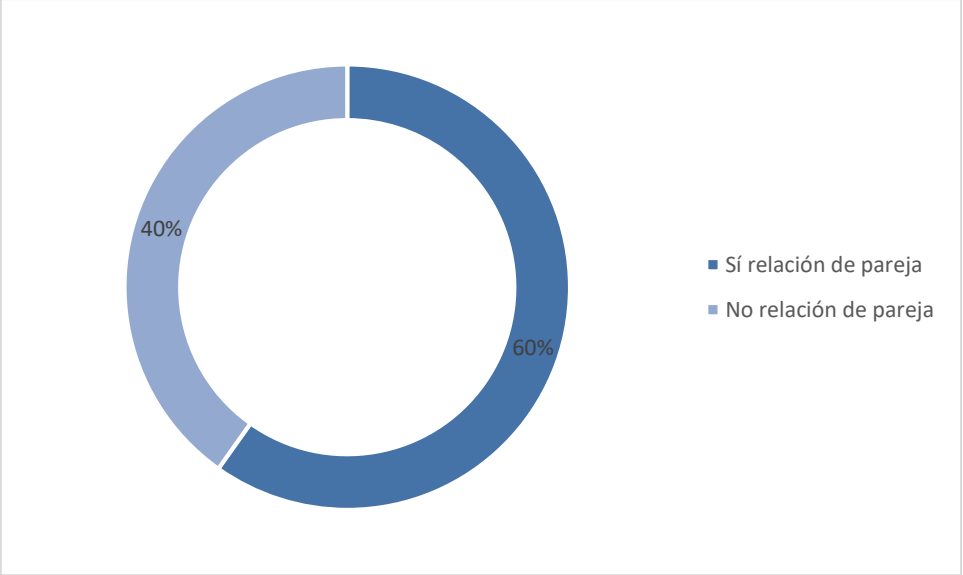
Para conocer la prevalencia de control de pareja a través de las TIC de los alumnos de enseñanza no universitaria de Castilla y León se han tenido en cuenta 3 tipologías distintas de control de pareja:

1. Pedir la retirada de fotos o comentarios de las redes sociales
2. Pedir que no se agregue o se elimine a personas de las redes sociales
3. Intentar influir en la información, el estado, el tablón o las fotos publicadas en redes sociales

Los análisis sobre la prevalencia de víctimas de control de pareja a través de las

TIC e Internet se han realizado sobre el conjunto de alumnos que han afirmado tener o haber tenido pareja alguna vez en su vida, ya que son los que se han podido ver expuestos a este tipo de control. Analizando esta información, se observa que el 60% (n = 2590) de los alumnos tiene o ha tenido alguna vez en su vida una relación de pareja, frente al 40% (n = 1739) que afirma no haber tenido nunca una relación de este tipo.

Gráfico 148. *Proporción de alumnos que han tenido o tienen pareja*

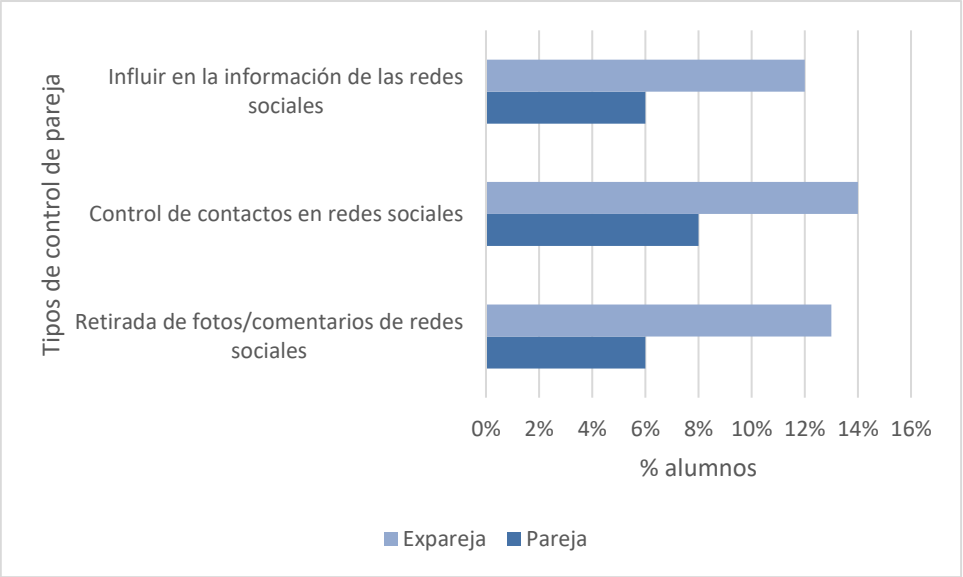


Cabe destacar que, al igual que en el caso del ciberacoso sexual, el control de pareja solo ha sido preguntado a los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM por considerar que el contenido no era adecuado para los alumnos más jóvenes.

En el siguiente gráfico se muestra la prevalencia de los distintos tipos de control de pareja anteriormente expuestos en función de si el control lo ejerce la pareja actual del alumno o si lo ejercía la expareja en su relación pasada. Como se puede observar, el tipo de control de pareja más frecuente, tanto si se tiene en cuenta la pareja como la expareja, es el control de los contactos de las redes sociales (pedir que se eliminen o no se agreguen contactos), al que se han visto

expuestos el 8% de alumnos en su relación actual (n = 146) y el 14% en su relación pasada (n = 333).

Gráfico 149. *Prevalencia de alumnos víctimas de los distintos tipos de control de pareja a través de las TIC*

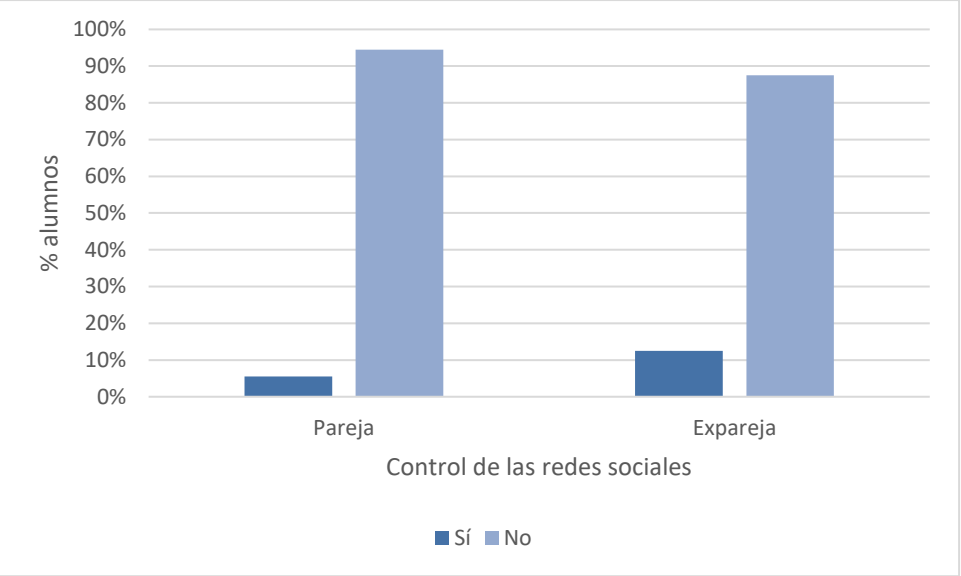


A continuación, se analiza en mayor profundidad cada conducta de control de pareja de forma individualizada para ver cómo afecta cada una de ellas al conjunto de los alumnos.

1. Pedir la retirada de fotos o comentarios de las redes sociales

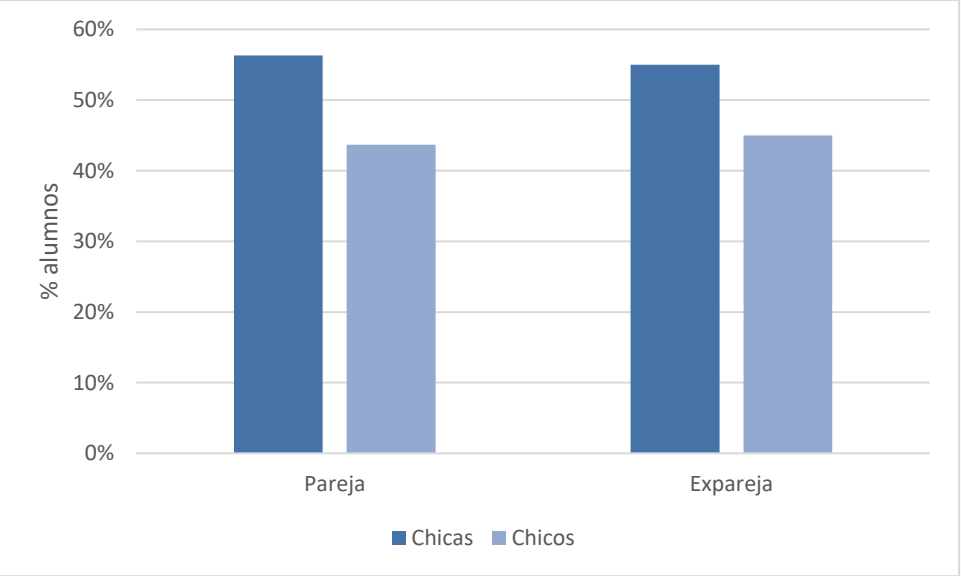
Los resultados obtenidos tras el análisis de este tipo de control de pareja indican que existe un 13% de los alumnos que afirma haber sido víctima de control de pareja en sus relaciones pasadas (n = 300) y un 6% que afirma ser víctima en sus actuales relaciones de pareja (n = 103). En general, las prevalencias no son muy elevadas, pero debe tenerse en cuenta que es posible que exista una elevada cifra negra por las características de este tipo de ataque, ya que se suele dar en el ámbito privado.

Gráfico 150. *Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen controlar la información publicada en redes sociales en relaciones actuales y relaciones pasadas*



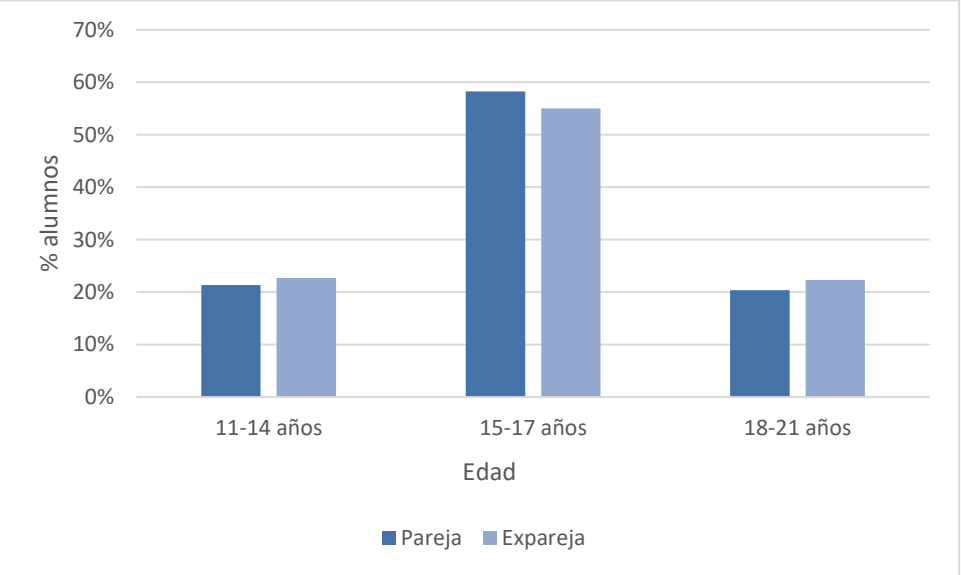
Del 6% de alumnos que consideran que sus parejas controlan la información que publican en redes sociales, las chicas representan el 56% (n = 58) y los chicos el 44% (n = 45). Por otro lado, del 13% de alumnos que se ha sentido controlado por sus exparejas, de forma similar al caso del control ejercido por la pareja actual, las chicas representan el 55% (n = 165) y los chicos el 45% (n = 135).

Gráfico 151. *Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen controlar la información publicada en redes sociales en relaciones actuales y relaciones pasadas según sexo*



Si en lugar de analizar los resultados según el sexo de los participantes se hace según su edad, se observa que del 6% de alumnos que se considera víctima en sus relaciones actuales, el 21% tiene entre 11 y 14 años, el 58% tiene entre 15 y 17 años y el 20% restante tiene entre 18 y 21 años. En el caso del control ejercido por la expareja en relaciones pasadas, el 23% de las víctimas tiene entre 11 y 14 años, el 55% tiene entre 15 y 17 años y el 22% restante entre 18 y 21 años. Como se observa en el siguiente gráfico y como indican los propios datos, las cifras son muy similares tanto si el control lo ejerce la pareja actual como si lo ejercía la expareja en la relación pasada.

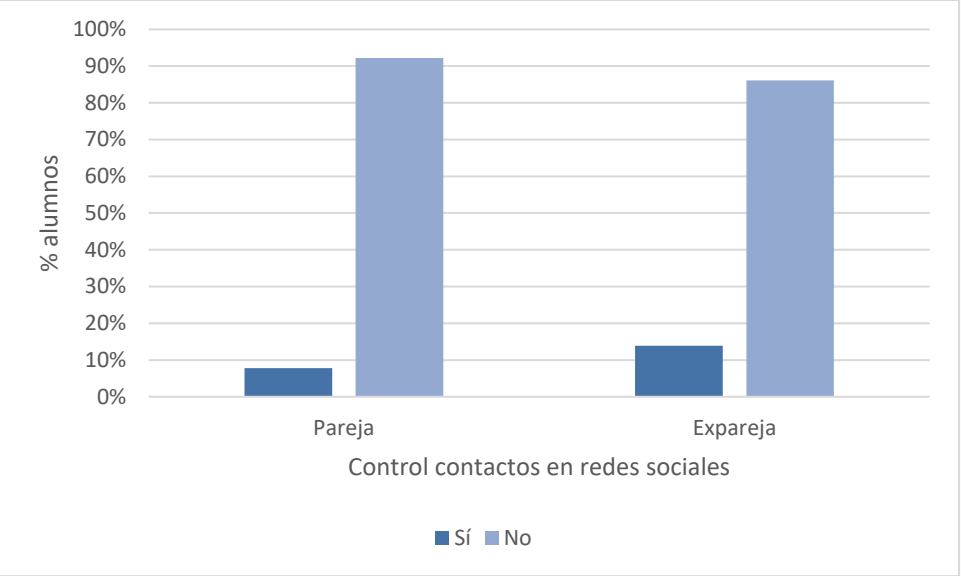
Gráfico 152. *Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen controlar la información publicada en redes sociales en relaciones actuales y relaciones pasadas según edad*



2. Pedir que no agregue o elimine personas de sus redes sociales

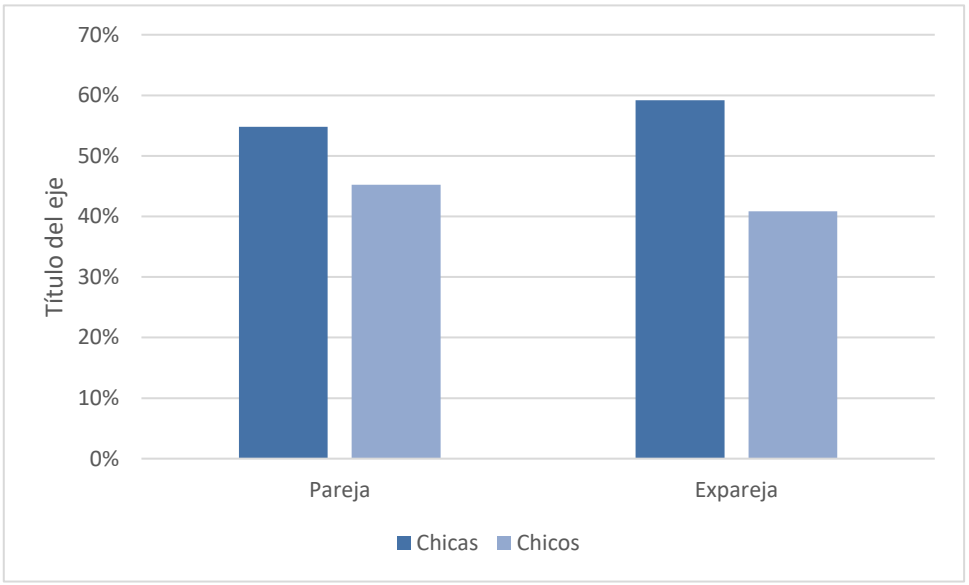
En este tipo de control de pareja los datos son prácticamente iguales que en el tipo anterior, ya que un 14% de alumnos refiere haber sido víctima en su relación pasada (n = 333) y un 8% afirma serlo en la actualidad por parte de sus parejas (n = 146).

Gráfico 153. *Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen controlar las amistades en redes sociales en relaciones actuales y relaciones pasadas*



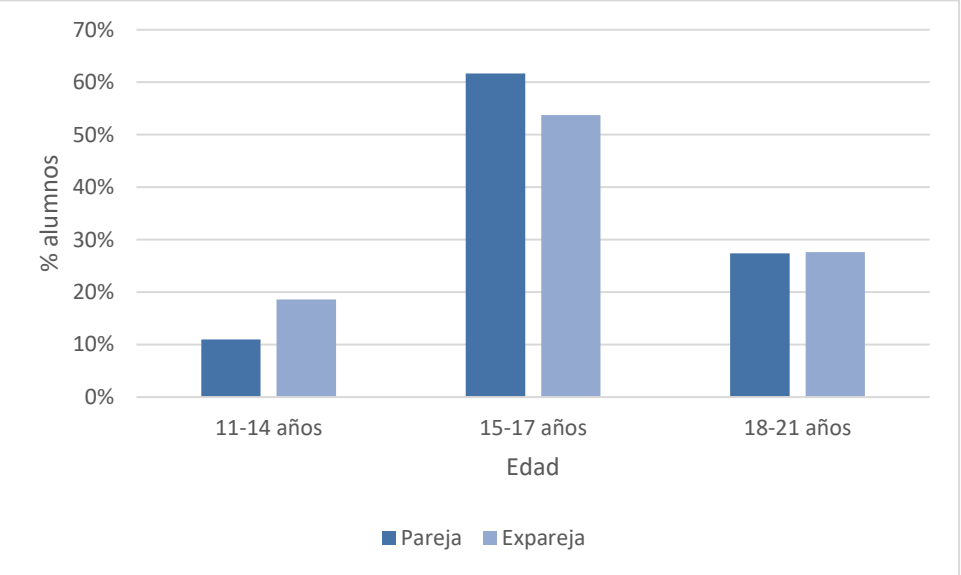
En este caso, del 8% de alumnos víctimas del control de los contactos de sus redes sociales por parte de sus parejas, el 55% son chicas (n = 80) y el 45% chicos (n = 66), mientras que del 14% de alumnos que ha sido víctima de sus exparejas, el 59% viene representado por las chicas (n = 197) y el 41% por los chicos (n = 136).

Gráfico 154. *Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen controlar las amistades en redes sociales en relaciones actuales y relaciones pasadas según sexo*



En la misma línea, del 8% de alumnos que considera que su pareja actual ha intentado controlar sus amistades en redes sociales, el 11% tiene entre 11 y 14 años, el 62% tiene entre 15 y 17 años y el 7% restante tiene entre 18 y 21 años. Estos mismos datos entre aquellas personas que han afirmado ser víctimas de este tipo de control de pareja en sus relaciones pasadas, cabe destacar que el 19% tiene entre 11 y 14 años, el 54% tiene entre 15 y 17 años y el 28% restante tiene entre 18 y 21 años.

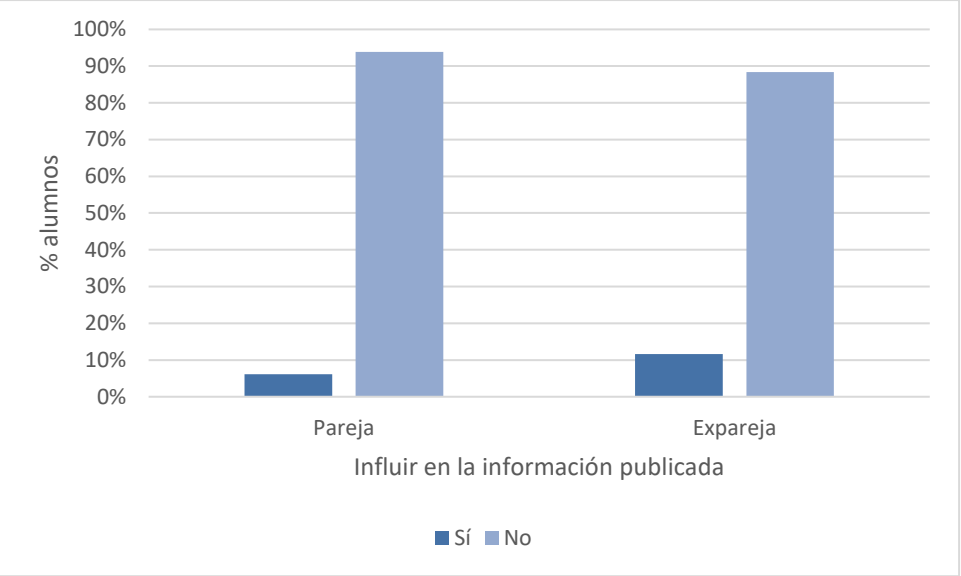
Gráfico 155. *Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen controlar las amistades en redes sociales en relaciones actuales y relaciones pasadas según edad*



3. Influir en información, el estado o las fotos publicadas en redes sociales

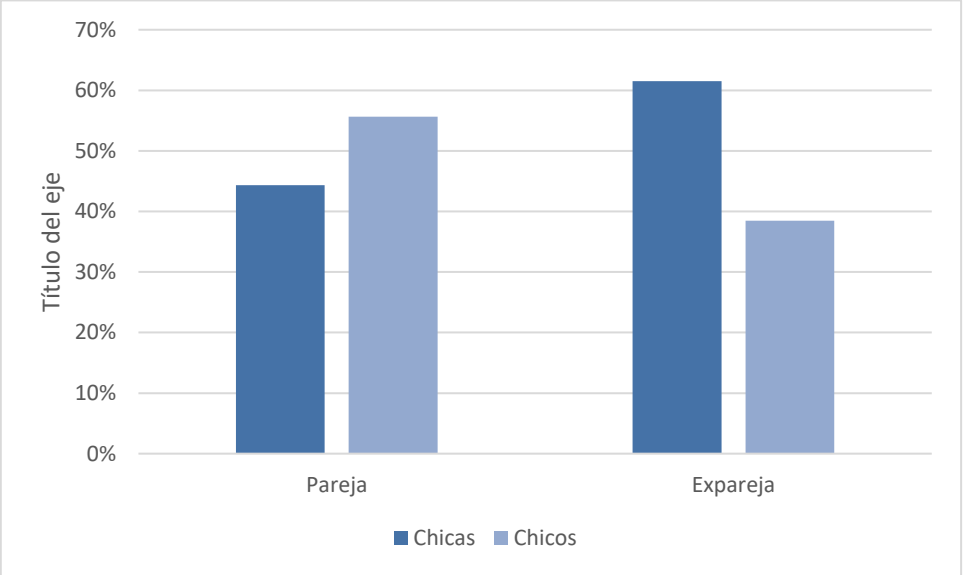
Finalmente, en este último tipo de control de pareja se observa que un 12% de alumnos afirma haber sido víctima en su relación pasada (n = 278), mientras que un 6% afirma sufrir este tipo de control por parte de sus parejas actuales (n = 115).

Gráfico 156. *Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen influir en la información publicada en redes sociales*



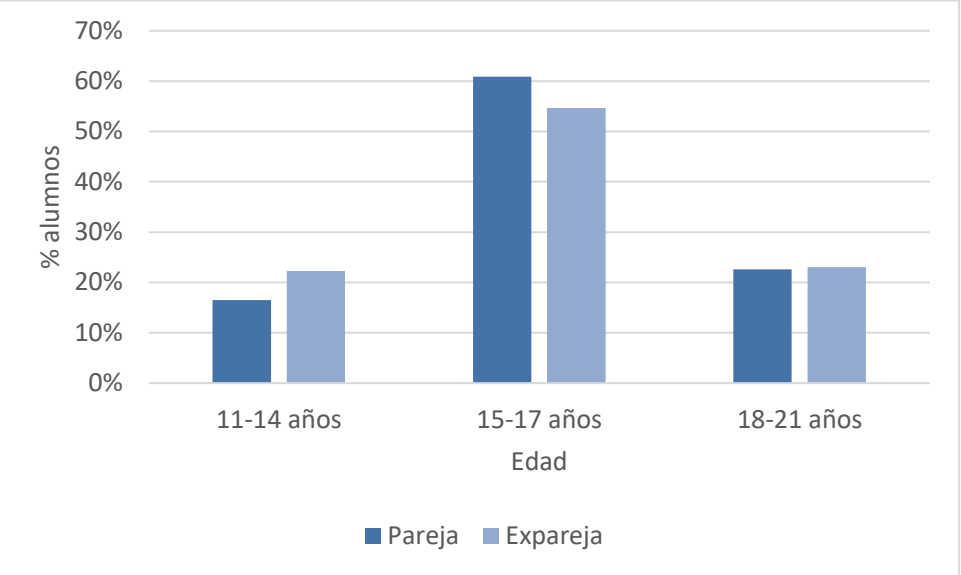
A diferencia de los dos tipos de control de pareja anteriormente expuestos, y teniendo en cuenta el control de la información publicada en redes sociales por parte de la pareja actual, en este caso hay más chicos (un 56%, n = 64) que dicen ser víctimas que chicas (un 44%, n = 51). En cuanto a este mismo control ejercido por exparejas en relaciones pasadas, sigue habiendo más chicas víctimas (un 62%, n = 171) que chicos (un 38%, n = 107).

Gráfico 157. *Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen influir en la información publicada en redes sociales según sexo*



De manera similar a los resultados obtenidos en los dos tipos de control de pareja analizados anteriormente, en este caso, el 11% de alumnos que afirma ser víctima en sus relaciones actuales y el 19% que afirma haber sido víctima en sus relaciones pasadas tienen entre 11 y 14 años. En cuanto a las otras dos franjas de edad, cabe destacar que el 62% de víctimas en relaciones actuales y el 54% de víctimas en relaciones pasadas tienen entre 15 y 17 años, mientras que el 27% y 28% restantes, respectivamente, tienen entre 18 y 21 años.

Gráfico 158. *Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen influir en la información publicada en redes sociales según edad*



4.3 CONDUCTAS DE USO DESVIADO DE INTERNET Y LAS TIC DE LOS JÓVENES DE CASTILLA Y LEÓN

Tal y como se expondrá en el apartado 4.5 del presente capítulo, tanto las Tecnologías de la Información y la Comunicación como Internet forman parte de la vida diaria de los jóvenes y están ampliamente instaurados en su día a día. Sin embargo, se requiere de experiencia para hacer un uso adecuado y responsable de estas herramientas y, de este modo, minimizar todo lo posible sus riesgos.

Algunos de los riesgos asociados a Internet que no se han mencionado hasta el momento hacen referencia al uso abusivo del mismo, a las apuestas online y al *sexting*. Son precisamente estos riesgos los que se exponen a lo largo de todo este apartado, en el cual se detalla, por un lado, la prevalencia de alumnos encuestados que presentan un uso abusivo de Internet y, por el otro, el porcentaje de alumnos que manifiesta realizar apuestas online y conductas de *sexting.*

4.3.1 Uso abusivo de Internet y las TIC

El abuso de Internet es una problemática que afecta, sobre todo, a los adolescentes, y hay que tener presente que muchas veces no es más que la manifestación de otro tipo de problemas. En palabras de Echeburúa y Del Corral (2010) "si hay una obsesión enfermiza por adquirir la última novedad tecnológica (…) o las TIC se transforman en el instrumento prioritario de placer, el ansia por estar a la última puede enmascarar necesidades más poderosas" (p. 92).

Para el análisis del abuso de Internet entre los jóvenes castellanoleonenses se ha utilizado el "Cuestionario de Experiencias Relacionadas con Internet" (CERI) elaborado por Beranuy, Chamarro, Graner y Carbonell (2009), que es una adaptación del cuestionario de "Problemas Relacionados con el uso de Internet" (PRI), de Young (1998, citado por De Gracia, Vigo, Fernández y Marcó, 2002). El CERI está formado por diez ítems con escala de respuesta de tipo Likert de cuatro puntos (Nunca, Rara vez, Frecuentemente y Siempre).

En este estudio, las cuatro categorías de respuesta se han recodificado en 1 (Nunca), 2 (Rara vez), 3 (Frecuentemente) y 4 (Siempre) con el objetivo de construir una escala de abuso de Internet, de modo que la puntuación global puede oscilar entre 10 (personas que han respondido la opción "Nunca" en todos los ítems) y 40 (personas que han respondido la opción "Siempre" en todos los ítems). Para establecer el punto de corte que indica si hay abuso de Internet se ha seguido el criterio empleado en estudios anteriores (Beranuy, Chamarro, Graner y Carbonell, 2009; Marín, 2017), los cuales lo establecen en una puntuación de 34 o superior.

Teniendo en cuenta el punto de corte mencionado en el párrafo anterior, se observa que la prevalencia de alumnos de Castilla y León que abusa de Internet es de menos del 1% (n = 72). Una amplia mayoría, más concretamente el 99,6%

(n = 7210) mantiene un uso normalizado. Entre este 1% que sí que abusa de Internet, cabe destacar que la mayoría, más concretamente el 64% (n = 46), son chicas, mientras que el 36% restante (n = 26) son chicos.

Gráfico 159. *Prevalencia de alumnos que abusa de Internet*

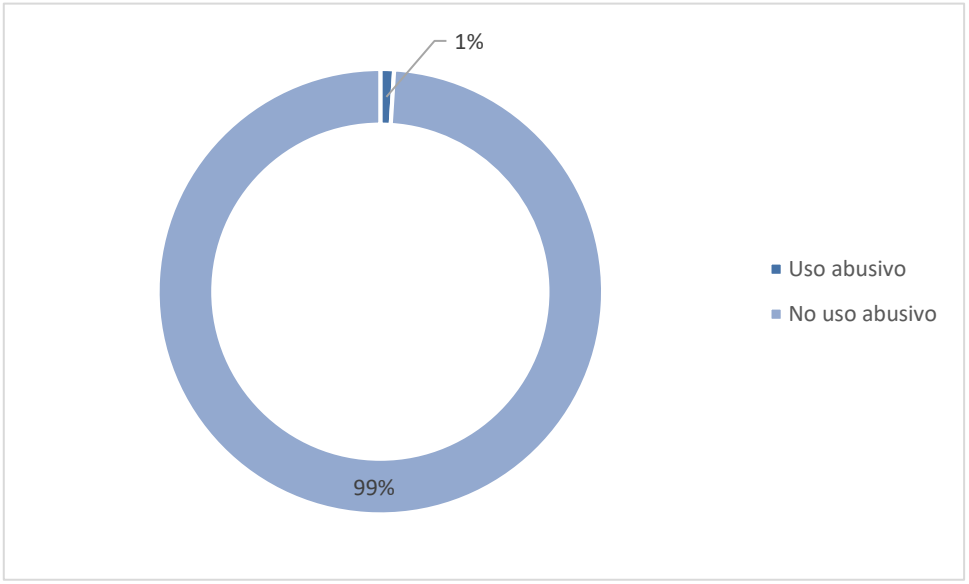
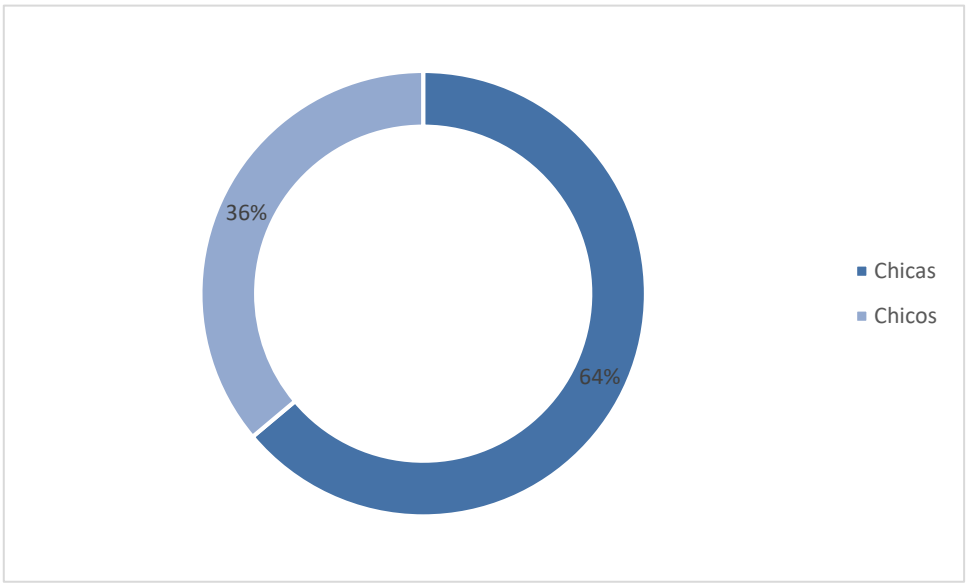
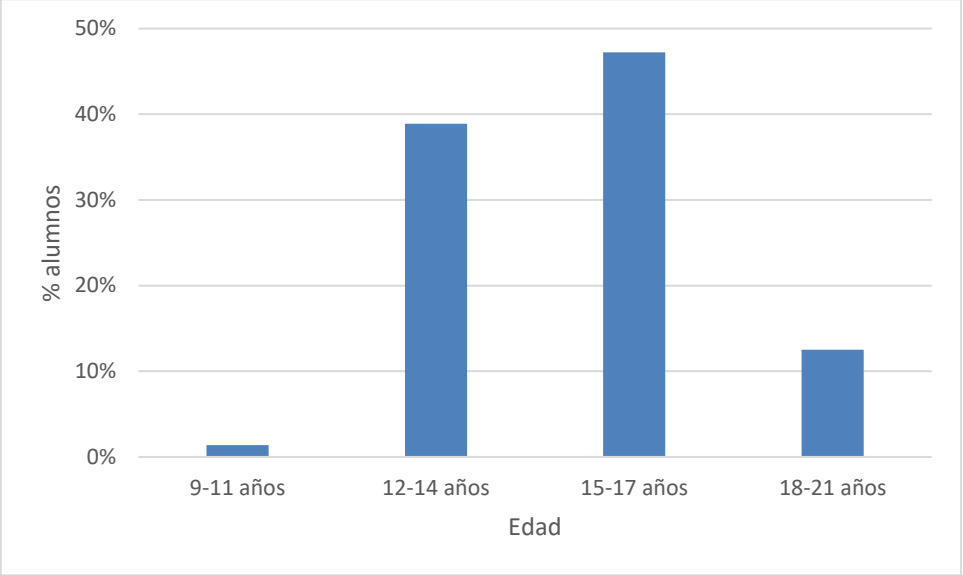


Gráfico 160. *Prevalencia de alumnos que abusan de Internet según sexo*



Si en vez de analizar los resultados según el sexo de los participantes se analizan según su edad, se observa que el 1% tiene entre 9 y 11 años (n = 1), el 39% tiene entre 12 y 14 años (n = 28), el 47% tiene entre 15 y 17 años (n = 34) y el 13% restante tiene entre 18 y 21 años (n = 9).

Gráfico 161. *Prevalencia de alumnos que abusan de Internet según edad*



4.3.2 Otras conductas desviadas

1. Apuestas online

Las apuestas online, conducta que solo se ha medido en los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, no son muy comunes entre los alumnos encuestados. Tan solo un 9% (n = 398) afirma haber realizado apuestas online en el último año. Además, una cantidad importante de estos alumnos no dedica actualmente ninguna hora a la semana a esta actividad (un 23%) y, de los que lo hacen, un 47% le dedica menos de una hora semanal.

Gráfico 162. *Proporción de alumnos que ha realizado apuestas online en el último año*

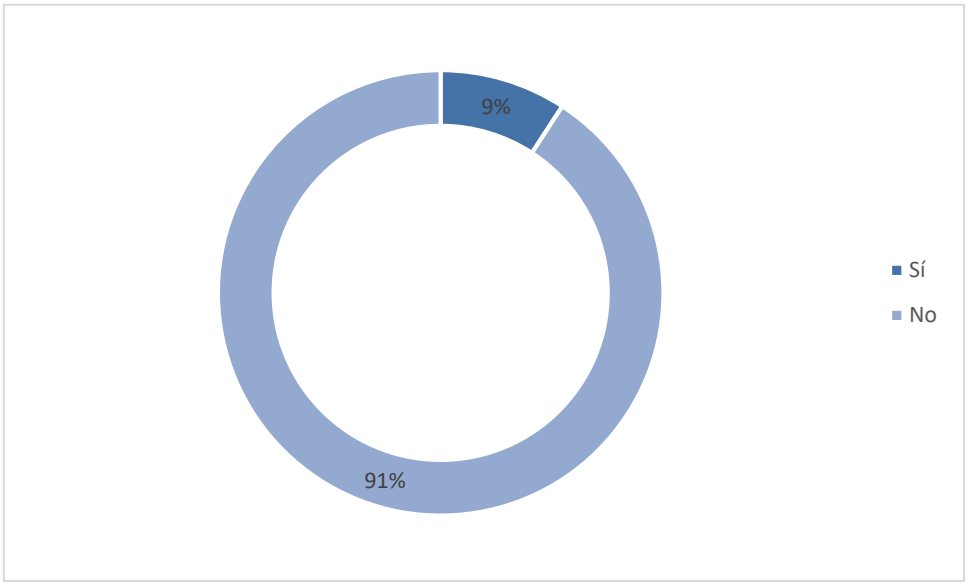
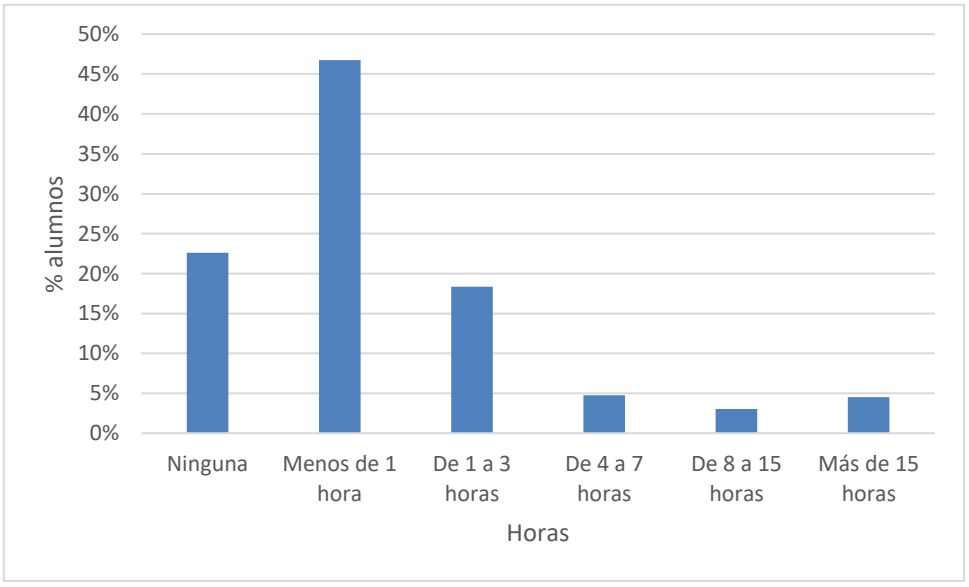


Gráfico 163. *Número de horas dedicadas a la semana a realizar apuestas online*



2. *Sexting*

La conducta de *sexting* hace referencia al acto de enviar o recibir fotos y/o vídeos provocativos o sugerentes a través de Internet de forma voluntaria. Se puede diferenciar entre dos tipos de *sexting*: el activo y el pasivo. El activo hace referencia a que alguien envía el material pornográfico a otra persona, mientras

que el pasivo consiste en que la persona es la receptora de dicho material. A continuación, se detallan los resultados en función del tipo de *sexting*.

1. *Sexting* activo

El 7% de los alumnos (n = 497) afirma haber realizado conductas de *sexting* activo en el último año. Más concretamente, la mayoría de estos alumnos (un 63%) informa de que las fotos o vídeos provocativos fueron enviados a su pareja, seguido de un 24% y 22% de alumnos que enviaron este material a conocidos ajenos al colegio y compañeros de clase, respectivamente.

Gráfico 164. *Proporción de alumnos que han realizado sexting*

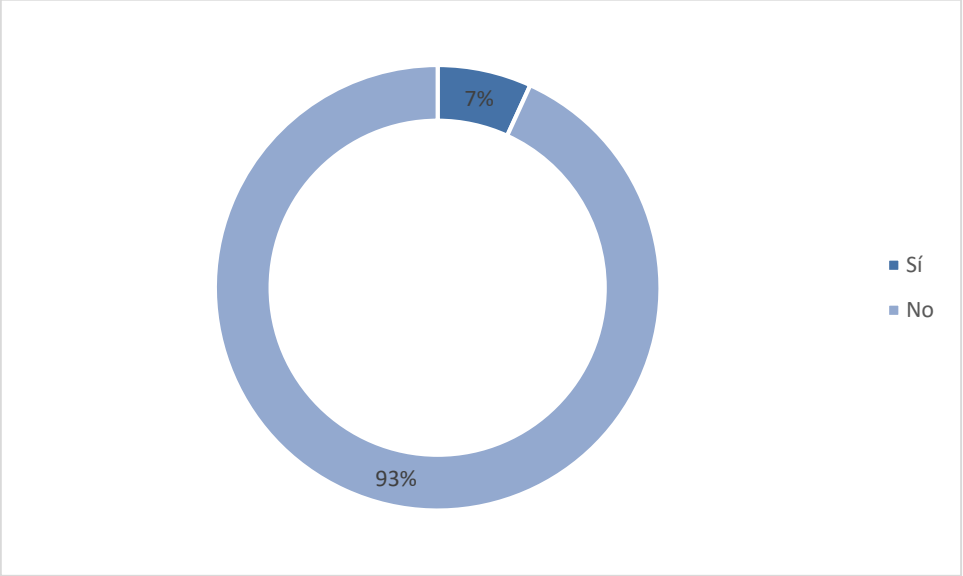
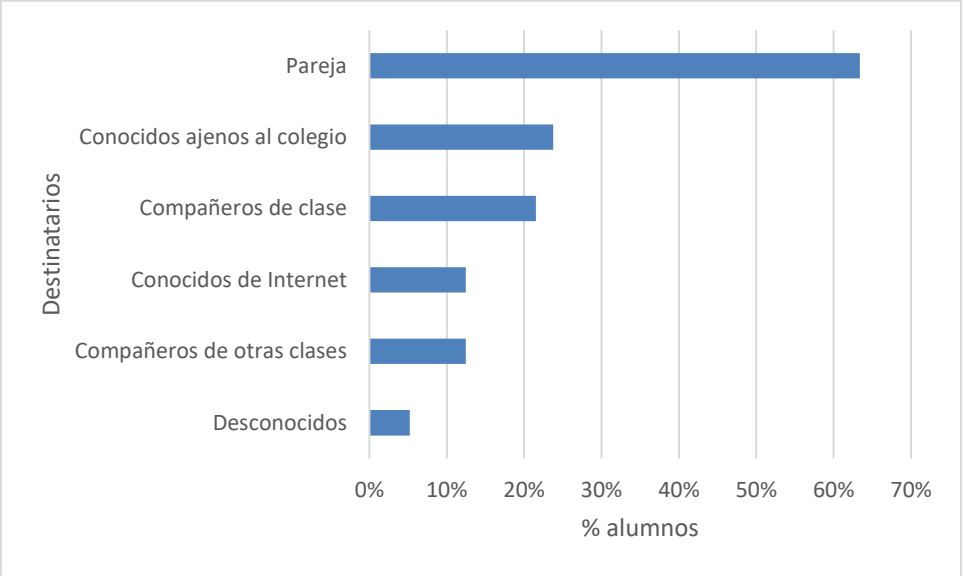
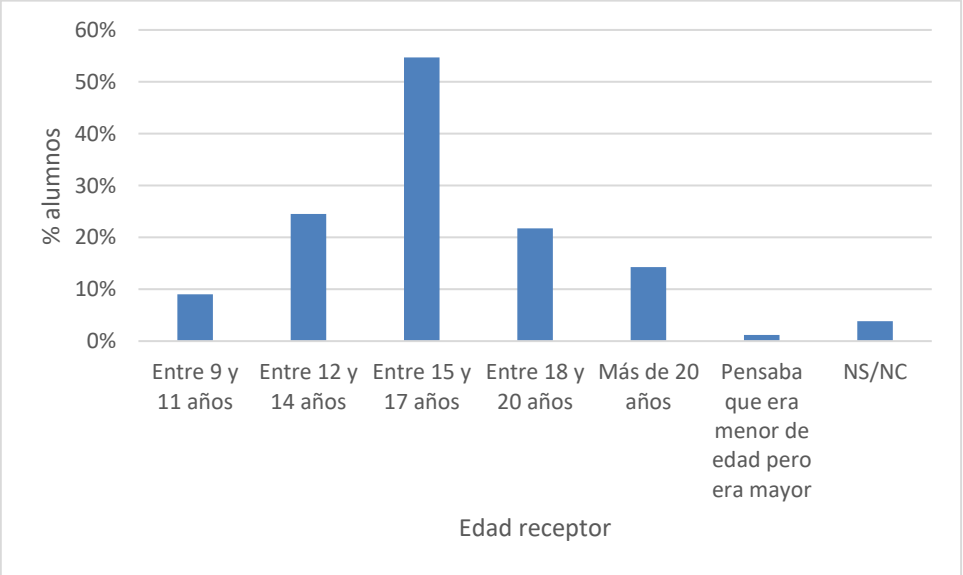


Gráfico 165. *Destinatarios del material pornográfico*



La edad de los receptores del material pornográfico se encuentra, mayoritariamente, entre los 12 y los 20 años y, más concretamente, entre los 15 y los 17, tal y como se puede observar en el gráfico 164.

Gráfico 166. *Edad de los receptores de material pornográfico*



2. *Sexting* pasivo

El 16% de los alumnos (n = 1195) afirma haber realizado conductas de *sexting* pasivo en el último año. Más concretamente, una gran parte de estos alumnos (un 36%) informa de que las fotos o vídeos provocativos fueron enviados por gente desconocida, seguido de un 28% y un 16% que informan que el material lo envió algún compañero de clase o su pareja, respectivamente.

Gráfico 167. *Proporción de alumnos que han realizado sexting pasivo*

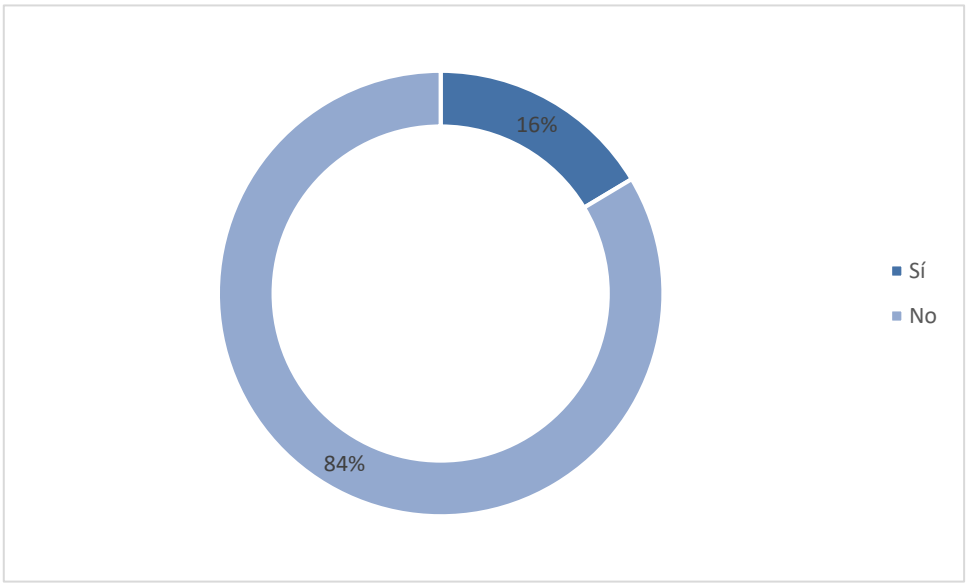
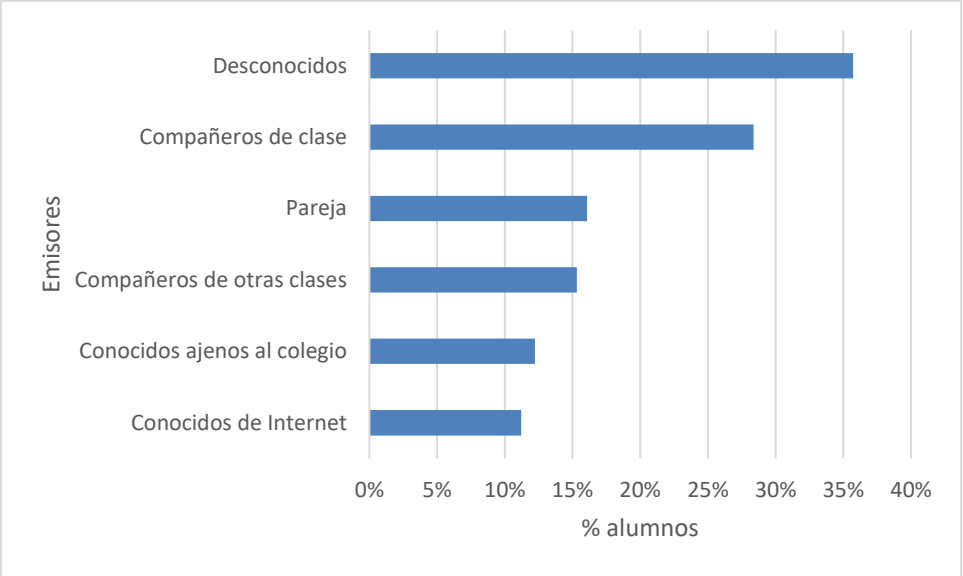
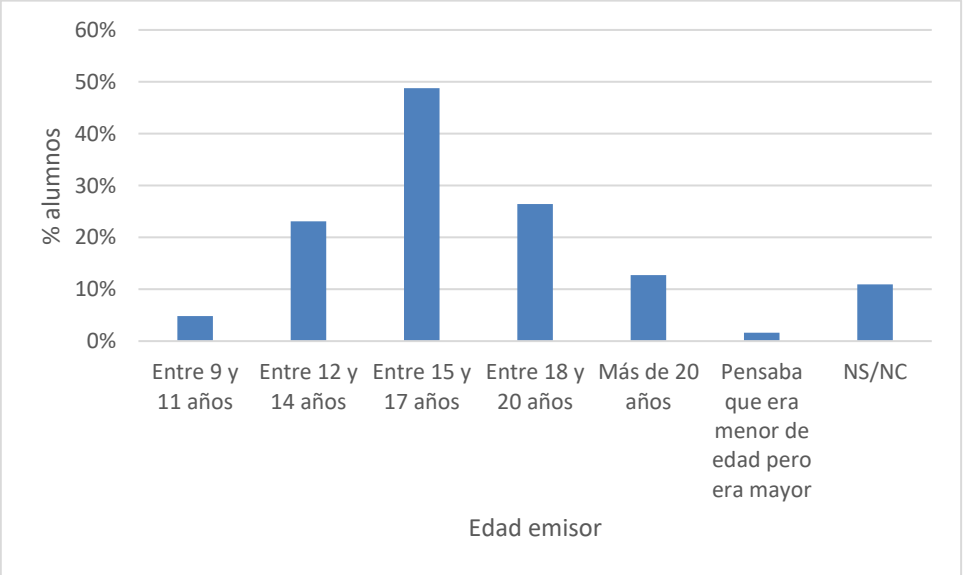


Gráfico 168. *Emisores del material pornográfico*



La edad de los emisores del material pornográfico se encuentra, mayoritariamente, entre los 12 y los 20 años y, más concretamente, entre los 15 y los 17, tal y como se puede observar en el gráfico 167.

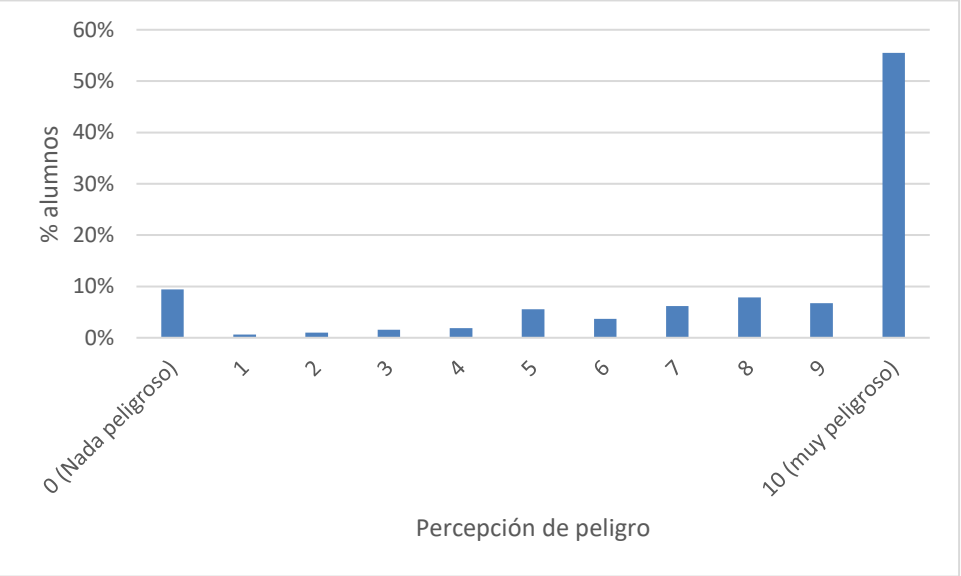
Gráfico 169. *Edad de los emisores de material pornográfico*



Finalmente, se ha preguntado a todos los alumnos, independientemente de si

han realizado o no conductas de sexting, sobre su percepción del peligro que conlleva realizar estas conductas. Los datos indican que más de la mitad de los alumnos, más concretamente, un 55% (n = 4040) considera que realizar conductas de sexting es muy peligroso. En cuanto a aquellos que consideran que no existe ningún tipo de peligro, cabe destacar que el porcentaje asciende al 9% (n = 685).

Gráfico 170. *Percepción de peligro de los alumnos sobre realizar conductas de sexting*



4.4 PERCEPCIÓN Y CONOCIMIENTO DE LOS DOCENTES SOBRE LOS CIBERATAQUES Y USO DESVIADO DE INTERNET QUE AFECTAN A LOS JÓVENES DE CASTILLA Y LEÓN

Tras analizar los datos de la prevalencia de alumnos víctimas de los distintos tipos de ciberataques, ya sean económicos o sociales, así como de alumnos que realizan un uso abusivo de Internet, se procede a analizar lo que los profesores perciben que sucede en los colegios, así como lo que saben. Se ha decidido realizar este análisis desde la perspectiva de los docentes porque, además de los propios alumnos, son los que pueden aportar conocimiento de primera mano y

de calidad sobre todo lo que rodea a los jóvenes. Además, pueden ofrecer su visión acerca de lo que consideran que pasa en sus aulas y cómo afecta ello a la convivencia y rendimiento escolar de los alumnos.

De este modo, en los siguientes apartados se presentan, por un lado, los resultados sobre lo que los docentes consideran que sucede en las escuelas, es decir, su percepción sobre los ciberataques y el uso desviado de Internet que afectan a los alumnos (*apartado 4.4.1*). Por el otro lado, se presentan los resultados sobre casos reales de cibervictimización y abuso de Internet que los docentes han conocido a lo largo de su trayectoria educativa (*apartado 4.4.2*).

4.4.1 Percepción de los docentes sobre la existencia de cibervictimización y uso desviado de Internet entre sus alumnos

A los docentes se les ha preguntado sobre su percepción acerca de la existencia de distintos tipos de cibervictimización, así como sobre la existencia de casos de uso desviado de Internet entre sus alumnos, en tres ámbitos distintos: en las aulas donde imparten clase, en otras aulas del mismo centro educativo en el que imparten clases y en otros centros educativos distintos a los suyos.

En general, cabe destacar que la tendencia general en todos los tipos analizados es que los docentes consideran que en sus centros educativos (tanto en las aulas donde imparten clases como en las otras) hay una prevalencia menor respecto a otros centros educativos. Es decir, los docentes consideran que estas problemáticas suceden con mayor frecuencia en otros centros educativos, pero no en los suyos.

A continuación, se presentan los resultados obtenidos de forma más detallada, analizando primero la percepción de prevalencia de cada conducta de forma individualizada para, después, realizar una comparativa entre los distintos ámbitos (propia aula, otras aulas y otros centros educativos).

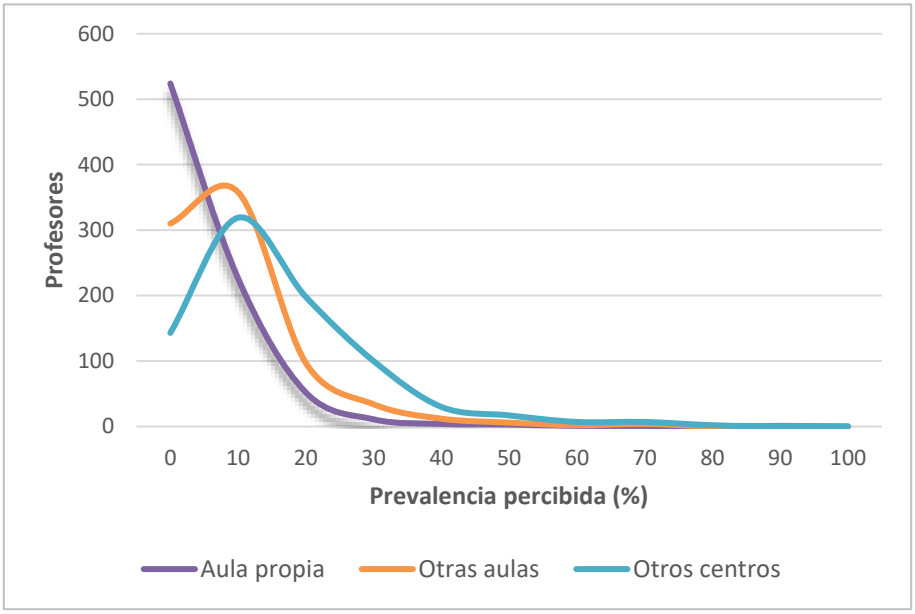
a) Ciberacoso

En cuanto a los casos de ciberacoso, los docentes perciben que en sus aulas hay pocos casos de ciberacoso (más del 60% considera que no hay ningún alumno que sufra dicha conducta), mientras que la prevalencia aumenta cuando se les pregunta por la existencia de ciberacoso en otras aulas y, más aun, en otros centros educativos, tal y como se observa en la tabla 4. Asimismo, se presentan los datos en formato de gráfico, donde se observa claramente la tendencia de considerar que en otros centros la prevalencia de ciberacoso es mayor que en el propio centro.

Tabla 4. *Percepción de los docentes sobre casos de ciberacoso en sus aulas, en otras aulas y en otros centros educativos (n) y (%)*

	En sus aulas		En otras aulas		En otros centros	
Prevalencia (%)	**n**	**p**	**n**	**p**	**n**	**p**
0 (ningún alumno)	524	63,7%	310	37,7%	143	17,4%
10	226	27,5%	358	43,5%	319	38,8%
20	52	6,3%	97	11,8%	198	24,1%
30	11	1,3%	34	4,1%	100	12,2%
40	4	0,5%	12	1,5%	30	3,6%
50	3	0,4%	6	0,7%	17	2,1%
60	1	0,1%	2	0,2%	7	0,9%
70	1	0,1%	4	0,5%	7	0,9%
80	0	0,0%	0	0,0%	2	0,2%
90	1	0,1%	0	0,0%	0	0,0%
100 (todos los alumnos)	0	0,0%	0	0,0%	0	0,0%

Gráfico 171. *Comparativa entre las distintas prevalencias percibidas por los docentes sobre casos de victimización por ciberacoso*



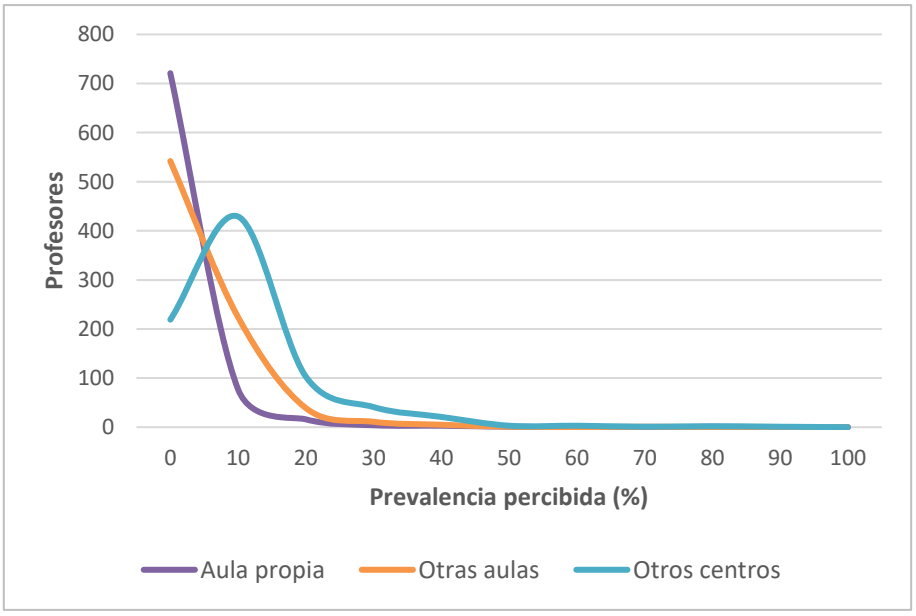
b) Ciberacoso sexual

En cuanto a los casos de cibervictimización sexual, los datos muestran una tendencia similar a lo sucedido en los casos de ciberacoso, aunque en este tipo de cibervictimización la percepción es generalmente más baja (casi un 90% considera que ninguno de sus alumnos sufre cibervictimización sexual, más de un 65% considera que esto no sucede en otras aulas y casi un 30% piensa que tampoco se da en otros centros). Además, en este caso la percepción sobre la existencia de cibervictimización en el aula y la percibida en otras aulas es mucho más similar que en casos de ciberacoso, tal y como se muestra a continuación.

Tabla 5. *Percepción de los docentes sobre casos de cibervictimización sexual en sus aulas, en otras aulas y en otros centros educativos (n) y (%)*

	En sus aulas		En otras aulas		En otros centros	
Prevalencia (%)	**n**	**p**	**n**	**p**	**n**	**p**
0 (ningún alumno)	721	87,6%	542	65,9%	219	26,6%
10	77	9,4%	224	27,2%	429	52,1%
20	16	1,9%	39	4,7%	103	12,5%
30	4	0,5%	11	1,3%	41	5,0%
40	3	0,4%	5	0,6%	21	2,6%
50	1	0,1%	1	0,1%	3	0,4%
60	0	0,0%	0	0,0%	3	0,4%
70	0	0,0%	1	0,1%	1	0,1%
80	1	0,1%	0	0,0%	2	0,2%
90	0	0,0%	0	0,0%	1	0,1%
100 (todos los alumnos)	0	0,0%	0	0,0%	0	0,0%

Gráfico 172. *Comparativa entre las distintas prevalencias percibidas por los docentes sobre casos de cibervictimización sexual*



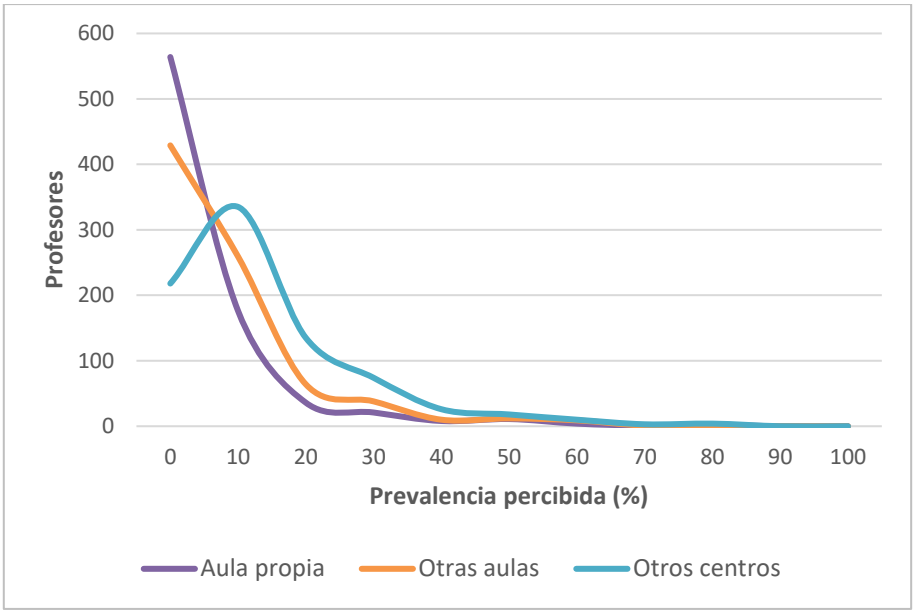
c) Control de pareja a través de las TIC e Internet

En este tipo de cibervictimización, cabe destacar que cuando se pregunta a los docentes sobre la existencia de control de pareja a través de Internet y las TIC en su propia aula y en otras aulas del mismo centro educativo, más de la mitad de los encuestados (68'5% en el primer caso y 52'1% en el segundo) considera que no hay ningún caso. En cambio, al preguntarles por la existencia de esta cibervictimización en otros centros educativos, el porcentaje que considera que no hay ningún caso no llega al 30%, percibiendo una mayor prevalencia en otros centros, la cual ronda el 10-30% de casos percibidos. A continuación, se presentan los datos detallados.

Tabla 6. *Percepción de los docentes sobre casos de control de pareja en sus aulas, en otras aulas y en otros centros educativos (n) y (%)*

	En sus aulas		En otras aulas		En otros centros	
Prevalencia (%)	**n**	**p**	**n**	**p**	**n**	**p**
0 (ningún alumno)	564	68,5%	429	52,1%	218	26,5%
10	176	21,4%	259	31,5%	335	40,7%
20	36	4,4%	64	7,8%	135	16,4%
30	21	2,6%	38	4,6%	74	9,0%
40	8	1,0%	10	1,2%	26	3,2%
50	11	1,3%	12	1,5%	18	2,2%
60	4	0,5%	9	1,1%	10	1,2%
70	1	0,1%	1	0,1%	3	0,4%
80	2	0,2%	1	0,1%	4	0,5%
90	0	0,0%	0	0,0%	0	0,0%
100 (todos los alumnos)	0	0,0%	0	0,0%	0	0,0%

Gráfico 173. *Comparativa entre las distintas prevalencias percibidas por los docentes sobre control de pareja*



d) Ciberataques económicos

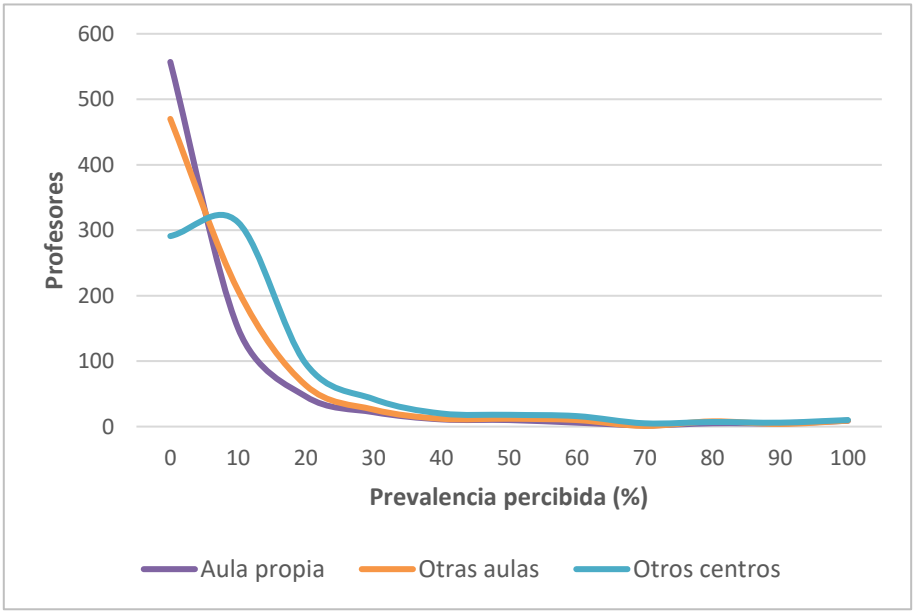
Uno de los aspectos más llamativos de la prevalencia percibida sobre este tipo de cibervictimización es que, en comparación con el resto de tipos analizados, este es el que presenta un mayor porcentaje de docentes que considera que todos sus alumnos han sido víctimas de algún ciberataque económico (un total de 9 profesores consideran que todos los alumnos de su aula han sufrido estos ataques, 10 docentes consideran que en otras aulas todos los alumnos lo han sufrido y 10 docentes consideran que en otros centros educativos, todos los alumnos han sido víctimas de estos casos).

Otro aspecto relevante es que, como en las tres conductas analizadas anteriormente, en este tipo de cibervictimización también existe una tendencia generalizada de pensar que en otros centros hay más casos de ciberataques económicos que en los propios centros y, más aun, que en las propias aulas.

Tabla 7. *Percepción de los docentes sobre casos de cibervictimización económica en sus aulas, en otras aulas y en otros centros educativos (n) y (%)*

	En sus aulas		En otras aulas		En otros centros	
Prevalencia (%)	**n**	**p**	**n**	**p**	**n**	**p**
0 (ningún alumno)	557	67,7%	470	57,1%	291	35,4%
10	150	18,2%	208	25,3%	312	37,9%
20	46	5,6%	63	7,7%	96	11,7%
30	22	2,7%	26	3,2%	42	5,1%
40	11	1,3%	12	1,5%	20	2,4%
50	10	1,2%	12	1,5%	18	2,2%
60	6	0,7%	10	1,2%	16	1,9%
70	2	0,2%	1	0,1%	5	0,6%
80	5	0,6%	8	1,0%	7	0,9%
90	5	0,6%	4	0,5%	6	0,7%
100 (todos los alumnos)	9	1,1%	9	1,1%	10	1,2%

Gráfico 174. *Comparativa entre las distintas prevalencias percibidas por los docentes sobre cibervictimización económica*



e) Uso desviado de Internet

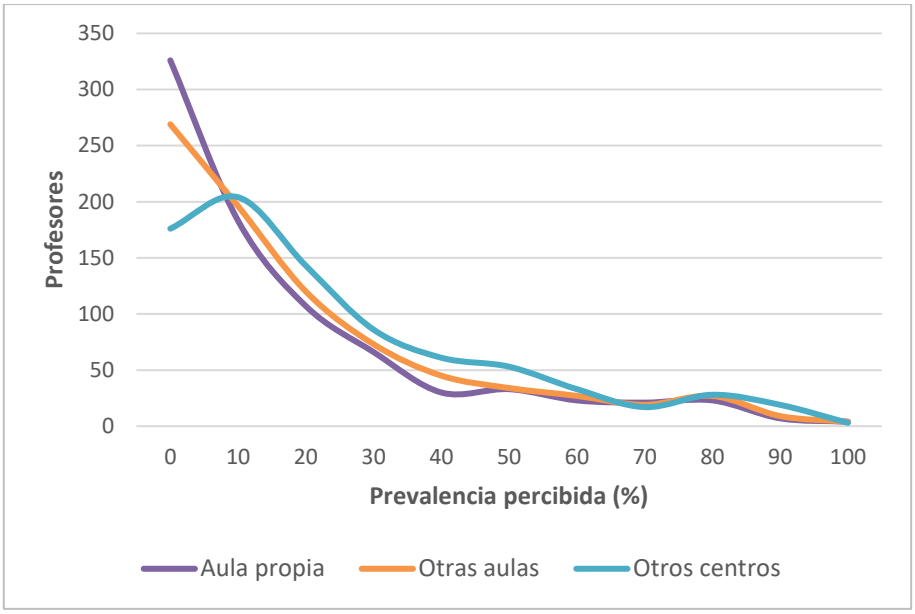
De las cinco conductas analizadas, esta es la que presenta una mayor heterogeneidad de respuestas por parte de los docentes. En otras palabras, es la

conducta en la que existe menos consenso entre docentes, sobre todo al preguntarles por la prevalencia en otros centros. Además, aunque en menor medida, también se observa la tendencia general de percibir que en las aulas donde dan clase no existen tantos casos de uso desviado de Internet como en otras aulas o en otros centros educativos.

Tabla 8. *Percepción de los docentes sobre casos de uso desviado de Internet en sus aulas, en otras aulas y en otros centros educativos (n) y (%)*

	En sus aulas		En otras aulas		En otros centros	
Prevalencia (%)	**n**	**p**	**n**	**p**	**n**	**p**
0 (ningún alumno)	326	39,60%	269	32,70%	176	21,40%
10	183	22,20%	196	23,80%	204	24,80%
20	107	13,00%	120	14,60%	143	17,40%
30	66	8,00%	73	8,90%	86	10,40%
40	30	3,60%	45	5,50%	61	7,40%
50	33	4,00%	34	4,10%	53	6,40%
60	23	2,80%	27	3,30%	33	4,00%
70	21	2,60%	19	2,30%	17	2,10%
80	23	2,80%	27	3,30%	28	3,40%
90	7	0,90%	9	1,10%	19	2,30%
100 (todos los alumnos)	4	0,50%	4	0,50%	3	0,40%

Gráfico 175. *Comparativa entre las distintas prevalencias percibidas por los docentes sobre uso desviado de Internet*



4.4.2 Conocimiento directo de los docentes sobre la existencia de cibervictimización y uso desviado de Internet entre sus alumnos

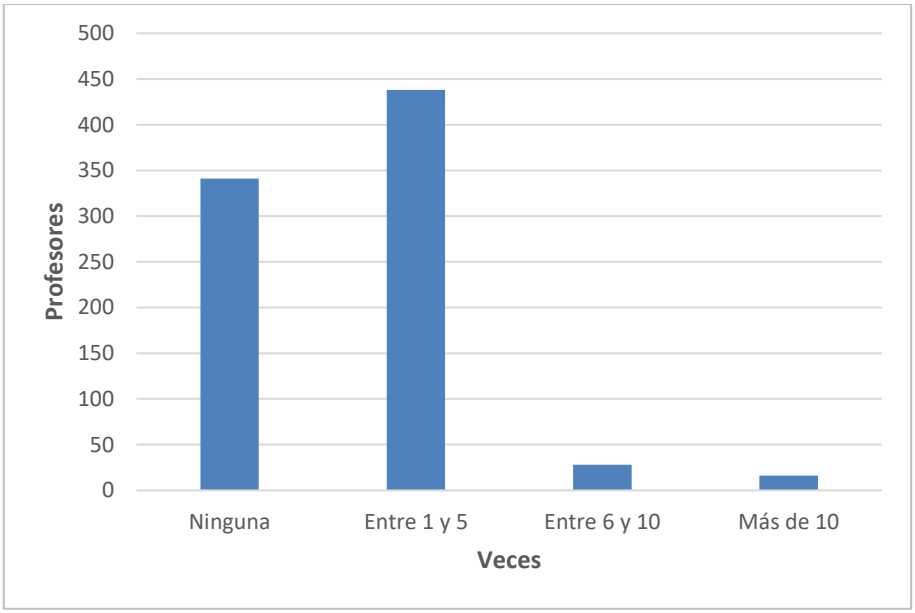
A lo largo de este apartado se presenta, por un lado, datos sobre las veces que los profesores han tenido conocimiento de los distintos tipos de cibervictimización (ciberacoso, ciberacoso sexual, control de pareja a través de las TIC y ciberataques económicos) y uso desviado de Internet entre sus alumnos. Asimismo, también se exponen los resultados sobre el grado de afectación que los profesores perciben que tuvieron esos ataques o uso desviado de Internet sobre el alumno.

Cabe destacar que en las conductas de ciberacoso y ciberacoso sexual también se exponen datos, por un lado, sobre los distintos subtipos que se incluyen dentro de estos ataques y, por el otro, sobre quien consideran los profesores que fue el responsable de estos ataques.

a) Ciberacoso

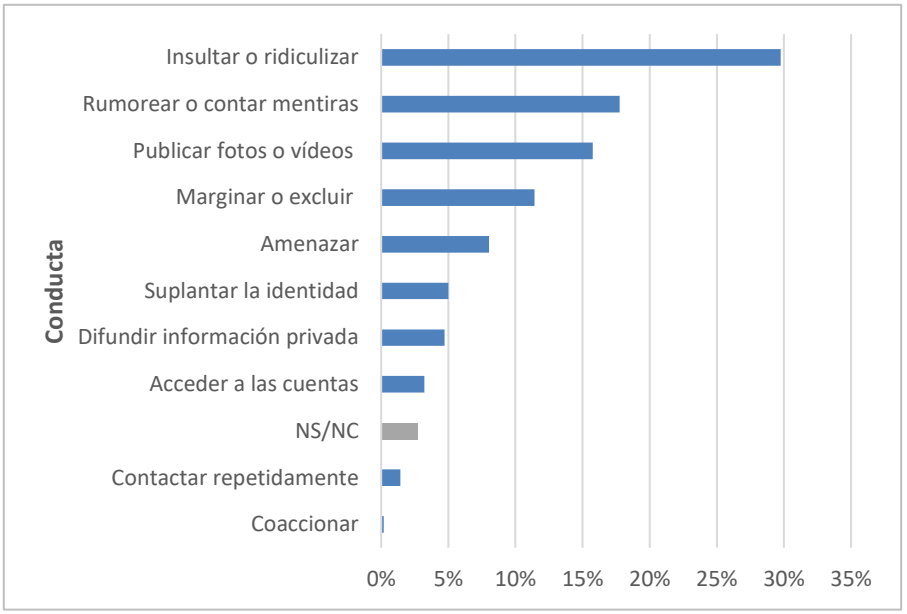
Son muchos los docentes que han detectado a lo largo de sus carreras como profesionales de la enseñanza algún caso de ciberacoso. Más concretamente, un 53,2% de los docentes encuestados ha detectado algún caso de ciberacoso entre 1 y 5 veces, un 3,4% lo ha detectado entre 6 y 10 veces y un 1,9% lo ha hecho en más de 10 ocasiones. En cambio, el porcentaje de docentes que no ha detectado ningún caso real de ciberacoso durante su trayectoria es del 41,4%. A continuación, se muestran estos datos de forma gráfica.

Gráfico 176. *Conocimiento directo del profesorado sobre casos de ciberacoso*



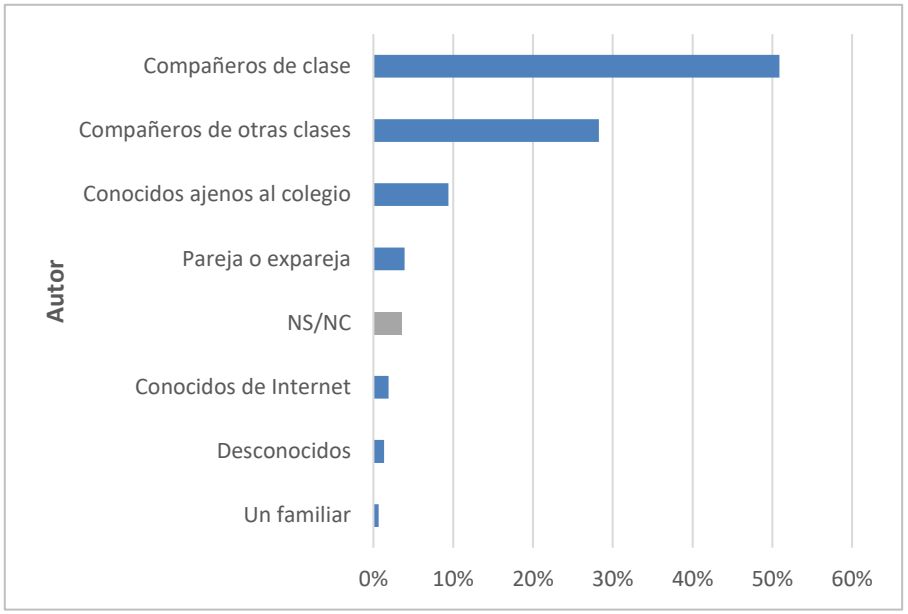
Entre aquellos profesores que sí han detectado casos reales de ciberacoso en sus aulas, se observa que los tipos más frecuentes de ciberacoso se relacionan con insultar o ridiculizar (un 29,7% de los docentes ha tenido un caso de este tipo), seguido de los rumores o mentiras (un 17'8% de los docentes) y la publicación de fotos o vídeos personales (15'8% de los docentes).

Gráfico 177. *Tipo de ciberacoso del que han tenido conocimiento directo los docentes*



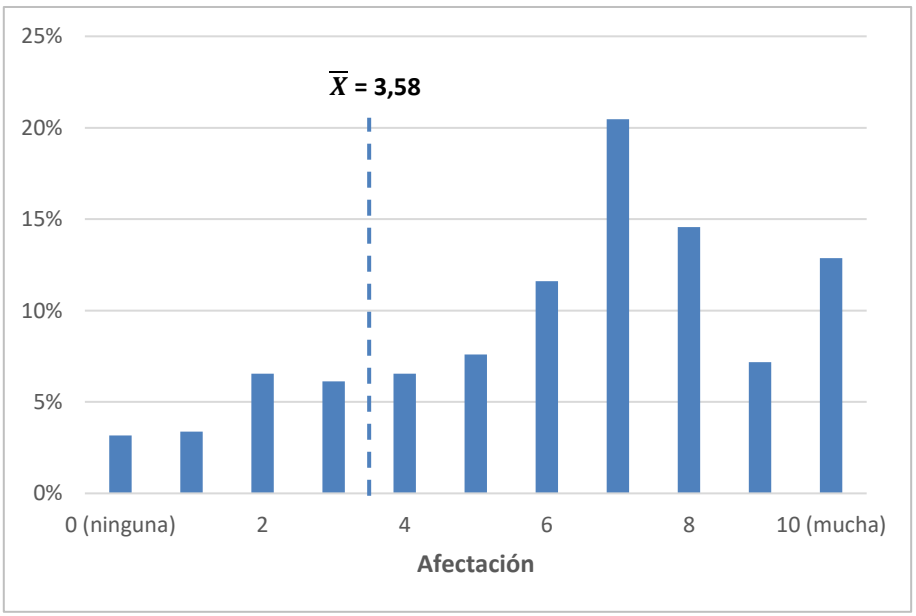
También se les ha preguntado si conocían al autor o autores de dicho ciberacoso, pudiendo escoger más de una opción. Más de un 50% de los profesores encuestados ha admitido que el responsable o los responsables del ciberacoso eran los compañeros de clase, seguido de un 28'3% que manifiesta que los responsables fueron otros compañeros de otras clases. Es decir, se observa que la mayoría de ciberacoso es realizado por compañeros de colegio, con los cuales los menores pasan gran parte del día. El gráfico 176 muestra esta tendencia de una forma muy visible.

Gráfico 178. *Autores de las conductas de ciberacoso de las que han tenido conocimiento directo los docentes*



Finalmente, a la hora de preguntar a los docentes sobre su percepción del grado de afectación en el alumno del ciberacoso sufrido, la mayoría afirma que la afectación es bastante alta, tal y como se observa en el gráfico 177.

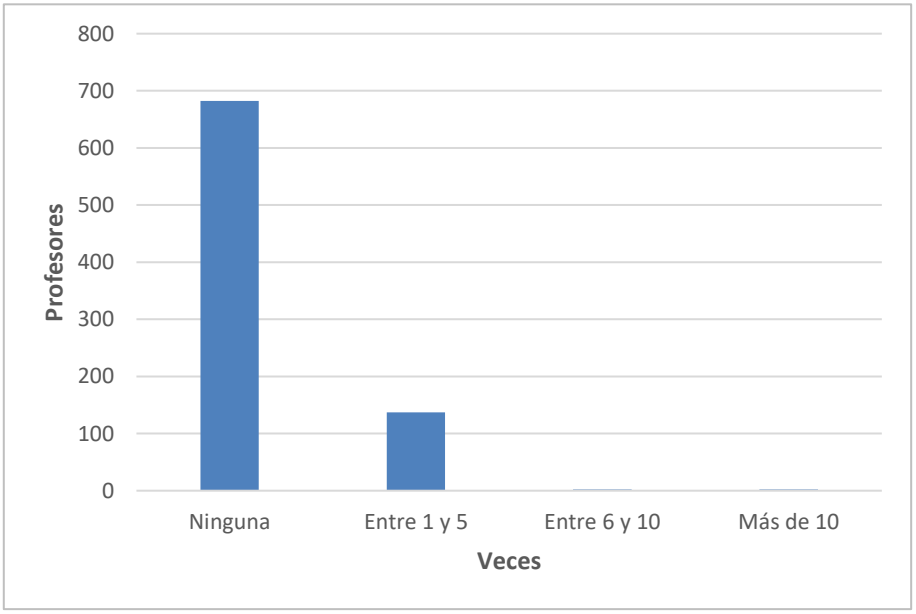
Gráfico 179. *Afectación percibida por los docentes del ciberacoso sufrido por el alumno*



b) Ciberacoso sexual

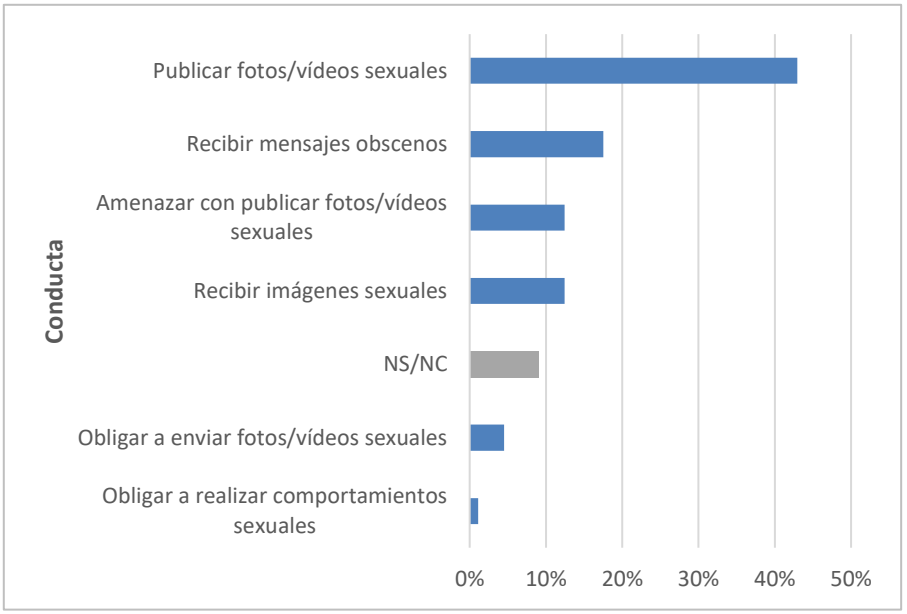
En este caso, el conocimiento directo es mucho menor que en los casos de ciberacoso. De hecho, un 83% de los docentes admite no haber tenido conocimiento de algún caso de ciberacoso sexual a lo largo de su trayectoria profesional. Cabe destacar, además, que el porcentaje de docentes que ha tenido conocimiento de 6 o más casos de ciberacoso sexual es menor al 0,5%. Este dato, sin embargo, no indica que no haya casos de ciberacoso sexual, sino que éste es detectado en menor medida por los docentes.

Gráfico 180. *Conocimiento directo del profesorado sobre casos de ciberacoso sexual*



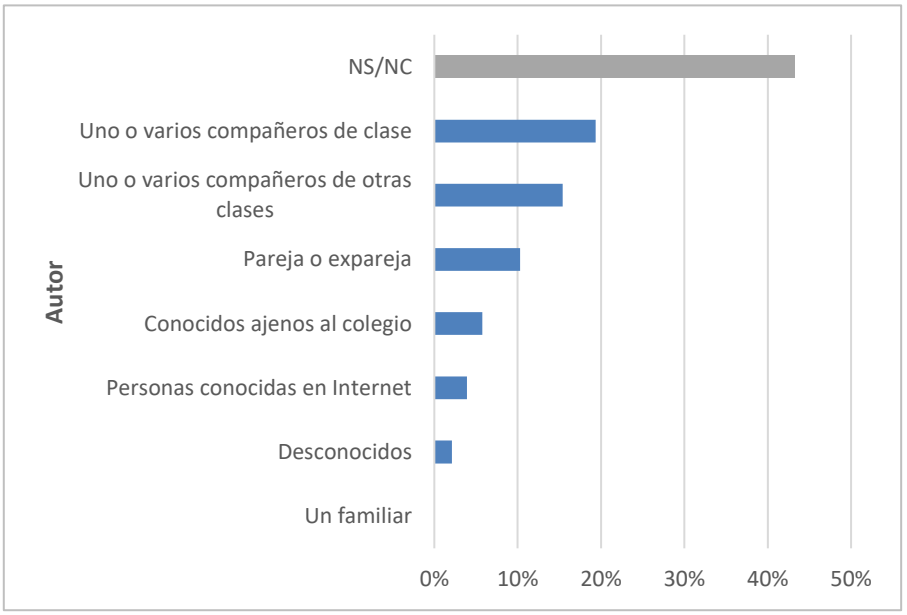
Entre aquellos profesores que han detectado casos de este tipo, un 43% afirma que el tipo de ciberacoso sexual más frecuente es el que consiste en publicar fotografías o vídeos de carácter sexual. Sin embargo, existen otros tipos de ciberacoso también presentes, como son recibir mensajes obscenos (el 17,5% de docentes afirma haber tenido casos de este tipo), ser amenazado con publicar fotos o vídeos de carácter sexual (el 12,4% de los docentes) y recibir imágenes de contenido sexual (también el 12,4% de los docentes).

Gráfico 181. *Tipo de ciberacoso del que han tenido conocimiento directo los docentes*



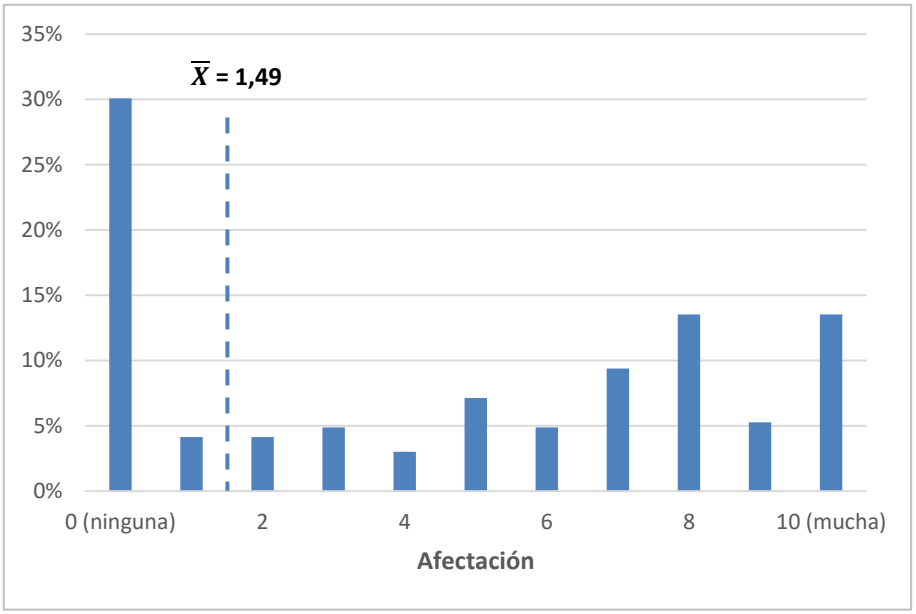
Además, en cuanto a los autores de dichas conductas, el 43,2% de los docentes no sabe quién fue, mientras que el 19,3% indica que fueron uno o varios compañeros de clase y el 15,4% informa que fueron uno o varios compañeros de otras clases. En general, existe un gran desconocimiento por parte de los docentes sobre todo lo que envuelve a las conductas de ciberacoso sexual, sobre todo en relación a los autores de dichas conductas.

Gráfico 182. *Autores de las conductas de ciberacoso sexual de las que han tenido conocimiento directo los docentes*



Finalmente, en cuanto a la percepción de los docentes sobre el grado de afectación en el alumno del ciberacoso sexual sufrido, son 80 los docentes (un 30,1%) que consideran que la situación no afectó en absoluto al menor. Sin embargo, el porcentaje de docentes que considera que la situación afectó mucho al alumno asciende a un 13,5%.

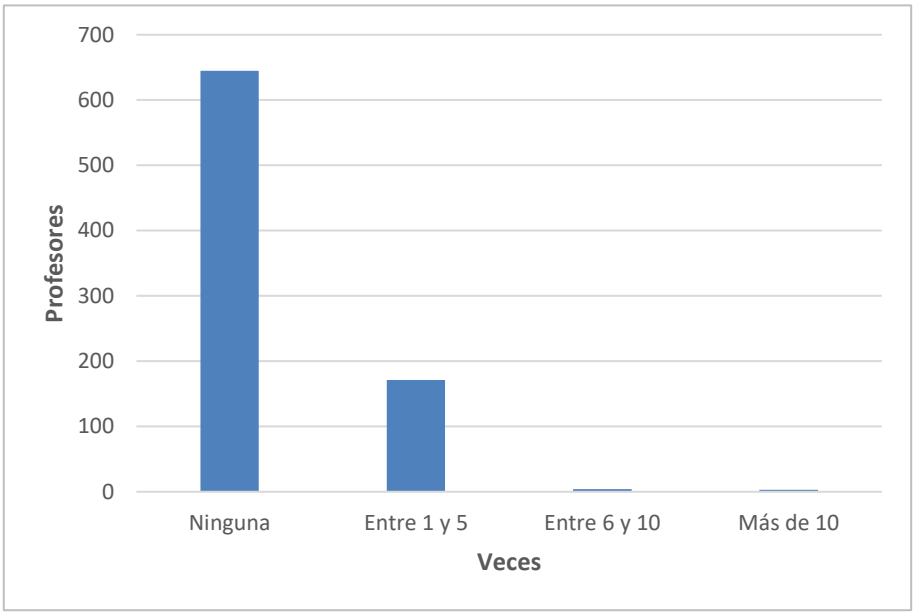
Gráfico 183. *Afectación percibida por los docentes del ciberacoso sexual sufrido por el alumno*



c) Control de pareja a través de las TIC e Internet

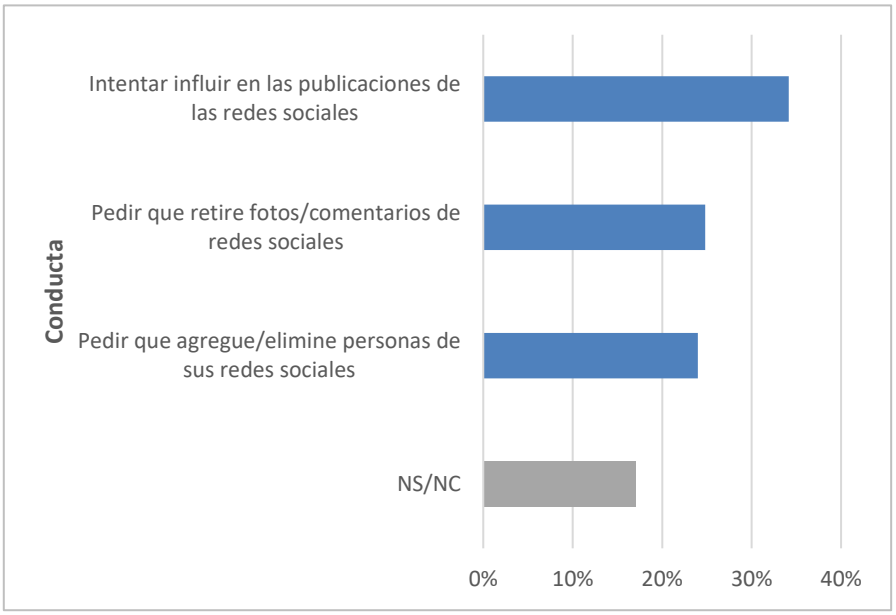
El porcentaje de docentes que ha tenido conocimiento entre 1 y 5 veces sobre algún caso de control de pareja a través de las TIC entre sus alumnos es ligeramente superior que en casos de ciberacoso sexual (un 20,8% de los docentes). Sin embargo, el porcentaje de docentes que nunca ha tenido casos de este tipo sigue siendo muy elevado, alcanzando la cifra del 78,4%.

Gráfico 184. *Conocimiento directo del profesorado sobre casos de control de pareja a través de las TIC e Internet*



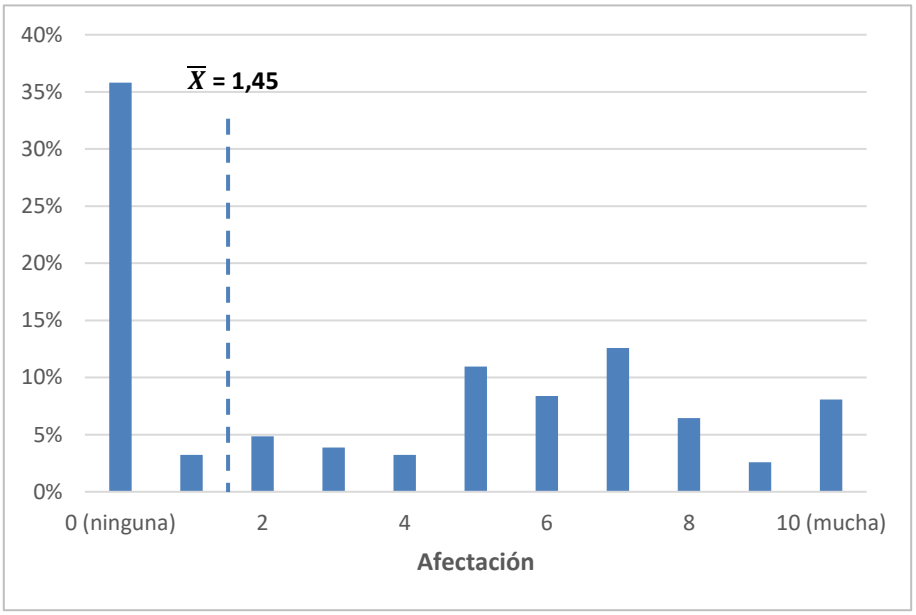
No se observan grandes diferencias en la prevalencia de los distintos tipos de control de pareja a través de las TIC conocidos por los docentes, aunque el que es detectado en mayor medida es el de intentar influir en las publicaciones de las redes sociales de la pareja (un 34,1% de docentes ha tenido conocimiento de este tipo de control de pareja). Además, continúa habiendo una cifra importante de docentes que no conoce el tipo de control ejercido (un 17% de los docentes).

Gráfico 185. *Tipos de control de pareja a través de las TIC de los que han tenido conocimiento directo los docentes*



Respecto al grado de afectación percibido por los docentes en este tipo de conductas, cabe destacar que un alto porcentaje (casi un 36%) considera que este hecho no afectó al alumno. Sin embargo, el resto de percepciones varían un poco más que en el caso del ciberacoso y el ciberacoso sexual.

Gráfico 186. *Afectación percibida por los docentes del control de pareja a través de las TIC sufrido por el alumno*



c) Ciberataques económicos

Este es el tipo de cibervictimización que presenta una menor prevalencia de conocimiento por parte de los docentes. Un 87% indica no haber tenido nunca un caso de este tipo, mientras que solo un 10% afirma haber tenido entre 1 y 5 casos a lo largo de toda su trayectoria. En el gráfico 185 se observan muy claramente las distintas prevalencias.

Respecto al tipo de cibervictimización detectada, el más frecuente es la infección por *malware* (27,7% de los docentes), seguido de la pérdida de información por infección de *malware* (20,5% de los docentes) y el *scam* (18,2% de los docentes). En general, las prevalencias son bastante similares en todos los tipos y el número de profesores que desconoce el tipo de ciberataque es menor que en las anteriores conductas analizadas (ciberacoso, ciberacoso sexual y control de pareja).

Gráfico 187. *Conocimiento directo del profesorado sobre casos de cibervictimización económica*

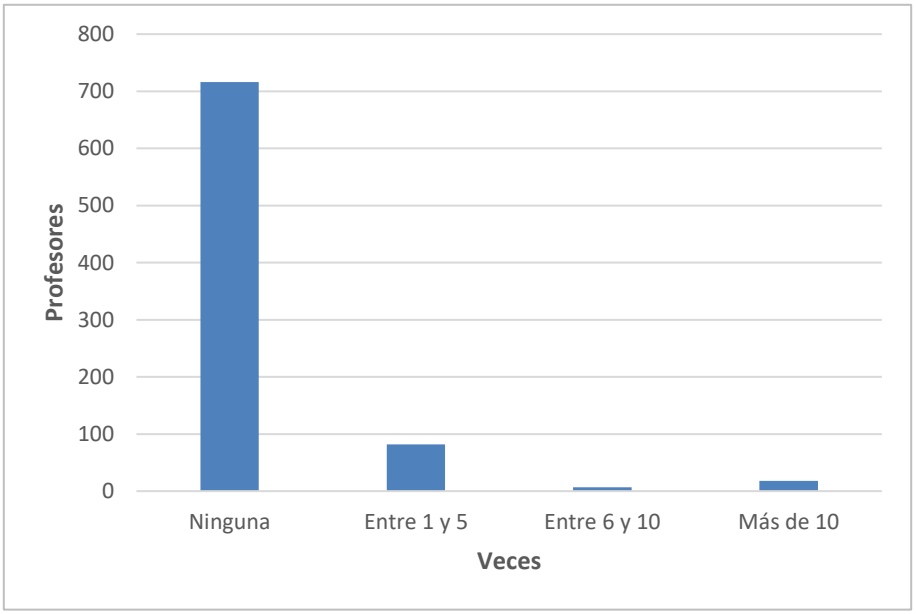
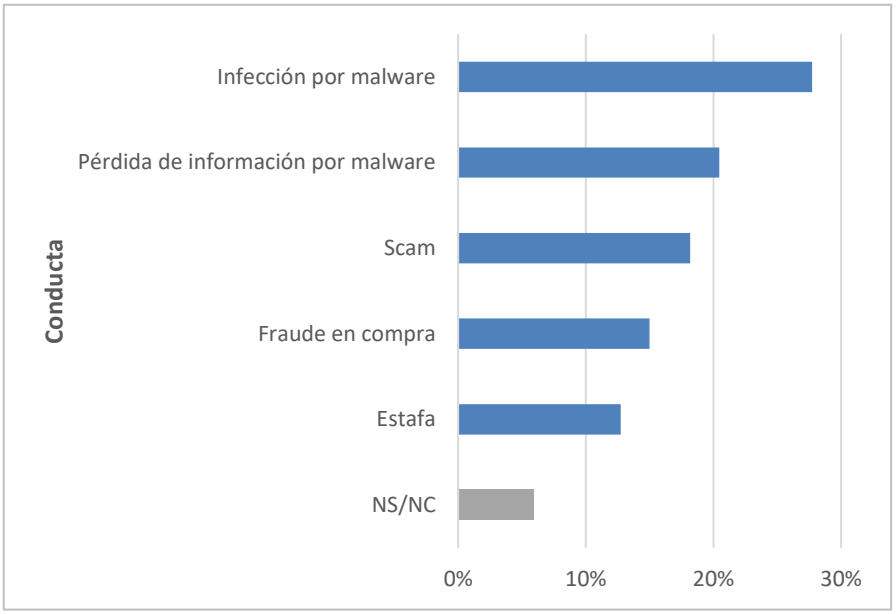
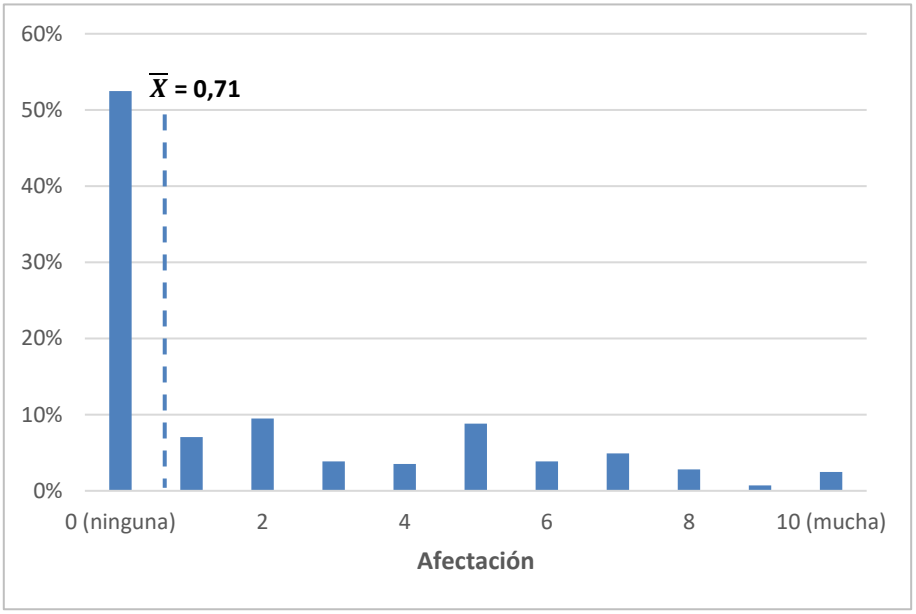


Gráfico 188. *Conocimiento directo del profesorado sobre casos cibervictimización económica*



En cuanto a la afectación percibida en el menor, la mayoría de los docentes (52,5%) considera que estos ataques no le afectaron nada, siendo muy pocos los docentes que consideran que estos ataques afectaron algo al menor, ya fuese en mayor o menor medida.

Gráfico 189. *Afectación percibida de los docentes de los ciberataques económicos sufridos por el alumno*



e) Uso desviado de Internet

Después del ciberacoso, esta es la conducta sobre la que mayor conocimiento tienen los docentes (casi un 30% tiene conocimiento de entre 1 y 5 casos). Además, el porcentaje de docentes que tienen conocimiento de más de 10 casos también es superior, llegando prácticamente al 6%. El porcentaje de docentes que no tiene conocimiento sobre casos de este tipo, aunque sigue siendo elevado, es más bajo que en el resto de conductas analizadas (un 62,3% de los docentes), a excepción del ciberacoso.

Además, el tipo de uso desviado de Internet más detectado por los docentes es el uso abusivo del mismo, cifra que asciende a casi el 75% de los docentes que han detectado casos de uso abusivo a lo largo de su carrera profesional.

Gráfico 190. *Conocimiento directo del profesorado sobre casos de uso desviado de Internet*

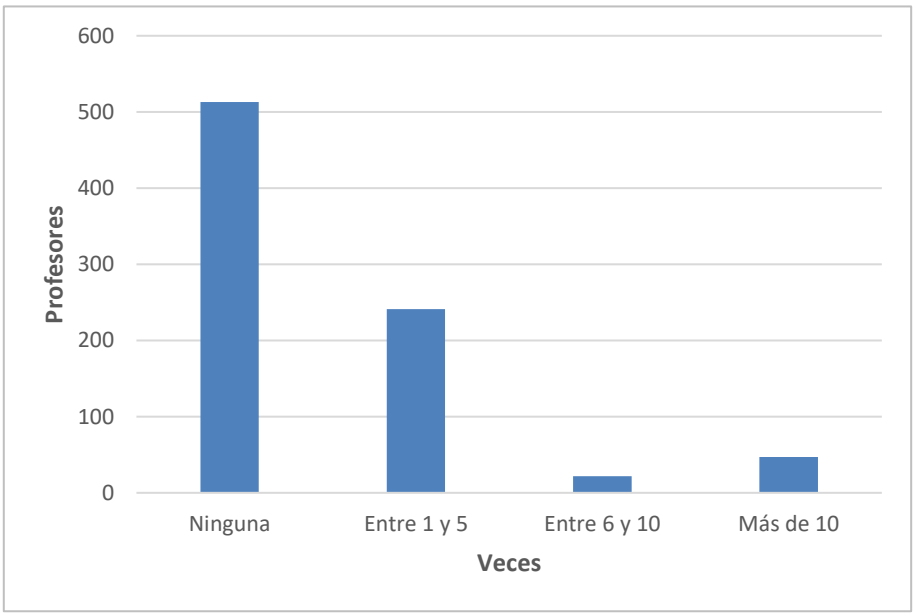
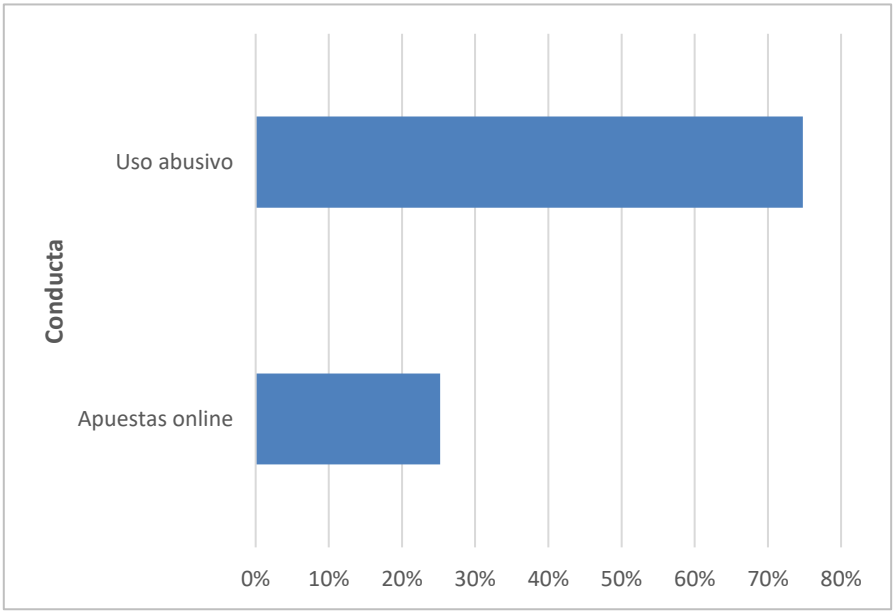


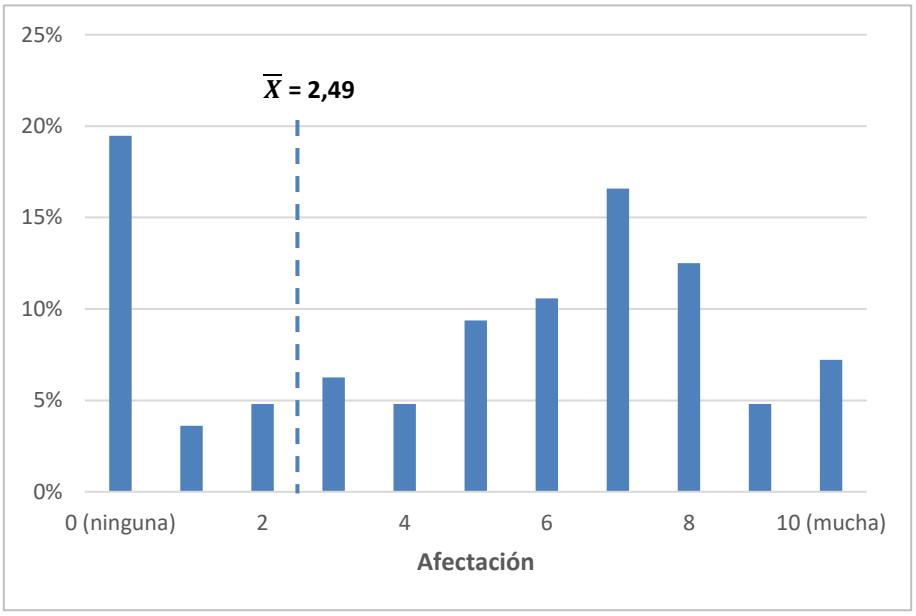
Gráfico 191. *Tipos de uso desviado de Internet del que han tenido conocimiento directo los docentes*



Finalmente, en este caso la afectación percibida en el menor por parte de los docentes es mucho más elevada que en el resto de victimizaciones analizadas, a excepción, de nuevo, del ciberacoso. Además, en este caso la percepción es mucho más heterogénea, ya que hay más variedad entre lo que piensan los

docentes, tal y como se observa en el siguiente gráfico.

Gráfico 192. *Afectación percibida de los docentes uso desviado de Internet del alumno*



4.5 HÁBITOS EN EL USO DE LAS TIC DE LOS JÓVENES DE CASTILLA Y LEÓN

Como bien se ha introducido al inicio del capítulo, el siguiente apartado está reservado a los resultados obtenidos tras el análisis del uso que hacen los alumnos de las TIC e Internet. La importancia de este análisis recae en el hecho de que los menores, con sus actos, pueden exponerse en mayor o menor medida a los ciberataques. Esta idea, presentada ya en el Capítulo II de este informe, se incluye en la reformulación que Miró (2013) hace de la Teoría de las Actividades Rutinarias de Cohen y Felson (1979). En otras palabras, toda interacción en el ciberespacio hace que la persona sea más visible por otras y, en consecuencia, el riesgo de ser víctima de un ciberataque aumente.

En definitiva, el análisis del uso que los alumnos realizan de las TIC y las actividades que realizan en Internet permitirá conocer cuáles son los factores de riesgo relacionados con el hecho de ser víctima de un ciberataque, información que se expondrá en la fase 2 del proyecto Saf_*e*.

La estructura de este apartado es, por tanto, la siguiente. En primer lugar, se presentan varios datos relacionados con el uso que hacen los alumnos del ordenador, el móvil y la tablet. En segundo lugar, se presentan las principales herramientas de comunicación utilizadas por los alumnos, que son las siguientes:

a) Redes sociales
b) Correo electrónico
c) Blogs, vídeo blogs y cuentas de YouTube
d) Videollamadas
e) Webs de contacto

Finalmente, se profundiza en las actividades que los alumnos realizan cuando navegan por Internet, las cuales se esquematizan en el siguiente listado:

a) Comprar por Internet
b) Facilitar datos personales
c) Contactar con desconocidos
d) Abrir enlaces o descargar archivos de Internet
e) Realizar comportamientos sexuales online
f) Jugar online
g) Guardar información en el ordenador y el móvil
h) Usar antivirus
i) Usar contraseñas

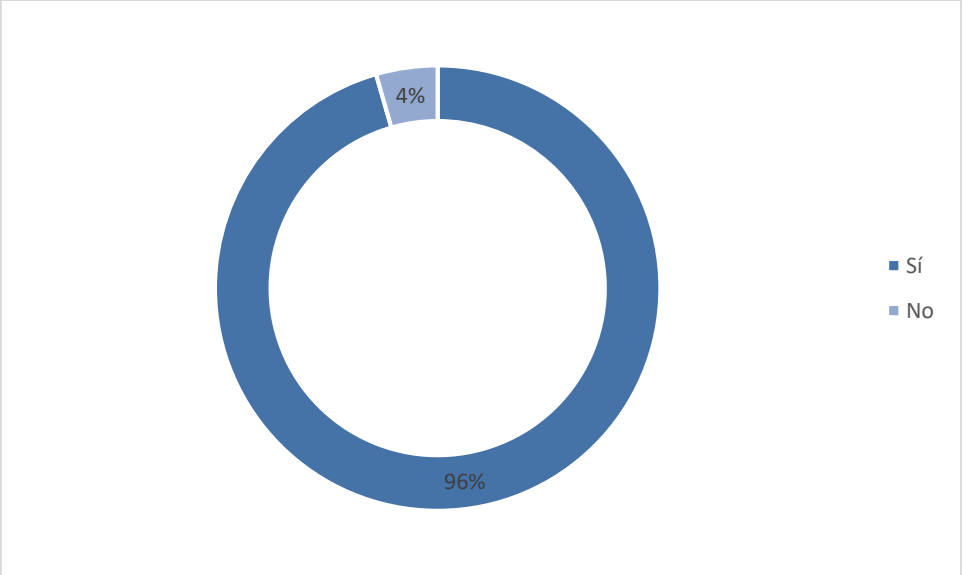
4.5.1 Uso de las Tecnologías de la Información y la Comunicación

a) Uso del ordenador

Hoy en día los ordenadores están plenamente integrados en la vida de las

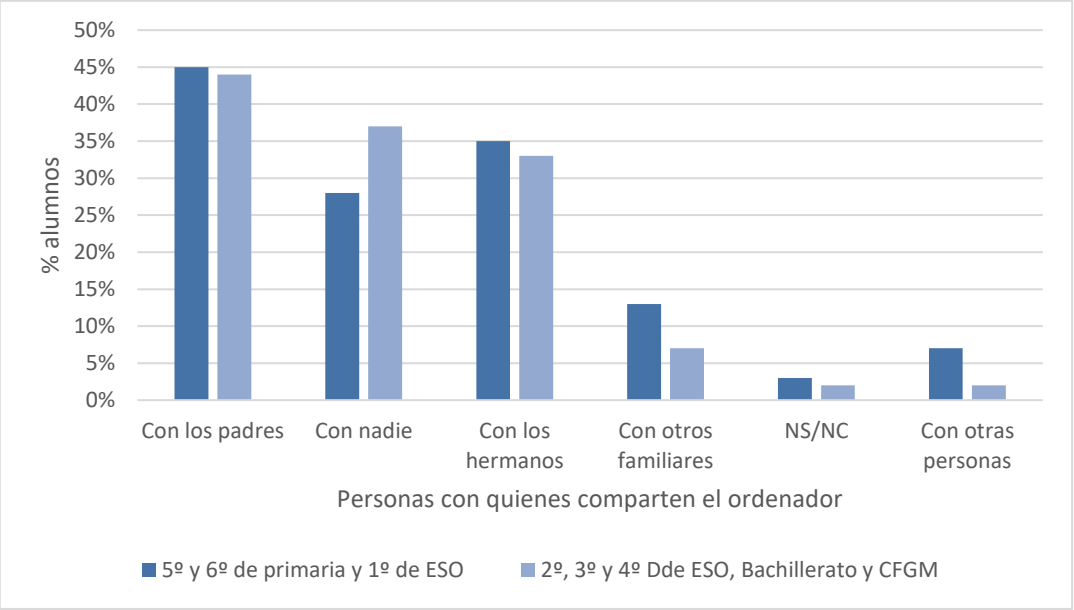
personas, sobre todo de las más jóvenes. Estas máquinas, cada vez más complejas, forman parte del crecimiento y desarrollo de los jóvenes y les ofrecen un amplio abanico de oportunidades para relacionarse, interaccionar y aprender a través de la red. En este estudio, el 96% de los alumnos dispone de un ordenador con conexión a Internet. Más concretamente, el 94% de alumnos más pequeños (5º y 6º de Primaria y 1º de ESO) y casi el 97% de mayor edad (resto de la ESO, Bachillerato y CFGM) dispone de esta herramienta.

Gráfico 193. *Menores que disponen de un ordenador con conexión a Internet (visión global)*



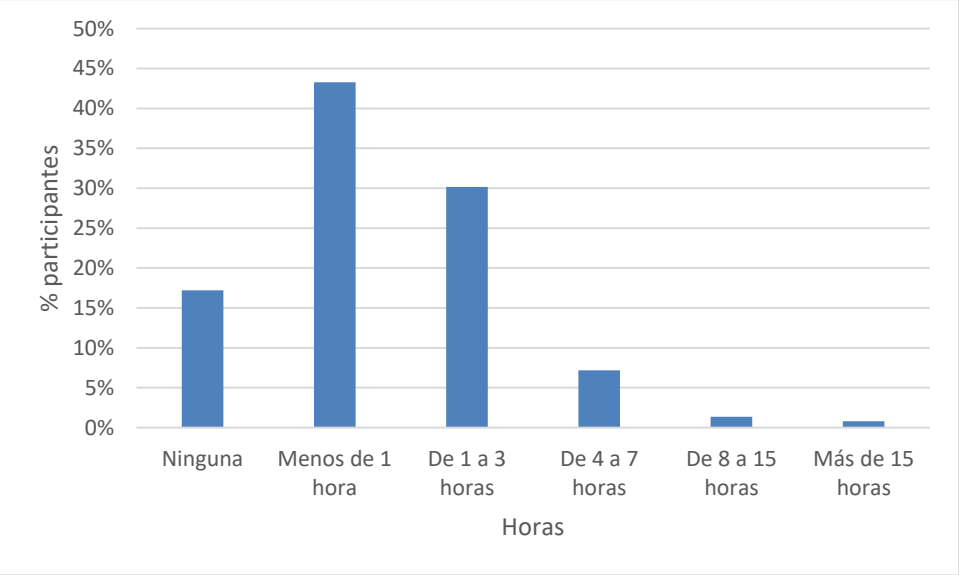
Entre los alumnos que tienen ordenador, cabe destacar algunos aspectos interesantes de analizar. Entre los más jóvenes, el 52% afirma compartir el ordenador con alguien, frente a un 54% de alumnos de mayor edad. La mayoría de alumnos, tanto en un caso como en otro, comparten el ordenador con sus padres y sus hermanos, tal y como se observa en el siguiente gráfico. Además, cabe destacar que existe una mayor proporción de alumnos de mayor edad que dice no compartir ordenador.

Gráfico 194. *Personas con quienes los alumnos comparten el ordenador*



En cuanto a las horas que pasan los jóvenes usando el ordenador, cabe mencionar que la mayoría pasa, como máximo, 3 horas al día. Prácticamente no existen diferencias en función de la etapa educativa, ya que los porcentajes son los mismos.

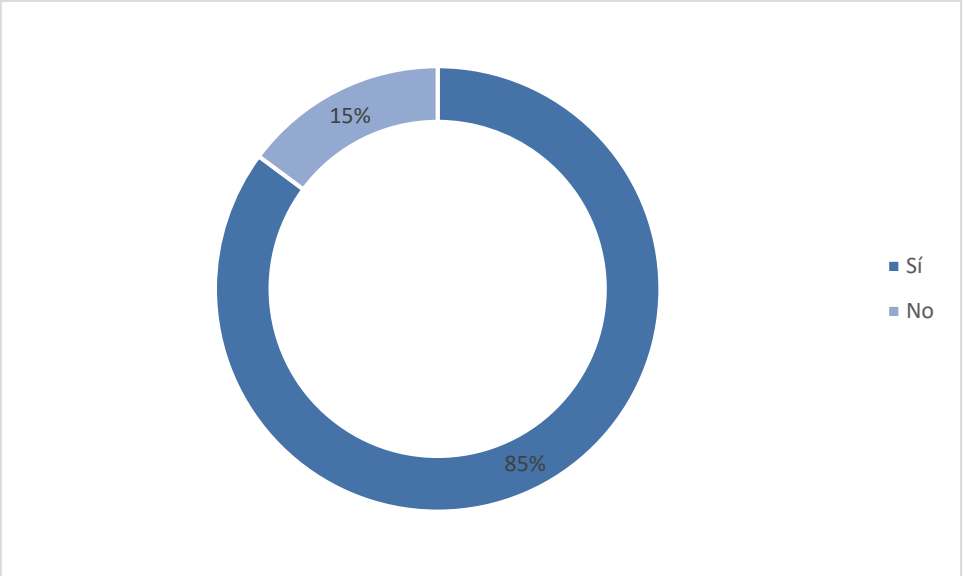
Gráfico 195. *Horas al día que pasan los alumnos utilizando el ordenador*



b) Uso del móvil y la tablet

El móvil, como el ordenador, también es un aparato integrado plenamente en la vida de los jóvenes, quienes lo usan a diario con finalidades muy distintas. Globalmente, el 85% de los alumnos (n = 6201) afirma disponer de un teléfono móvil con conexión a Internet.

Gráfico 196. *Proporción de menores que dispone de un teléfono móvil con conexión a Internet*

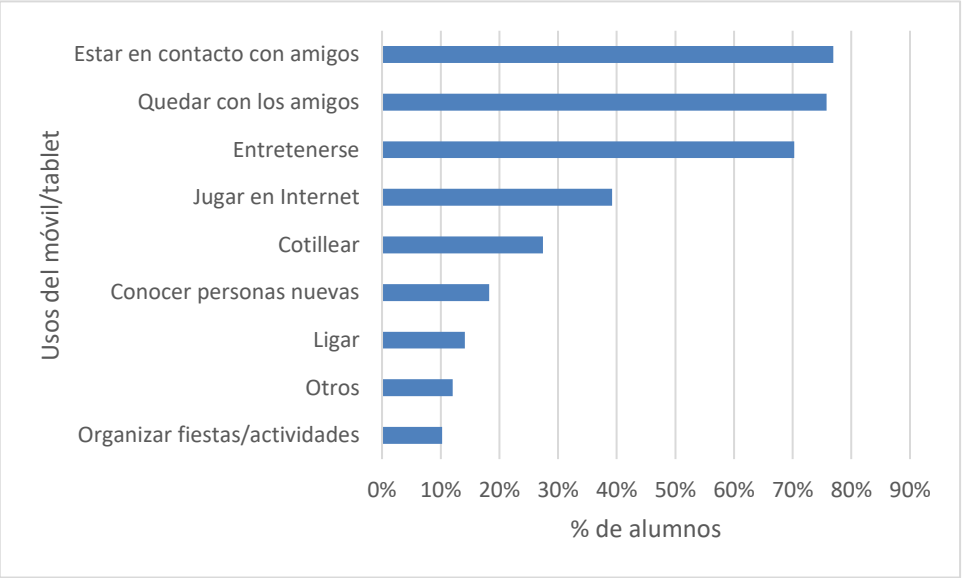


En este caso, sin embargo, sí que existen diferencias más marcadas entre los alumnos de menor edad y los que son un poco más mayores. En el caso de los más pequeños, un 67,4% afirma disponer de un teléfono móvil o tablet con conexión a Internet, cifra mucho más baja que en el caso del ordenador. En cuanto a los más grandes, el 97,3% afirma tener un móvil o tablet con conexión a Internet, cifra prácticamente idéntica a la que se ha obtenido en el caso del ordenador.

Entre aquellos que han afirmado que disponen de un teléfono móvil con conexión a Internet, se observa que la mayoría, tanto en un rango de edad como en otro, lo utilizan para quedar con los amigos o estar en contacto con ellos. En

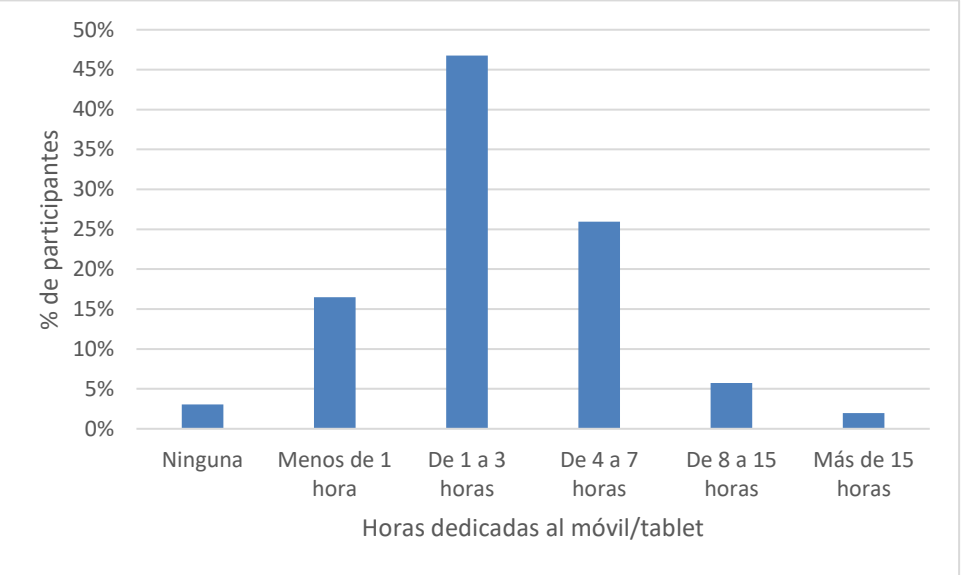
general, los usos que dan a esta herramienta son muy similares en ambos casos.

Gráfico 197. *Usos que dan los alumnos al móvil o tablet*



En cuanto a las horas diarias dedicadas a utilizar el teléfono móvil, información que solo está disponible en el caso de los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM debido a que se eliminó dicha pregunta del cuestionario adaptado para los alumnos más pequeños, cabe destacar que el tiempo de uso es mayor que en el caso del ordenador.

Gráfico 198. *Horas al día que pasan los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM utilizando el móvil o la tablet*

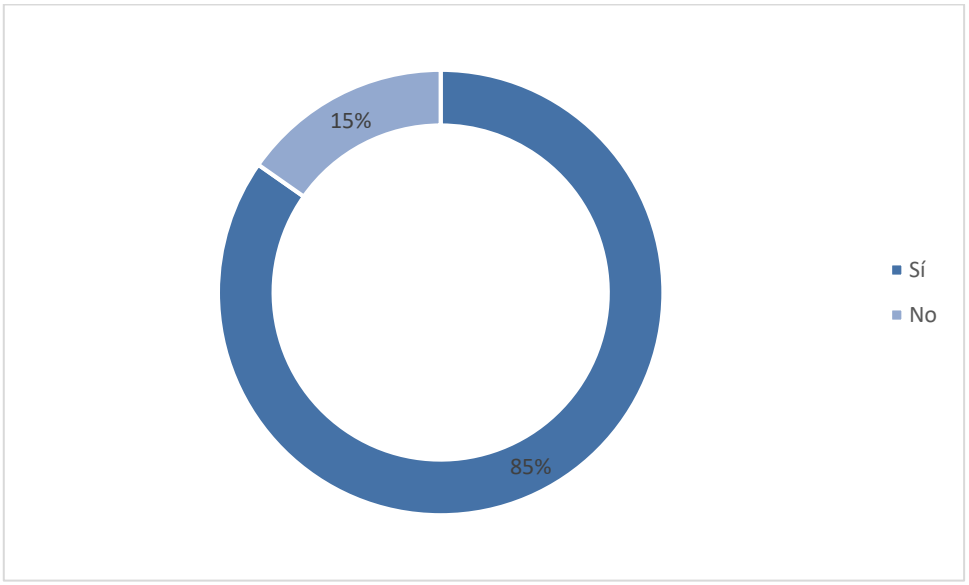


4.5.2 Uso de las herramientas de comunicación

a) Redes sociales

Al igual que sucede con el uso del móvil y el ordenador, el uso de las redes sociales también está muy generalizado entre los jóvenes hoy en día. Tan extendido está que, del total de alumnos encuestados, el 85% (n = 6170) afirma usar redes sociales diariamente.

Gráfico 199. *Proporción de alumnos que usa redes sociales*



Más concretamente, en el caso de los alumnos de menor edad la prevalencia es del 68%, mientras que en los de mayor edad la cifra asciende hasta el 96%. Los datos parecen indicar que cuanto mayores son los alumnos, mayor uso hacen de las redes sociales.

Gráfico 200. *Proporción de alumnos de 5º y 6º de primaria y 1º de ESO que usan redes sociales a diario*

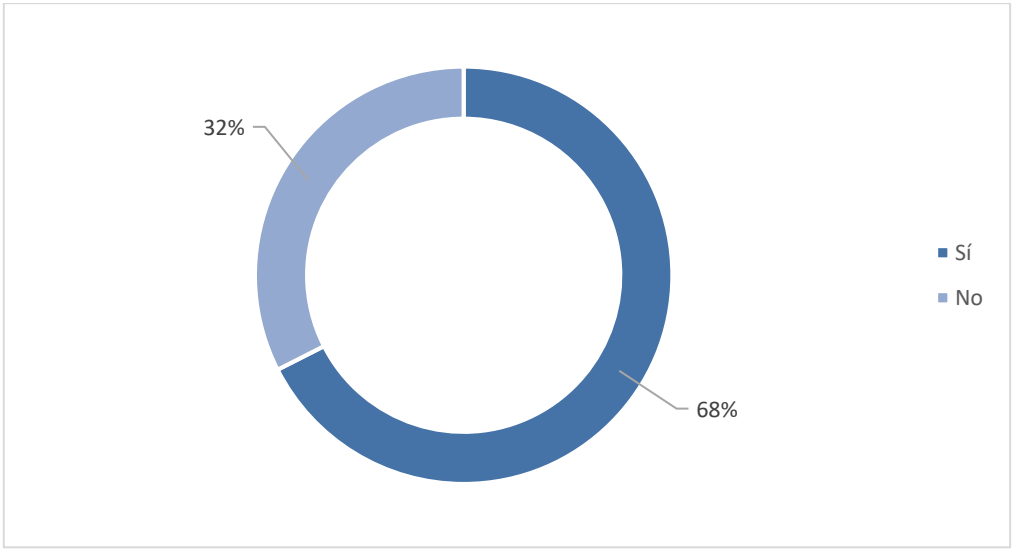
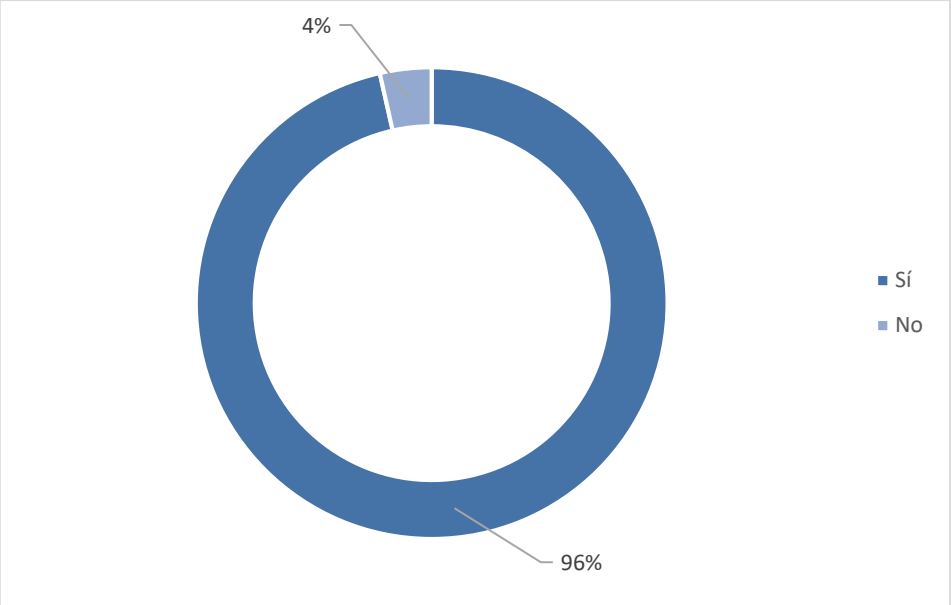
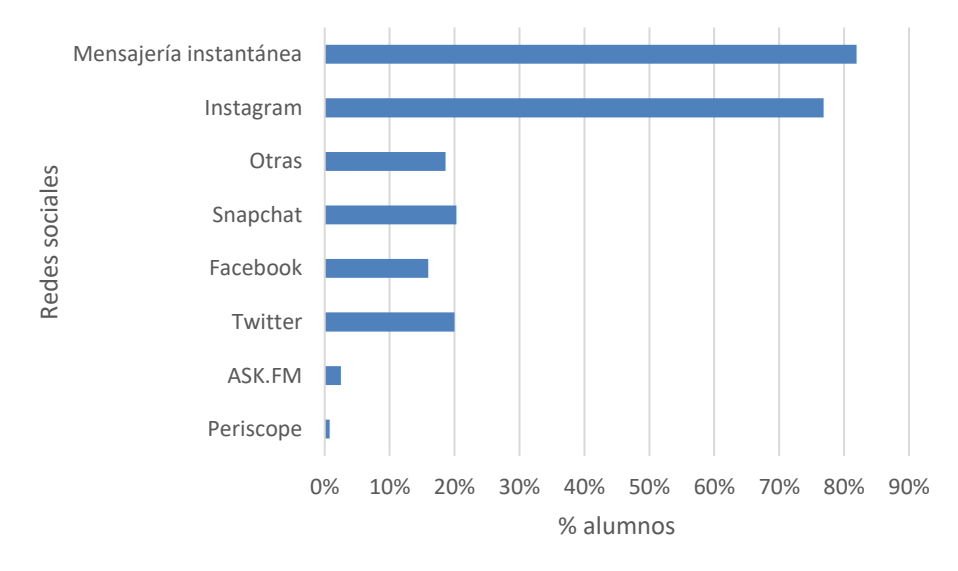


Gráfico 201. *Proporción de alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM que usan redes sociales a diario*



En general, y teniendo en cuenta a todo el conjunto de alumnos, las redes sociales más usadas por la amplia mayoría de jóvenes son la mensajería instantánea (WhatsApp, sobre todo) e Instagram, con una prevalencia del 82% y 77%, respectivamente, tal y como se observa en el siguiente gráfico.

Gráfico 202. Redes sociales utilizadas por los alumnos



Aunque los datos indiquen que la mayoría de los alumnos utilizan redes sociales, ello no significa que todos le den la misma utilidad. A la hora de analizar con qué frecuencia publican datos en redes sociales, el 40% afirma que nunca publica nada. Entre los que sí que lo hacen, la mayor parte de las veces los datos publicados son fotos (un 85% de los alumnos que publican datos personales ha indicado que publican fotos suyas) o el propio nombre y apellidos (un 50% de los alumnos). Otros datos que publican de manera frecuente son la edad (un 25%) y la ubicación en la que se encuentran (un 22%).

Gráfico 203. *Frecuencia de publicación en redes sociales*

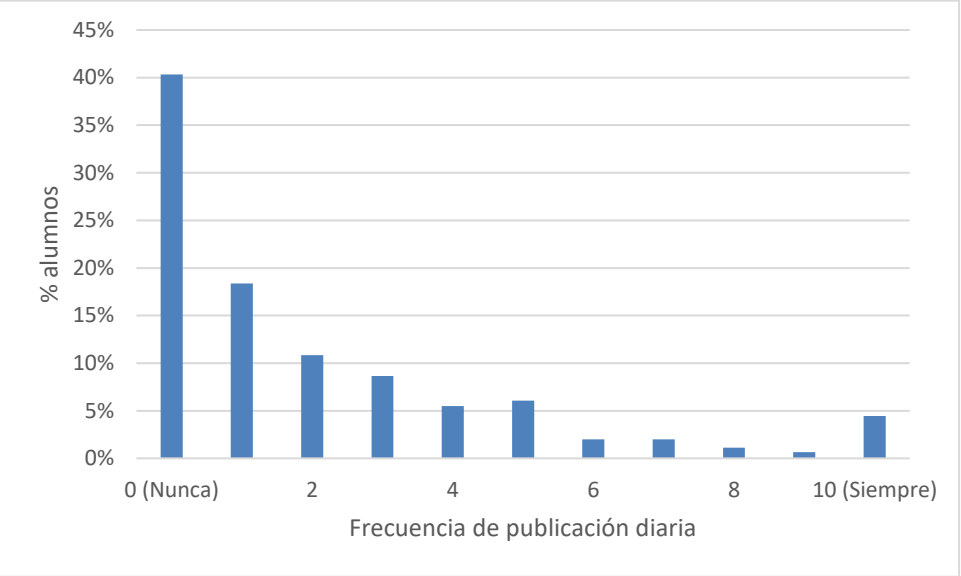
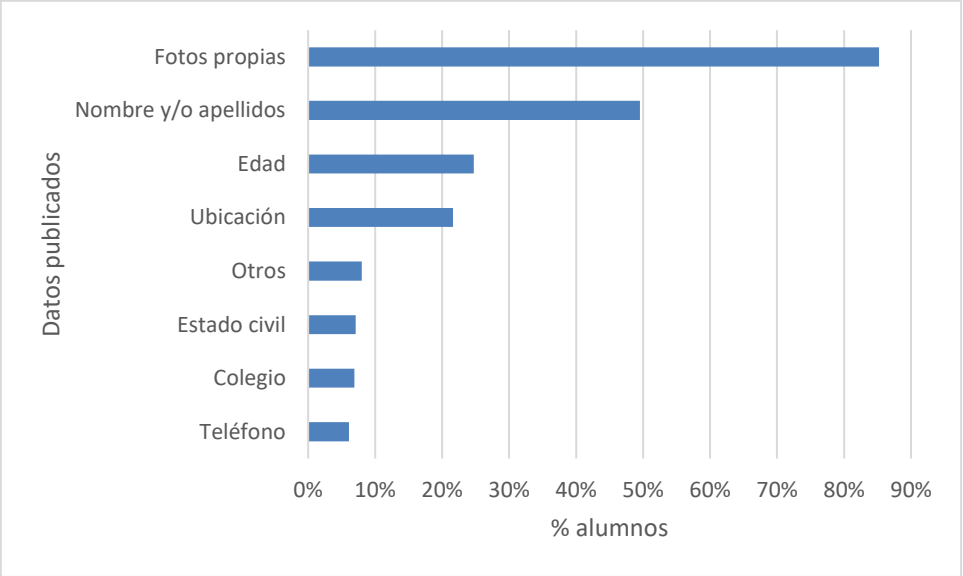
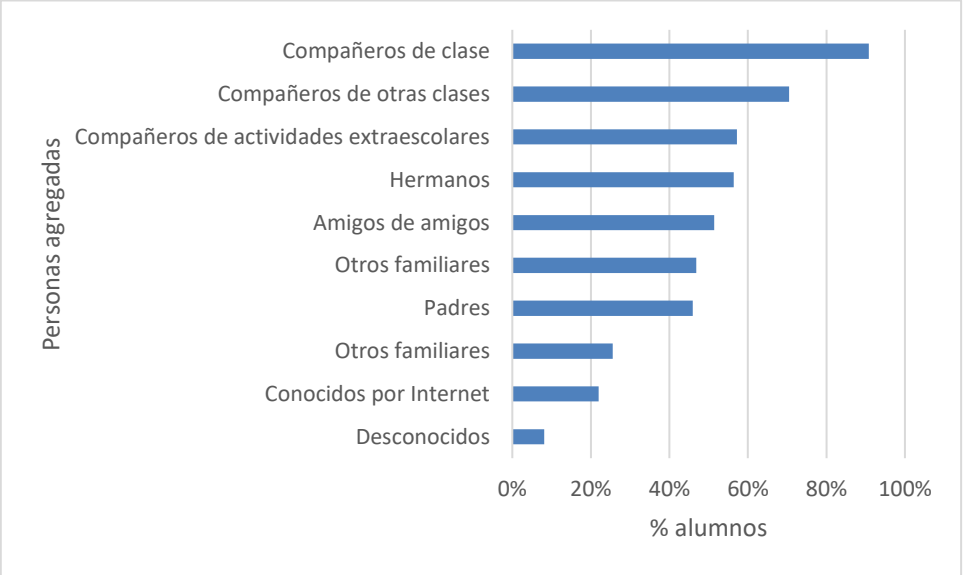


Gráfico 204. *Tipo de datos personales publicados en redes sociales*



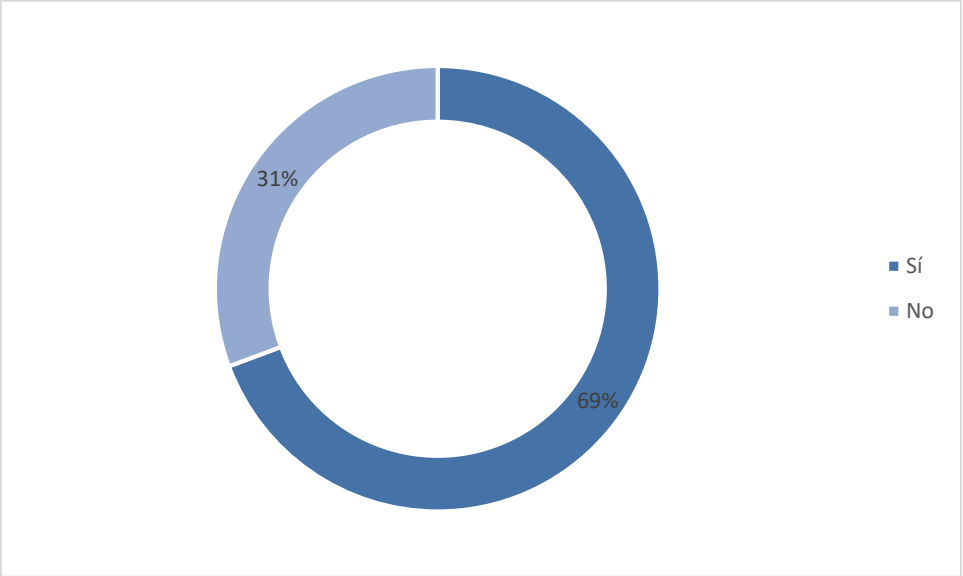
En cuanto a las personas a las que los alumnos agregan a sus redes sociales y, en consecuencia, tienen un mayor acceso a los datos publicados en ellas, se observa que la mayoría de estas personas son compañeros de clase o de otras clases (un 91% y un 70% de alumnos, respectivamente), compañeros de actividades extraescolares (un 57%), hermanos (un 56%) y amigos de amigos (un 51%).

Gráfico 205. *Personas que los alumnos agregan a sus redes sociales*



Otro detalle importante a tener en cuenta es que hay jóvenes que deciden limitar el acceso a sus redes sociales, lo que conlleva que sean menos visibles en el ciberespacio o que sus datos estén más protegidos. En este estudio, el 78% de alumnos que usan redes sociales (n = 4828) afirma limitar el acceso a sus redes sociales frente a un 22% (n = 1342) que no lo hace. Si bien es cierto que la amplia mayoría limita el acceso, que un 22% no lo haga indica que existe un elevado número de alumnos que podrían estar en mayor riesgo de cara a ser víctimas de ciberataques, ya sean económicos o sociales.

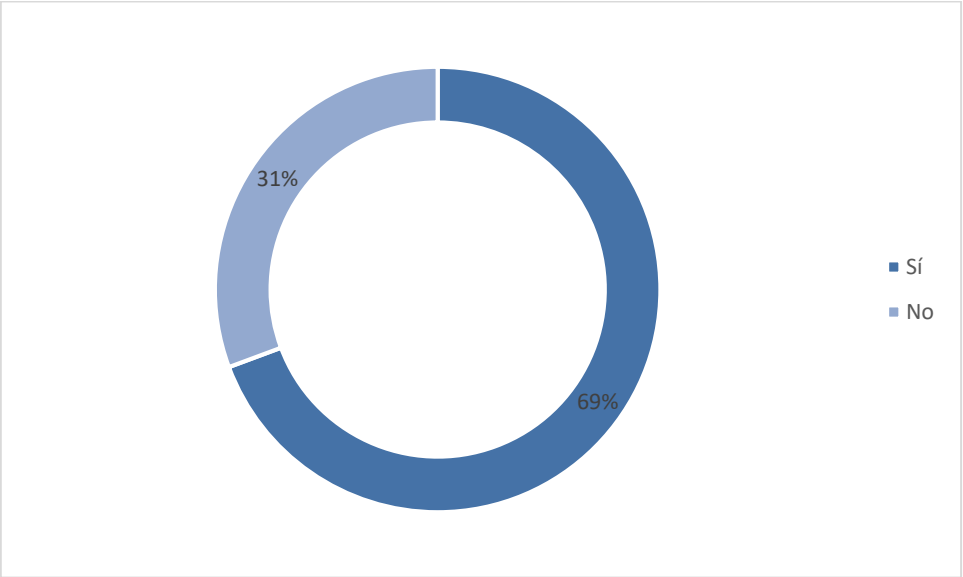
Gráfico 206. *Proporción de alumnos que limitan el acceso a sus redes sociales*



b) Correo electrónico

Entre los alumnos encuestados, se observa que el 69% (n = 5049) hace uso del correo electrónico frente a un 31% (n = 2233) que no. Más concretamente, se observa que entre los alumnos más pequeños (5º y 6º de primaria y 1º de ESO), el porcentaje de aquellos que utilizan correo electrónico es mucho menor que entre los alumnos de mayor edad (2º, 3º y 4º de ESO, Bachillerato y CFGM). En el primer grupo, el porcentaje de alumnos que utiliza correo electrónico es de un 47%, mientras que en el segundo grupo la cifra asciende al 85%.

Gráfico 207. *Proporción de alumnos que utilizan el correo electrónico*



c) Blogs, vídeo blogs y cuentas de YouTube

Un 17% de alumnos (n = 1205) encuestados afirma tener un blog, un vídeo blog o una cuenta de YouTube frente a un 83% que no (n = 6077). Entre los alumnos que tienen blog, cabe destacar que muchos de ellos no le dedican ninguna hora a la semana (un 34% de alumnos), le dedican menos de una hora (un 31%) o entre una y tres horas (un 20%).

Gráfico 208. *Proporción de alumnos que tienen blog, vídeo blogs o cuentas de YouTube*

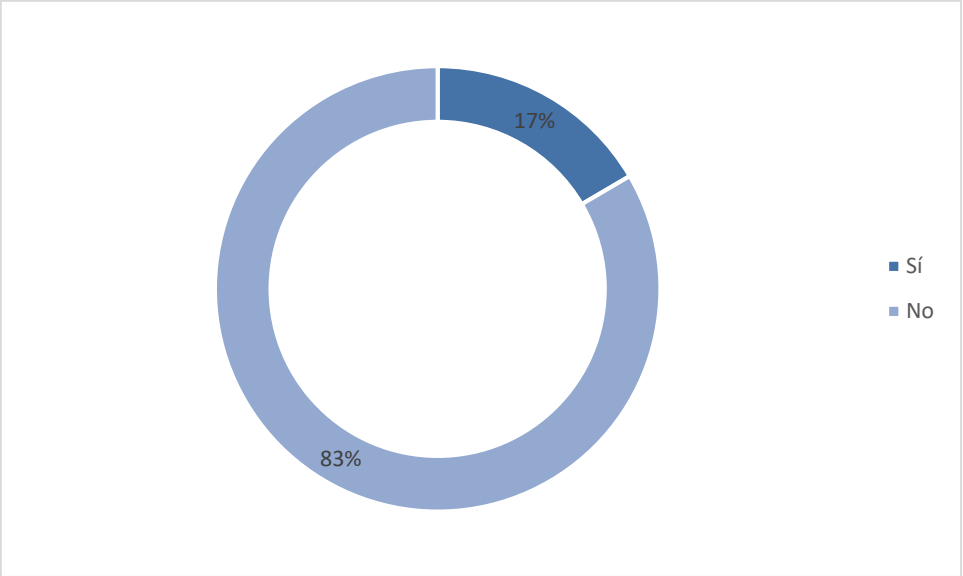
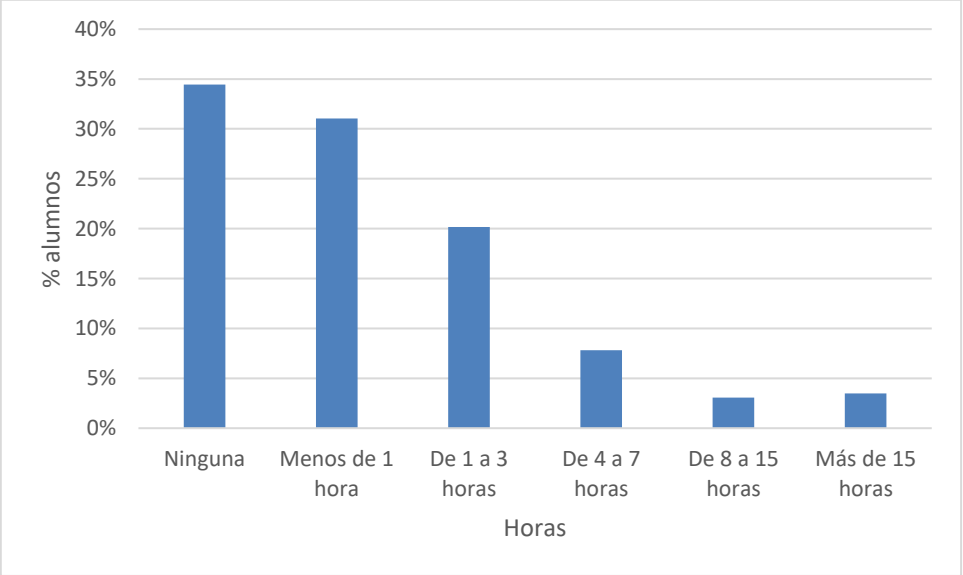


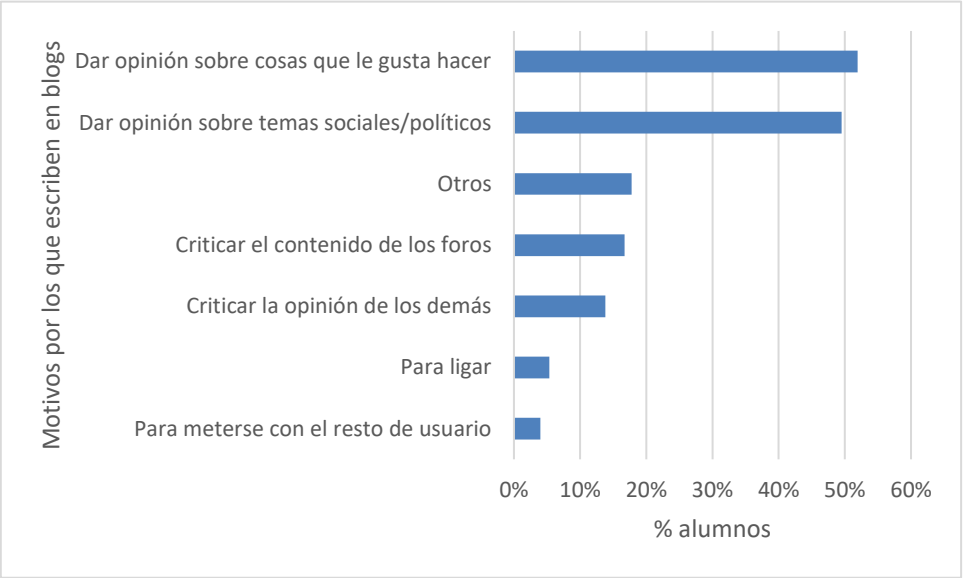
Gráfico 209. *Horas dedicadas a la semana al blog, vídeo blog o cuenta de YouTube*



Al margen de tener un blog o no, si se analiza la cantidad de alumnos que escriben en blogs o foros en Internet se observa que la cifra asciende al 23% (n = 1699) frente al 77% (n = 5583) que sostiene que no realiza esta conducta. Los motivos más frecuentes por los que deciden escribir en foros públicos se relacionan con dar sus opiniones, ya sean sobre las cosas que les gusta hacer (el

52% de alumnos) o sobre temas sociales y/o políticos (49% de alumnos). Son pocos los alumnos que escriben en foros para meterse con otras personas (un 4%) o ligar (un 5%).

Gráfico 210. *Motivos por los que los alumnos escriben en foros y blogs públicos*



d) Videollamadas

El 44% de los alumnos encuestados (n = 3234) afirma realizar videollamadas a lo largo de la semana frente a un 56% que no (n = 4048). La mayoría (un 84%) afirma que realiza estas videollamadas para hablar con sus amigos, aunque existen otros motivos como, por ejemplo, hablar con familiares (un 48%), hablar con compañeros del colegio (un 36%) o hablar con la pareja (un 18%).

Gráfico 211. *Proporción de alumnos que realizan videollamadas*

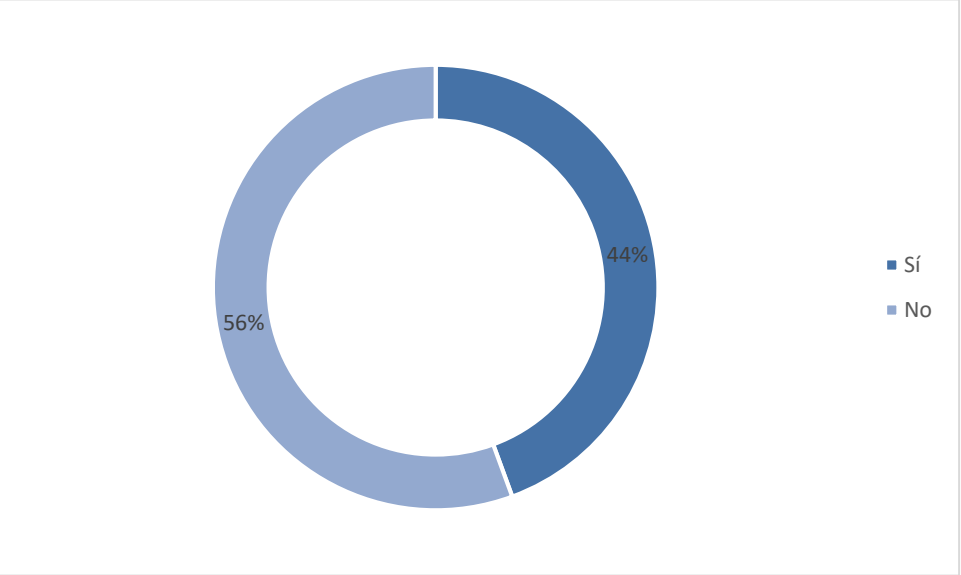
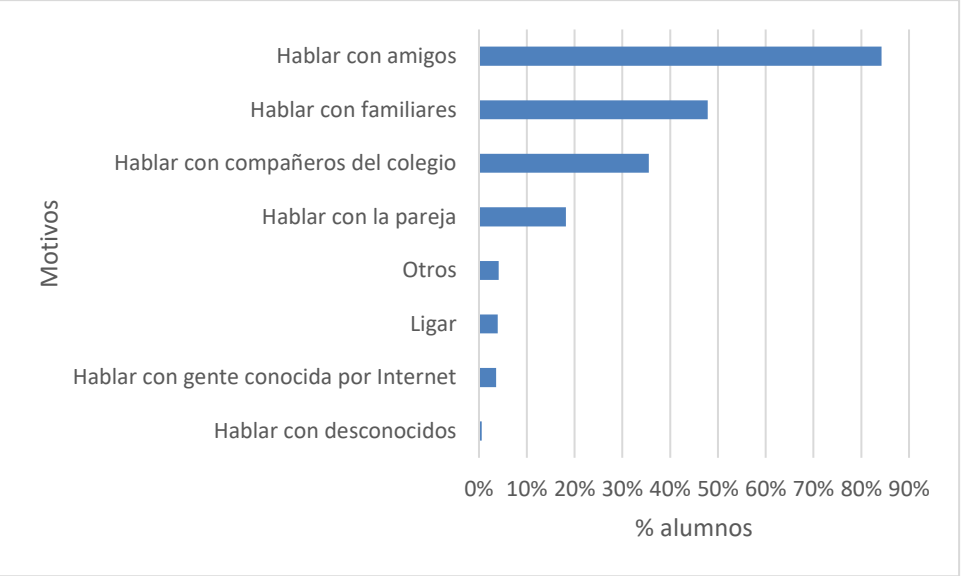


Gráfico 212. *Motivos por los que los alumnos deciden realizar videollamadas*



e) Webs de contacto

Son pocos los alumnos que usan webs de contacto[13]. De hecho, solo el 3% (n =

[13] Este apartado se ha analizado teniendo en cuenta solamente a los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, ya que se ha considerado que por cuestiones de edad no era apropiado preguntar sobre ello a los alumnos de 5º y 6º de primaria y 1º de ESO.

131) afirma tener alguna cuenta en webs de contacto, mientras que el 97% restante (n = 4198) lo niega. Entre los alumnos que sí tienen cuentas en estas plataformas, cabe destacar que, aunque la mayoría tiene menos de cinco cuentas, existe un 17% de alumnos que afirma tener más de 10 cuentas.

Gráfico 213. *Proporción de alumnos que tienen cuentas en webs de contactos*

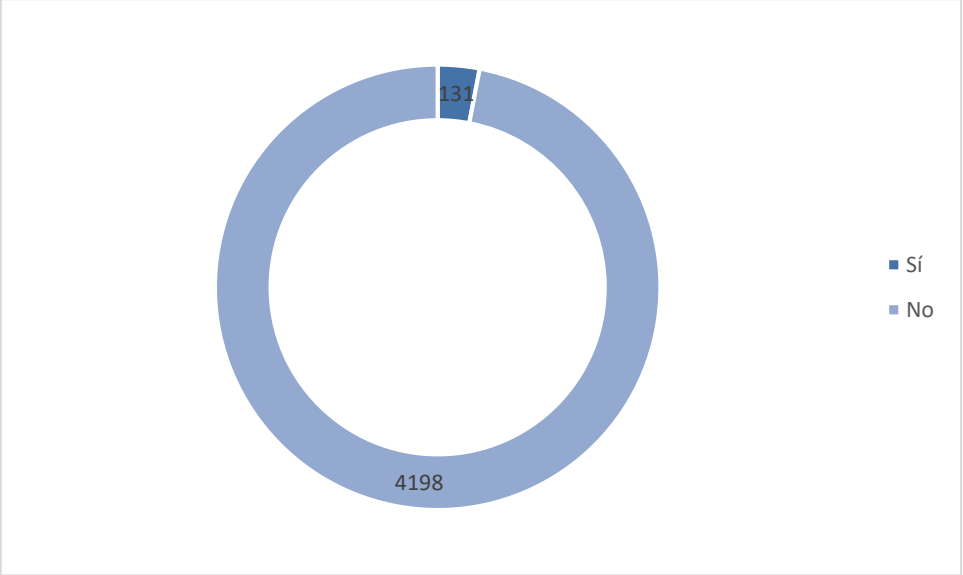
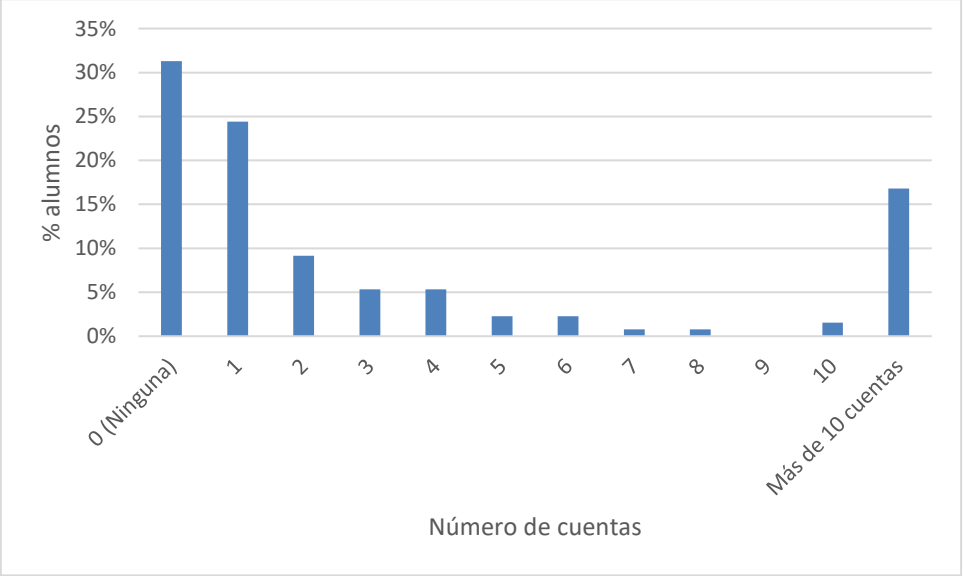


Gráfico 214. *Número de cuentas en webs de contacto*

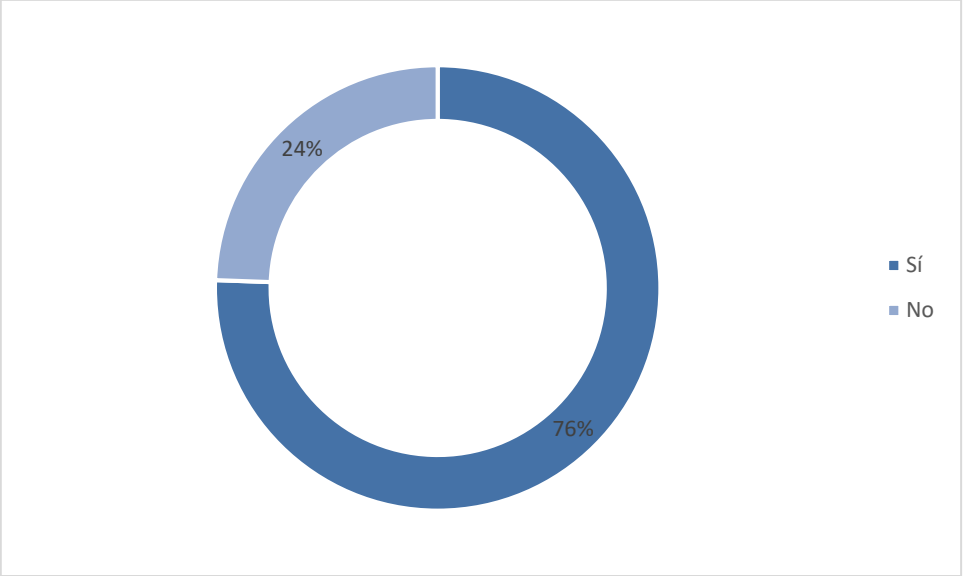


4.5.3 Actividades cotidianas de los jóvenes en Internet

a) Comprar por Internet

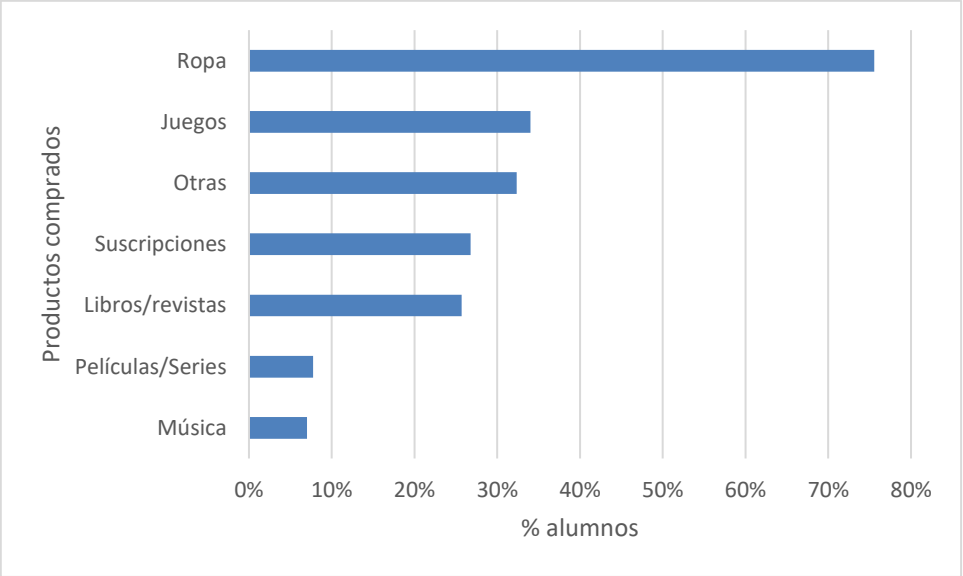
El 76% de los alumnos encuestados (n = 3271) afirma haber comprado por Internet alguna vez en su vida.[14] Una mayoría de alumnos afirma que ha realizado las compras a través del ordenador (un 63,4%), mientras que un 31,4% y un 13,4% afirman haberlas realizado a través del móvil y la tablet, respectivamente. Una de las cuestiones interesantes relacionadas con las compras en Internet es conocer qué compran los alumnos. Una inmensa mayoría (un 76% de los alumnos) afirma que compra ropa, seguido de un 34% que afirma comprar juegos.

Gráfico 215. *Proporción de alumnos que han realizado compras por Internet*



[14] Este apartado se ha analizado teniendo en cuenta solamente a los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, ya que se ha considerado que por cuestiones de edad no era apropiado preguntar sobre ello a los alumnos de 5º y 6º de primaria y 1º de ESO.

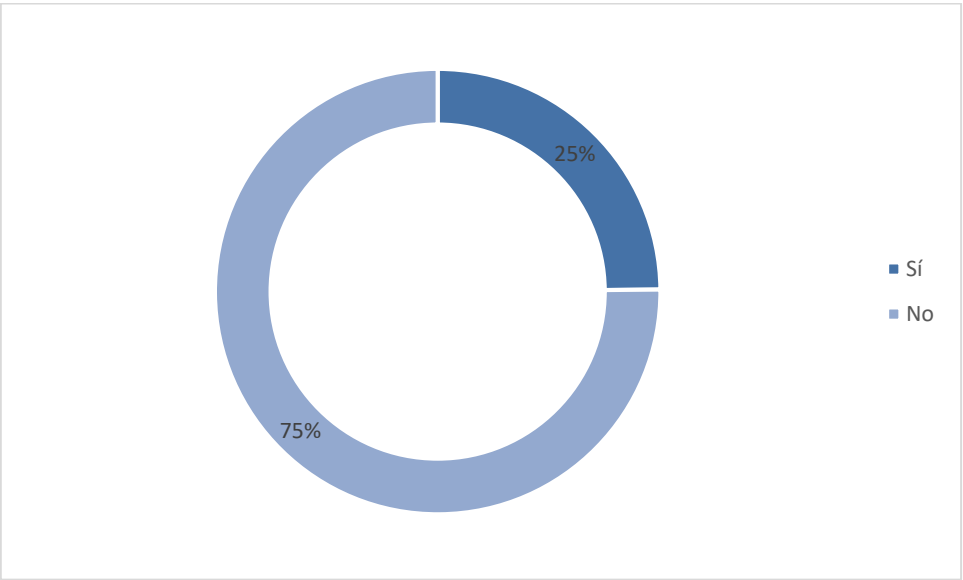
Gráfico 216. *Productos comprados a través de Internet*



b) Facilitar datos personales

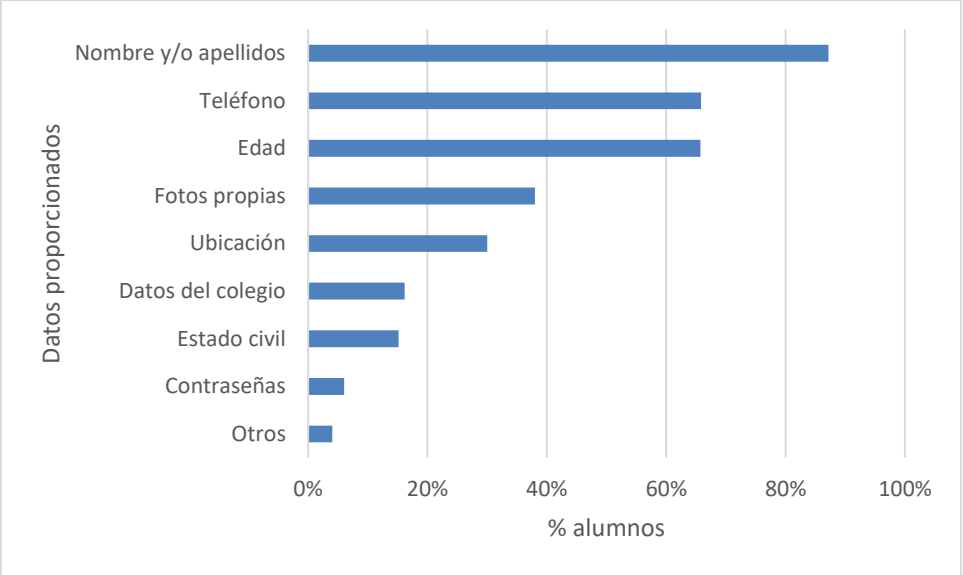
Uno de los aspectos más importantes que pueden estar relacionados con que una persona pueda llegar a ser víctima de ciberataques es el hecho de que facilite datos personales. En este estudio, el 25% de alumnos (n = 1810) afirma haber facilitado datos suyos a través de Internet alguna vez en su vida.

Gráfico 217. *Proporción de alumnos que facilitan datos personales en Internet*



Entre los datos personales más proporcionados se encuentran, por orden descendente, el nombre y los apellidos (un 87% de alumnos), el número de teléfono (un 66%), la edad (un 66%) y la ubicación donde se encuentra el joven (un 38%). Como se observa, existe una amplia variedad de datos que los menores facilitan a través de Internet, los cuales pueden favorecer, a su vez, que se vean expuestos a un mayor riesgo de ser víctimas de ciberataques, tanto económicos como sociales.

Gráfico 218. *Datos personales facilitados por los alumnos*



c) Contactar con desconocidos

El 44% de alumnos encuestados (n = 3189) afirma haber contactado con desconocidos a lo largo del último año. Más concretamente, un 44% de estos alumnos afirma que la finalidad principal era mantener una relación de amistad (un 44% de los alumnos), aunque también existen otras finalidades como, por ejemplo, jugar online (un 22%) o mantener una relación esporádica (un 10%).

Gráfico 219. *Proporción de alumnos que ha contactado con desconocidos en el último año*

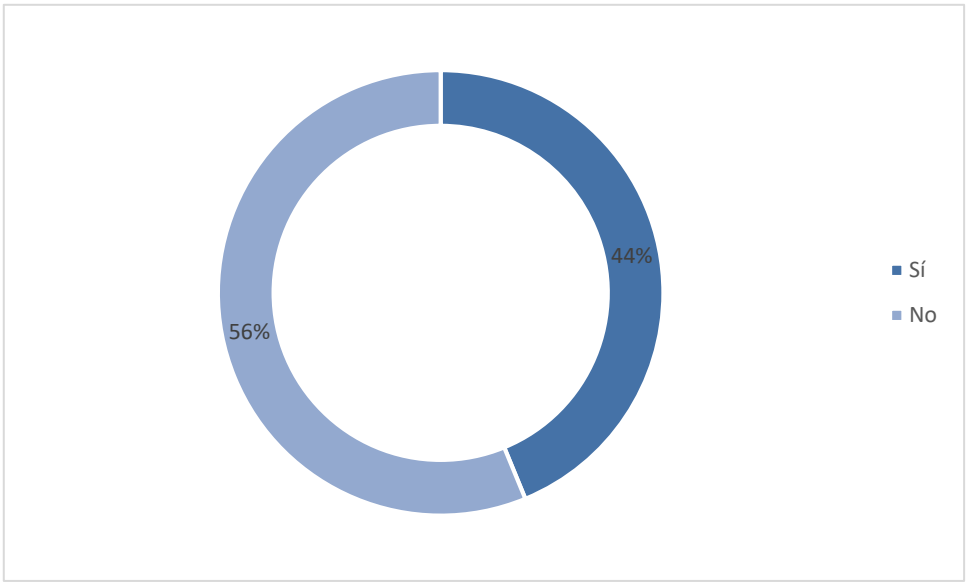
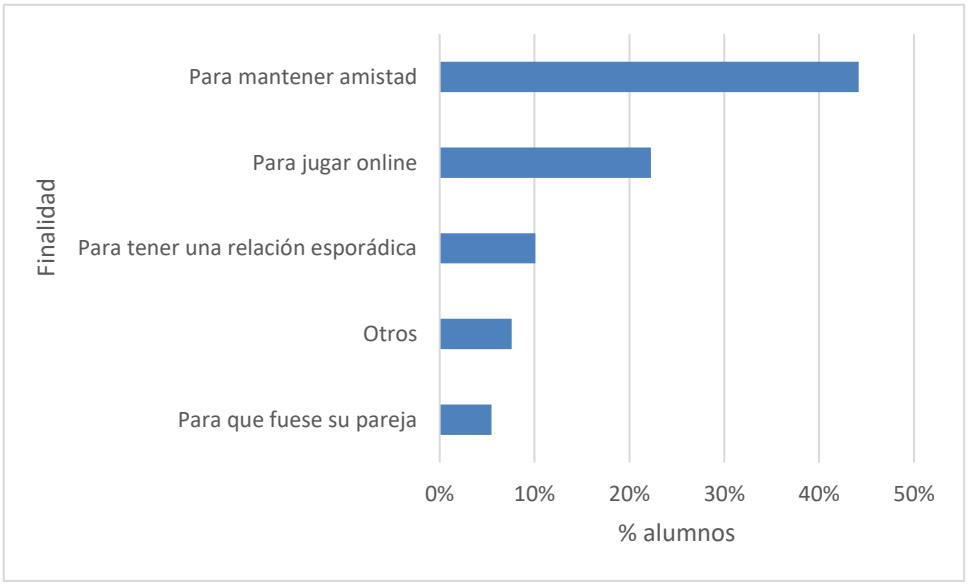


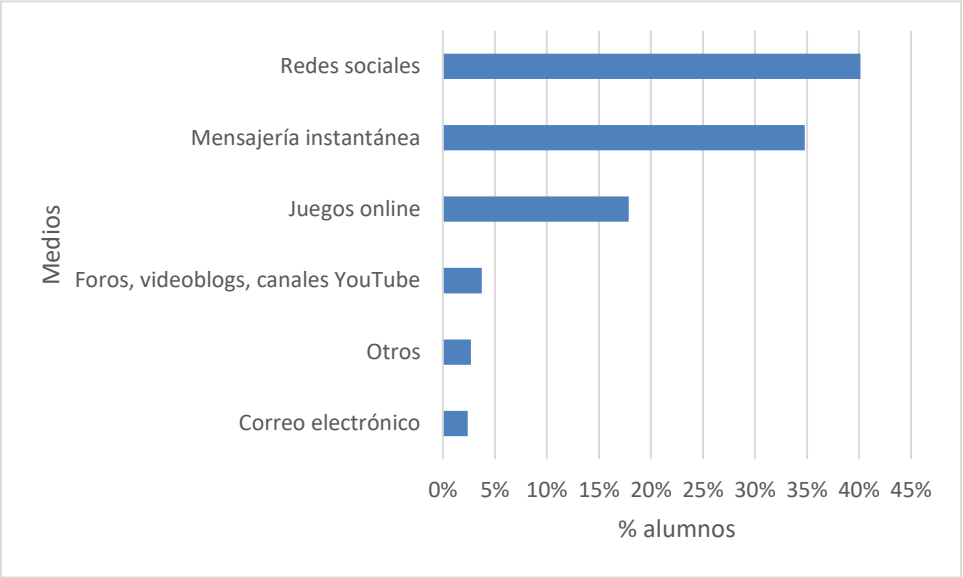
Gráfico 220. *Finalidad con la que los alumnos han contactado con desconocidos*



El medio de contacto más utilizado por los alumnos es a través de redes sociales (un 40% de los alumnos afirma haber utilizado este canal), mientras que el menos utilizado es el correo electrónico (un 2%). Es importante tener en cuenta este detalle de cara a analizar si el hecho de usar redes sociales y usarlas con la finalidad de contactar con desconocidos se relaciona, de alguna manera, con el

hecho de ser víctimas de ciberataques.

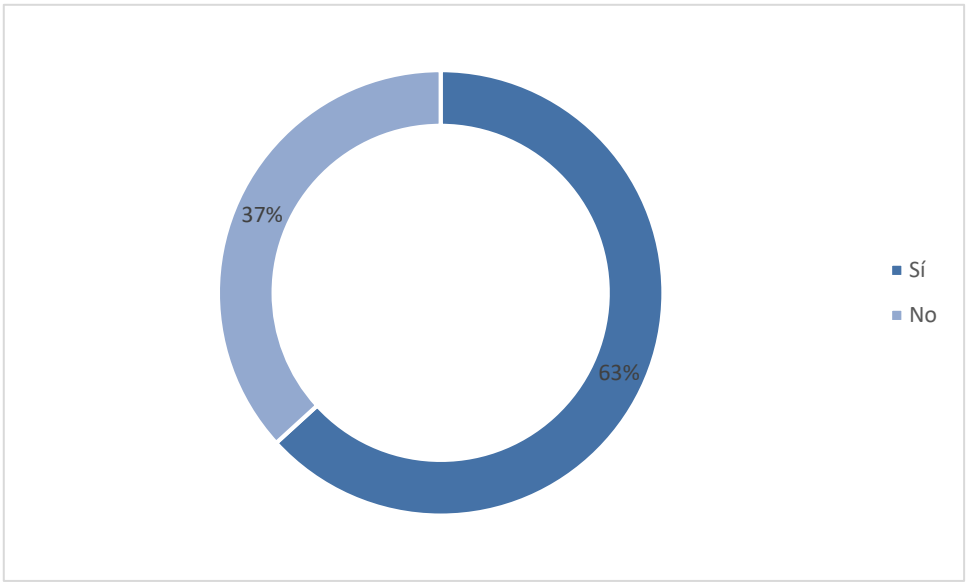
Gráfico 221. *Medios de contacto con desconocidos*



d) Abrir enlaces o descargar archivos de Internet

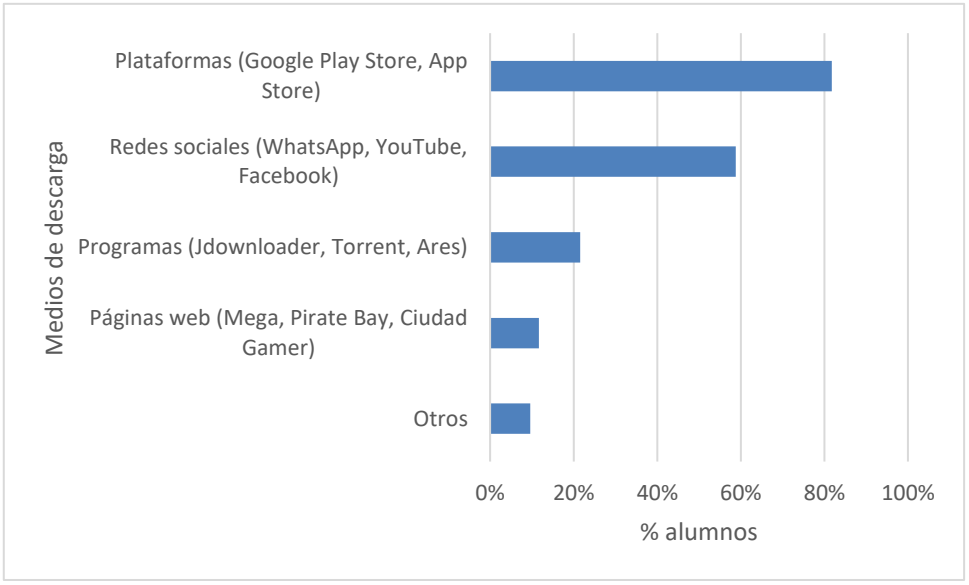
Abrir enlaces o descargar archivos de Internet puede ser un factor de riesgo a la hora de convertirse en una víctima de un ciberataque, sobre todo económico. Entre los alumnos encuestados, el 63% (n = 4604) afirma haber descargado algún archivo de Internet en el último año.

Gráfico 222. *Proporción de alumnos que ha descargado archivos de Internet en el último año*



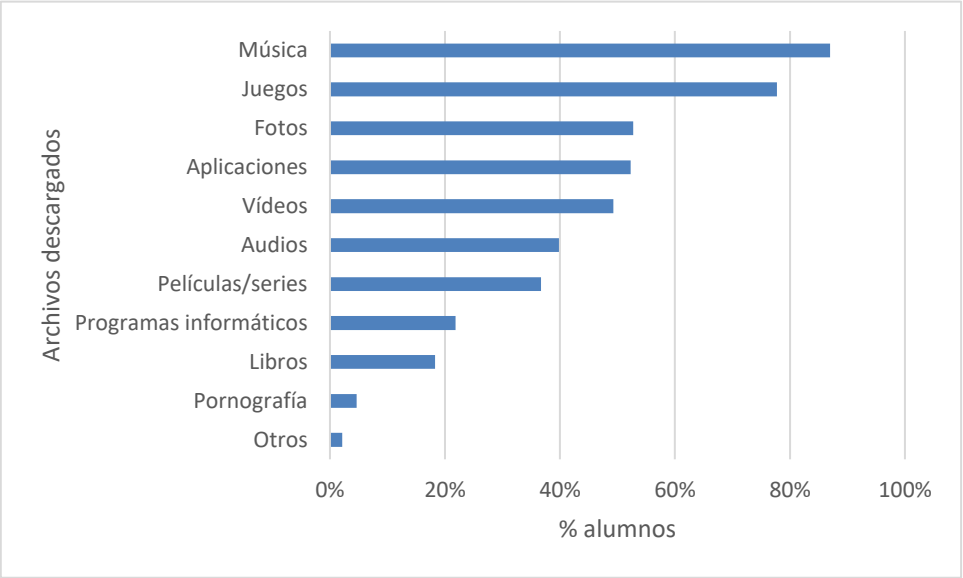
Principalmente, el medio utilizado para descargar los archivos, en un 82% de los alumnos, es el conjunto de plataformas como Google Play Store, App Store o Play Music, entre otras. El siguiente medio más utilizado para estas descargas son las redes sociales (WhatsApp, YouTube, Facebook, entre otras), con un 59% de los alumnos que afirma utilizar estos medios.

Gráfico 223. *Medios utilizados para descargar archivos de Internet*



Los archivos más descargados, tal y como se muestra en el siguiente gráfico, son música, juegos, fotos y aplicaciones, con un 87%, 78%, 53% y 52% de los alumnos que afirman haber descargado estos archivos, respectivamente.

Gráfico 224. *Archivos descargados a través de Internet*



e) Realizar comportamientos sexuales online

Esta conducta es otra de las que solo se han medido en los alumnos de mayor edad, esto es, los de 2º, 3º y 4º de ESO, Bachillerato y CFGM. Los datos indican que solo un 3% de la muestra (n = 139) ha realizado comportamientos sexuales a través de Internet. Cabe destacar que una gran mayoría de estos alumnos, más concretamente un 64%, afirma haber realizado estos comportamientos con su pareja, seguido de un 23% que sostiene que los ha realizado con conocidos ajenos al colegio en el que estudian. Igual de interesante es destacar que un 14% de los encuestados refiere haber realizado dichos comportamientos con completos desconocidos.

Gráfico 225. *Proporción de alumnos que han realizado comportamientos sexuales online*

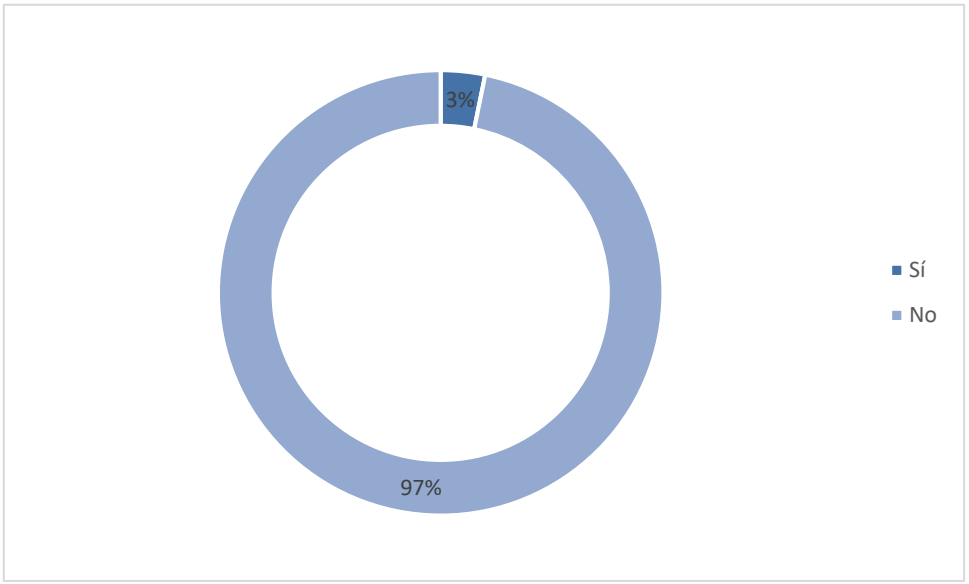
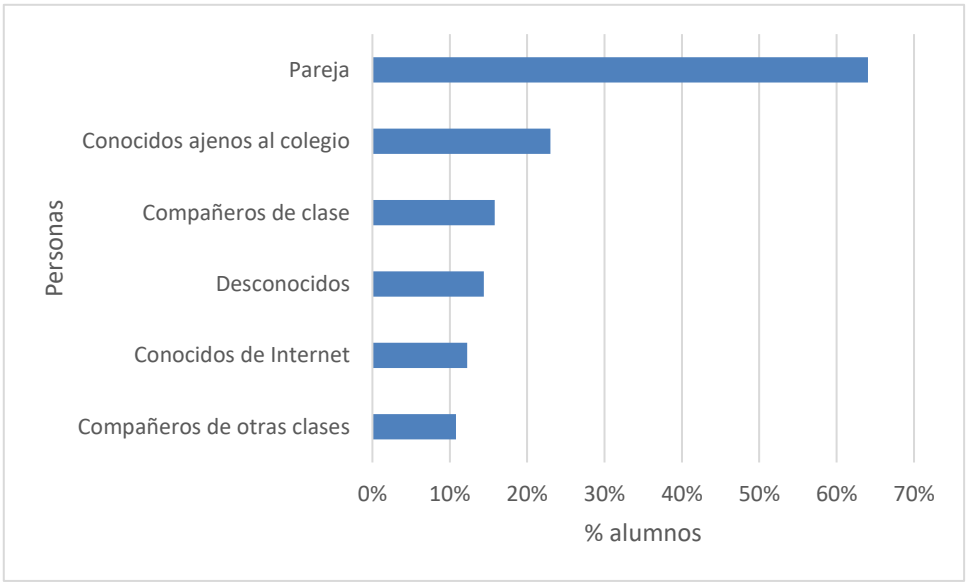
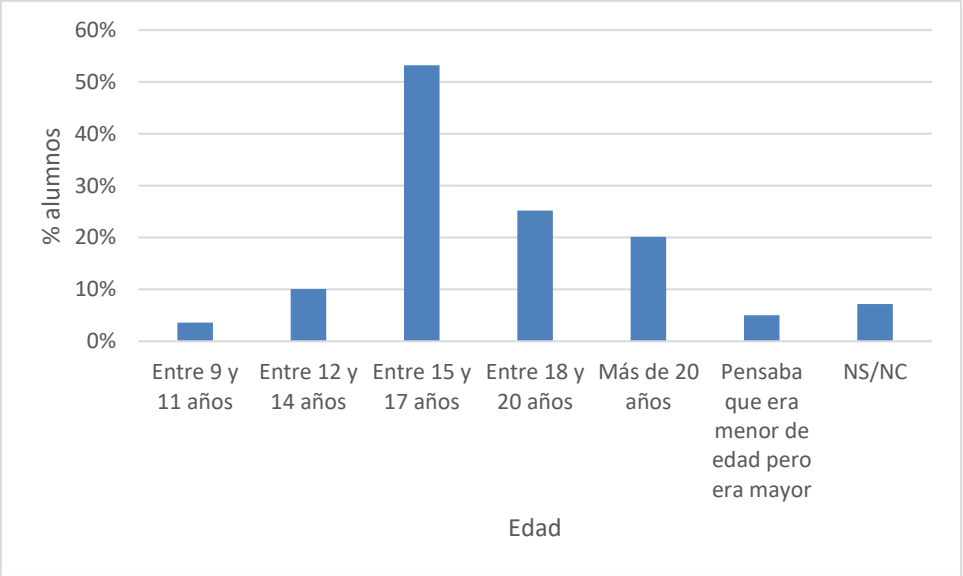


Gráfico 226. *Personas con quien los alumnos han realizado comportamientos sexuales*



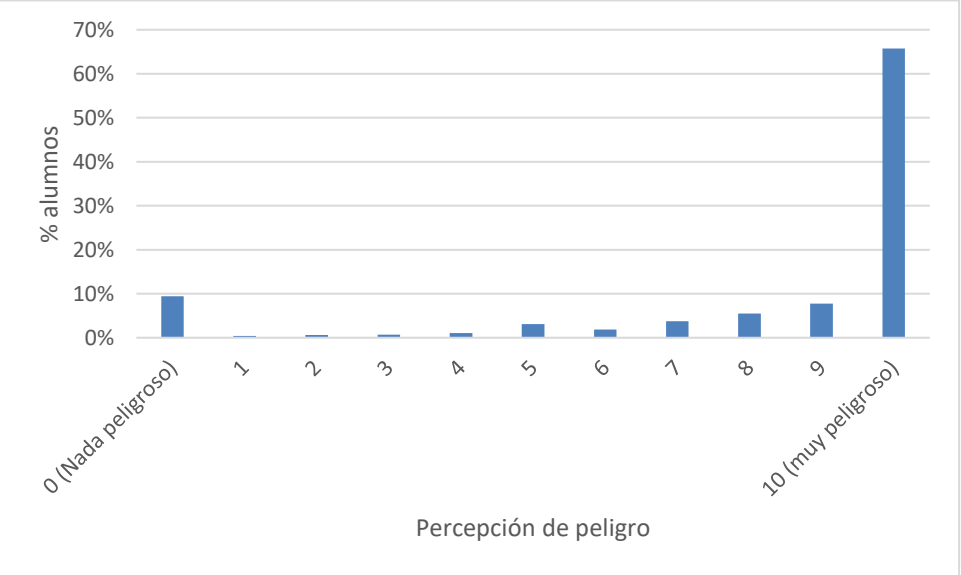
La edad de los emisores del material pornográfico se encuentra, mayoritariamente, entre los 15 y los 20 años y, más concretamente, entre los 15 y los 17, tal y como se puede observar en el gráfico 225.

Gráfico 227. *Edad de las personas con las que los alumnos realizan comportamientos sexuales*



Finalmente, se ha preguntado a todos los alumnos, independientemente de si han realizado o no comportamientos sexuales por Internet, sobre su percepción del peligro que conlleva realizar estas conductas. Los datos indican que, en este caso, el porcentaje de alumnos que considera que es muy peligroso ha alcanza hasta un 66% (n = 4788). Por el contrario, el porcentaje de alumnos que considera que no es nada peligroso ha descendido hasta el 9% (n = 689).

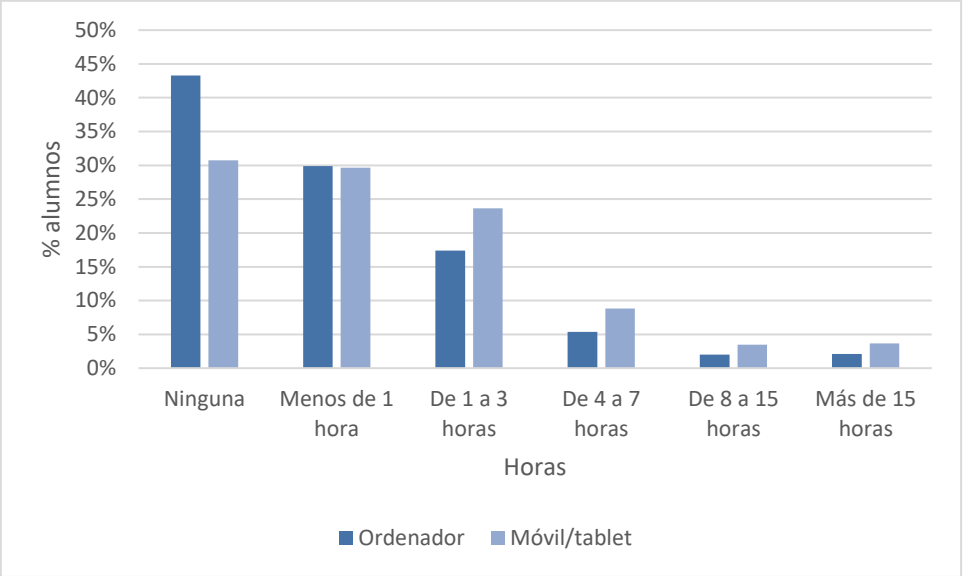
Gráfico 228. *Percepción de los alumnos sobre el peligro de realizar comportamientos sexuales a través de Internet*



f) Jugar online

En general, una gran parte de los alumnos no dedica ninguna hora a la semana a jugar videojuegos y, si lo hacen, pasan menos de una hora o, como mucho, entre una y tres horas. Tal y como se observa en el gráfico, en general los alumnos dedican más horas a jugar a través del móvil o la tablet que del ordenador, aunque las diferencias no son muy elevadas.

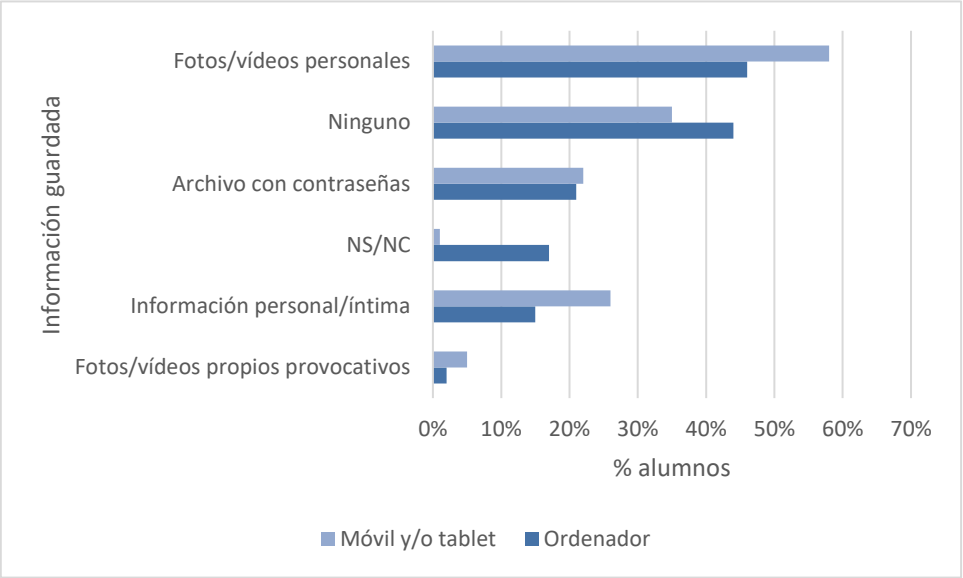
Gráfico 229. *Horas que los alumnos dedican a jugar a videojuegos a la semana*



g) Guardar información en el ordenador y el móvil

En general, los alumnos encuestados guardan información muy variada en sus dispositivos electrónicos. Más concretamente, en el caso del ordenador lo más común es guardar fotos y vídeos personales (un 46% de los alumnos) y un archivo donde están las contraseñas apuntadas (un 21%). En el caso del móvil, una gran mayoría (casi un 60%) guarda fotos y vídeos personales, seguido de un 26% que guarda información personal o íntima. Cabe destacar que un alto porcentaje también ha afirmado no guardar ningún tipo de información ni en el ordenador (un 44% de los alumnos) ni en el móvil o la tablet (un 35%).

Gráfico 230. *Información guardada en el ordenador y en el móvil/tablet*

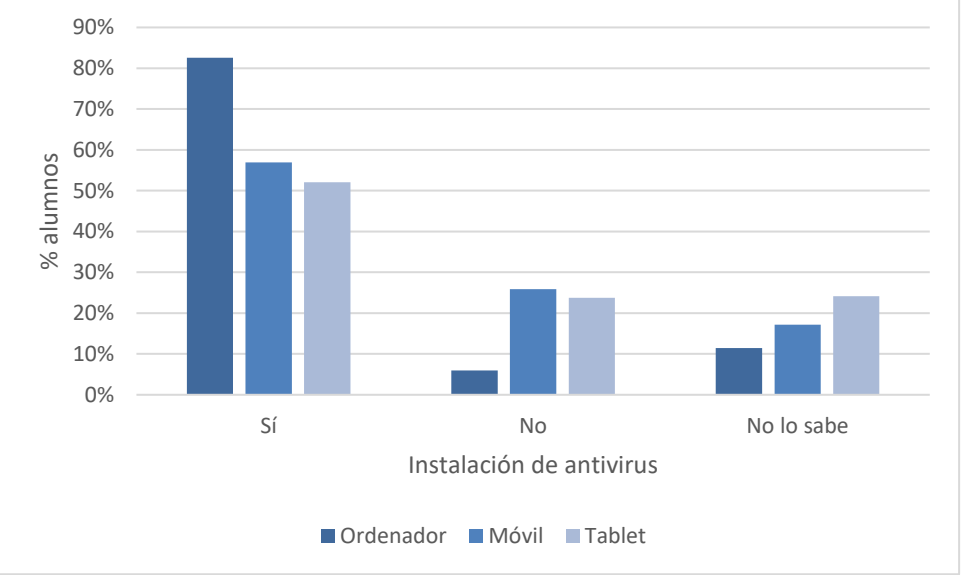


h) Usar antivirus

El uso de antivirus, el cual se relaciona estrechamente con la infección por *malware* y la pérdida de archivos por la infección por *malware*, está bastante generalizado entre los alumnos. De hecho, un 83% de ellos (n = 5581) afirma tener instalado el antivirus en el ordenador, mientras en el móvil y la tablet la cifra desciende al 57% (n = 3708) y al 52% (n = 2977), respectivamente. A pesar de que en estos dos dispositivos el número de alumnos que utiliza antivirus es menor, sigue siendo más de la mayoría, por lo que puede deducirse que el uso del antivirus está bastante generalizado entre los alumnos independientemente del dispositivo utilizado.

Igual de interesante es mencionar que existe un porcentaje importante de alumnos que desconoce si el antivirus está instalado en sus dispositivos, especialmente cuando se trata de la tablet, tal y como se observa en el gráfico. Esto podría indicar un desconocimiento acerca del funcionamiento del dispositivo, entre otras razones.

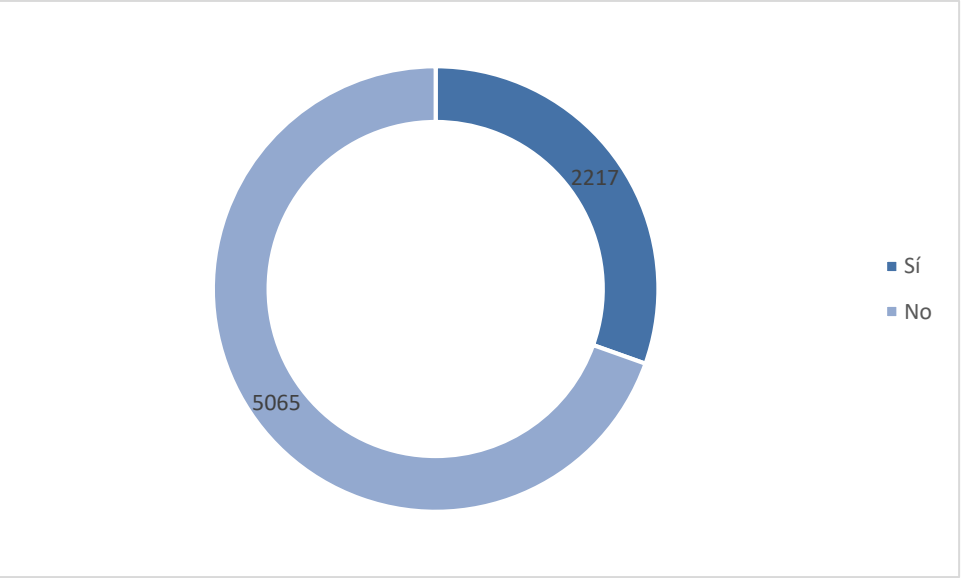
Gráfico 231. *Uso del antivirus en los distintos dispositivos utilizados por los alumnos*



i) Usar contraseñas

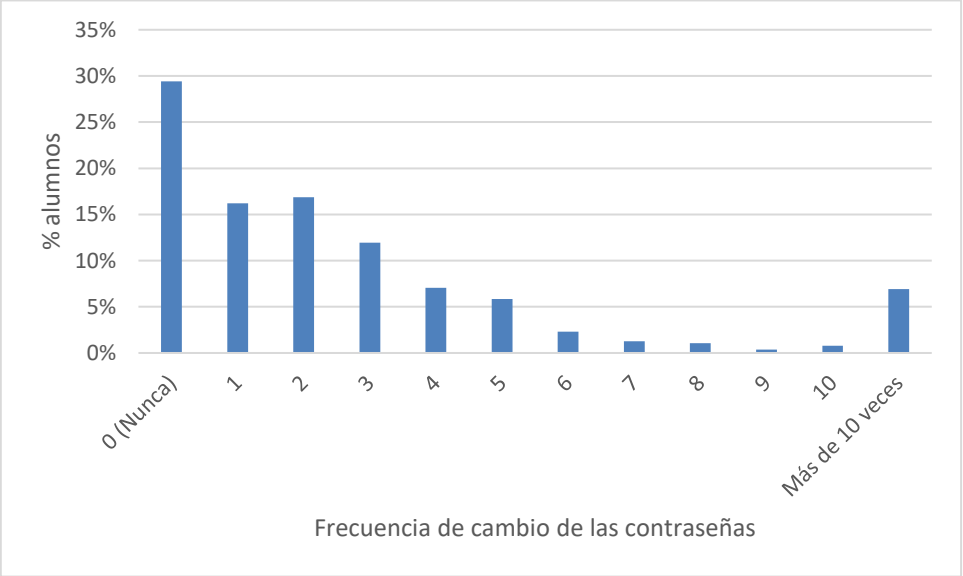
En cuanto al uso de las contraseñas, el 70% (n = 5065) de los alumnos afirma que usa distintas contraseñas para distintas aplicaciones, plataformas o páginas web a las que se conectan.

Gráfico 232. *Prevalencia de alumnos que utilizan la misma contraseña para todo*



Este dato, a priori, es positivo, ya que podría indicar una concienciación de los alumnos acerca del peligro de utilizar la misma contraseña para todo. Sin embargo, si se observa la frecuencia con la que los alumnos cambian las contraseñas, se obtiene que casi un 30% no cambia nunca las contraseñas. Además, entre la mayoría que sí lo hace, la frecuencia es bastante baja (entre 1 y 2 veces al año).

Gráfico 233. *Frecuencia del cambio de contraseñas por parte de los alumnos en el último año*



4.6 SUPERVISIÓN PARENTAL DEL USO DE LAS TIC

El control parental es muy importante de cara a proteger a los jóvenes de los peligros de Internet. De hecho, existen estudios como el de Marcum (2008) que muestran que cuanto más controlados están los menores por sus padres, menor es la probabilidad de que sean víctimas de un ciberataque. Los padres, por tanto, pueden prevenir que sus hijos sean víctimas de estos ciberataques "estableciendo un control directo sobre las actividades cotidianas de los menores en el ciberespacio, o bien frecuentando los mismos espacios virtuales por los que se mueve el menor" (García, 2017, p. 141).

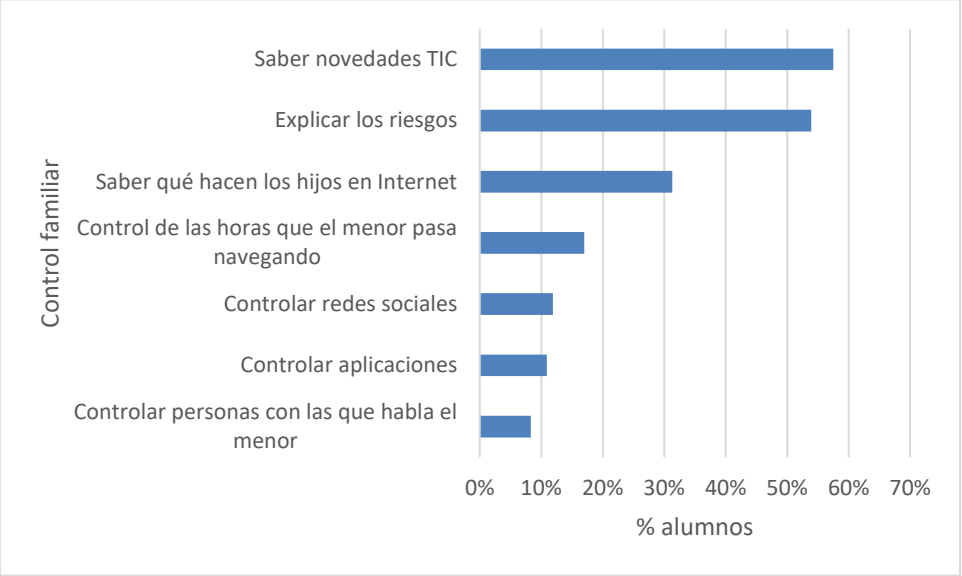
Entre los alumnos encuestados, más de la mitad sostiene que sus padres les explican los riesgos que tiene Internet (un 86% de los alumnos), saben lo que hacen cuando navegan por él (un 80%), están al tanto de las novedades de las TIC (un 75%) y controlan las horas que pasan navegando por Internet (un 64%). En general, los datos parecen indicar que los padres ejercen control sobre lo que sus hijos hacen en el ciberespacio.

Gráfico 234. *Control parental ejercido sobre los alumnos en el uso de las TIC*

Igual de interesante es analizar si, al margen de los padres, otros familiares ejercen control sobre las actividades desarrolladas en el ciberespacio[15]. En este caso, los datos indican que el control es menor, aunque aun así sigue siendo elevado, sobre todo, en dos categorías: saber las novedades de las TIC (un 58% de alumnos afirma que sus familiares están informados) y explicar los riesgos que tiene Internet (un 54%).

[15] El control familiar solo ha sido preguntado entre los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, por lo que los alumnos de 5º y 6º de primaria y 1º de ESO quedan excluidos de este análisis.

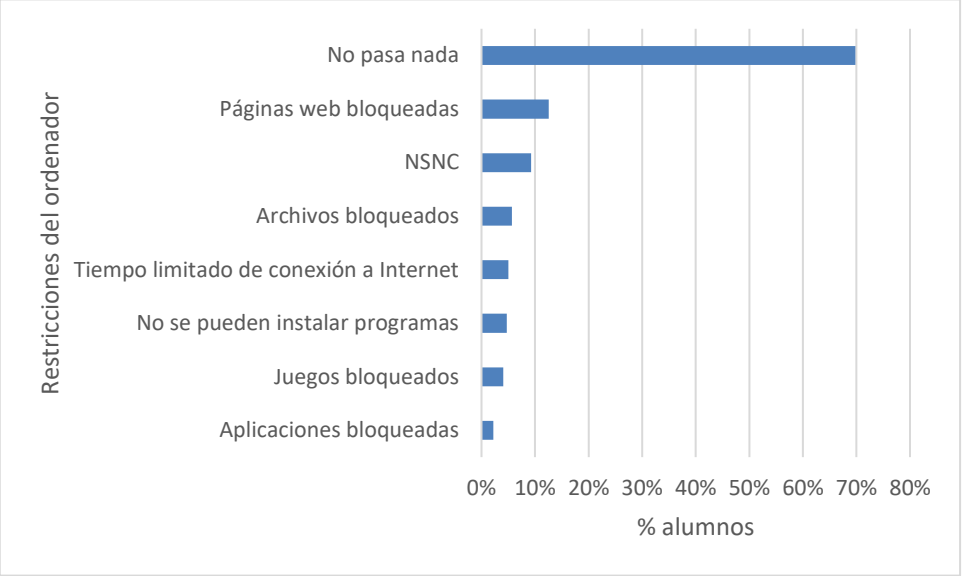
Gráfico 235. *Control familiar ejercido sobre los alumnos en el uso de las TIC*



Además del control directo ejercido por padres y familiares, existe otro tipo de control indirecto dirigido a prevenir los ciberataques a los que se pueden ver expuestos los alumnos. Este control indirecto hace referencia a un conjunto de restricciones presentes en los ordenadores como, por ejemplo, el bloqueo de ciertas páginas web o aplicaciones.

Como se ha analizado anteriormente, muchos de los alumnos afirman que sus padres ejercen bastante control sobre lo que realizan en Internet. Sin embargo, a la hora de preguntar por las restricciones del ordenador, sorprende que un 70% (n = 5081) de los alumnos encuestados indique que no sucede nada. Es decir, más de la mitad de estos alumnos pueden navegar y utilizar el ordenador sin ningún tipo de impedimento o barrera. Entre las restricciones que sí están presentes, conviene destacar que la más frecuente es que haya páginas web bloqueadas (un 13%) o archivos bloqueados (un 6%), aunque las prevalencias son un tanto bajas.

Gráfico 236. *Restricciones que tienen los ordenadores que utilizan los alumnos*



4.7 MECANISMOS DE PREVENCIÓN E INTERVENCIÓN DE LOS CENTROS EDUCATIVOS ANTE CASOS DE CIBERVICTIMIZACIÓN Y USO DESVIADO DE INTERNET

Los jóvenes pasan muchas horas al día en el ámbito escolar, lo que hace que la escuela se convierta en un actor muy importante en la prevención de los riesgos de Internet y del uso desviado del mismo. Más concretamente, son los docentes de los centros educativos los que representan ser una figura clave en la detección, prevención e intervención de la cibervictimización y el uso desviado de Internet de sus alumnos, ya que los conocen mejor que cualquier otro profesional al mantener una relación cercana y pasar una gran cantidad de horas a la semana con ellos. Esto permite que, teniendo a su alcance los mecanismos necesarios, puedan realizar una correcta detección que permita intervenir ante estas situaciones.

Por todo ello, es interesante analizar qué mecanismos de prevención e intervención existen en los centros para prevenir y actuar cuando algún alumno

es víctima de algún ciberataque o realiza un mal uso de las TIC e Internet. En concreto, es interesante analizar lo que opinan, por un lado, los alumnos y, por el otro, los docentes. Ello permitirá conocer la opinión individualizada de cada colectivo para, posteriormente, realizar una comparación entre lo que dicen unos y otros y, así, ver las semejanzas y diferencias entre ambos grupos.

A continuación, se exponen los resultados sobre lo que opinan alumnos y docentes que actualmente están cursando sus estudios o impartiendo clases, respectivamente, en los centros de educación no universitaria de Castilla y León sobre los mecanismos de prevención e intervención ante casos de ciberataques o uso desviado de Internet. Cabe destacar que los mecanismos de prevención hacen referencia a aquellos mecanismos destinados a evitar, cuando no ha habido ningún caso todavía, que exista algún tipo de ciberataque o uso abusivo de Internet. Por el contrario, los mecanismos de intervención hacen referencia a aquellas actuaciones llevadas a cabo cuando ya ha habido alguno de estos casos.

4.7.1 Mecanismos de prevención de los riesgos de Internet y del uso desviado existentes en los centros educativos

En este apartado se exponen los distintos mecanismos de prevención que, según los alumnos y los profesores, existen en los centros educativos a los que pertenecen, para prevenir, por un lado, los riesgos de Internet -entre los cuales se incluyen el ciberacoso, el ciberacoso sexual, el control de pareja a través de las TIC e Internet y los ciberataques económicos- y, por el otro, el uso desviado de Internet.

Asimismo, también se expone la percepción de eficacia de ambos colectivos sobre dichos mecanismos, así como una comparativa de los resultados obtenidos en uno y otro caso, mostrando tanto las semejanzas como las diferencias en las respuestas dadas por alumnos y profesores.

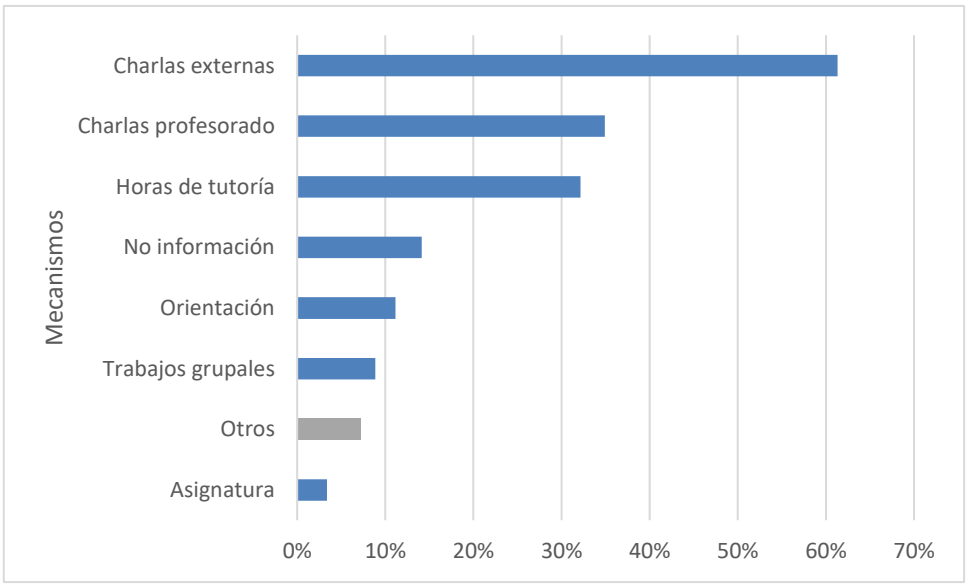
a) Mecanismos de prevención de los riesgos de Internet

1. Conocimiento de los alumnos

El mecanismo más frecuente de prevención de los riesgos de Internet disponible en los centros educativos de los alumnos encuestados es el de las charlas externas, es decir, que profesionales externos al colegio vayan a dar charlas y aporten información sobre estos riesgos. De hecho, más de la mitad de los alumnos, más concretamente un 61%, ha afirmado disponer de este mecanismo en su colegio. Los siguientes dos mecanismos más frecuentes son, por orden descendente, que los propios profesores del colegio den charlas (un 35%) y hablar sobre estos riesgos en las horas de tutoría (un 32%).

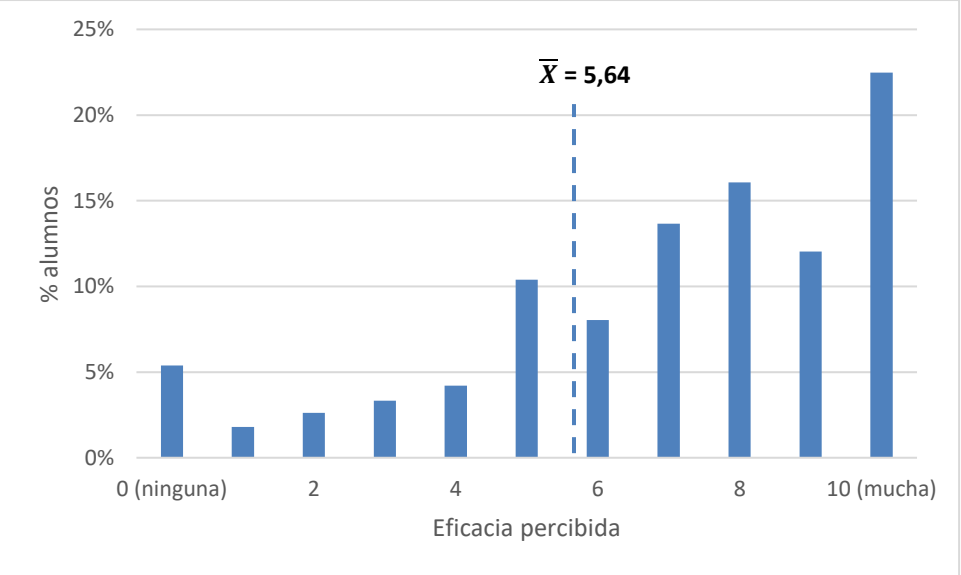
También debe tenerse en cuenta que un alto porcentaje de alumnos, más concretamente un 14%, ha comunicado que en sus centros educativos no se hace nada para prevenir los riesgos de Internet, lo cual indica una falta de actuaciones por parte de los centros educativos de pertenencia.

Gráfico 237. *Mecanismos de prevención de los riesgos de Internet existentes en los centros educativos según los alumnos*



En general, los alumnos perciben que estos mecanismos sí son eficaces. Más concretamente, la forma como se ha medido esta eficacia es preguntándoles cuánto consideran que han aprendido tras haber aplicado el mecanismo de prevención. Como se observa en el siguiente gráfico, la mayoría de alumnos da una puntuación de entre 6 y 10 a la eficacia de estos mecanismos. Sin embargo, la media no es demasiado elevada, ya que no alcanza ni una puntuación de 6.

Gráfico 238. *Percepción de los alumnos sobre la eficacia de los mecanismos de prevención de los riesgos de Internet*

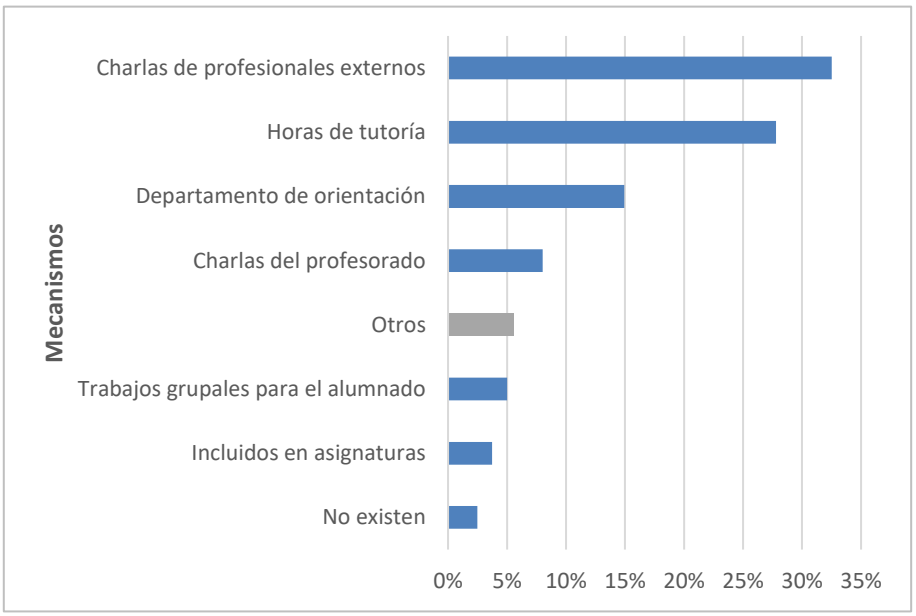


2. Conocimiento de los docentes

Respecto a los riesgos de Internet, un importante porcentaje de docentes (un 32,5%) afirma que lo que más se realiza en sus centros educativos a modo de prevención son charlas impartidas por profesionales externos a los centros educativos, seguido de un 27,8% de docentes que afirma que dedican algunas horas de tutoría a hablar de dichos riesgos. Los mecanismos de prevención menos frecuentes, según los docentes, son la realización de trabajos grupales para el alumnado (un 5%) o contenidos incluidos en las propias asignaturas (un 3,7%). Además, cabe destacar que casi un 3% de los docentes ha reconocido que

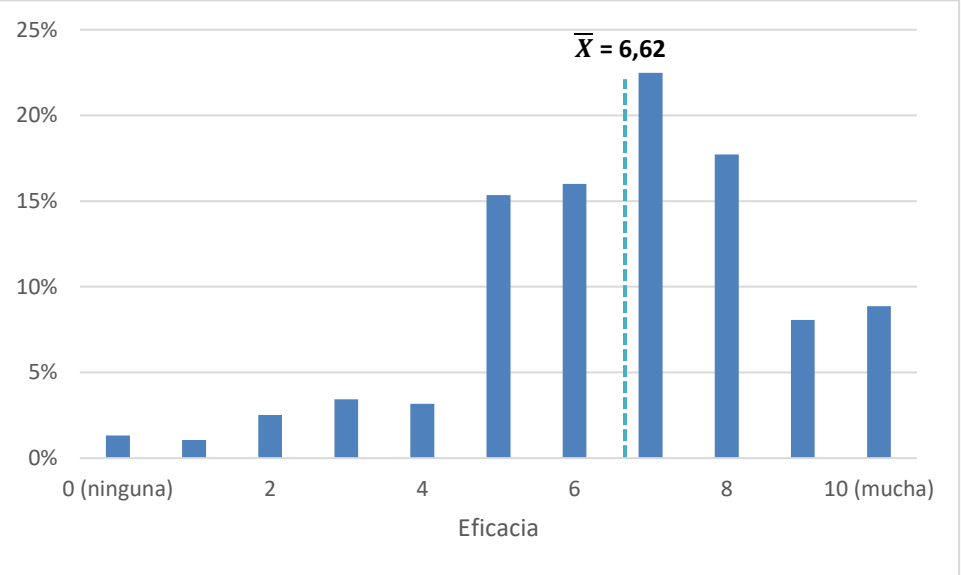
en sus centros educativos no existen mecanismos de prevención dirigidos a prevenir los riesgos de Internet.

Gráfico 239. *Mecanismos de prevención de los riesgos de Internet existentes en los centros educativos según los docentes*



A la hora de preguntar a los docentes por el grado de eficacia de los mecanismos de prevención anteriormente expuestos, la mayoría se ha decantado por afirmar que éstos tienen una eficacia moderada-alta, siendo la media de casi 7, tal y como se observa en el siguiente gráfico.

Gráfico 240. *Percepción de los docentes sobre la eficacia de los mecanismos de prevención de los riesgos de Internet*

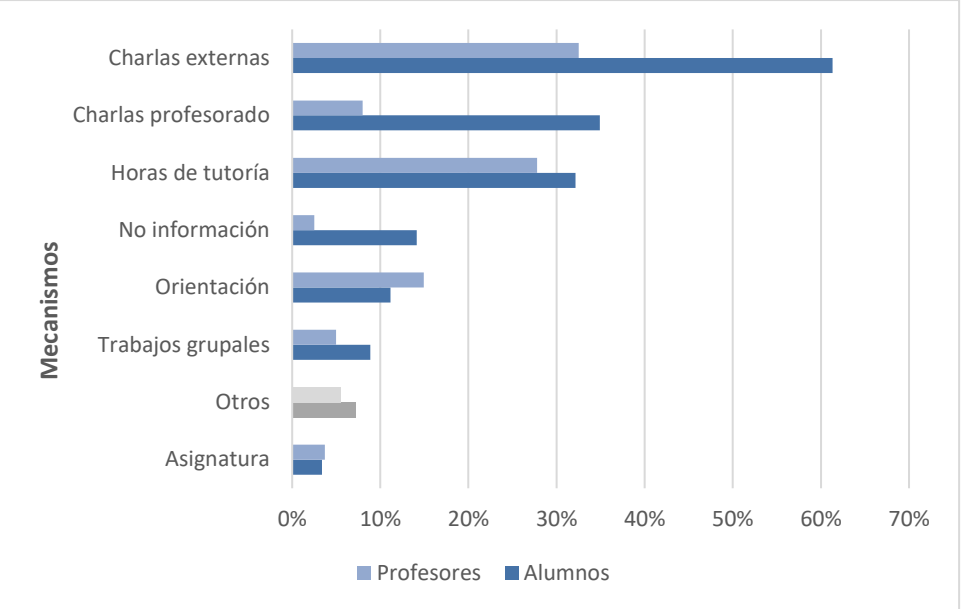


3. Comparación entre alumnos y docentes

Poniendo en común lo que han informado los alumnos con lo que han expuesto los docentes en relación a los mecanismos de prevención ante los riesgos de Internet, tanto unos como otros coinciden en que las charlas impartidas por profesionales externos son el principal mecanismo utilizado. No obstante, el porcentaje difiere bastante en dicha consideración (61% y 32,5%, respectivamente).

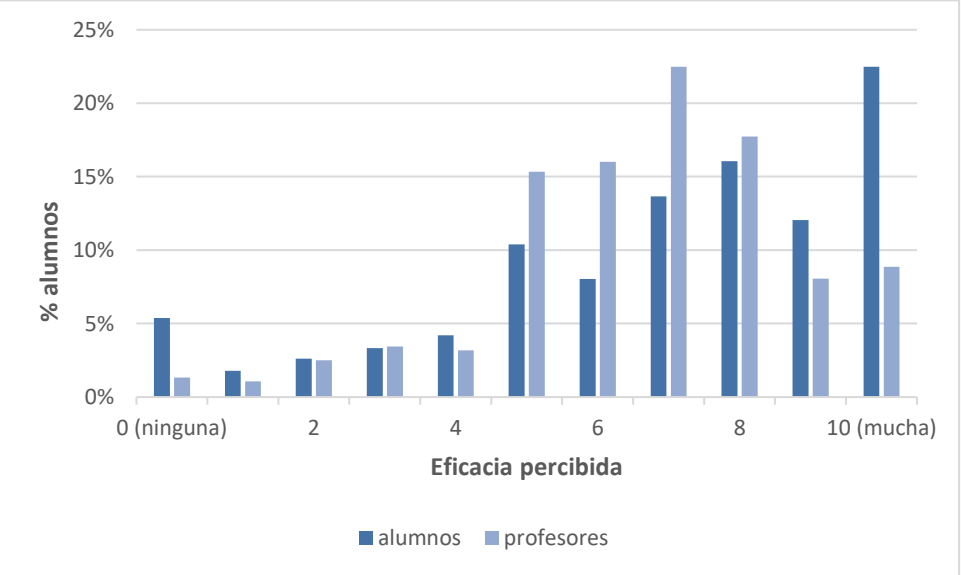
Tanto alumnos como docentes también coinciden en que los mecanismos menos utilizados son la realización de trabajos grupales o los contenidos incluidos en las propias asignaturas. Por otro lado, una diferencia importante entre ambos grupos se encuentra a la hora de afirmar que no existen medios de prevención o que no se actúa para prevenir. Mientras que un 14% de los alumnos afirma esta información, es tan solo un 2% de los docentes quien la respalda.

Gráfico 241. *Comparación de los mecanismos de prevención de los riesgos de Internet informados por los docentes y por los alumnos*



En cuanto a la eficacia percibida del conjunto de estos mecanismos, los profesores presentan una media superior ($\overline{X}$ = 6,62) a la de los alumnos ($\overline{X}$ = 5,64), no obstante, como dato a destacar, el mayor porcentaje del alumnado la ha calificado con un 10, mientras que en el caso del profesorado la calificación mayoritaria es de 7.

Gráfico 242. *Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de prevención de los riesgos de Internet existentes en sus centros educativos*



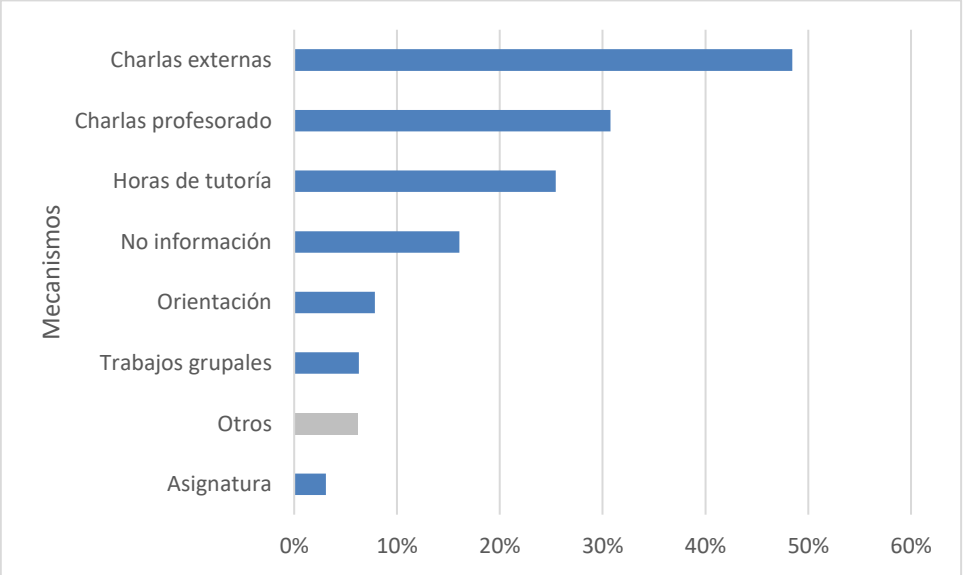
b) Mecanismos de prevención del uso desviado de Internet

1. Conocimiento de los alumnos

El mecanismo más frecuente de prevención del uso desviado de Internet disponible en los centros educativos de los alumnos encuestados es, de nuevo, el de las charlas externas, aunque en este caso el porcentaje de alumnos que refieren disponer de dicho mecanismo no es tan elevado (un 48%). Los siguientes dos mecanismos más frecuentes son, también, que los propios profesores del colegio den charlas (un 31%) y hablar sobre estos riesgos en las horas de tutoría (un 25%).

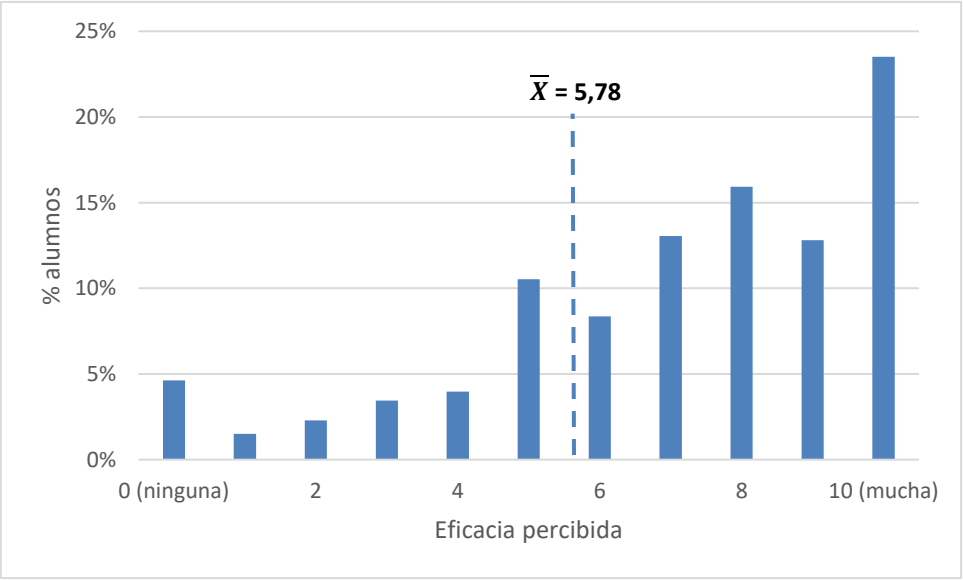
En este caso, el porcentaje de alumnos que informa de que en sus centros escolares no se da ningún tipo de información aumenta ligeramente en comparación con el caso de los riesgos de Internet, alcanzado una cifra de un 16%.

Gráfico 243. *Mecanismos de prevención del uso desviado de Internet existentes en los centros educativos según los alumnos*



Asimismo, la eficacia percibida de los alumnos sobre estos mecanismos es también bastante elevada, incluso un poco más que en el caso de los riesgos de Internet ($\overline{X}$ = 5,78), tal y como se observa en el siguiente gráfico.

Gráfico 244. *Percepción de los alumnos sobre la eficacia de los mecanismos de prevención del uso desviado de Internet*

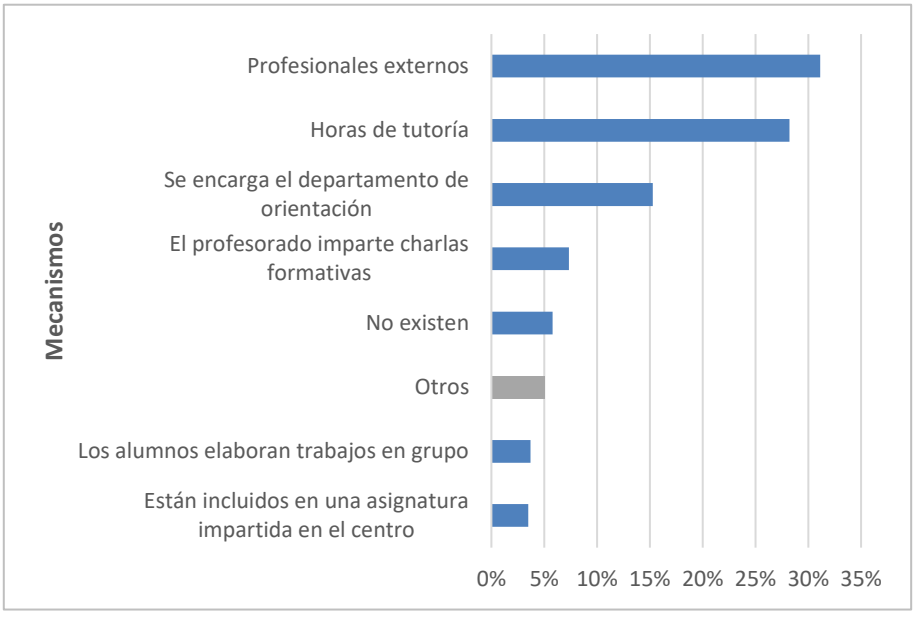


2. Conocimiento de los docentes

La situación de los mecanismos de prevención del uso desviado de Internet es muy similar a la de los riesgos de Internet, ya que los mecanismos más presentes en los centros educativos según los profesores son que profesionales externos den charlas (un 31,1% de los docentes afirma tener este mecanismo en su centro) y que los propios docentes den charlas en las horas de tutoría (un 28,2% de los docentes ha respondido a esta opción).

Sin embargo, en este caso el porcentaje de docentes que afirma que los centros educativos en los que trabajan no disponen de mecanismos de prevención es más elevado, llegando casi al 6%. Este dato permite hipotetizar que, generalmente, en los centros educativos analizados se destinan más recursos a prevenir los riesgos de Internet que el uso abusivo del mismo.

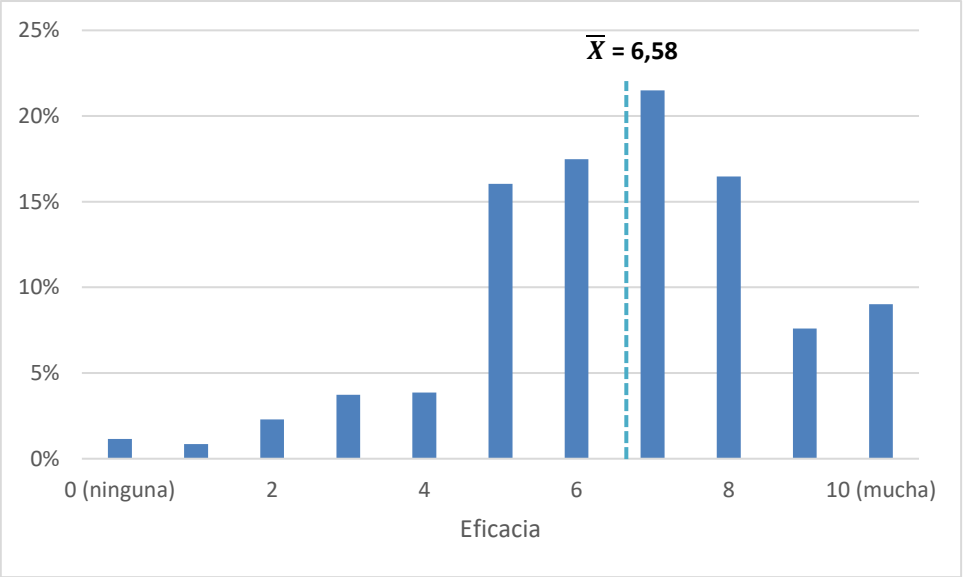
Gráfico 245. *Mecanismos de prevención del uso desviado de Internet existentes en los centros educativos según los docentes*



En cuanto a la eficacia percibida de estos mecanismos, la situación es prácticamente igual al caso anterior, ya que la mayoría de profesores considera

que la eficacia es moderada-alta, encontrándose la media en 6’6 sobre 10.

Gráfico 246. *Percepción de los docentes sobre la eficacia de los mecanismos de prevención del uso desviado de Internet*

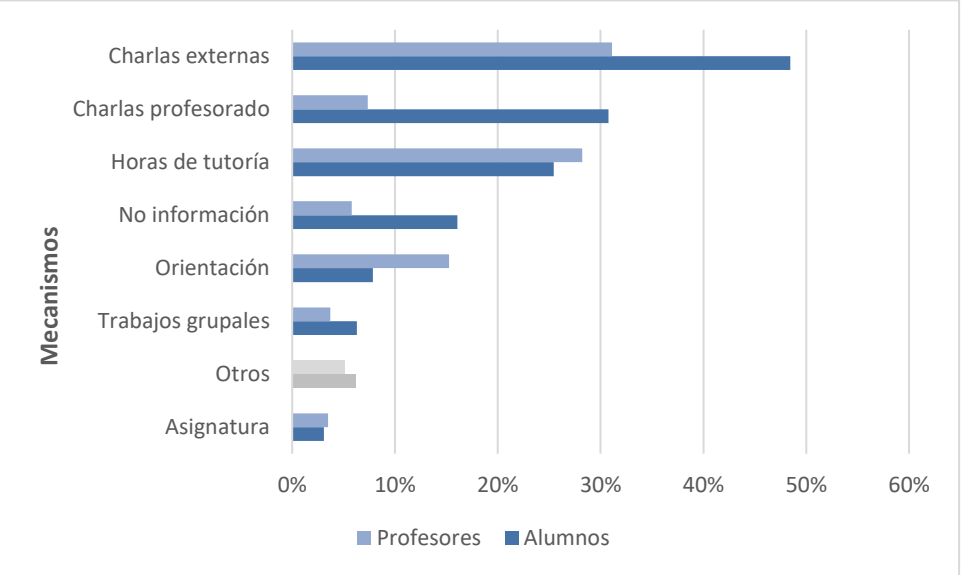


3. Comparación entre alumnos y docentes

Atendiendo a las estrategias de prevención del uso desviado de internet, las charlas externas siguen siendo consideras como el mecanismo utilizado con mayor frecuencia, como en el caso de los riesgos de Internet. No obstante, en este caso la diferencia en los porcentajes es menor (un 48% de los alumnos y un 31,1% de los docentes). En la misma línea, las dos estrategias que tanto alumnos como docentes consideran que se utilizan menos siguen siendo la realización de trabajos grupales e incluir los contenidos de prevención en las propias asignaturas impartidas en los centros.

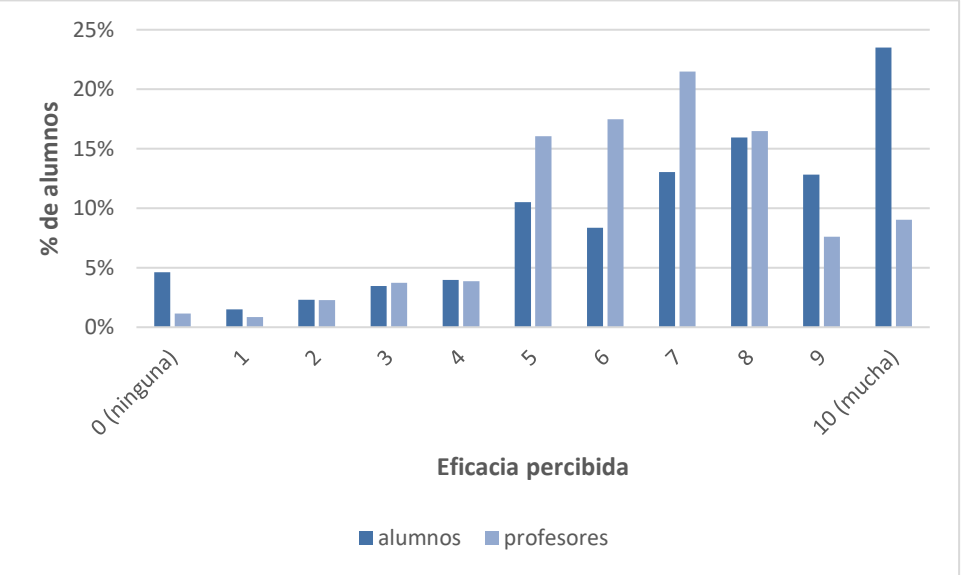
Otro dato relevante es la frecuencia con la que los alumnos consideran que se utilizan las charlas impartidas por los propios profesores como medio de prevención (31%), en comparación con la poca proporción indicada por los docentes del centro (7,3%).

Gráfico 247. *Comparación de los mecanismos de prevención del uso desviado de Internet informados por los docentes y por los alumnos*



Al igual que en el caso anterior, la media de la eficacia percibida del profesorado es superior ($\overline{X}$ = 6,58) a la del alumnado ($\overline{X}$ = 5,78). Además, el mayor porcentaje de alumnos la ha puntuado con un 10, mientras que en el caso de los profesores la puntuación más común es la de 7.

Gráfico 248. *Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de prevención del uso desviado de Internet existentes en sus centros educativos*



4.7.2 Mecanismos de intervención sobre los riesgos de Internet y el uso desviado en los centros educativos

Una vez vistos los mecanismos de prevención, en este apartado se detallan los resultados obtenidos respecto a los mecanismos de intervención, es decir, qué hacen los centros educativos, según los alumnos y sus profesores, para poner solución a una problemática de cibervictimización o uso desviado de Internet cuando ya ha aparecido un caso. Para ello, se analizan de manera individualizada los cuatro tipos de cibervictimización que se han ido estudiando a lo largo del presente informe (ciberacoso, ciberacoso sexual, control de pareja a través de las TIC y ciberataques económicos), así como el uso desviado de Internet.

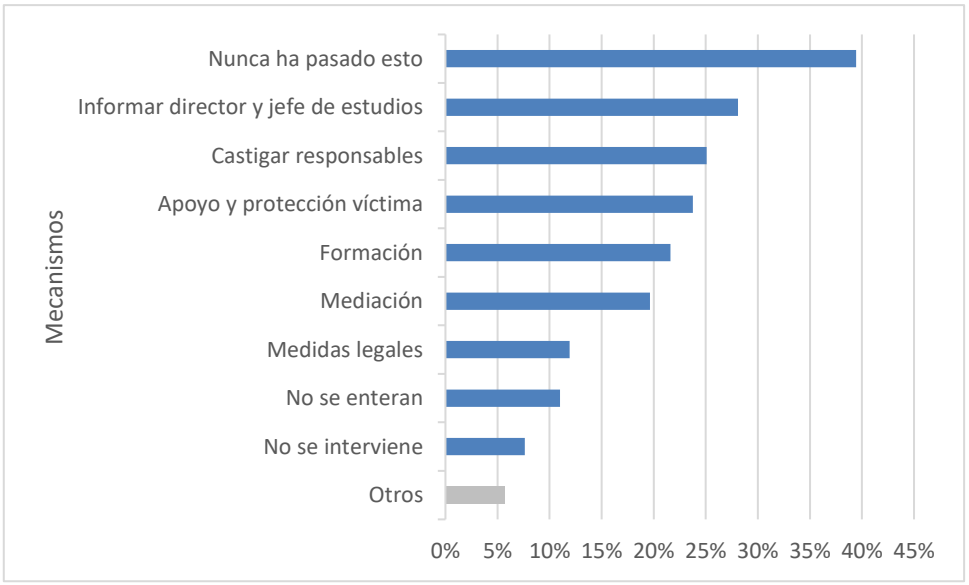
Asimismo, como en el apartado anterior, se analiza la eficacia percibida de unos y otros sobre dichos mecanismos de intervención y se realiza una comparación detallada de las respuestas dadas por ambos en cada caso.

a) Mecanismos de intervención en el ciberacoso

1. Conocimiento de los alumnos

Antes de analizar los mecanismos de intervención que tienen los centros educativos para actuar ante casos de ciberacoso, es interesante destacar que un importante porcentaje de alumnos (un 39%) considera que en sus centros nunca ha habido ningún caso de ciberacoso. Entre los que consideran que sí que ha habido casos de estas características, los mecanismos de intervención más frecuentes son informar al director y al jefe de estudios (un 28% de alumnos), castigar a los responsables (un 25%) y dar apoyo y protección a la víctima (un 24%). Cabe destacar que un 8% afirma que nunca se interviene, mientras que un 11% informa de que en el centro escolar no se suelen enterar de lo que sucede.

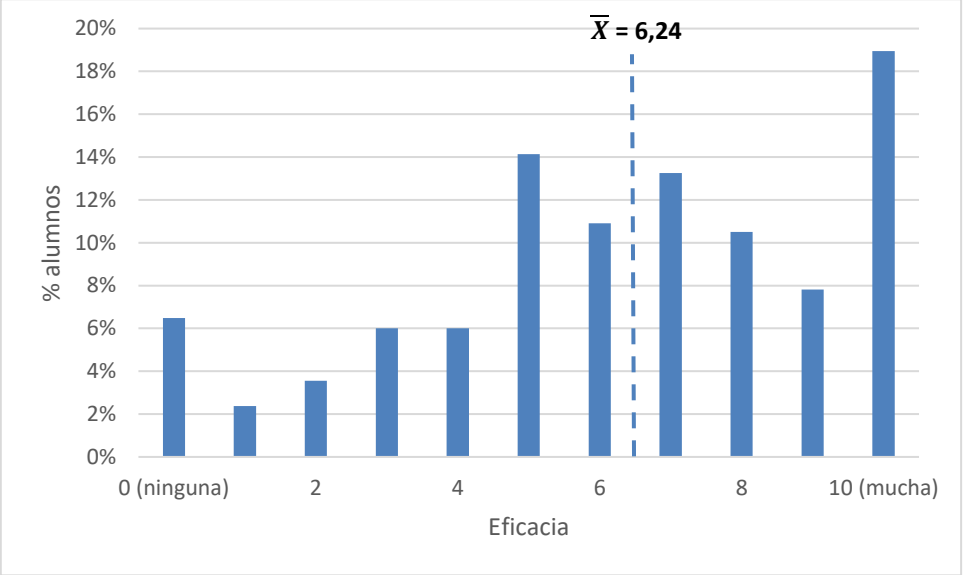
Gráfico 249. *Mecanismos de intervención ante casos de ciberacoso existentes en los centros educativos según los alumnos*



En cuanto a la eficacia percibida, casi un 20% de los alumnos considera que la situación del compañero que estaba sufriendo ciberacoso mejoró tras la intervención del centro educativo, en contraposición con un 6% de alumnos que

considera que la situación no mejoró absolutamente nada. En general, la eficacia percibida se distribuye de una forma bastante heterogénea, tal y como se observa en el siguiente gráfico.

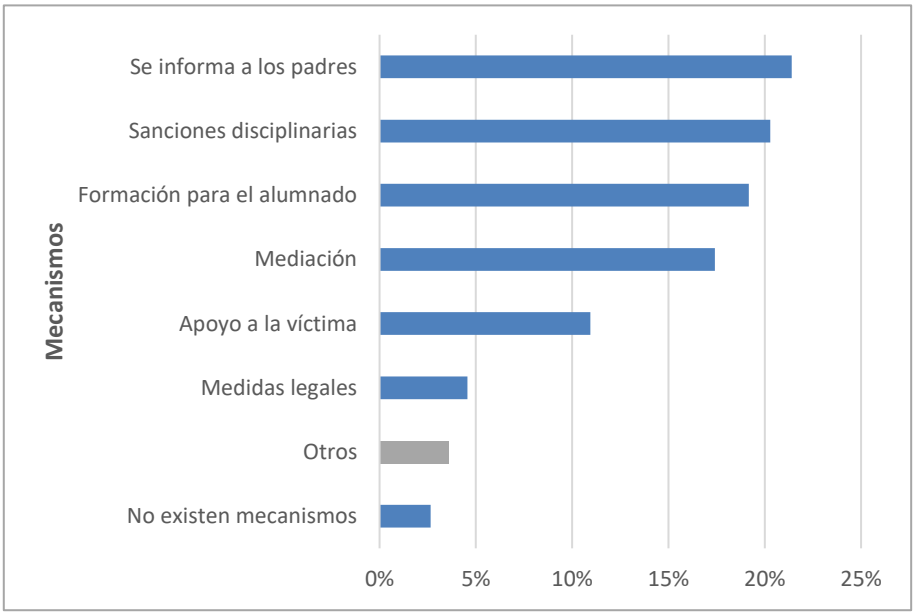
Gráfico 250. *Percepción de los alumnos sobre la eficacia de los mecanismos de intervención ante casos de ciberacoso*



2. Conocimiento de los docentes

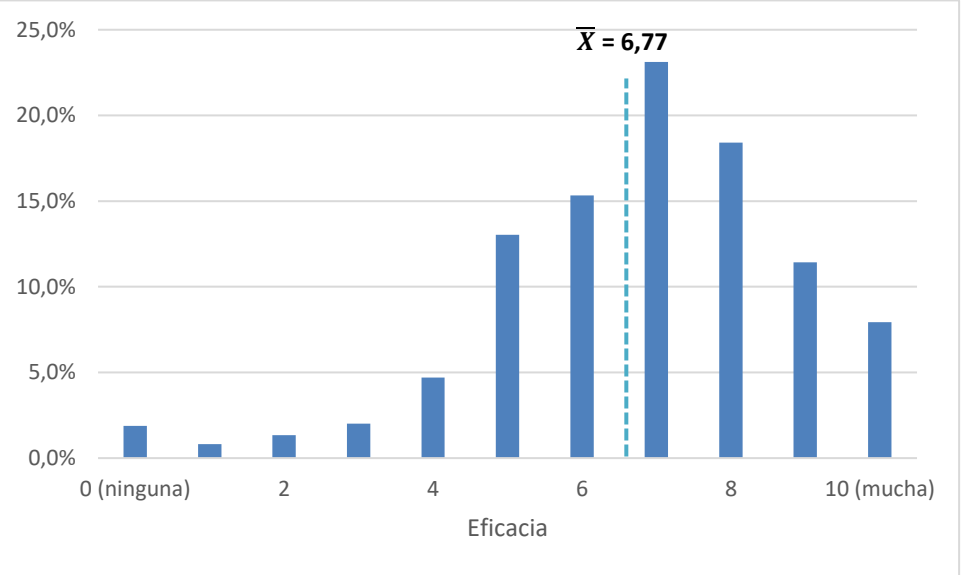
Son varios los mecanismos orientados a intervenir ante casos de ciberacoso. En la mayoría de centros, los cuatro mecanismos más comunes, según los docentes, son informar a los padres (un 21,4% de los docentes afirma tener dicho mecanismo en su centro), aplicar sanciones disciplinarias (20,3% de docentes), formar al alumnado (19,2% de docentes) y hacer mediación (17,4%). Existe casi un 3% de docentes que afirma que en sus centros educativos no existe ningún tipo de mecanismo de intervención para el ciberacoso.

Gráfico 251. *Mecanismos de intervención ante casos de ciberacoso existentes en los centros educativos según los docentes*



Además, cabe destacar que, en general, los docentes consideran que los mecanismos de intervención presentes en sus centros educativos son eficaces. De hecho, la media se encuentra en un 6,8 sobre 10, aproximadamente, tal y como se observa en el siguiente gráfico.

Gráfico 252. *Percepción de los docentes sobre la eficacia de los mecanismos de intervención ante casos de ciberacoso*



3. Comparación entre alumnos y docentes

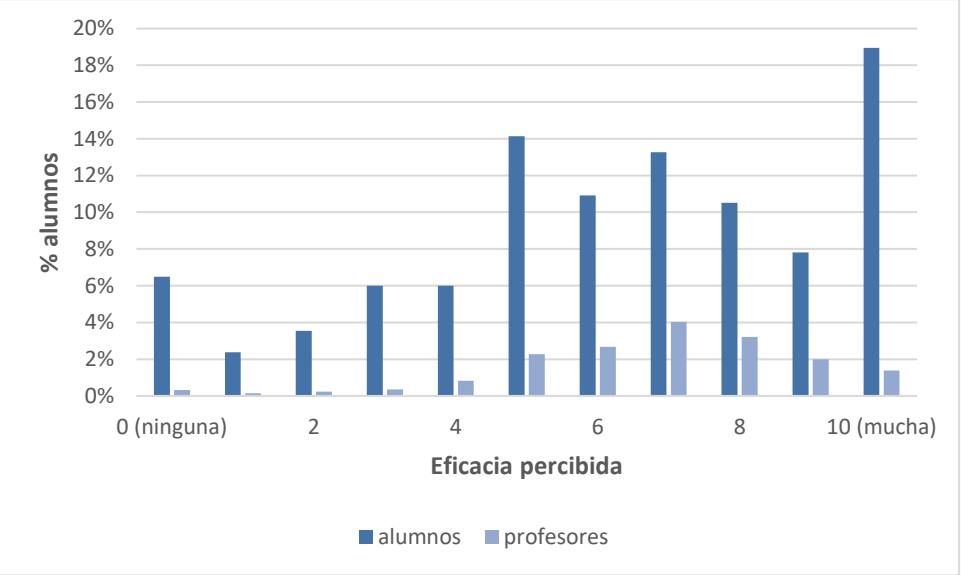
En lo que respecta a los mecanismos de intervención utilizados para actuar ante casos de ciberacoso, existen discrepancias entre los alumnos y los profesores. Los primeros consideran que el principal mecanismo es informar al director y al jefe de estudios (28%), seguido por castigar a los responsables (25%) y dar apoyo y protección a la víctima (24%). Sin embargo, los profesores posicionan en primer lugar informar a los padres (21,4%), seguido, al igual que consideran los alumnos, de aplicar sanciones disciplinares (20,3%) y de formar al alumno (19,2%).

Una semejanza importante hallada es el bajo porcentaje, tanto de alumnos como de profesores, que considera que no se utiliza ningún tipo de mecanismo concreto, ya sea por considerar que no existen, como es el caso de los profesores, o porque directamente no se interviene ante estos casos, como afirman los alumnos (2,7% y 8%, respectivamente).

En este caso, la media de los alumnos y los profesores en cuanto a la percepción

de eficacia difiere en menor medida (6,24 y 6,77, respectivamente). Además, la puntuación que tiene un mayor consenso, como en los dos casos anteriores, sigue siendo de 10 en alumnos y de 7 en profesores.

Gráfico 253. *Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de intervención ante casos de ciberacoso existentes en sus centros educativos*



b) Mecanismos de intervención ante el ciberacoso sexual

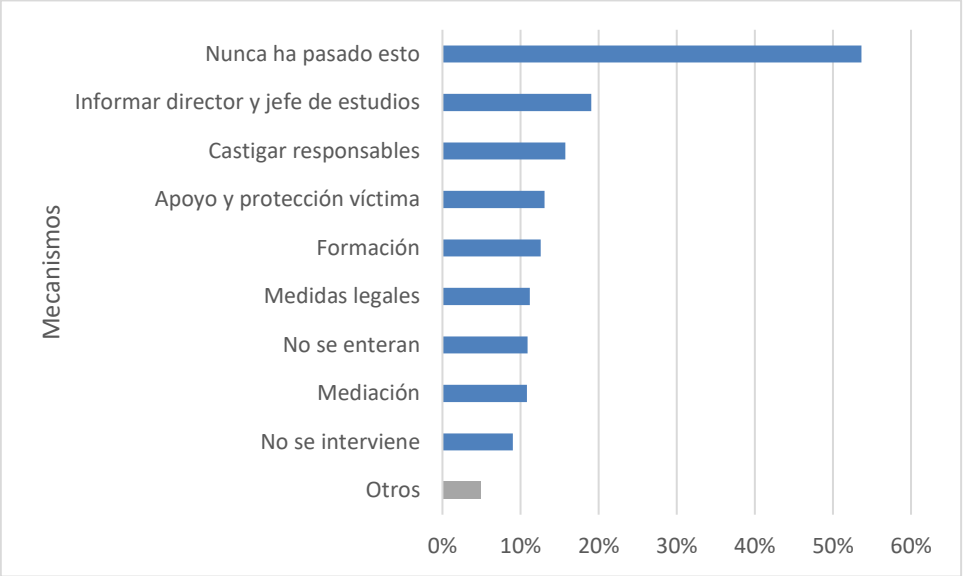
1. Conocimiento de los alumnos

Igual que sucede en el caso del ciberacoso, en el ciberacoso sexual el porcentaje de alumnos que considera que nunca ha habido ningún caso de este tipo en sus centros educativos es bastante elevado, llegando incluso a superar la mayoría (un 54%)[16]. Entre los que consideran que sí que ha habido casos de estas características, los mecanismos de intervención más frecuentes son informar al director y al jefe de estudios (un 19% de alumnos), castigar a los responsables

[16] Los mecanismos de intervención ante el ciberacoso sexual solo han sido preguntados entre los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, por lo que los alumnos de 5º y 6º de primaria y 1º de ESO quedan excluidos de este análisis.

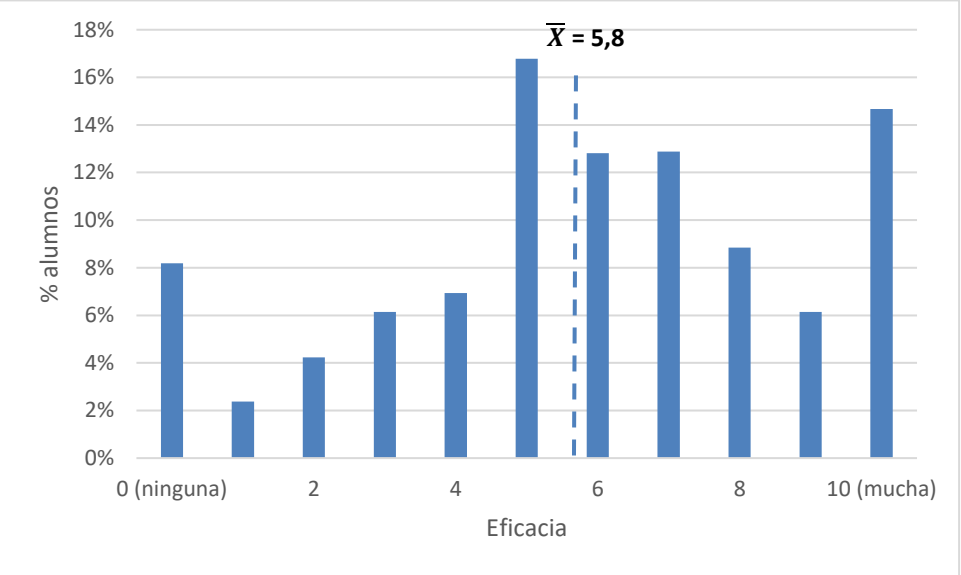
(un 16%) y dar apoyo y protección a la víctima (un 13%). Ante estos casos, los datos parecen indicar que se dedican más recursos a castigar a los responsables que dar apoyo a la víctima. Cabe destacar que el porcentaje de alumnos que considera que el colegio no actúa se reduce a un 9% en comparación con el caso del ciberacoso.

Gráfico 254. *Mecanismos de intervención ante casos de ciberacoso sexual existentes en los centros educativos según los alumnos*



En cuanto a la eficacia percibida, un 15% de los alumnos considera que la situación del compañero que estaba sufriendo ciberacoso sexual mejoró tras la intervención del centro educativo, en contraposición con un 8% de alumnos que considera que la situación no mejoró absolutamente nada. En general, la eficacia percibida se distribuye de una forma bastante heterogénea, como en el caso del ciberacoso, pero ésta parece ser más baja. De hecho, casi un 20% de los alumnos ha puntuado con un 5, cifra no muy elevada, la eficacia de dichos mecanismos.

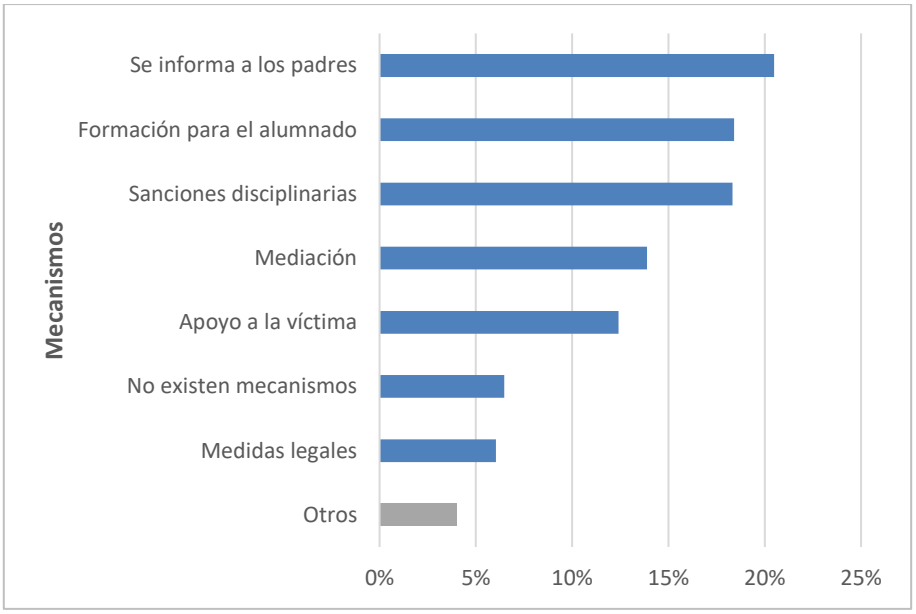
Gráfico 255. *Percepción de los alumnos sobre la eficacia de los mecanismos de intervención ante casos de ciberacoso sexual*



2. Conocimiento de los docentes

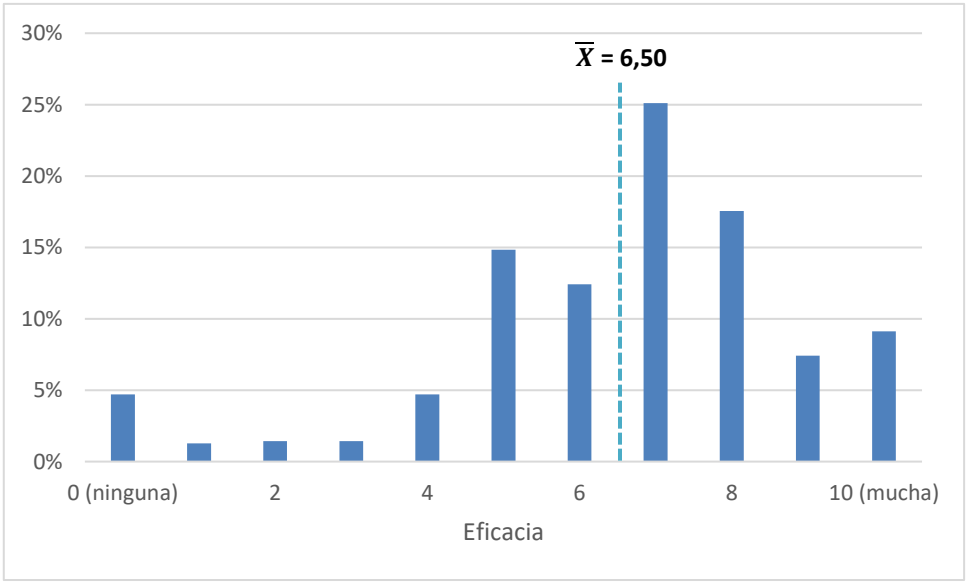
En este caso los mecanismos de intervención son los mismos que en el ciberacoso y, además, los tres mecanismos más comunes también coinciden con el primer tipo de cibervictimización: informar a los padres (un 20,5% de los docentes afirma que se usa este mecanismo), formar al alumnado (un 18,4%) y aplicar sanciones disciplinarias (un 18,3%). Sin embargo, en este tipo de cibervictimización hay un porcentaje más elevado de docentes (casi un 7%) que considera que no existe ningún tipo de mecanismo de intervención que en el caso del ciberacoso.

Gráfico 256. *Mecanismos de intervención ante casos de ciberacoso sexual existentes en los centros educativos según los docentes*



En cuanto a la eficacia percibida de estos mecanismos por parte de los docentes, ésta es muy similar a la del ciberacoso, siendo la media un poco más baja en este caso (un 6,5 sobre 10).

Gráfico 257. *Percepción de los docentes sobre la eficacia de los mecanismos de intervención ante casos de ciberacoso sexual*



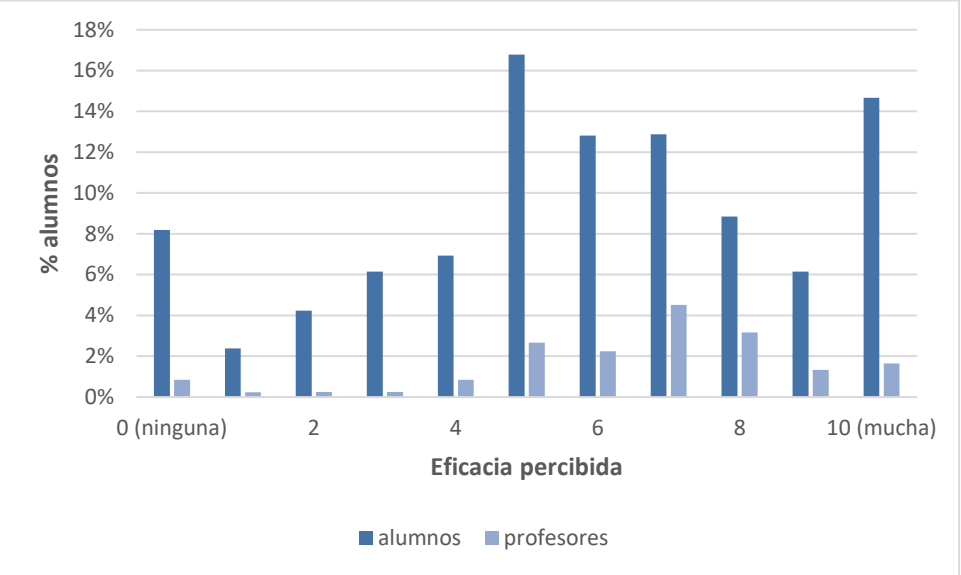
3. Comparación entre alumnos y docentes

Frente a casos de ciberacoso sexual, tanto alumnos como profesores informan de que los mecanismos más utilizados son los mismos que ante casos de ciberacoso, aunque mostrando porcentajes más bajos. Un 19% de los alumnos considera que informar al director y al jefe de estudios es el más utilizado, frente a un 20,5% de los profesores que sostienen que informar a los padres es el más frecuente.

Ambos colectivos coinciden en que utilizar sanciones disciplinarias es también uno de los mecanismos utilizados con mayor frecuencia por los centros educativos, con una proporción del 17%, aproximadamente, en ambos casos, un porcentaje que, además, no se aleja demasiado de las consideradas como las más utilizadas.

La media de la eficacia percibida de los mecanismos de intervención ante casos de ciberacoso sigue siendo superior en el caso del profesorado (6,5 frente a 5,8). En este tipo de ciberacoso, el mayor porcentaje de profesores los sigue calificando con un 7, aunque en el caso del alumnado la situación cambia, ya que la mayoría los ha puntuado con un 5.

Gráfico 258. *Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de intervención ante casos de ciberacoso sexual existentes en sus centros educativos*



c) Mecanismos de intervención en el control de pareja a través de las TIC e Internet

1. Conocimiento de los alumnos

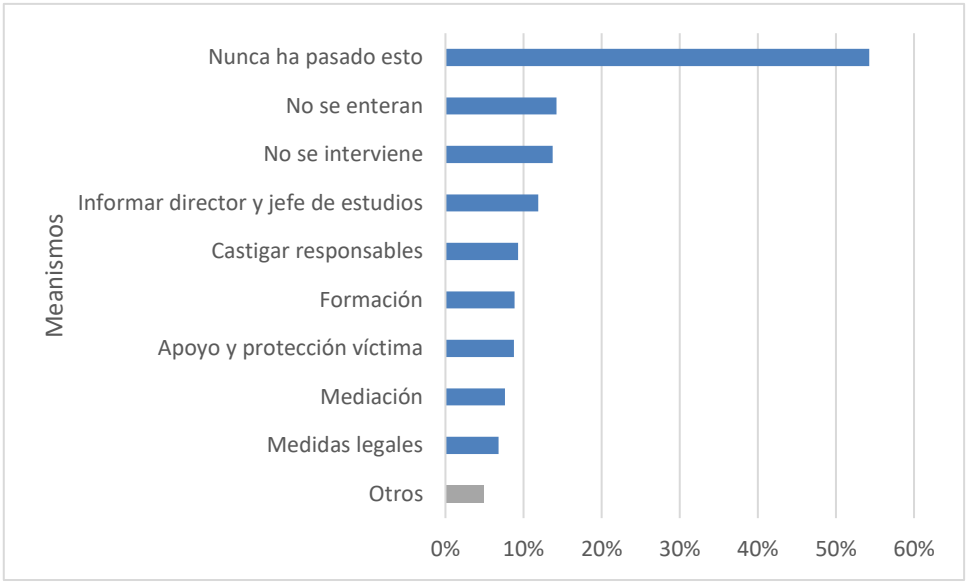
El control de pareja a través de las TIC e Internet es una de las conductas que más consenso presenta a la hora de afirmar que nunca ha sucedido en los centros educativos. De hecho, más de la mayoría de alumnos (un 54%) afirma que en sus colegios nunca ha habido casos de este tipo[17]. Entre los que consideran que sí que ha habido casos de estas características, destaca que un 14% de los alumnos considera que o bien los profesores no se enteran o, si lo hacen, no intervienen. Estos resultados podrían indicar que existe un gran desconocimiento en los centros educativos sobre casos de control de pareja, por

[17] Los mecanismos de intervención ante el control de pareja a través de las TIC e Internet solo han sido preguntados entre los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, por lo que los alumnos de 5º y 6º de primaria y 1º de ESO quedan excluidos de este análisis

ser una conducta que tiene lugar mayoritariamente en el ámbito privado.

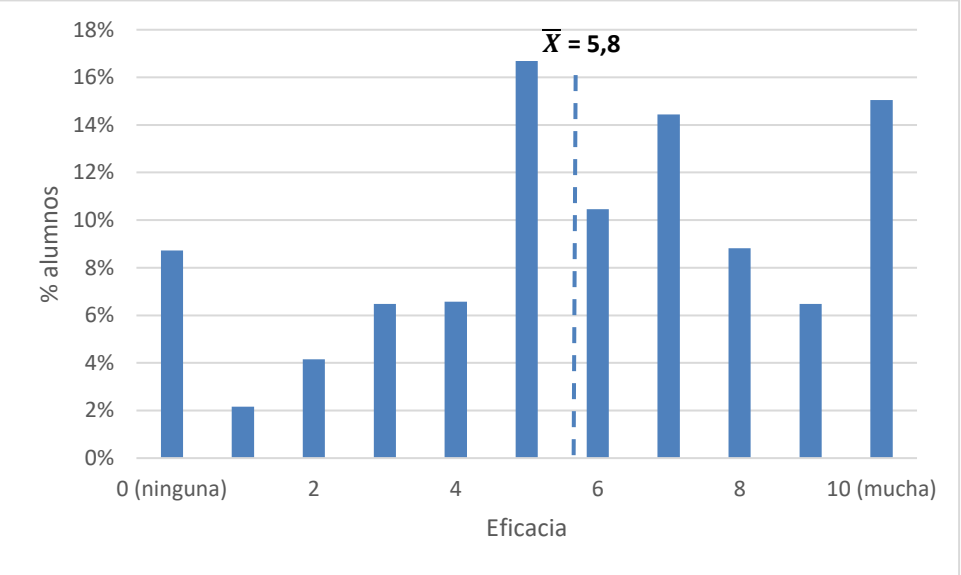
Entre los mecanismos más frecuentes se encuentran, según un 12% de los alumnos, informar al director y al jefe de estudios y, según un 9%, castigar a los responsables, explicar a los alumnos lo que sucede y las consecuencias negativas (formación), apoyar y proteger a la víctima y realizar mediaciones. En general, los análisis realizados hasta el momento tanto en el caso del ciberacoso, como en el del ciberacoso sexual y el control de pareja, indican que es más frecuente dedicar esfuerzos a castigar a los responsables de los ciberataques que proteger y dar apoyo a las víctimas.

Gráfico 259. *Mecanismos de intervención ante casos de control de pareja a través de las TIC existentes en los centros educativos según los alumnos*



En cuanto a la eficacia percibida, un 15% de los alumnos considera que la situación del compañero que estaba sufriendo ciberacoso sexual mejoró tras la intervención del centro educativo, en contraposición con un 9% de alumnos que considera que la situación no mejoró absolutamente nada. En general, la eficacia percibida se distribuye de una forma bastante heterogénea, como en el caso del ciberacoso y el ciberacoso sexual.

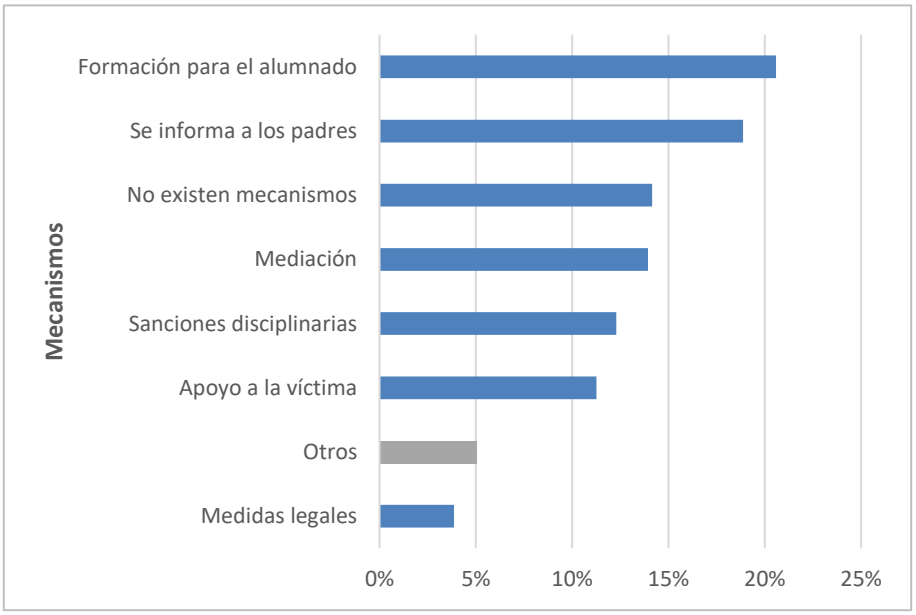
Gráfico 260. *Percepción de los alumnos sobre la eficacia de los mecanismos de intervención ante casos de control de pareja a través de las TIC*



2. Conocimiento de los docentes

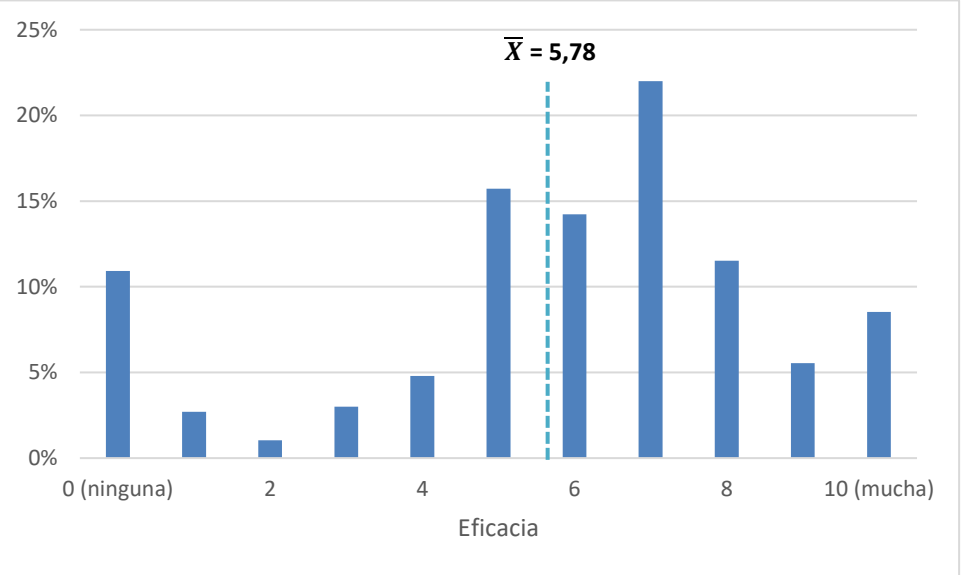
El control de pareja a través de las TIC e Internet presenta algunas similitudes y algunas diferencias respecto a las dos anteriores cibervictimizaciones -ciberacoso y ciberacoso sexual-. En cuanto a las similitudes, se observa que los dos mecanismos más detectados por los docentes son formar al alumnado (un 20,6% de los docentes ha respondido esta opción) e informar a los padres (18,9% de los docentes). La principal diferencia, sin embargo, es que un 14% de los docentes considera que no existen mecanismos de intervención en estos casos, siendo una cifra muy superior a las de las otras cibervictimizaciones. Es decir, los datos obtenidos indican que ante casos de control de pareja a través de los TIC los profesores consideran que se interviene menos.

Gráfico 261. *Mecanismos de intervención ante casos de control de pareja a través de las TIC e Internet existentes en los centros educativos según los docentes*



Además, en este caso la eficacia percibida de dichos mecanismos por parte de los docentes es también menor que en el ciberacoso y el ciberacoso sexual, siendo la media de 5,8 sobre 10.

Gráfico 262. *Percepción de los docentes sobre los mecanismos de intervención ante casos de control de pareja a través de las TIC e Internet*

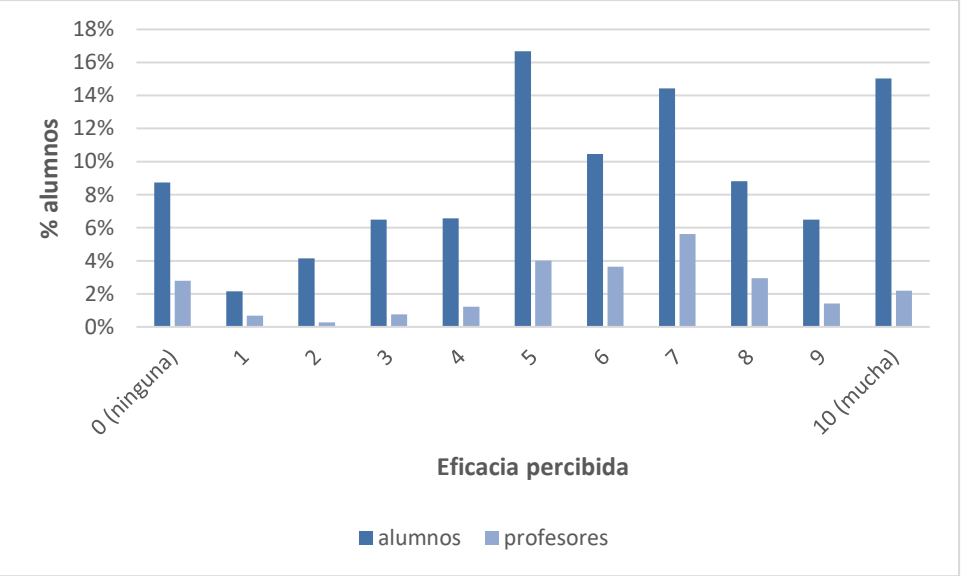


3. Comparación entre alumnos y docentes

Atendiendo a los mecanismos utilizados en el caso del control de pareja a través de las TIC e Internet, las diferencias entre alumnos y profesores son algo mayores, ya que los alumnos valoran que informar al director y jefe de estudios es la más utilizada (un 12%), mientras que los profesores consideran que la principal estrategia es formar al alumnado (un 20,6%), seguido de informar a los padres (un 18,9%). No obstante, en este caso sí coinciden en afirmar que emplear medidas legales y dar apoyo a la víctima son las menos utilizadas, con unos porcentajes que no alcanzan el 12% ni entre los alumnos ni entre los docentes.

En este caso, las medias de eficacia percibida no varían en absoluto (5,8 en ambos casos) y, como en el caso anterior, la mayor proporción de alumnos la ha calificado con un 5 y la de profesores con un 7.

Gráfico 263. *Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de intervención ante casos de control de pareja a través de las TIC existentes en sus centros educativos*



d) Mecanismos de intervención en la cibervictimización económica

1. Conocimiento de los alumnos

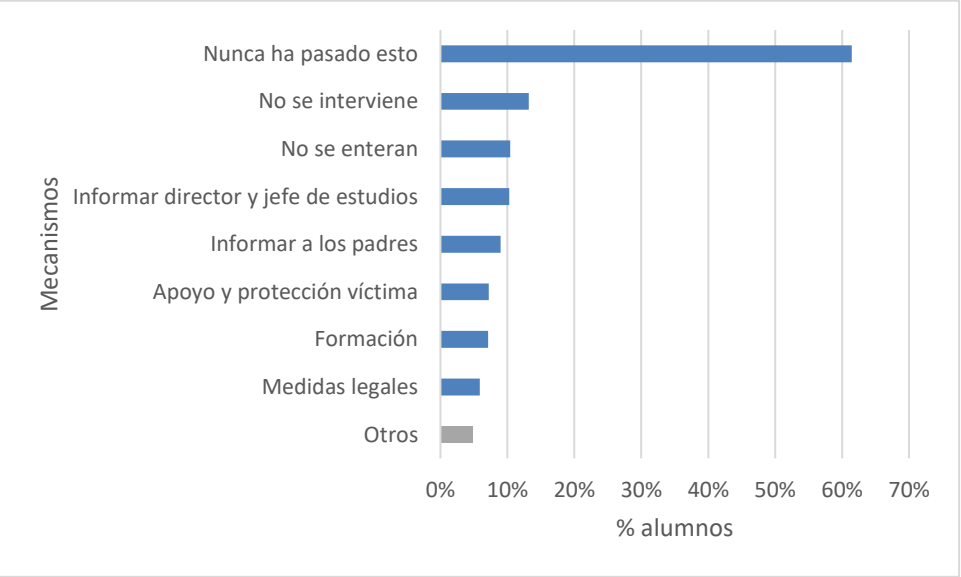
Los ciberataques económicos son la categoría de ataques que presenta un mayor consenso entre los alumnos a la hora de afirmar que nunca ha sucedido en los centros educativos, ya que como muestra el gráfico, más de un 60% de alumnos afirma que en sus colegios nunca ha habido casos de este tipo[18]. Entre los que consideran que sí que ha habido casos de estas características, destaca que un 13% de los alumnos considera que no se interviene y un 10% opina que los profesores no llegan a enterarse de lo que sucede. Estos resultados podrían indicar, como en el caso del control de pareja, que existe un gran

[18] Los mecanismos de intervención ante casos de ciberataques económicos solo han sido preguntados entre los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, por lo que los alumnos de 5º y 6º de primaria y 1º de ESO quedan excluidos de este análisis

desconocimiento en los centros educativos sobre la cibervictimización económica.

Entre los mecanismos más frecuentes se encuentran, según un 10% de los alumnos, informar al director y al jefe de estudios, según un 9%, informar a los padres del alumno víctima y, según un 7%, dar apoyo y protección al alumno víctima e informar al resto de alumnos de lo que ha sucedido, sus consecuencias negativas y cómo evitar que vuelva a suceder (formación).

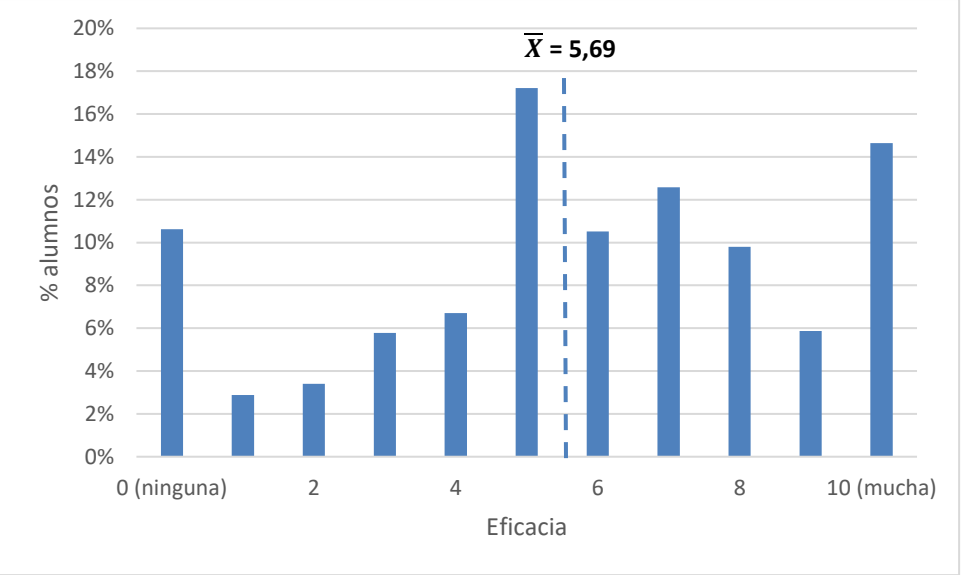
Gráfico 264. *Mecanismos de intervención ante casos de ciberataques económicos existentes en los centros educativos según los alumnos*



Respecto a la percepción de eficacia de los alumnos, un 15% de ellos considera que la situación del compañero que sufrió el ciberataque económico mejoró tras la intervención del centro educativo, en contraposición con un 11% de alumnos que considera que la situación no mejoró absolutamente nada. Es decir, los porcentajes entre aquellos que consideran que la intervención fue muy eficaz y aquellos que consideran que no lo fue en absoluto son bastante similares, lo que muestra que la muestra está bastante polarizada. A pesar de ello, en general, la eficacia percibida se distribuye de una forma bastante heterogénea, como en el

caso de los tres tipos de cibervictimización social analizados anteriormente.

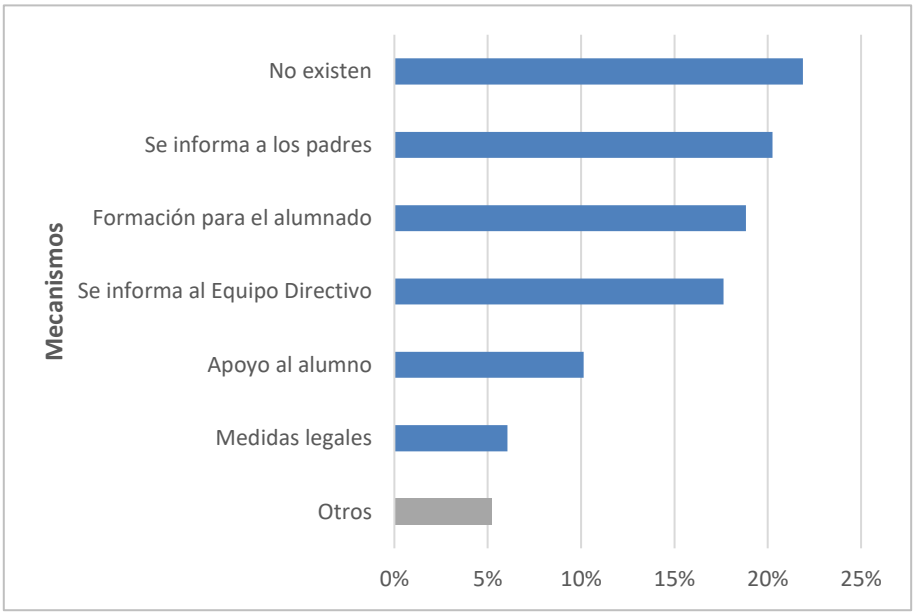
Gráfico 265. *Percepción de los alumnos sobre la eficacia de los mecanismos de intervención ante caos de ciberataques económicos*



2. Conocimiento de los docentes

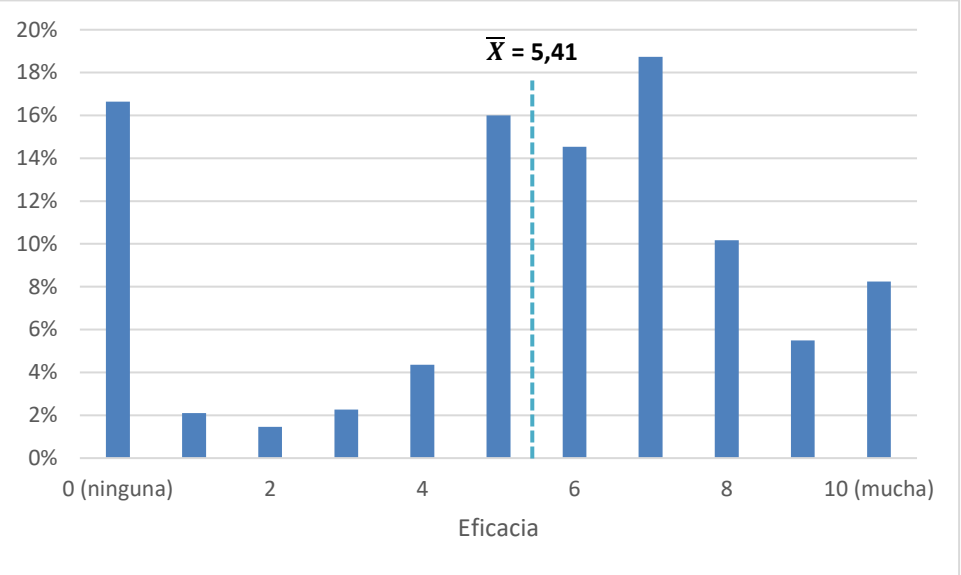
Según los docentes, los mecanismos más comunes a la hora de intervenir ante casos de cibervictimización económica son informar tanto a los padres (un 20,3% de los docentes) como al equipo directivo (un 17,6%) y formar al alumnado (un 18,8%). Sin embargo, el porcentaje más alto (casi un 22% de los docentes) corresponde a la opción "No existen mecanismos de intervención ante casos de cibervictimización económica". Es decir, a la hora de preguntar sobre los mecanismos de intervención en casos de cibervictimización económica, la respuesta más común es que no existen dichos mecanismos, lo que podría indicar que, en general, este tipo de cibervictimización no se tiene en cuenta en los centros educativos.

Gráfico 266. *Mecanismos de intervención ante casos de ciberataques económicos existentes en los centros educativos según los docentes*



Además, la eficacia percibida es baja (la media se encuentra en un 5,4 sobre 10). De hecho, es destacable mencionar que un 16,6% de los docentes considera que dichos mecanismos son totalmente ineficaces.

Gráfico 267. *Percepción de los docentes sobre la eficacia de los mecanismos de intervención ante casos de ciberataques económicos*



3. Comparación entre alumnos y docentes

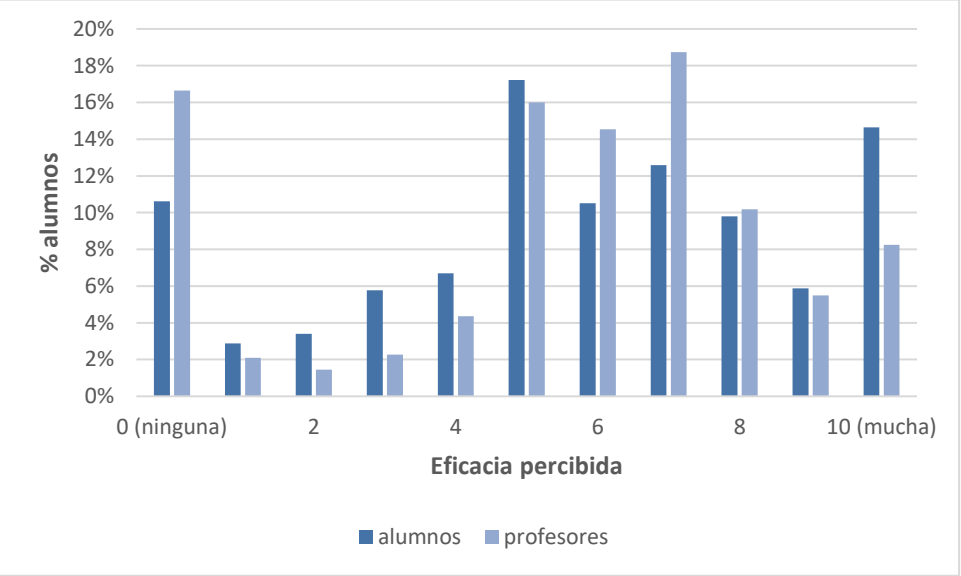
Con un porcentaje muy bajo (un 10%), los alumnos consideran que informar al director y al jefe de estudios es el mecanismo de intervención más frecuente frente a la cibervictimización económica, mientras que los profesores informan que informar a los padres es el utilizado con mayor frecuencia (un 20,3%), posicionando el mecanismo de informar al equipo directivo como el tercero de más utilidad, seguido de formar al alumnado.

Atendiendo a las semejanzas, ambos vuelven a coincidir, con apenas diferencias, en que utilizar medidas legales y ofrecer apoyo y protección a la víctima son los menos utilizados.

Con respecto al grado de eficacia percibida en este caso, la media tampoco varía en gran medida, siendo de 5,69 en el caso del alumnado y de 5,41 en el del profesorado. La mayoría de los alumnos ha calificado la eficacia de los mecanismos de intervención con un 5. En cuanto a los docentes, a pesar de que

la mayoría de ellos ha puntuado con un 7, hay un porcentaje elevado a destacar que los ha calificado como nada útiles (16,6%).

Gráfico 268. *Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de intervención ante casos de ciberataques económicos existentes en sus centros educativos*



e) Mecanismos de intervención ante conductas desviadas en el uso de Internet

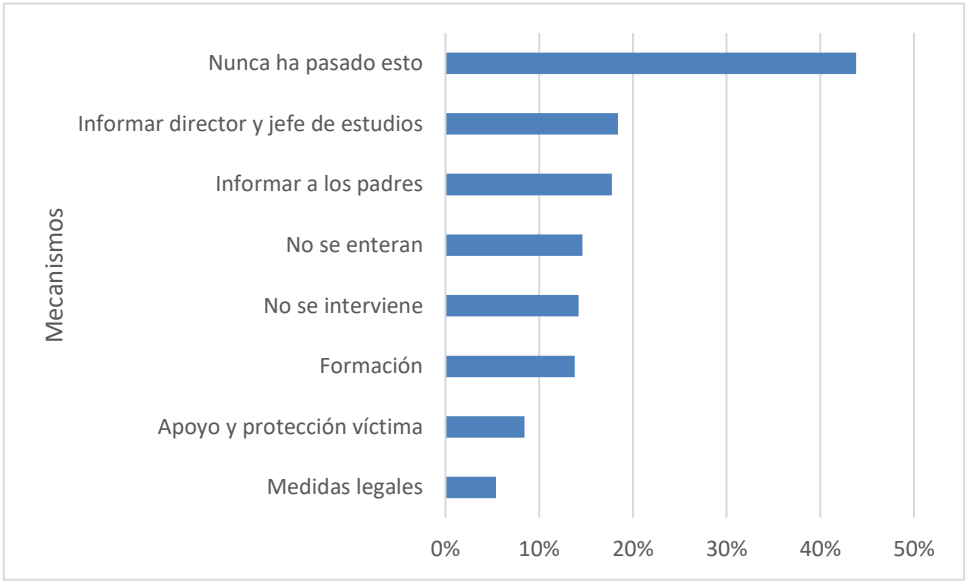
1. Conocimiento de los alumnos

Igual que sucede en las cuatro conductas analizadas anteriormente, el porcentaje de alumnos que considera que nunca ha habido ningún caso de este tipo en sus centros educativos es bastante elevado (un 44%)[19]. Entre los que consideran que sí que ha habido casos de estas características, los mecanismos de intervención más frecuentes son informar al director y al jefe de estudios y a los padres (un 18% de alumnos) y formar al alumnado (un 14%). De nuevo, un porcentaje

[19] Los mecanismos de intervención ante casos de uso desviado de Internet solo han sido preguntados entre los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM, por lo que los alumnos de 5º y 6º de primaria y 1º de ESO quedan excluidos de este análisis.

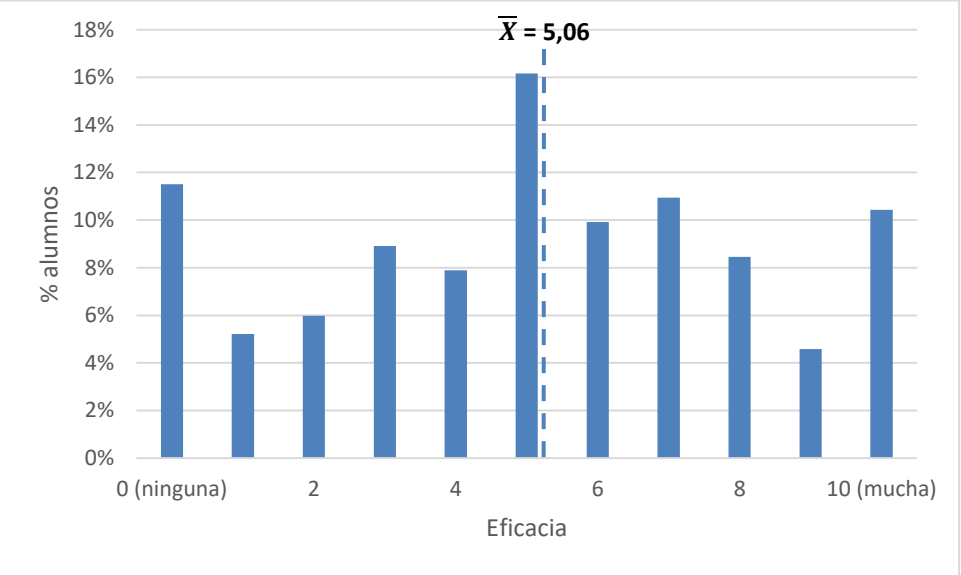
importante de alumnos comunica que o bien los profesores no se enteran (un 15%) o, si lo hacen, no intervienen (un 14%).

Gráfico 269. *Mecanismos de intervención ante casos de uso desviado de Internet existentes en los centros educativos según los alumnos*



Respecto a la percepción de eficacia de los alumnos, el porcentaje de los que consideran que la intervención del centro educativo no sirvió de nada es superior a los que consideran que sirvió muchísimo (un 12% en el primer caso frente a un 10% en el segundo). En general, la eficacia percibida parece ser bastante buena, ya que una gran parte de alumnos ha dado una puntuación de entre 5 y 7 a la eficacia de las actuaciones. Sin embargo, la media es prácticamente de 5, tal y como muestra el gráfico.

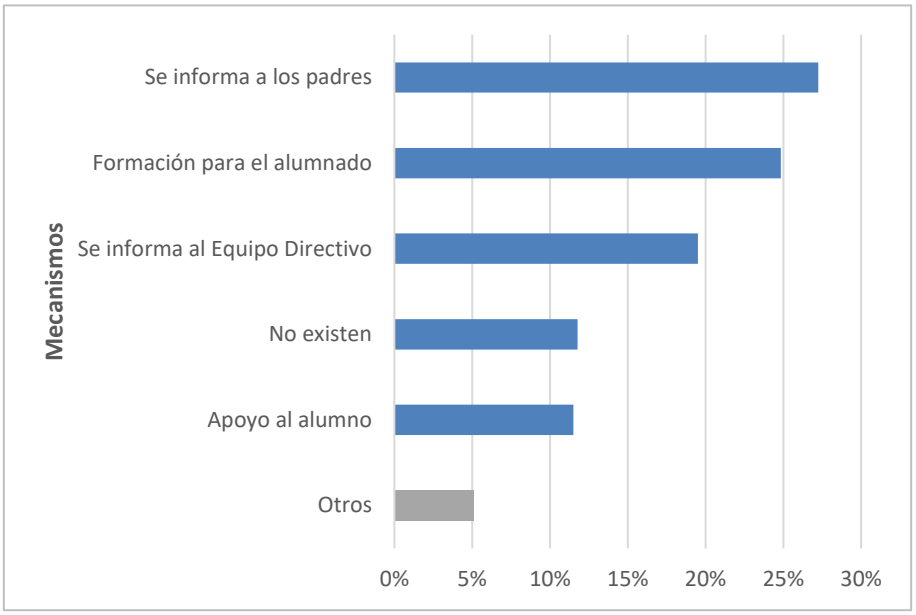
Gráfico 270. *Percepción de los alumnos sobre la eficacia de los mecanismos de intervención ante casos de uso desviado de Internet*



2. Conocimiento de los docentes

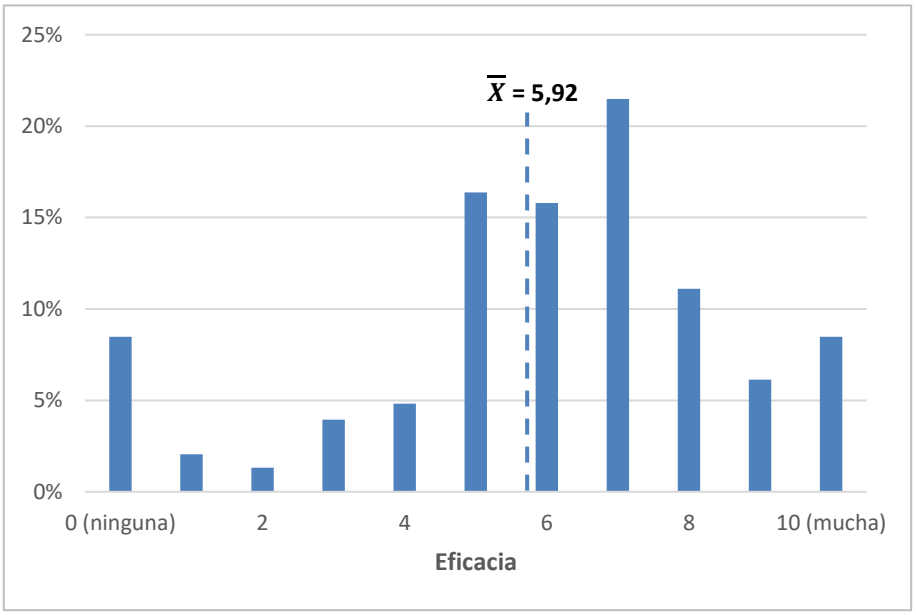
Como en los cuatro casos anteriores, los dos mecanismos de intervención más comunes ante casos de uso desviado de Internet son informar a los padres (un 27,2% de los docentes) y formar al alumnado (un 24,9%). Además, el porcentaje de docentes que considera que no existen mecanismos también es importante, ya que alcanza casi un 12%.

Gráfico 271. *Mecanismos de intervención ante casos de uso desviado de Internet existentes en los centros educativos según los docentes*



En cuanto a la eficacia percibida, cabe destacar que, aunque ésta no es muy elevada, sí que es superior a la del control de pareja a través de las TIC y la cibervictimización económica, encontrándose la media en un 5,9 sobre 10.

Gráfico 272. Percepción de los docentes sobre la eficacia de los mecanismos *de intervención ante casos de uso desviado de Internet*

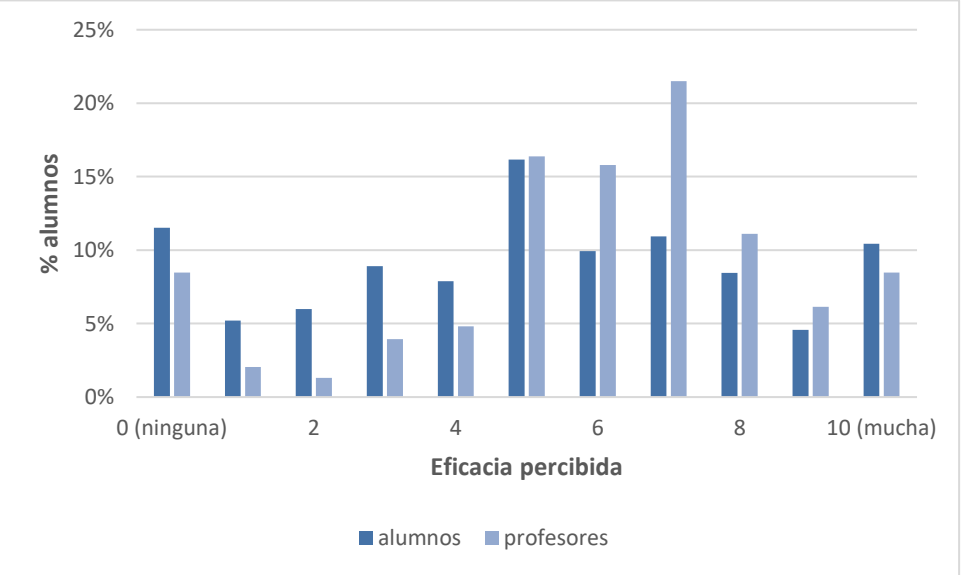


3. Comparación entre alumnos y docentes

Por último, haciendo mención a los mecanismos de intervención ante conductas de uso desviado de Internet, el principal mecanismo utilizado considerado por los alumnos sigue siendo informar al director y al feje de estudios (un 18%), seguido en por informar a los padres. En este sentido, existen diferencias respecto a los profesores, quienes siguen considerando que el principal mecanismo es informar a los padres (un 27,2%), seguido de formar al alumnado (un 24,9%). Por otro lado, siguen coincidiendo en que el dar apoyo a la víctima es uno de los mecanismos menos utilizados.

En esta última conducta analizada, la media de eficacia percibida vuelve a ser superior en el caso de los profesores (5,92 frente a 5,06) y el mayor porcentaje de puntuación sigue siendo 7 en este caso y 5 en el de los alumnos.

Gráfico 273. *Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de intervención ante casos de uso desviado de Internet existentes en sus centros educativos*



V. RECAPITULACIÓN Y CONCLUSIONES

El ciberespacio, como bien se ha expuesto al inicio de este informe, tiene unas características concretas –es anónimo, no tiene fronteras y en él no existe la censura, entre otras– que hacen que haya un mayor riesgo de ser víctima de un delito en comparación con el espacio físico. Sin embargo, las personas también tienen cierto nivel de control a la hora de decidir si quieren ser víctimas de un ciberdelito, ya que, siguiendo la reformulación de Miró (2013) sobre la Teoría de las Actividades Rutinarias de Cohen y Felson (1979), éstas, con sus actos y hábitos, pueden disminuir la probabilidad de recibir un ataque a través del ciberespacio.

Internet ha supuesto la aparición de nuevos riesgos y nuevas formas de victimización que han provocado una gran alarma social, sobre todo cuando éstos afectan a los más jóvenes. Sin embargo, a pesar de la creciente

preocupación de la sociedad acerca de los peligros de Internet a los que se ven expuestos aquellos sectores más jóvenes de la población, la realidad muestra que existe poco conocimiento entre los adultos, sobre todo entre los que son padres y madres, sobre estos riesgos y la manera de actuar sobre ellos para evitarlos.

Especial mención merece el hecho de que apenas existen estudios sobre la cibervictimización de los jóvenes, aunque los datos oficiales parecen indicar un aumento de las cifras de este fenómeno año tras año, siendo las chicas más victimizadas en prácticamente todas las categorías delictivas relacionadas con la ciberdelincuencia.

Teniendo en cuenta todo ello, nace Saf_*e*, un proyecto que pretende, entre otros objetivos, analizar las conductas que los alumnos de enseñanza no universitaria de la comunidad autónoma de Castilla y León realizan cuando navegan por Internet y cómo ello se relaciona con la probabilidad de que sean víctimas de un ciberdelito. Posteriormente, todo ello permitirá la creación de un protocolo de actuación sobre uso seguro de las TIC, convivencia escolar y riesgos de Internet en Castilla y León.

A lo largo de este primer informe, correspondiente a la fase 1 del proyecto Saf_*e*, se han ido exponiendo los resultados obtenidos tras el análisis de las respuestas dadas en los cuestionarios cumplimentados tanto por los alumnos como por sus profesores. Estos resultados se han dividido en siete grandes bloques temáticos:

1. Ciberataques que afectan a los jóvenes de Castilla y León
2. Conductas de uso desviado de Internet y las TIC de los jóvenes de Castilla y León
3. Percepción y conocimiento de los docentes sobre los ciberataques y uso

desviado de Internet que afectan a los jóvenes de Castilla y León

4. Hábitos en el uso de las TIC de los jóvenes de Castilla y León
5. Supervisión parental del uso de las TIC
6. Mecanismos de prevención e intervención de los centros educativos ante casos de cibervictimización y uso desviado de Internet
7. Ciberataques sociales autoinformados por los alumnos

A lo largo de los siguientes puntos se exponen, de manera esquemática, las principales conclusiones extraídas tras el análisis de los datos:

1. El 68% de alumnos que cursan 5º y 6º de primaria y 1º de ESO ha sido víctima de ciberataques económicos alguna vez en su vida, mientras que en el caso de los alumnos que cursan 2º, 3º y 4º de ESO, Bachillerato y CFGM la cifra asciende a un 84%.
2. El 10% de los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM que han realizado compras por Internet alguna vez en su vida ha sido víctima de fraude en compra en el último año. Además, el tipo de fraude más frecuente se relaciona con que el producto nunca llegó.
3. El 62% de alumnos que tiene ordenador ha sido avisado por el antivirus, alguna vez en su vida, de la existencia de infección por *malware.*
4. El 48% de los alumnos afirma haber perdido información o sufrido daños derivados de un virus informático en su ordenador alguna vez en su vida.
5. El 22% de los alumnos ha sido víctima, en el último año, de *scam*.
6. El 20% de los alumnos ha sido víctima, en el último año, de *spam*.

7. El 66% de los alumnos que cursan 2º, 3º y 4º de ESO, Bachillerato y CFGM ha sido víctima, alguna vez en su vida, de ciberataques sociales.

8. El 35% de alumnos que cursan 5º y 6º de primaria y 1º de ESO ha sido víctima de ciberacoso en el último año, mientras que la cifra asciende a un 53% en el caso de los alumnos que cursan 2º, 3º y 4º de ESO, Bachillerato y CFGM.

9. El tipo de ciberacoso más frecuentemente sufrido por los alumnos de menor edad (5º y 6º de primaria y 1º de ESO) es el de la exclusión social, con una prevalencia del 13%. En el caso de los alumnos de mayor edad (2º, 3º y 4º de ESO, Bachillerato y CFGM), el tipo de ciberacoso más frecuente es el de los insultos y las ridiculizaciones, con una prevalencia del 25%.

10. Un 40% de los alumnos afirma que los responsables de los insultos fueron compañeros de clase, seguido de un 29% que afirma que fueron compañeros de otras clases.

11. El 30% de alumnos que cursan 2º, 3º y 4º de ESO, Bachillerato y CFGM ha sido víctima, en el último año, de algún tipo de ciberacoso sexual.

12. El tipo de ciberacoso sexual más frecuente entre los alumnos de Castilla y León encuestados es el de recibir mensajes obscenos o peticiones sexuales, con una prevalencia del 18%.

13. El 8% de alumnos que cursa 2º, 3º y 4º de ESO, Bachillerato y CFGM, tiene pareja y afirma ser víctima de control por parte de ésta, indica que el tipo de control de pareja más frecuente se relaciona con el control de los contactos que la víctima tiene agregados en redes sociales.

14. Menos del 1% de los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM

presenta un comportamiento abusivo de Internet.

15. Existe una tendencia generalizada de los docentes a considerar que en las aulas en las que imparten clase hay menos casos de cibervictimización y uso desviado de Internet que en otras clases del mismo centro y, menos aún, que en otros centros educativos.

16. Los tipos de ciberacoso más frecuentemente detectados por los docentes son: insultar y ridiculizar (un 29,7% de docentes), contar rumores y mentiras (un 17,8% de los docentes) y publicar fotos o vídeos personales (un 15,8% de docentes).

17. Más de un 50% de los profesores encuestados afirma que el responsable o los responsables del ciberacoso fueron uno o varios compañeros de clase.

18. Un 43% de profesores afirma que el tipo de ciberacoso sexual más frecuente detectado entre sus alumnos consiste en publicar fotografías o vídeos de carácter sexual.

19. Un alto porcentaje de docentes (un 43,2%) reconoce no saber quien fue el autor del ciberacoso sexual sufrido por alguno de sus alumnos.

20. El tipo de control de pareja a través de las TIC más detectado por los docentes es el que consiste en tratar de influir en las publicaciones de las redes sociales de a pareja (un 34,1% de docentes hace esta afirmación).

21. El tipo de ciberataque económico más detectado entre los docentes es, en un 27,7% de los casos, el de infección por *malware*.

22. Un 75% de profesores afirma que el tipo de uso desviado de Internet más común detectado entre sus alumnos es el de abuso de Internet.

23. El 96% de los alumnos encuestados dispone de un ordenador con conexión a Internet, y el 85% afirma tener un teléfono móvil desde el que pueden conectarse a Internet.

24. Un 85% de los alumnos afirma usar diariamente las redes sociales. Concretamente, las más utilizadas son la mensajería instantánea (WhatsApp, sobre todo) e Instagram.

25. Un 40% de los alumnos mantiene que el medio más utilizado para contactar con desconocidos a través de Internet son las redes sociales.

26. Un 64% de alumnos que afirma haber realizado comportamientos sexuales online sostiene que lo hizo con su pareja.

27. Un 46% de los alumnos afirma guardar fotos y vídeos personales en el ordenador, cifra que aumenta a casi un 60% cuando se trata del móvil.

28. Un 30% de los alumnos reconoce no cambiar nunca las contraseñas que utilizan para acceder a sus cuentas personales.

29. Un 70% de los alumnos manifiesta que el ordenador que utilizan no tiene ningún tipo de restricción que les impida acceder a ciertas páginas web o aplicaciones, entre otros.

30. Tanto los alumnos como los profesores consideran que el principal mecanismo de prevención utilizado en los centros educativos para luchar contra los riesgos y el uso desviado de Internet es que profesionales externos vayan al colegio/instituto a dar charlas formativas.

31. El tipo de ciberacoso más frecuentemente realizado por los alumnos consiste en acceder a las cuentas personales de otras personas sin su consentimiento (un 52% de los alumnos afirma este dato).

VI. REFERENCIAS

Beranuy, M., Chamarro, A., Graner, C. y Carbonell, X. (2009). Validación de dos escalas breves para evaluar la adicción a Internet y el abuso de móvil. *Psicothema*, *21*(3), pp. 480-485.

Cerezo, F. (2009). Bullying: análisis de la situación en las aulas españolas. *International Journal of Psychology and Psychological Therapy*, *9*(3), pp. 367-378.

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

De Gracia, M., Vigo, M., Fernández, M.J. y Marcó, M. (2002). Problemas conductuales relacionados con el uso de Internet: Un estudio exploratorio**.** *Anales de Psicología, 18*(2), pp. 273-292.

Echeburúa, E. y De Corral, P. (2010). Adicción a las nuevas tecnologías y a las redes sociales en jóvenes: un nuevo reto. *Adicciones, 22*(2), pp. 91-96.

García, N. (2017). *El ciberacoso. Análisis de la victimización de menores en el ciberespacio desde la Teoría de las actividades cotidianas.* Madrid: EDISOFER

Hernández Prados, M.Á., y Solano Fernández, I.M. (2007). Ciberbullying, un problema de acoso escolar. *RIED: Revista iberoamericana de educación a distancia*, *10*(1), pp. 17-36.

Marcum, C.D. (2008). Identifying Potential Factors of Adolescent Online Victimization for High School Seniors. *Interntional Journal of Cyber Criminology, 2*(2), pp. 1-18.

Marín Vila, M. (2017). *Rendimiento cognitivo en adolescentes con abuso de Internet*. [Tesis doctoral]. Dir. José Luís Carballo Crespo. Universidad Miguel

Hernández.

Ministerio del Interior. (2015-2016). *Estudio sobre la cibercriminalidad en España*. Madrid: Ministerio del Interior

Miró, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. 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*, *5*(11), pp. 1-35.

Olweus D (1978). *Aggression in the schools: Bullies and whipping boys*. Washington, D.C. Hemisphere.

Prensky, M. (2010). *Nativos e Inmigrantes Digitales*. Distribuidora SEK.

Rodríguez, S., Fernández, E.B. y Bautista, R. (2017). Prevención de la cibervictimización en menores de la provincia de Alicante. *Revista Española de Investigación Criminológica, 2*(15), pp. 1-25.

VII. ÍNDICE DE GRÁFICOS

Gráfico 1. Evolución global de los hechos conocidos sobre cibercriminalidad entre 2012 y 2016 17
Gráfico 2. Evolución global de los hechos esclarecidos entre 2012 y 2016..... 18
Gráfico 3. Evolución global de las detenciones e imputaciones entre 2012 y 2016..... 19
Gráfico 4. Evolución de cibervictimización registrada en España entre 2014 y 2016 20
Gráfico 5. Prevalencia de la cibervictimización por sexos en menores en el año 2016 en España 21
Gráfico 6. Prevalencia de alumnos que han realizado conductas de ciberacoso 29

Gráfico 7. Tipos de ciberacoso autoinformados por los alumnos 30
Gráfico 8. Prevalencia de alumnos que han realizado conductas de ciberacoso sexual .. 31
Gráfico 9. Tipos de ciberacoso sexual autoinformados por los alumnos 31
Gráfico 10. Prevalencia de alumnos que han realizado conductas de control de pareja a través de las TIC 32
Gráfico 11. Tipos de control de pareja autoinformados por los alumnos 33
Gráfico 12. Prevalencia de alumnos de 5º y 6º de primaria y 1º de ESO que han sido víctimas de algún ataque cibereconómico 36
Gráfico 13. Prevalencia de alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM que han sido víctimas de algún ataque cibereconómico 36
Gráfico 14. Prevalencia de jóvenes víctimas de fraude en compra en el último año 37
Gráfico 15. Prevalencia de jóvenes víctimas de fraude en compra en el último año según sexo 38
Gráfico 16. Prevalencia de jóvenes víctimas de fraude en compra en el último año según edad 38
Gráfico 17. Tipos de fraude en compra sufridos 39
Gráfico 18. Tipos de fraude en compra sufridos según el sexo de la víctima 40
Gráfico 19. Tipos de fraude en compra sufridos según la edad de la víctima 40
Gráfico 20. Prevalencia de alumnos víctimas de infección de malware según dispositivo 42
Gráfico 21. Prevalencia de alumnos víctimas de infección de malware según sexo 42
Gráfico 22. Prevalencia de alumnos víctimas de infección de malware según edad 43
Gráfico 23. Prevalencia de alumnos víctimas de pérdida de información por infección de malware según dispositivo 44
Gráfico 24. Prevalencia de alumnos víctimas de pérdida de información por infección de malware según sexo 44
Gráfico 25. Prevalencia de alumnos víctimas de pérdida de información por infección de malware según edad 45
Gráfico 26. Prevalencia de alumnos víctimas de scam en el último año 46
Gráfico 27. Prevalencia de alumnos víctimas de scam en el último año según sexo 46
Gráfico 28. Prevalencia de alumnos víctimas de scam en el último año según edad 47

Gráfico 29. Prevalencia de alumnos víctimas de spam en el último año..... 48
Gráfico 30. Prevalencia de alumnos víctimas de spam en el último año según sexo..... 48
Gráfico 31. Prevalencia de alumnos víctimas de spam en el último año según edad 49
Gráfico 32. Prevalencia de alumnos víctimas de algún tipo de ciberataque social 50
Gráfico 33. Prevalencia de alumnos víctimas de cyberbullying 53
Gráfico 34. Número de conductas de cyberbullying sufridas por los alumnos 54
Gráfico 35. Prevalencia de alumnos de 5º y 6º de Primaria y 1º de ESO víctimas de ciberacoso 55
Gráfico 36. Prevalencia de alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM víctimas de ciberacoso 55
Gráfico 37. Prevalencias de las distintas tipologías de ciberacoso 56
Gráfico 38. Prevalencia de alumnos víctimas de insultos a través de Internet 57
Gráfico 39. Prevalencia de alumnos víctimas de insultos a través de Internet según sexo 58
Gráfico 40. Prevalencia de alumnos víctimas de insultos a través de Internet según edad 58
Gráfico 41. Responsables de los insultos según las víctimas 59
Gráfico 42. Responsables de los insultos según el sexo de la víctima 60
Gráfico 43. Responsables de los insultos según la edad de la víctima 61
Gráfico 44. Prevalencia de alumnos víctimas de rumores a través de Internet 62
Gráfico 45. Prevalencia de alumnos víctimas de rumores a través de Internet según sexo 62
Gráfico 46. Prevalencia de alumnos víctimas de rumores a través de Internet según edad 63
Gráfico 47. Responsables de los rumores según las víctimas 64
Gráfico 48. Responsables de los rumores según el sexo de la víctima 65
Gráfico 49. Responsables de los rumores según la edad de la víctima 66
Gráfico 50. Prevalencia de alumnos víctimas de publicación de fotos o vídeos suyos sin consentimiento a través de Internet 67
Gráfico 51. Prevalencia de alumnos víctimas de publicación de fotos o vídeos suyos sin consentimiento a través de Internet según sexo..... 67

Gráfico 52. Prevalencia de alumnos víctimas de publicación de fotos o vídeos suyos sin consentimiento a través de Internet según edad 68
Gráfico 53. Responsables de la publicación de fotos o vídeos sin consentimiento según las víctimas 69
Gráfico 54. Responsables de la publicación de fotos o vídeos sin consentimiento según el sexo de la víctima 70
Gráfico 55. Responsables de la publicación de fotos o vídeos sin consentimiento según la edad de la víctima 71
Gráfico 56. Prevalencia de alumnos víctimas difusión de información íntima a través de Internet 72
Gráfico 57. Prevalencia de alumnos víctimas difusión de información íntima a través de Internet según sexo 72
Gráfico 58. Prevalencia de alumnos víctimas difusión de información íntima a través de Internet según edad 73
Gráfico 59. Responsables de la difusión de información íntima según las víctimas 74
Gráfico 60. Responsables de la difusión de información íntima según el sexo de la víctima 75
Gráfico 61. Responsables de la difusión de información íntima según la edad de la víctima 76
Gráfico 62. Prevalencia de alumnos víctimas de acceder a sus cuentas personales sin autorización a través de Internet 77
Gráfico 63. Prevalencia de alumnos víctimas de acceder a sus cuentas personales sin autorización a través de Internet según sexo 77
Gráfico 64. Prevalencia de alumnos víctimas de acceder a sus cuentas personales sin autorización a través de Internet según edad 78
Gráfico 65. Responsables del acceso a las cuentas personales sin autorización según las víctimas 79
Gráfico 66. Responsables del acceso a las cuentas personales sin autorización según el sexo de la víctima 80
Gráfico 67. Responsables del acceso a las cuentas personales sin autorización según la edad de la víctima 81

Gráfico 68. Prevalencia de alumnos víctimas de exclusión social a través de Internet.... 82
Gráfico 69. Prevalencia de alumnos víctimas de exclusión social a través de Internet según sexo..... 82
Gráfico 70. Prevalencia de alumnos víctimas de exclusión social a través de Internet según edad..... 83
Gráfico 71. Responsables de la exclusión social según las víctimas 84
Gráfico 72. Responsables de la exclusión social según el sexo de la víctima 85
Gráfico 73. Responsables de la exclusión social según la edad de la víctima..... 86
Gráfico 74. Prevalencia de alumnos víctimas de amenazas a través de Internet..... 87
Gráfico 75. Prevalencia de alumnos víctimas de amenazas a través de Internet según sexo 87
Gráfico 76. Prevalencia de alumnos víctimas de amenazas a través de Internet según edad 88
Gráfico 77. Responsables de las amenazas según las víctimas..... 89
Gráfico 78. Responsables de las amenazas según el sexo de la víctima..... 90
Gráfico 79. Responsables de las amenazas según la edad de la víctima 91
Gráfico 80. Prevalencia de alumnos víctimas de coacciones a través de Internet 92
Gráfico 81. Prevalencia de alumnos víctimas de coacciones a través de Internet según sexo 92
Gráfico 82. Prevalencia de alumnos víctimas de coacciones a través de Internet según edad 93
Gráfico 83. Responsables de las coacciones según las víctimas 94
Gráfico 84. Responsables de las coacciones según el sexo de la víctima 95
Gráfico 85. Responsables de las coacciones según la edad de la víctima..... 96
Gráfico 86. Prevalencia de alumnos víctimas de suplantación de identidad a través de Internet 97
Gráfico 87. Prevalencia de alumnos víctimas de suplantación de identidad a través de Internet según sexo..... 97
Gráfico 88. Prevalencia de alumnos víctimas de suplantación de identidad a través de Internet según edad..... 98
Gráfico 89. Responsables de la suplantación de identidad según las víctimas 99

Gráfico 90. Responsables de la suplantación de identidad según el sexo de la víctima 100
Gráfico 91. Responsables de la suplantación de identidad según la edad de la víctima 101
Gráfico 92. Prevalencia de alumnos víctimas de contacto repetido no deseado a través de Internet 102
Gráfico 93. Prevalencia de alumnos víctimas de contacto repetido no deseado a través de Internet según sexo..... 102
Gráfico 94. Prevalencia de alumnos víctimas de contacto repetido no deseado a través de Internet según edad..... 103
Gráfico 95. Responsables del contacto repetido no deseado según las víctimas 104
Gráfico 96. Responsables del contacto repetido no deseado según el sexo de la víctima 105
Gráfico 97. Responsables del contacto repetido no deseado según la edad de la víctima 106
Gráfico 98. Prevalencia de alumnos que han sido víctimas de ciberacoso sexual 107
Gráfico 99. Prevalencia de los distintos tipos de ciberacoso sexual..... 108
Gráfico 100. Prevalencia de alumnos víctimas de haber recibido imágenes sexuales en el último año..... 109
Gráfico 101. Prevalencia de alumnos víctimas de haber recibido comentarios obscenos en el último año 109
Gráfico 102. Prevalencia de alumnos víctimas de haber recibido imágenes sexuales en el último año según sexo 110
Gráfico 103. Prevalencia de alumnos víctimas de haber recibido comentarios obscenos en el último año según sexo 111
Gráfico 104. Prevalencia de alumnos víctimas de haber recibido imágenes sexuales en el último año según edad..... 112
Gráfico 105. Prevalencia de alumnos víctimas de haber recibido comentarios obscenos en el último año según edad..... 112
Gráfico 106. Responsables de enviar imágenes sexuales y mensajes obscenos 113
Gráfico 107. Responsables de enviar imágenes sexuales según el sexo de la víctima ... 114
Gráfico 108. Responsables de enviar mensajes obscenos según el sexo de la víctima .. 115
Gráfico 109. Responsables de enviar imágenes sexuales según la edad de la víctima .. 116

Gráfico 110. Responsables de enviar mensajes obscenos según la edad de la víctima . 117
Gráfico 111. Edad de los responsables de enviar imágenes sexuales y mensajes obscenos 118
Gráfico 112. Prevalencia de alumnos víctimas de haber sido obligados a enviar fotos/vídeos sexuales propios 119
Gráfico 113. Prevalencia de alumnos víctimas de haber sido obligados a realizar comportamientos sexuales 119
Gráfico 114. Prevalencia de alumnos víctimas de haber sido obligados a enviar fotos o vídeos sexuales propios según sexo 120
Gráfico 115. Prevalencia de alumnos víctimas de haber sido obligados a realizar comportamientos sexuales según sexo 120
Gráfico 116. Prevalencia de alumnos víctimas de haber sido obligados a enviar fotos o vídeos sexuales propios según edad 121
Gráfico 117. Prevalencia de alumnos víctimas de haber sido obligados a realizar comportamientos sexuales según edad 121
Gráfico 118. Responsables de los dos tipos de coacciones sexuales 123
Gráfico 119. Responsables de obligar a enviar fotos o vídeos sexuales propios según el sexo de la víctima 124
Gráfico 120. Responsables de obligar a realizar comportamientos sexuales según el sexo de la víctima 124
Gráfico 121. Responsables de obligar a enviar fotos o vídeos sexuales propios según la edad de la víctima 125
Gráfico 122. Responsables de obligar a realizar comportamientos sexuales según la edad de la víctima 126
Gráfico 123. Edad de la persona responsable de ambos tipos de coacciones sexuales. 127
Gráfico 124. Prevalencia de alumnos víctimas de sextorsión 128
Gráfico 125. Prevalencia de alumnos víctimas de sextorsión según sexo 128
Gráfico 126. Prevalencia de alumnos víctimas de sextorsión según edad 129
Gráfico 127. Persona responsable de la sextorsión 130
Gráfico 128. Persona responsable de la sextorsión según el sexo de la víctima 131
Gráfico 129. Persona responsable de la sextorsión según la edad de la víctima 132

Gráfico 130. Edad de la persona responsable de la sextorsión 132
Gráfico 131. Tipo de material exigido en la sextorsión..... 133
Gráfico 132. Tipo de material exigido en la sextorsión según el sexo de la víctima..... 134
Gráfico 133. Tipo de material exigido en la sextorsión según la edad de la víctima 135
Gráfico 134. Mecanismo por el cual el responsable de la sextorsión obtuvo el material 135
Gráfico 135. Mecanismo por el cual el responsable de la sextorsión obtuvo el material según el sexo de la víctima..... 136
Gráfico 136. Mecanismo por el cual el responsable de la sextorsión obtuvo el material según la edad de la víctima 137
Gráfico 137. Prevalencia de alumnos víctimas de publicación o difusión de imágenes o vídeos sexuales sin consentimiento..... 138
Gráfico 138. Prevalencia de alumnos víctimas de publicación o difusión de imágenes o vídeos sexuales sin consentimiento según sexo 138
Gráfico 139. Prevalencia de alumnos víctimas de publicación o difusión de imágenes o vídeos sexuales sin consentimiento según edad 139
Gráfico 140. Persona responsable de la publicación o difusión de imágenes o vídeos sexuales sin consentimiento 140
Gráfico 141. Persona responsable de la publicación o difusión de imágenes o vídeos sexuales sin consentimiento según el sexo de la víctima 141
Gráfico 142. Persona responsable de la publicación o difusión de imágenes o vídeos sexuales sin consentimiento según la edad de la víctima..... 142
Gráfico 143. Edad de la persona responsable de publicar o difundir imágenes o vídeos sexuales sin consentimiento 143
Gráfico 144. Prevalencia de alumnos víctimas de haber sido presionados para quedar en persona por un desconocido..... 144
Gráfico 145. Prevalencia de alumnos víctimas de haber sido presionados para quedar en persona por un desconocido según sexo..... 144
Gráfico 146. Prevalencia de alumnos víctimas de haber sido presionados para quedar en persona por un desconocido según edad 145
Gráfico 147. Edad de la persona responsable de presionar para quedar en persona.... 146

Gráfico 148. Proporción de alumnos que han tenido o tienen pareja 147
Gráfico 149. Prevalencia de alumnos víctimas de los distintos tipos de control de pareja a través de las TIC 148
Gráfico 150. Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen controlar la información publicada en redes sociales en relaciones actuales y relaciones pasadas..... 149
Gráfico 151. Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen controlar la información publicada en redes sociales en relaciones actuales y relaciones pasadas según sexo..... 150
Gráfico 152. Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen controlar la información publicada en redes sociales en relaciones actuales y relaciones pasadas según edad 151
Gráfico 153. Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen controlar las amistades en redes sociales en relaciones actuales y relaciones pasadas 152
Gráfico 154. Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen controlar las amistades en redes sociales en relaciones actuales y relaciones pasadas según sexo..... 153
Gráfico 155. Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen controlar las amistades en redes sociales en relaciones actuales y relaciones pasadas según edad 154
Gráfico 156. Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen influir en la información publicada en redes sociales..... 155
Gráfico 157. Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen influir en la información publicada en redes sociales según sexo 156
Gráfico 158. Prevalencia de alumnos víctimas de que sus parejas/exparejas intentasen influir en la información publicada en redes sociales según edad 157
Gráfico 159. Prevalencia de alumnos que abusa de Internet..... 159
Gráfico 160. Prevalencia de alumnos que abusan de Internet según sexo 159
Gráfico 161. Prevalencia de alumnos que abusan de Internet según edad 160
Gráfico 162. Proporción de alumnos que ha realizado apuestas online en el último año 161

Gráfico 163. Número de horas dedicadas a la semana a realizar apuestas online 161
Gráfico 164. Proporción de alumnos que han realizado sexting 162
Gráfico 165. Destinatarios del material pornográfico 163
Gráfico 166. Edad de los receptores de material pornográfico 163
Gráfico 167. Proporción de alumnos que han realizado sexting pasivo 164
Gráfico 168. Emisores del material pornográfico 165
Gráfico 169. Edad de los emisores de material pornográfico 165
Gráfico 170. Percepción de peligro de los alumnos sobre realizar conductas de sexting 166
Gráfico 171. Comparativa entre las distintas prevalencias percibidas por los docentes sobre casos de victimización por ciberacoso 169
Gráfico 172. Comparativa entre las distintas prevalencias percibidas por los docentes sobre casos de cibervictimización sexual 170
Gráfico 173. Comparativa entre las distintas prevalencias percibidas por los docentes sobre control de pareja 172
Gráfico 174. Comparativa entre las distintas prevalencias percibidas por los docentes sobre cibervictimización económica 173
Gráfico 175. Comparativa entre las distintas prevalencias percibidas por los docentes sobre uso desviado de Internet 175
Gráfico 176. Conocimiento directo del profesorado sobre casos de ciberacoso 176
Gráfico 177. Tipo de ciberacoso del que han tenido conocimiento directo los docentes 177
Gráfico 178. Autores de las conductas de ciberacoso de las que han tenido conocimiento directo los docentes 178
Gráfico 179. Afectación percibida por los docentes del ciberacoso sufrido por el alumno 178
Gráfico 180. Conocimiento directo del profesorado sobre casos de ciberacoso sexual 179
Gráfico 181. Tipo de ciberacoso del que han tenido conocimiento directo los docentes 180
Gráfico 182. Autores de las conductas de ciberacoso sexual de las que han tenido conocimiento directo los docentes 181

Gráfico 183. Afectación percibida por los docentes del ciberacoso sexual sufrido por el alumno 182
Gráfico 184. Conocimiento directo del profesorado sobre casos de control de pareja a través de las TIC e Internet 183
Gráfico 185. Tipos de control de pareja a través de las TIC de los que han tenido conocimiento directo los docentes 184
Gráfico 186. Afectación percibida por los docentes del control de pareja a través de las TIC sufrido por el alumno 185
Gráfico 187. Conocimiento directo del profesorado sobre casos de cibervictimización económica 186
Gráfico 188. Conocimiento directo del profesorado sobre casos cibervictimización económica 186
Gráfico 189. Afectación percibida de los docentes de los ciberataques económicos sufridos por el alumno 187
Gráfico 190. Conocimiento directo del profesorado sobre casos de uso desviado de Internet 188
Gráfico 191. Tipos de uso desviado de Internet del que han tenido conocimiento directo los docentes 188
Gráfico 192. Afectación percibida de los docentes uso desviado de Internet del alumno 189
Gráfico 193. Menores que disponen de un ordenador con conexión a Internet (visión global) 191
Gráfico 194. Personas con quienes los alumnos comparten el ordenador 192
Gráfico 195. Horas al día que pasan los alumnos utilizando el ordenador 192
Gráfico 196. Proporción de menores que dispone de un teléfono móvil con conexión a Internet 193
Gráfico 197. Usos que dan los alumnos al móvil o tablet 194
Gráfico 198. Horas al día que pasan los alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM utilizando el móvil o la tablet 195
Gráfico 199. Proporción de alumnos que usa redes sociales 196

Gráfico 200. Proporción de alumnos de 5º y 6º de primaria y 1º de ESO que usan redes sociales a diario 196
Gráfico 201. Proporción de alumnos de 2º, 3º y 4º de ESO, Bachillerato y CFGM que usan redes sociales a diario 197
Gráfico 202. Redes sociales utilizadas por los alumnos 197
Gráfico 203. Frecuencia de publicación en redes sociales 198
Gráfico 204. Tipo de datos personales publicados en redes sociales 199
Gráfico 205. Personas que los alumnos agregan a sus redes sociales 199
Gráfico 206. Proporción de alumnos que limitan el acceso a sus redes sociales 200
Gráfico 207. Proporción de alumnos que utilizan el correo electrónico 201
Gráfico 208. Proporción de alumnos que tienen blog, vídeo blogs o cuentas de YouTube 202
Gráfico 209. Horas dedicadas a la semana al blog, vídeo blog o cuenta de YouTube 202
Gráfico 210. Motivos por los que los alumnos escriben en foros y blogs públicos 203
Gráfico 211. Proporción de alumnos que realizan videollamadas 204
Gráfico 212. Motivos por los que los alumnos deciden realizar videollamadas 204
Gráfico 213. Proporción de alumnos que tienen cuentas en webs de contactos 205
Gráfico 214. Número de cuentas en webs de contacto 205
Gráfico 215. Proporción de alumnos que han realizado compras por Internet 206
Gráfico 216. Productos comprados a través de Internet 207
Gráfico 217. Proporción de alumnos que facilitan datos personales en Internet 207
Gráfico 218. Datos personales facilitados por los alumnos 208
Gráfico 219. Proporción de alumnos que ha contactado con desconocidos en el último año 209
Gráfico 220. Finalidad con la que los alumnos han contactado con desconocidos 209
Gráfico 221. Medios de contacto con desconocidos 210
Gráfico 222. Proporción de alumnos que ha descargado archivos de Internet en el último año 211
Gráfico 223. Medios utilizados para descargar archivos de Internet 211
Gráfico 224. Archivos descargados a través de Internet 212

Gráfico 225. Proporción de alumnos que han realizado comportamientos sexuales online 213
Gráfico 226. Personas con quien los alumnos han realizado comportamientos sexuales 213
Gráfico 227. Edad de las personas con las que los alumnos realizan comportamientos sexuales 214
Gráfico 228. Percepción de los alumnos sobre el peligro de realizar comportamientos sexuales a través de Internet 215
Gráfico 229. Horas que los alumnos dedican a jugar a videojuegos a la semana 216
Gráfico 230. Información guardada en el ordenador y en el móvil/tablet 217
Gráfico 231. Uso del antivirus en los distintos dispositivos utilizados por los alumnos. 218
Gráfico 232. Prevalencia de alumnos que utilizan la misma contraseña para todo 218
Gráfico 233. Frecuencia del cambio de contraseñas por parte de los alumnos en el último año 219
Gráfico 234. Control parental ejercido sobre los alumnos en el uso de las TIC 220
Gráfico 235. Control familiar ejercido sobre los alumnos en el uso de las TIC 221
Gráfico 236. Restricciones que tienen los ordenadores que utilizan los alumnos 222
Gráfico 237. Mecanismos de prevención de los riesgos de Internet existentes en los centros educativos según los alumnos 224
Gráfico 238. Percepción de los alumnos sobre la eficacia de los mecanismos de prevención de los riesgos de Internet 225
Gráfico 239. Mecanismos de prevención de los riesgos de Internet existentes en los centros educativos según los docentes 226
Gráfico 240. Percepción de los docentes sobre la eficacia de los mecanismos de prevención de los riesgos de Internet 227
Gráfico 241. Comparación de los mecanismos de prevención de los riesgos de Internet informados por los docentes y por los alumnos 228
Gráfico 242. Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de prevención de los riesgos de Internet existentes en sus centros educativos 229

Gráfico 243. Mecanismos de prevención del uso desviado de Internet existentes en los centros educativos según los alumnos 230
Gráfico 244. Percepción de los alumnos sobre la eficacia de los mecanismos de prevención del uso desviado de Internet 230
Gráfico 245. Mecanismos de prevención del uso desviado de Internet existentes en los centros educativos según los docentes 231
Gráfico 246. Percepción de los docentes sobre la eficacia de los mecanismos de prevención del uso desviado de Internet 232
Gráfico 247. Comparación de los mecanismos de prevención del uso desviado de Internet informados por los docentes y por los alumnos 233
Gráfico 248. Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de prevención del uso desviado de Internet existentes en sus centros educativos 234
Gráfico 249. Mecanismos de intervención ante casos de ciberacoso existentes en los centros educativos según los alumnos 235
Gráfico 250. Percepción de los alumnos sobre la eficacia de los mecanismos de intervención ante casos de ciberacoso 236
Gráfico 251. Mecanismos de intervención ante casos de ciberacoso existentes en los centros educativos según los docentes 237
Gráfico 252. Percepción de los docentes sobre la eficacia de los mecanismos de intervención ante casos de ciberacoso 238
Gráfico 253. Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de intervención ante casos de ciberacoso existentes en sus centros educativos 239
Gráfico 254. Mecanismos de intervención ante casos de ciberacoso sexual existentes en los centros educativos según los alumnos 240
Gráfico 255. Percepción de los alumnos sobre la eficacia de los mecanismos de intervención ante casos de ciberacoso sexual 241
Gráfico 256. Mecanismos de intervención ante casos de ciberacoso sexual existentes en los centros educativos según los docentes 242

Gráfico 257. Percepción de los docentes sobre la eficacia de los mecanismos de intervención ante casos de ciberacoso sexual 242
Gráfico 258. Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de intervención ante casos de ciberacoso sexual existentes en sus centros educativos 244
Gráfico 259. Mecanismos de intervención ante casos de control de pareja a través de las TIC existentes en los centros educativos según los alumnos 245
Gráfico 260. Percepción de los alumnos sobre la eficacia de los mecanismos de intervención ante casos de control de pareja a través de las TIC..... 246
Gráfico 261. Mecanismos de intervención ante casos de control de pareja a través de las TIC e Internet existentes en los centros educativos según los docentes..... 247
Gráfico 262. Percepción de los docentes sobre los mecanismos de intervención ante casos de control de pareja a través de las TIC e Internet 248
Gráfico 263. Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de intervención ante casos de control de pareja a través de las TIC existentes en sus centros educativos..... 249
Gráfico 264. Mecanismos de intervención ante casos de ciberataques económicos existentes en los centros educativos según los alumnos 250
Gráfico 265. Percepción de los alumnos sobre la eficacia de los mecanismos de intervención ante caos de ciberataques económicos..... 251
Gráfico 266. Mecanismos de intervención ante casos de ciberataques económicos existentes en los centros educativos según los docentes..... 252
Gráfico 267. Percepción de los docentes sobre la eficacia de los mecanismos de intervención ante casos de ciberataques económicos 253
Gráfico 268. Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de intervención ante casos de ciberataques económicos existentes en sus centros educativos 254
Gráfico 269. Mecanismos de intervención ante casos de uso desviado de Internet existentes en los centros educativos según los alumnos 255
Gráfico 270. Percepción de los alumnos sobre la eficacia de los mecanismos de intervención ante casos de uso desviado de Internet 256

Gráfico 271. Mecanismos de intervención ante casos de uso desviado de Internet existentes en los centros educativos según los docentes..... 257
Gráfico 272. Percepción de los docentes sobre la eficacia de los mecanismos de intervención ante casos de uso desviado de Internet 258
Gráfico 273. Comparación de la eficacia percibida de los alumnos y los docentes sobre los mecanismos de intervención ante casos de uso desviado de Internet existentes en sus centros educativos..... 259

VIII. ÍNDICE DE TABLAS

Tabla 1. Evolución de las victimizaciones registradas en España entre 2014 y 2016 según edad 20
Tabla 2. Prevalencia de la cibervictimización por tipología penal en menores en el año 2016 en España 21
Tabla 3. Prevalencia de la cibervictimización por tipología penal y sexo en menores en el año 2016 en España 22
Tabla 4. Percepción de los docentes sobre casos de ciberacoso en sus aulas, en otras aulas y en otros centros educativos (n) y (%) 168
Tabla 5. Percepción de los docentes sobre casos de cibervictimización sexual en sus aulas, en otras aulas y en otros centros educativos (n) y (%)..... 170
Tabla 6. Percepción de los docentes sobre casos de control de pareja en sus aulas, en otras aulas y en otros centros educativos (n) y (%) 171
Tabla 7. Percepción de los docentes sobre casos de cibervictimización económica en sus aulas, en otras aulas y en otros centros educativos (n) y (%)..... 173
Tabla 8. Percepción de los docentes sobre casos de uso desviado de Internet en sus aulas, en otras aulas y en otros centros educativos (n) y (%)..... 174

Centro para el estudio y prevención de la delincuencia

Universidad Miguel Hernández de Elche
Avda. de la Universidad s/n. Edificio Hélike
Elche (Alicante) 03201, España
Teléfono: +34 966 658 380
email: secretaria@crimina.es

www.crimina.es