UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

TESIS DOCTORAL

Estudio sobre cibercriminalidad social y económica en el ámbito de los menores, autónomos y micropymes de la ciudad de Vinaròs (Castellón)

D. Adrián Giménez Pérez

2023

UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

TESIS DOCTORAL

Estudio sobre cibercriminalidad social y económica en el ámbito de los menores, autónomos y micropymes de la ciudad de Vinaròs (Castellón)

Autor: D. Adrián Giménez Pérez

Director/es: D. Samuel Rodríguez Ferrández

UNIVERSIDAD DE MURCIA

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD
DE LA TESIS PRESENTADA PARA OBTENER EL TÍTULO DE DOCTOR

Aprobado por la Comisión General de Doctorado el 19-10-2022

D./Dña. Adrián Giménez Pérez

doctorando del Programa de Doctorado en

Criminología

de la Escuela Internacional de Doctorado de la Universidad Murcia, como autor/a de la tesis presentada para la obtención del título de Doctor y titulada:

Estudio sobre cibercriminalidad social y económica en el ámbito de los menores, autónomos y micropymes de la ciudad de Vinaròs (Castellón)

y dirigida por,

D./Dña. Samuel Rodríguez Ferrández

D./Dña.

D./Dña.

DECLARO QUE:

La tesis es una obra original que no infringe los derechos de propiedad intelectual ni los derechos de propiedad industrial u otros, de acuerdo con el ordenamiento jurídico vigente, en particular, la Ley de Propiedad Intelectual (R.D. legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, modificado por la Ley 2/2019, de 1 de marzo, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia), en particular, las disposiciones referidas al derecho de cita, cuando se han utilizado sus resultados o publicaciones.

Si la tesis hubiera sido autorizada como tesis por compendio de publicaciones o incluyese 1 o 2 publicaciones (como prevé el artículo 29.8 del reglamento), declarar que cuenta con:

- *La aceptación por escrito de los coautores de las publicaciones de que el doctorando las presente como parte de la tesis.*
- *En su caso, la renuncia por escrito de los coautores no doctores de dichos trabajos a presentarlos como parte de otras tesis doctorales en la Universidad de Murcia o en cualquier otra universidad.*

Del mismo modo, asumo ante la Universidad cualquier responsabilidad que pudiera derivarse de la autoría o falta de originalidad del contenido de la tesis presentada, en caso de plagio, de conformidad con el ordenamiento jurídico vigente.

En Murcia, a 26 de abril de 2023

Fdo.: Adrián Giménez Pérez

GIMENEZ PEREZ, ADRIAN (FIRMA)

Firmado digitalmente por GIMENEZ PEREZ, ADRIAN (FIRMA)
Fecha: 2023.04.26 15:52:30 +02'00'

Esta DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD debe ser insertada en la primera página de la tesis presentada para la obtención del título de Doctor.

Información básica sobre protección de sus datos personales aportados	
Responsable:	Universidad de Murcia. Avenida teniente Flomesta, 5. Edificio de la Convalecencia. 30003; Murcia. Delegado de Protección de Datos: dpd@um.es
Legitimación:	La Universidad de Murcia se encuentra legitimada para el tratamiento de sus datos por ser necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. art. 6.1.c) del Reglamento General de Protección de Datos
Finalidad:	Gestionar su declaración de autoría y originalidad
Destinatarios:	No se prevén comunicaciones de datos
Derechos:	Los interesados pueden ejercer sus derechos de acceso, rectificación, cancelación, oposición, limitación del tratamiento, olvido y portabilidad a través del procedimiento establecido a tal efecto en el Registro Electrónico o mediante la presentación de la correspondiente solicitud en las Oficinas de Asistencia en Materia de Registro de la Universidad de Murcia

AGRADECIMIENTOS

A la Universidad de Murcia por darme la oportunidad de poder realizar la tesis presente, y especialmente, a mi director/tutor Samuel Rodríguez Ferrández por su apoyo durante mi trayectoria.

Al Ayuntamiento de Vinaròs (Castellón), concretamente, a las Concejalías de Comercio y Servicios Sociales, por facilitarme la labor para poder realizar las encuestas de victimización correspondientes.

A los centros educativos que han participado en el estudio de investigación: Colegio Nuestra Señora de la Consolación, Colegio Nuestra Señora Divina Providencia, IES José Vilaplana e IES Leopoldo Querol, respectivamente.

ÍNDICE

PARTE I: MARCO TEÓRICO DEL ESTUDIO

INTRODUCCION

Internet ha abierto una puerta a una infinidad de posibilidades para poder delinquir en el ciberespacio a través de las tecnologías de la información y comunicación (TIC, en adelante) tales como ordenadores, telefonía móvil, etc., generándose una nueva tipología delictiva, concretamente, los delitos informáticos.

Podríamos afirmar que la oportunidad constituye el primer eslabón de la comisión del delito. En este sentido, el Diccionario de la Real Academia Española (en adelante, RAE), la define como: "Momento o circunstancia oportunos o convenientes para algo" (RAE, 2020).[1]

No obstante, en lo atinente al concepto de delito, en virtud de lo establecido en el artículo 10 del vigente Código Penal (CP, en adelante), "son delitos las acciones y omisiones dolosas o imprudentes penadas por la ley" (CP, 2015, p.27086).

Para Felson y Clarke (1998), muchos delincuentes en el supuesto de hallarse con serias dificultades para ejecutar la comisión de delitos renunciarán, motivo por el cual, la conducta de la víctima es de vital importancia en el ámbito de la cibercriminalidad, quien deberá convertirse en su propio autoguardián y, a la vez, evitar la realización de conductas que faciliten la ejecución del delito.

El objetivo de la presente tesis es realizar un estudio que se compondrá de dos partes. La primera se centra en la cibercriminalidad social en el ámbito de los menores adolescentes de Vinaròs, para lo cual emplearemos una encuesta anónima de victimización en la que se le pregunte al menor sobre hábitos de uso de las TIC y otros hábitos de actividades cotidianas, así como hechos o conductas realizados en el ámbito del ciberespacio, de manera que mediante la relación de las respuestas marcadas con una "X", poder identificar factores de riesgo y de protección, en su caso. La muestra objeto de estudio se obtendrá del alumnado de los cuatro Institutos de Secundaria de la población objeto de estudio (dos públicos y dos concertados).

Asimismo, se realizarán unas charlas informativas sobre peligros en la red tales como *cyberbullying*, *online grooming*, *sexting*, *sextorsion* y violencia de género digital en la adolescencia en dichos centros educativos, apoyadas con una presentación de

[1]Real Academia Española, s.f., definición 1.

PowerPoint en las que se ha aplicado como técnica de investigación el grupo de discusión, tras la formulación de determinadas preguntas al colectivo del alumnado del aula donde se impartido la charla y resuelto dudas al respecto, en su caso.

La segunda parte del estudio, se focaliza en la cibercriminalidad económica (*spam*, *scam*, *phishing*, etc.) en el ámbito de los autónomos y micropymes de Vinaròs, concretamente, bares y restaurantes y pequeño comercio tradicional, para lo cual se empleará una encuesta anónima de victimización en la que se le pregunte al regente o empleado/a del establecimiento o comercio, en su caso, sobre hábitos de uso de las TIC y otros hábitos de actividades cotidianas, conocimientos de ciberseguridad, así como hechos o conductas realizados en el ámbito del ciberespacio, de manera que mediante la relación de las respuestas marcadas con una "X", poder identificar factores de riesgo y de protección, en su caso.

En este sentido, para el objeto del presente estudio se ha tomado una muestra de comercios y establecimientos públicos tradicionales y/o micropymes, en su caso.

CAPITULO I: PREVENCION DEL CIBERCRIMEN.

I.1 Conceptos básicos clave del estudio.

En primer lugar, antes de adentrarnos en este estudio, hemos de conocer una serie de conceptos elementales en la materia como, por ejemplo, el lugar donde los ciberdelincuentes ejecutan sus actos delictivos a través de un gran abanico de modalidades de modus operandi. Concretamente, me refiero al ciberespacio, que especialistas en la materia como Miró (2012) lo definen como "término que indica el lugar de comunicación social transnacional, universal, popularizado y en permanente evolución derivado del uso de las TIC". (p. 301).

Para Cano Paños (2008) el ciberespacio "se ha convertido en muchos sentidos en un nuevo escenario de conflicto" (p.88), de manera que, en concreto, "la red global ofrece fácil acceso, poco o ningún control gubernamental, un anonimato de las comunicaciones, un flujo rápido de información, un público potencialmente enorme y una difusión a nivel planetario" (p.88).

Miró (2012), también define otros conceptos muy importantes en este campo como son el cibercrimen como "cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que de ello se derivan" (p. 301).

No obstante, en nuestro ordenamiento jurídico vigente también aparece la definición de ciberespacio, y para ser más exactos, en la Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas, como: "Dominio global y dinámico compuesto por infraestructuras de tecnología de la información —incluyendo internet—, redes de telecomunicaciones y sistemas de información. y ciberseguridad". (p.4154)

Dicha Orden Ministerial también contempla otros conceptos que caben destacar como:

-ciberataque: "Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan". (p. 4154)

-ciberseguridad: "Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los

servicios que prestan y la información que manejan (p. 4155).

A parte de la definición técnica de ciberseguridad que aparece en la Orden Ministerial mencionada, ¿Qué podemos entender por ciberseguridad?

Para Ale Cortes (2021) la ciberseguridad es "tener en cuenta todo lo que puede fallar en el ámbito de la tecnología y actuar en consecuencia para evitar que ocurra".

Comparativamente otros profesionales expertos en la materia como Nicolás Rodríguez (2021) la define como "práctica enfocada a identificar el peligro real de exposición a las nuevas amenazas que nos rodean (…)".

Para Pablo F. Iglesias (2021), *hacker* fundador de la consultora de presencia digital y reputación online "*cyberbrainers*" entiende que la ciberseguridad es "aquello que las organizaciones y los particulares echan en falta solo cuando el mal ya está hecho, y el cibercriminal ha salido victorioso".

Actualmente, el borrador de la futura Directiva europea NIS2, según Faes (2021) contempla que "la ciberseguridad se reconozca expresamente como una responsabilidad empresarial al más alto nivel gerencial".

Así las cosas, es recomendable para cualquier autónomo o empresa, en su caso, que se tomen en serio la ciberseguridad puesto que, aunque no lo parezca, está en juego la continuidad de numerosos negocios.

No obstante, la ciberseguridad también es una asignatura pendiente para la ciudadanía en general como usuarios que interactúan en internet, redes sociales, etc., incluyendo a los menores de edad que, aunque muchos de ellos sean nativos digitales deben aprender a protegerse de las ciberamenazas y evitar ciberriesgos, en su caso.

I.2 Prevención situacional del cibercrimen: Análisis teórico.

En el ámbito del ciberespacio la víctima es la pieza clave en la prevención del delito, tal y como opina Miró (2012) influyen tres factores. El primero es la capacidad que tiene la víctima de evitar los riesgos, de manera que si no interactúa en Internet no correría ningún riesgo de victimización, al igual que si no conducimos nunca un vehículo no podemos tener un accidente de tráfico evitando así el riesgo de ser una víctima potencial vial.

El segundo factor lo constituyen las actividades cotidianas *online* de la víctima que determinarán la probabilidad de ser víctima de agresores motivados, y el tercer factor es la potestad que posee la víctima de autoprotegerse mediante un guardián o guardianes

eficaces, es decir, en síntesis, la víctima es el mejor cortafuegos o antivirus *offline* que pueda existir.

Para Felson y Clarke (1998) "las oportunidades delictivas son condiciones necesarias para que el delito suceda" (p.194).

En este sentido, si tuviésemos que poner un ejemplo extrapolable al presente estudio, podríamos poner los hurtos en los comercios y establecimientos públicos de Vinaròs. Si entre los establecimientos de pequeño comercio de la zona centro hubiese una tienda de ropa, por ejemplo, que no tuviese sistema de videovigilancia, etiquetaje de seguridad en las prendas, y para las dimensiones de las tienda y aforo máximo, hubiese poco personal para atender al público, etc., constituiría un incentivo para los delincuentes a la hora de delinquir.

Felson y Clarke (1998) abordan tres teorías o enfoques de la oportunidad delictiva siendo éstas y con sus características correspondientes, las que a continuación expongo:

a) Enfoque de la actividad rutinaria o teoría de las actividades cotidianas: Su génesis radica en los delitos predatorios para lo que debe existir una convergencia en el espacio tiempo de tres elementos básicos: "un posible delincuente, un objetivo apropiado y la ausencia de un vigilante adecuado al delito" (p.197).

No obstante, este triángulo básico del delito si lo extrapolásemos al ciberespacio, podemos comprobar el papel tan importante que juega la víctima en los delitos *online.*

b) Teoría del patrón delictivo: posee tres conceptos fundamentales que son: nodos, rutas y límites. "Nodos, un término proveniente del transporte, se refiere a desde dónde y hacia dónde se trasladan las personas. No sólo se generan delitos en estos lugares, sino también cerca de ellos" (p.200).

Respeto a las rutas, podemos decir que son los itinerarios que realizan las personas habitualmente, en el ejercicio de sus actividades cotidianas.

Por último, el concepto de límites "se refiere a los confines de las áreas donde la gente habita, trabaja, compra o busca entretenimiento" (p.200).

No obstante, para Brantingham y Brantingham (1994), según esta teoría el delincuente utiliza un esquema o guion derivado de la experiencia previa en situaciones análogas para ejecutar o cometer un delito. Garrido, Stangeland y Redondo (2001) añaden

a este esquema el concepto de obstáculo (medida de protección física o de índole social) que es el que, finalmente, determinará el curso de la acción delictiva. De hecho, no podríamos descartar la posibilidad de que tras una serie de experiencias infructuosas en la ejecución del esquema o patrón delictivo provoque que el delincuente adopte un patrón diferente de comportamiento.

c) La perspectiva de la elección racional:

> su premisa principal es que el delito es una conducta intencional, diseñada para beneficiar de alguna manera al delincuente (...) Esta teoría y su investigación están estrechamente vinculados a la prevención situacional del delito, la cual está explícitamente diseñada para reducir las oportunidades delictivas (Felson y Clarke, 1998, pp. 200-201).

En este orden de cosas, podemos afirmar que se puede prevenir la comisión de actos delictivos reduciendo sus oportunidades, y entre los diferentes enfoques existentes para conseguir nuestro objetivo, destacaremos la prevención situacional del crimen o cibercrimen, en su caso.

Por ejemplo, si tuviésemos un problema de cibercriminalidad relacionado con los enlaces maliciosos enviados por ciberdelincuentes a través de emails, suplantando la identidad de la empresa con el objeto de robar nuestros datos personales. En este caso, podríamos utilizar como método de prevención situacional, la aprobación de unas normas establecidas en un protocolo interno que establezcan que no debemos clicar sobre enlaces sospechosos o que soliciten datos personales, en su caso, eliminándolos *ipso facto.*

Según Felson y Clarke (1998):

> se han identificado dieciséis técnicas de reducción de la oportunidad, que pueden agruparse en cuatro objetivos derivados de la teoría de la elección racional: aumentar el esfuerzo delictivo percibido, aumentar los riesgos percibidos, reducir las recompensas esperadas y eliminar las excusas para delinquir (p. 222).

I.3 Realidad estadística de la cibercriminalidad en España.

El estudio que nos ocupa se centra en la ciudad de Vinaròs (Castellón), población costera con una población de derecho según el Instituto Nacional de Estadística[2] a uno de

[2] https://www.ine.es/nomen2/index.do?accion=busquedaRapida&subaccion=&numPag=0&ordenAnios=A

enero de 2019, de 28.682 habitantes, de los que 14.169 son hombres y 14.513 mujeres, tal y como podemos observar representado en la figura 1.

Sin embargo, en la figura 2 podemos apreciar como en España, a uno de enero de 2019[3], había una población de casi 47 millones de habitantes, concretamente, 46.937.060, de los que 23.009.259 eran hombres y 23.927.801 mujeres, coincidiendo porcentualmente con la reseñada en el municipio de Vinaròs.

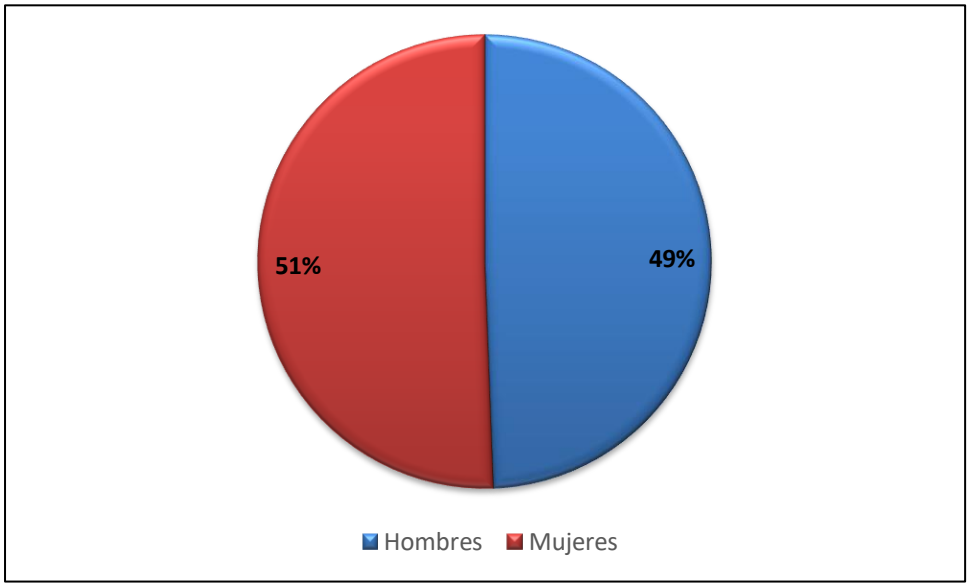

Figura 1.Población Vinaròs (2019)

SC&nombrePoblacion=vinaros&botonBusquedaRapida=Consultar+selecci%C3%B3n

[3] https://www.ine.es/jaxiT3/Datos.htm?t=9688#!tabs-tabla

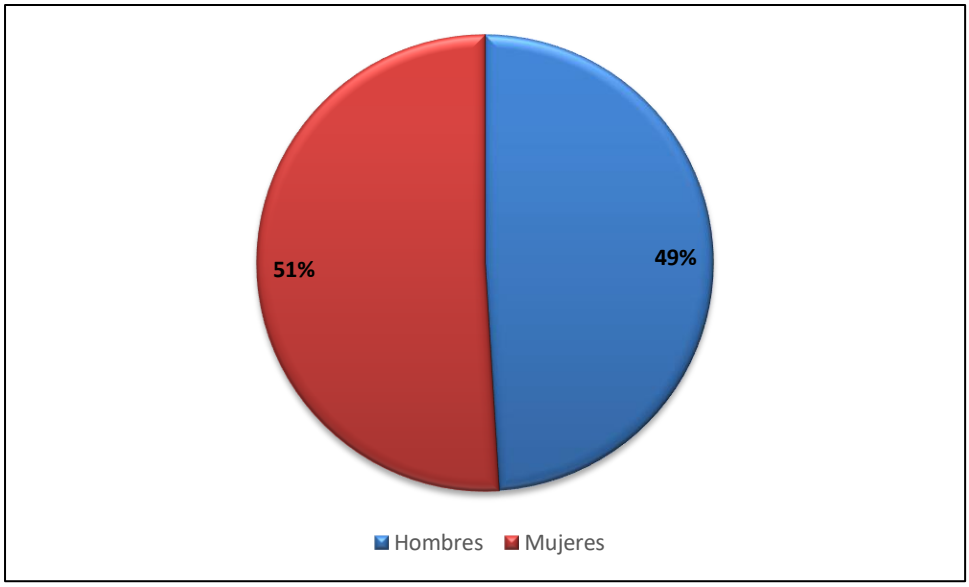

Figura 2. Población España (2019)

Para hacernos una somera idea generalizada sobre la realidad de la cibercriminalidad en España en comparativa con los resultados obtenidos sobre Vinaròs que veremos, posteriormente, en la segunda parte del presente estudio, partimos del informe sobre el estudio de cibercriminalidad en España de 2018[4] publicado en la web del Ministerio del Interior.

Sobre la base del informe público reseñado, en el rango de población de 20.000 a 50.000 habitantes, el 78,6% de los hogares tenían ordenador, y un 86,9% tenía acceso a internet.

Por otra parte, con relación a los menores con rango de edad de 10 a 15 años, respectivamente, en el último trimestre del año 2018 había utilizado el ordenador un 91,3% frente a un 8,7% que no lo había utilizado, según podemos apreciar en la Figura 3, y un 92,8% había accedido a internet mientras que un 7,2% no había accedido (ver Figura 4), siendo mayoritario el acceso a Internet por parte de las chicas con un 93,2%, que de los chicos con un 92,5%.

Asimismo, en lo atinente a las personas que han comprado por internet, durante el ejercicio 2018 podemos ver en la Figura 5, como un 43,5% de la población lo había hecho alguna vez y, por el contrario, un 56,5% no había comprado nunca.

[4] www.interior.gob.es/es/prensa/balances-e-informes/2018

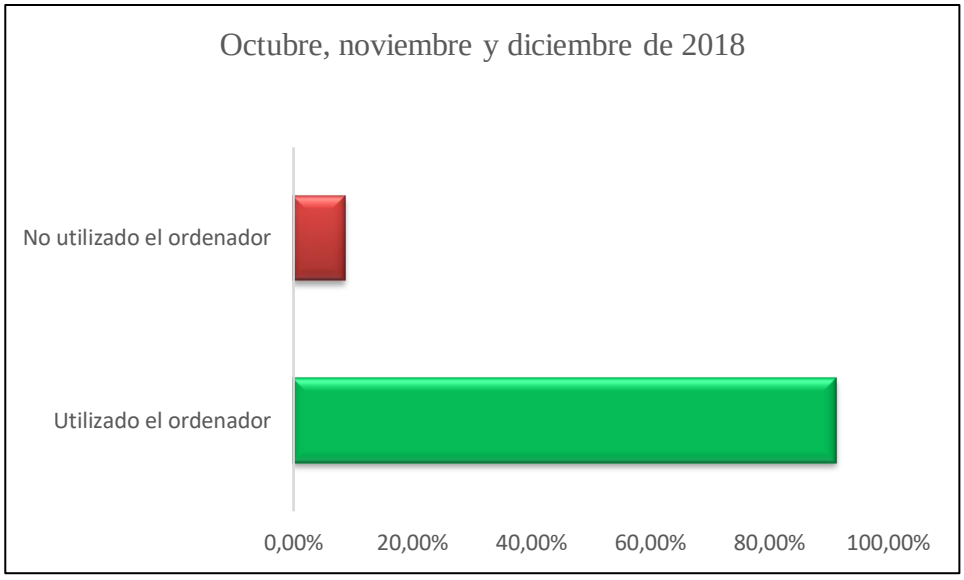

Figura 3. Porcentaje de menores que han utilizado el ordenador

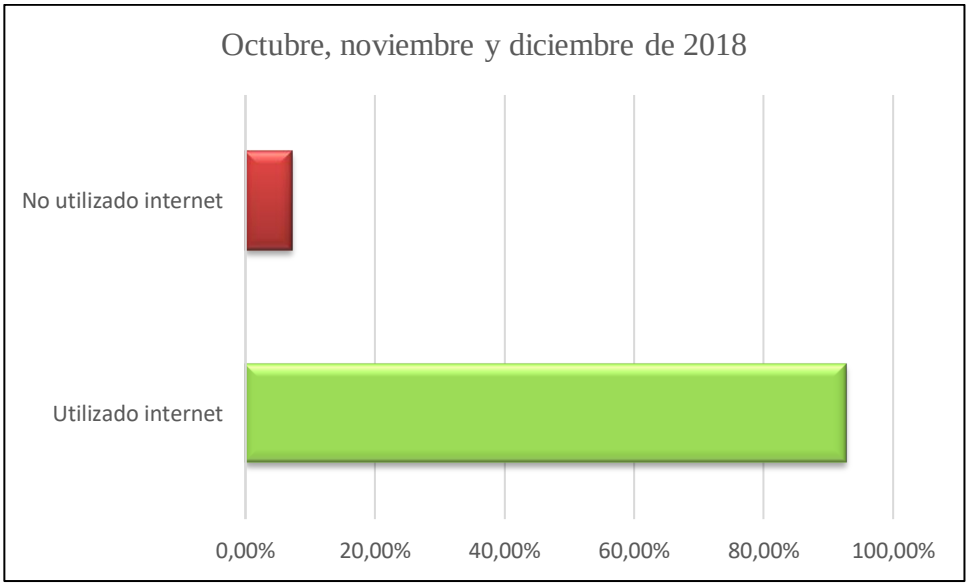

Figura 4. Porcentaje de menores que han accedido a Internet

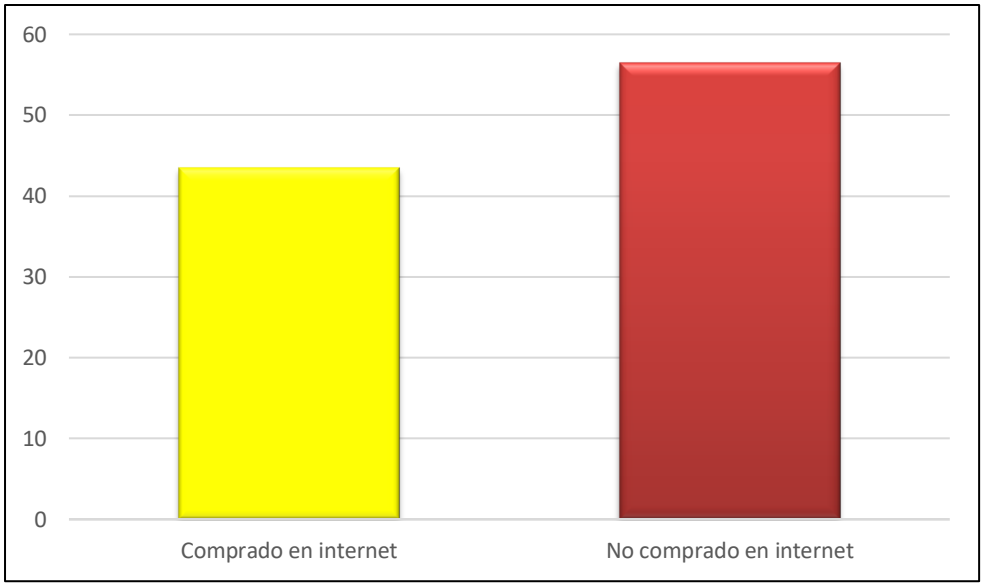

Figura 5. Porcentaje de personas que han comprado por internet en 2018

En la tabla 1, podemos observar los ciberdelitos denunciados en 2018, destacando en primer lugar con un 80,24% los fraudes informáticos, y en segundo lugar las amenazas y coacciones con un 10,81%. A contrario sensu, tenemos los delitos contra la propiedad intelectual e industrial que son los que se encuentran en último lugar con un 0,20% (ver figura 6).

En el año 2018, según Elvira Tejada[5], Fiscal de Sala Coordinadora en materia de Criminalidad Informática de la Fiscalía General del Estado, se incoaron 9.069 procedimientos judiciales relacionados con los delitos informáticos. Para Elvira (2019, p.1) en la materia que nos ocupa:

> se viene observando un desplazamiento generalizado hacia la Red de todo tipo de actividades criminales, dado que el ámbito tecnológico ofrece mayores facilidades para la planificación y ejecución criminal y mejores oportunidades de lograr la impunidad debido, entre otras circunstancias, a las múltiples posibilidades disponibles para el anonimato u ocultación del propio rastro, a la volatilidad de las evidencias y al carácter trasnacional del ciberespacio.

[5] Fiscal.es (2019). *Las estafas son los delitos que más se denuncian en la red*. Recuperado de https://www.fiscal.es/web/fiscal/-/elvira-tejada-fiscal-de-sala-de-criminalidad-informatica-las-estafas-son-los-delitos-que-mas-se-denuncian-en-la-red-

Tabla 1. *Ciberdelitos denunciados en 2018*

Hechos delictivos por grupos penales		Porcentaje
Acceso e interceptación ilícita	2.750	2,49
Amenazas y coacciones	11.960	10,81
Contra el honor	1.423	1,29
Contra propiedad industrial /intelectual	217	0,20
Delitos sexuales (*)	1.393	1,26
Falsificación informática	3.095	2,80
Fraude informático	88.760	80,24
Interferencia datos y en sistema	1.015	0,92
Total	110.613	100

(*) Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración.

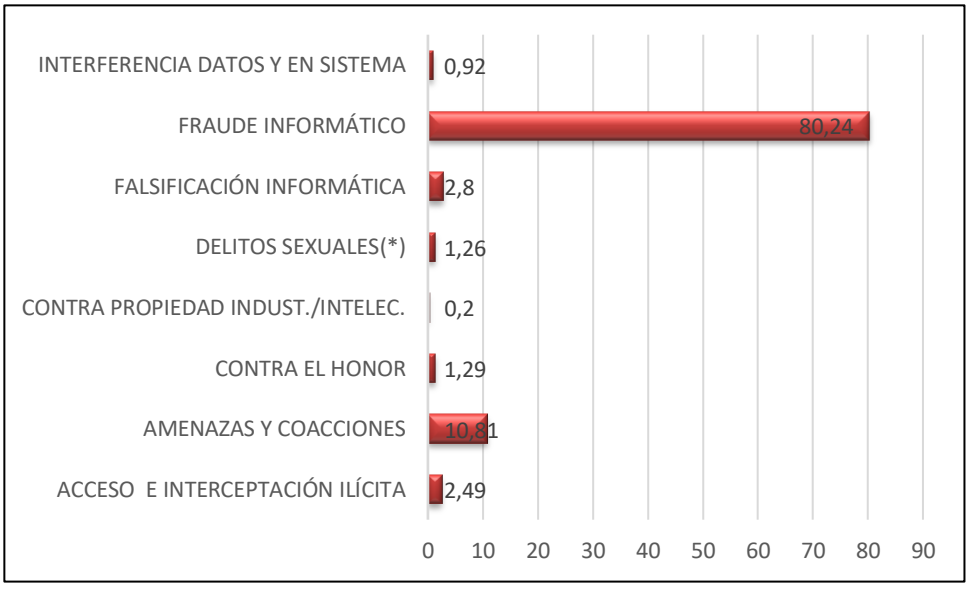

Figura 6. Porcentaje de ciberdelitos denunciados en 2018

No obstante, si focalizamos nuestra atención en el colectivo de cibervíctimas menores con rango de edad de 10 a 15 años de la tabla 2, se registraron en 2018 en primer

lugar con un 36,70%, los delitos de amenazas y coacciones y en segundo lugar los delitos sexuales con un 35,27% en el ámbito del ciberespacio, quedando en último lugar los delitos contra la propiedad intelectual e industrial con un 0%, es decir, no se denunció ningún hecho durante el año (ver figura 6).

Tabla 2. *Cibervictimizaciones registradas en menores 2018*

Grupo penal		Porcentaje
Acceso e interceptación ilícita	258	11,13
Amenazas y coacciones	851	36,70
Contra el honor	102	4,40
Contra propiedad industrial /intelectual	0	0,00
Delitos sexuales (*)	818	35,27
Falsificación informática	93	4,01
Fraude informático	185	7,98
Interferencia datos y en sistema	12	0,52
Total	2.319	100,00

(*) Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración.

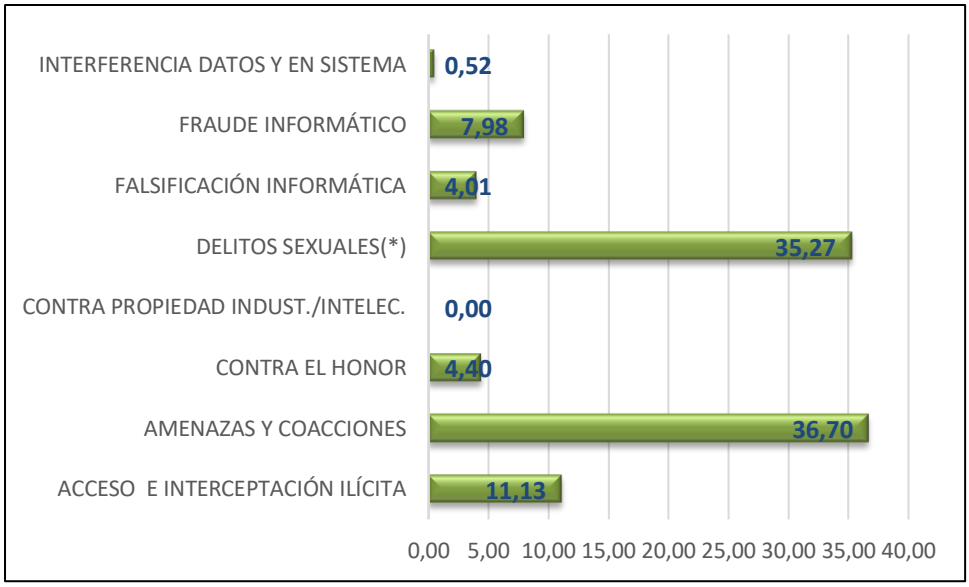

Figura 7. Porcentaje de cibervictimizaciones de menores en 2018

I.4 Derechos digitales: Marco jurídico.

Nuestra Carta Magna contempla en su artículo 18.4 que: "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" (p.29317).

Por lo que respecta al marco jurídico en materia de protección de datos *stricto sensu*, destacaremos las siguientes normas:

1) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (en adelante RGPD).

2) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

3)Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

4) Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

De la normativa reseñada nos centraremos en el RGPD y en la LOPDGDD. En primer lugar, comenzaremos destacando que el RGPD, establece entre sus objetivos:

> -establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.
> -proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales (p. L 119/32).

En los dos objetivos reseñados, podemos observar dos conceptos muy importantes que aparecen y que debemos tener perfectamente claro qué significan, y que en el artículo 4, apartados 1) y 2) del RGPD se definen, así:

> 1) datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;
>
> 2) tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción (p. L 119/33).

Pero ¿Cuándo se considera que el tratamiento de datos personales es licito o ilícito, en su caso? El RGPD en su artículo 6.1 contempla que el tratamiento de datos personales solo será lícito si se cumple como mínimo una de las siguientes condiciones:

> a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
>
> b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño (no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones) (p. L 119/36).

En segundo lugar, abordaremos la LOPDGDD cuyo objeto es: "adaptar el ordenamiento jurídico español al RGPD y garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución" (p. 119800).

La LOPDGDD en sus artículos 79 a 97, ambos inclusive, contempla un catálogo de derechos digitales cuyo contenido en síntesis es el siguiente:

a) derecho a la neutralidad de Internet, es decir, que todos los datos de la red deben de ser tratados de la misma forma.

b) derecho de acceso universal a Internet, de manera que se garantizará "un acceso universal, asequible, de calidad y no discriminatorio para toda la población" (p. 119836).

c) derecho a la seguridad digital: los proveedores de Internet deberán informar a sus usuarios de sus derechos y las comunicaciones recibidas y transmitidas deberán ser seguras.

d) derecho a la educación digital: es decir que todos los planes del sistema educativo deberán incluir formación para usar las nuevas tecnologías digitales de modo seguro y respetuoso, en su caso.

e) protección de los menores en Internet: involucrándose para ello tutores, representantes legales y familias que:

> procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales (p.119837).

f) derecho de rectificación en Internet, que los responsables de redes sociales y servicios equivalentes posibilitaran mediante la adopción de protocolos adecuados ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, en su caso.

g) derecho a la actualización de informaciones en medios de comunicación digitales: es decir, que toda persona puede:

> solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio (p.119837).

h) derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral: los empleadores deberán establecer los criterios de uso de los dispositivos digitales junto con los representantes de los trabajadores.

i) derecho a la desconexión digital en el ámbito laboral: es decir, que las empresas no podrán contactar con sus trabajadores fuera del horario laboral o en períodos de descanso, permisos y vacaciones.

j) derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo: admitiéndose únicamente, en su caso, "cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo" (p. 119838).

k) derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral: es decir, que se podrá geolocalizar a los trabajadores siempre y cuando, previamente, éstos y sus representantes estén debidamente informados "acerca de la existencia y características de estos dispositivos" (p. 119839), por parte del empleador.

l) derechos digitales en la negociación colectiva: se contempla que los convenios colectivos puedan establecer las garantías y derechos para el tratamiento de datos personales de los trabajadores en el trabajo.

m) protección de datos de los menores en Internet: para ello, se contempla que el menor debe tener el consentimiento de sus representantes legales y a partir de los 14 años podrá otorgarlo él mismo, en su caso.

n) derecho al olvido en búsquedas de Internet: es decir que:

toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, etc. (p.119839).

o) derecho al olvido en servicios de redes sociales y servicios equivalentes: en este caso podríamos decir que se trata de una extensión del derecho al olvido para abarcar a las redes sociales y servicios equivalentes.

p) derecho de portabilidad en servicios de redes sociales y servicios equivalentes: es decir que los usuarios de estos servicios tienen derecho a recibir y transmitir contenidos y datos personales que hubieran facilitado de una red social a otra de manera automática.

q) derecho al testamento digital: es decir que si la persona fallecida no ha dejado testamento (abintestato o sucesión intestada), las personas vinculadas por razones familiares podrán acceder al correo electrónico, redes sociales y servicios de mensajería instantánea, pudiendo borrar o modificar los datos que contengan, en su caso.

I.5 Cibervictimización: La pieza clave.

Desde una perspectiva jurídica, el artículo 2 de la Ley 4/2015, de 27 de abril, del Estatuto de la víctima del delito, contempla el concepto general de víctima, distinguiendo entre víctima directa e indirecta, respectivamente.

En este sentido, nos centraremos en el concepto de víctima directa, cuya definición es la siguiente: "toda persona física que haya sufrido un daño o perjuicio sobre su propia persona o patrimonio, en especial lesiones físicas o psíquicas, daños emocionales o perjuicios económicos directamente causados por la comisión de un delito" (p. 36575).

Por otra parte, Burt (1983) propone un concepto de víctima como un proceso dividido en las cuatro etapas siguientes:

-1) experimentación de daños, ofensas o sufrimiento causados por otras personas o instituciones:

-2) definirse a sí mismo como víctima.

-3) los individuos se perciben a sí mismos victimizados y dañados, y además tratan

de conseguir de que alguien más reconozca el daño y valide la reclamación de que ha sido victimizada.

-4) los individuos reciben la validación de su demanda del rol de víctima y son considerados víctimas reales o víctimas oficiales (citado por Laguna, 2010).

Actualmente, todas las personas que interactúan en Internet y redes sociales tienen riesgo de ser cibervíctimas. De hecho, se producen ciberataques de manera constante en todo el mundo.

Para Giménez (2020) podemos ser testigos de la guerra digital en la que vivimos, simplemente entrando en determinadas páginas webs como las siguientes:

- https://www.fireeye.com/cyber-map/threat-map.html
- https://cybermap.kaspersky.com/
- https://threatmap.fortiguard.com/
- http://www.digitalattackmap.com/

No obstante, hay que destacar que para Miró (2012) "son muchos los ciberataques que se realizan en el ciberespacio sin un objetivo determinado, siendo el concreto interactuar de la víctima, el que la convierte en el objetivo adecuado y no la voluntad del cibercriminal..." (p.191).

En la vida real, cuando realizamos nuestras actividades cotidianas diarias *offline*, si en vez de ir por calles con buena iluminación, vigiladas y muy transitadas deambulamos por calles que prácticamente no transite la gente y estén poco iluminadas y vigiladas, la probabilidad de que nos convirtamos en víctimas aumenta con nuestra decisión. Pues lo mismo ocurre cuando llevamos a cabo nuestras actividades cotidianas diarias *on line*.

Por lo tanto, podemos comprobar que la afirmación de que la falacia del crimen azaroso que constatan Felson y Boba (2009, citado por Miró, 2012) según la creencia errónea por parte de la gente de que el delito se produce independientemente de nuestra interacción o actos que ejecutemos "se manifiesta de forma más expresiva en el ciberespacio" (p. 194).

De manera que:

si la conducta de la víctima va a ser un determinante especialmente significativo del delito, también será por ello un importante condicionante para su prevención. La educación de la víctima en seguridad informática, su concienciación para la

adopción del software de protección y de rutinas seguras en su actuar cotidiano en el ciberespacio, así como la información real sobre los riesgos en el ciberespacio, serían los primeros pasos por adoptar para la prevención del cibercrimen" (Miró, 2012, p.194).

Así las cosas, Miró et al. (2014) en el proyecto del trabajo "CiberApp, estudio sobre el alcance de la cibercriminalidad de los menores de la provincia de Alicante", recogió por medio de la encuesta "Cibervictimización y hábitos de los menores en Internet", los datos de una muestra de 2038 menores estudiantes de veinte centros de la ESO de toda la provincia de Alicante. En sus conclusiones, determinó una serie de factores de riesgo y protección asociados a la cibervictimización social y económica que a mi juicio por analogía, son perfectamente extrapolables y aplicables a otros menores que cursen la ESO del territorio nacional, como es el caso del presente estudio enfocado a los menores que cursan la ESO de la ciudad de Vinaròs, máxime cuando se evaluó la eficacia del citado proyecto por Rodríguez, Fernández, y Bautista (2017) en un estudio con el objeto de reducir las tasas de cibervictimación en menores de la provincia de Alicante detectadas en el año 2014.

Por otra parte, en lo que respecta al ámbito de la cibercriminalidad económica que contempla este estudio, aunque vaya dirigido a mayores de edad que regentan establecimientos públicos, comercios y micropymes, en su caso, entiendo que en parte podrían también ser tenidos en cuenta o serles de aplicación los factores de riesgo y protección asociados, puesto que la población adulta también comete imprudencias asumiendo riesgos en el ciberespacio ya sea por desconocimiento o por exceso de confianza.

I.5.1 Factores de riesgo y protección asociados a la cibervictimización social.

Podríamos decir que según Miró et al. (2014) los factores de riesgo y protección relacionados con la cibervictimización social serían:

a) factores de riesgo:

ser usuario de redes sociales, ser usuario de foros, jugar a videojuegos online, realizar videollamadas, ser usuario de mensajería instantánea, ser usuario de blog, contactar con desconocidos, abrir enlaces o descargar archivos enviados por desconocidos, facilitar información personal, facilitar contraseñas, usar datos

personales reales para abrir cuentas en redes sociales y no compartir el ordenador con otras personas.

b) factores de protección:
no guardar información personal en el ordenador desde el que se accede a Internet, no guardar información personal en el móvil desde el que se accede a Internet, control por parte de los padres sobre las horas de uso del móvil, compartir el ordenador con los padres y limitar el acceso a las redes sociales.

I.5.2 Factores de riesgo y protección asociados a la cibervictimización económica.

Para Miró et al. (2014), los factores de riesgo y protección asociados a la cibervictimización económica serían los siguientes:

a)factores de riesgo: ser usuario de correo electrónico, ser usuario de redes sociales, ser usuario de foros, realizar videollamadas, ser usuario de mensajería instantánea, ser usuario de blog, contactar con desconocidos, abrir enlaces o descargar archivos enviados por desconocidos, facilitar información personal, usar datos personales reales para abrir cuentas en redes sociales y facilitar contraseñas.

b) factores de protección: no guardar información personal en el ordenador desde el que se accede a Internet, no guardar información personal en el móvil desde el que se accede a Internet, control por parte de los padres sobre las horas de uso del teléfono móvil, control por parte de los padres sobre el uso del teléfono móvil y control por parte de los padres sobre el uso del ordenador.

I.6 Identificación y descripción de ciberriesgos.

La Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad (INCIBE, en adelante) en su guía de ciberataques (2020) para usuarios no técnicos propone una clasificación de éstos en función de si el ataque es a contraseñas, por ingeniería social, a las conexiones y ataques por *malware* o programas malignos (ver tabla 3).

La guía referenciada pretende dar a conocer a la ciudadanía los tipos de ciberataques a los que están expuestos y de los que podrían ser víctimas cuando navegan por Internet.

Por otra parte, Miró (2012) propone otra clasificación de elaboración propia, en lo atinente a los ciberataques, distinguiendo entre:

-ciberataques puros: Son aquellos que únicamente pueden cometerse en el ciberespacio como por ejemplo infecciones por programas malignos, denegación de servicios, etc.

-ciberataques réplica: Son aquellos que utilizan el ciberespacio como nuevo medio para cometer delitos tradicionales como por ejemplo el ciberfraude, el ciberacoso sexual, etc.

-ciberataques de contenido: Son aquellos en los que el centro de la infracción lo constituye el contenido que se comunica o transmite a través de Internet como por ejemplo la pornografía infantil, ciberpiratería intelectual, etc.

Tabla 3. *Ciberriesgos asociados a la cibercriminalidad en función del tipo de ciberataque*

Ciberriesgos	Medidas preventivas
-Ataques a contraseñas (fuerza bruta y diccionario).	Utilizar contraseñas robustas; aplicar el factor de autentificación múltiple; utilizar gestores de contraseñas.
-Ataques por ingeniería social (*phishing*, *vishing*, *smishing*, *baiting*, *shoulder surfing*, *dumpster diving*, *spam*, fraudes *online*, etc.)	Detectar errores gramaticales en el mensaje; Revisar que el enlace coincide con la dirección a la que apunta; Comprobar el remitente del mensaje; No descargar ningún archivo adjunto y analizarlo previamente con el antivirus; Evitar conectar dispositivos de almacenamiento externo o con conexión USB a nuestros equipos; Mantener nuestro sistema actualizado y las herramientas de protección tales como antivirus, activadas y actualizadas; utilizar filtros anti-espía; Eliminar la información de modo seguro; No utilizar nunca la cuenta de correo electrónico principal para registrarnos en ofertas o promociones por Internet, etc.

-Ataques a conexiones (wifi falsas, *spoofing*, ataques a *cookies*, ataques DDoS, *man in the middle*, *sniffing*, etc.)	Aprender a identificar redes wifi falsas; recurrir a una VPN; Realizar una configuración segura del router; Utilizar firma digital en el envío de emails; Restringir conexiones remotas al router; Actualizar el navegador y no guardar contraseñas en él; Actualizar el software; No conectarse a redes wifi públicas; No navegar por webs fraudulentas, etc.
-Ataques por *malware* (virus, adware, *spyware*, troyanos, gusanos, *botnets*, apps maliciosas, etc.)	Evitar el software pirata; Ignorar los anuncios y ventanas emergentes; Mantener equipo y antivirus actualizados; Confiar solo en las herramientas de seguridad legítimas; Hacer copias de seguridad.

Fuente: OSI (2020)

Pero, aparte de las clasificaciones referenciadas, Miró (2012) también contempla otra basada desde una perspectiva criminológica afirmando la existencia de tres categorías, cibercriminalidad social, cibercriminalidad económica y cibercriminalidad política, respectivamente.

La primera engloba todos los ataques en los que el objetivo "es una persona individual, en cualquiera de los aspectos de su desarrollo personal" (p.116), y la segunda que aglutina a todos los ataques "cuyo propósito último es la obtención de un beneficio patrimonial" (p. 116). La tercera es aquella que reúne los ataques cuyo objetivo es ideológico o institucional.

No obstante, por la temática de la tesis y el estudio llevado a cabo, nos centraremos únicamente en la primera y en la segunda categoría que veremos posteriormente.

I.7 Propuesta de plan de actuación preventivo municipal contra la cibercriminalidad y sus daños colaterales.

Para el presente estudio relacionado con la cibercriminalidad económica (autónomos y micropymes o microempresas) y social (menores que cursan la ESO) en el ámbito de la ciudad de Vinaròs, se propone un plan de actuación preventivo a nivel local

o municipal con el objeto de disminuir los riesgos para las cibervíctimas mediante la información y la formación permanente, y por ende, tanto los efectos negativos para la salud física y psíquica que puedan ocasionar a las cibervíctimas así como económicos, en su caso, que como daños colaterales pueden provocar la interacción en Internet y la utilización de las tecnologías de la información y comunicación (TIC, en adelante).

A mi juicio, los ayuntamientos como base de la Administración Pública y que goza del privilegio de tener un contacto más directo con los ciudadanos, debe cumplir con la obligación que le impone la Constitución Española en su precepto 43, de cuyo contenido, en síntesis, debemos destacar que: "se reconoce el derecho a la protección de la salud. Compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios (...)" (p.29320).

En este sentido, para poder llevar a cabo el proyecto del plan de actuación preventivo a nivel municipal debemos realizar un análisis DAFO, es decir, tener en cuenta sus características internas (debilidades y fortalezas) y externas (amenazas y oportunidades), que, entre otras, podrían ser las siguientes:

-debilidades: la administración local no percibe la importancia del proyecto a ejecutar, la falta de presupuesto municipal, la falta de formación específica de empleados públicos del ayuntamiento para poder impartir la información y/o formación requerida, etc.

-amenazas: la administración local no tiene interés y no se ejecuta el proyecto.

-fortalezas: se trata de un proyecto que favorecería la información y formación de los vecinos o ciudadanos de Vinaròs, tanto en el ámbito de la cibercriminalidad económica como social que podría ayudar a reducir los riesgos de cibervictimización y las consecuencias para la salud que podría acarrear la interacción en Internet y el uso de las TIC, en su caso, como son estrés, tecnoadicciones, etc.

-oportunidades: el proyecto podría resultar atractivo para los centros educativos así como para los autónomos y microempresas de la ciudad de Vinaròs, el proyecto ayudaría a mejorar la información y formación de los menores de edad en edad escolar así como para los regentes y clientes del pequeño comercio y microempresas de la población, el proyecto podrá potenciar el inicio de un proceso de especialización profesional en el seno de la Policía Local de Vinaròs en colaboración con los servicios sociales del ayuntamiento, como agentes tutores para dar respuesta a los problemas de la ciudadanía de Vinaròs con relación a su interacción con Internet y las TIC.

Pero, en este orden de cosas, ¿qué acciones concretas implementaríamos en el proyecto?

Las acciones concretas para implementar y conseguir resultados al respecto, las podríamos dividir en a corto, medio y largo plazo, respectivamente, así:

-Acciones a corto plazo:

a) formación en ciberseguridad sobre uso seguro TIC y RRSS.

b) establecer en Junta Local de Seguridad un acuerdo de colaboración y coordinación con la Guardia Civil y su grupo de delitos telemáticos, así como con el Observatorio Español de Delitos Informáticos (OEDI).

c) formación para la educación en igualdad e información de las aplicaciones móviles que se pueden descargar para mejorar su seguridad tales como UrSafe, Sister o Life 360.[6]

-Acciones a medio plazo:

a) formación en ciberseguridad sobre uso seguro TIC y RRSS.

b) la creación de un punto de atención temprana a víctimas de delitos informáticos en el seno de la Policía Local de Vinaròs.

-Acciones a largo plazo:

a) formación en ciberseguridad sobre uso seguro TIC y RRSS.

b) estudiar el contenido y ofrecimiento de un servicio municipal cuyo objeto sea la aplicación de un plan de seguridad con medidas de autoprotección y/o mediación policial para cibervíctimas de riesgo alto o extremo, en su caso.

Por último, realizaremos un seguimiento y evaluación de las acciones llevadas a cabo, y por ende del plan de actuación preventivo municipal contra la cibercriminalidad y sus daños colaterales. En este sentido, con la información que obtengamos realizaremos unas conclusiones que plasmaremos en un informe final anual que remitiremos a la Jefatura de Policía Local para que lo incluya como anexo en la Memoria anual del Cuerpo.

I.8 El informe criminológico como herramienta preventiva aplicado a la valoración del riesgo de cibervictimización.

En primer lugar, debemos tener claro el concepto de informe criminológico, es decir, ¿qué es?, ¿qué ámbitos de aplicación tiene?, y ¿qué tipo y finalidad pueden tener?

Iciar Iriondo (2020) lo define como "documento de carácter técnico a través del

[6] https://www.enter.co/chips-bits/apps-software/tres-apps-para-la-seguridad-de-las-mujeres/

cual, se estudia y se analiza de manera objetiva, las características y circunstancias de un hecho criminal o sobre un aspecto de conflicto o problema social relacionado con esta disciplina" (p.7).

Otros autores lo definen como:

> una exposición de las circunstancias personales, sociales, delictivas y coyunturales del investigado o sentenciado, que ayuda al juez a la mejor comprensión de los hechos, y lo asiste para que disponga de la mayor información posible con el objetivo que adopte las medidas más idóneas para favorecer un mejor cumplimiento de las consecuencias sancionadoras del delito cometido y posibilitar su integración social (Larrauri y Zorrilla, 2014; Climent, Garrido y Guardiola, 2012).

En lo atinente al ámbito de aplicación del informe criminológico podríamos decir que podría ser tanto el ámbito judicial como extrajudicial, en su caso.

Por lo que respecta a los tipos y finalidades del informe criminológico en los diferentes ámbitos de aplicación referenciados, podríamos decir que son: penal, penitenciario, civil y extrajudicial.

No obstante, en el ámbito extrajudicial tenemos que destacar que uno de los campos donde más cabida tiene el informe criminológico es el relacionado con la prevención del delito mediante el diseño urbano o a través de la prevención situacional, es decir, en la criminología ambiental que, según la definición de A. Bottoms y P. Wiles consiste en:

> el estudio del delito, la criminalidad y la victimización en relación con determinados lugares en particular y con la forma en que las personas y las organizaciones desarrollan sus actividades desde el punto de vista espacial, para lo que dependen de ciertos factores espaciales o de lugar (2002, citado por Antón, 2007).

En el ámbito extrajudicial, el informe criminológico también puede abarcar multitud de aspectos relacionados con el conflicto social, tanto de adultos como de menores de edad, por lo tanto, lo primero de todo que hay valorar es el asunto que pretendemos tratar para determinar la posibilidad de ayudarnos mediante un enfoque o aplicación criminológica en aras a resolver un problema o poder tomar las medidas preventivas correspondientes, en su caso.

En este sentido, con motivo del estudio criminológico que nos ocupa, nos interesa

su aplicación extrajudicial, concretamente, como herramienta preventiva aplicado a la valoración del riesgo de cibervictimización social (menores que cursan la ESO) y económica (autónomos y micropymes), respectivamente.

Pero ¿qué estructura debería contener el informe criminológico para el estudio referenciado?

Un ejemplo del contenido podría ser el siguiente:

a) cabecera o carátula: número o referencia del informe criminológico, asunto sobre aquello que se informa, datos del policía local firmante o firmantes, en su caso, y a quién va dirigido (Jefatura de Policía Local, Servicios Sociales, etc.).

b) índice.

c) introducción.

d) objetivos generales y específicos.

e) material y métodos utilizados.

f) resultados.

g) discusión y Conclusiones.

h) bibliografía.

I.9. El rol preventivo de los observadores ante el ciberacoso.

La mayoría de los estudios que se han realizado en torno al ciberacoso se centran en la figura del agresor y la víctima, pero ¿qué papel juegan los observadores? ¿pueden ayudar a prevenir conductas de ciberacoso?

Según un estudio realizado por González (2015), en la que tomó como muestra 190 alumnos de 2º y 3º de la ESO de dos centros educativos, se obtuvieron unos resultados, de los que podríamos destacar lo siguiente:

a) casi el 75% de los participantes entrevistados afirmó haber observado en alguna ocasión conductas de ciberacoso tales como enviar mensajes ofensivos, acosar sexualmente a través del teléfono móvil, robar la contraseña a compañeros/as, etc.

b) casi el 75% no respondieron a la pregunta de cómo actúan cuando observan conductas de ciberacoso, es decir, no hacen nada.

Para González (2015) los observadores de estas conductas reseñadas "juegan un papel muy importante, ya que pueden frenar el acoso apoyando a las víctimas y denunciando a los agresores" (p.88).

En conclusión, se deben incrementar y fomentar los esfuerzos para intentar concienciar a los observadores del rol que desempeñan en el ámbito del ciberacoso, y "ofrecerles formas sencillas y probablemente anónimas para que lo denuncien ante la más mínima sospecha" (González, 2015, p.89).

CAPITULO II: CIBERCRIMINALIDAD SOCIAL EN EL ÁMBITO DE LOS MENORES DE LA CIUDAD DE VINAROS.

II.1 Concepto de cibercrimen social.

El cibercrimen social es definido por Miró (2012) como: "Grupo de delitos en Internet que tienen que ver con las relaciones sociales entre las personas y que no son más que la trasposición al ciberespacio de los crímenes tradicionales derivados de conflictos entre personas". (p.301)

II.2 Convivencia, derechos y deberes de los menores.

El Diccionario de la lengua española define convivir como "vivir en compañía de otro u otros" (RAE 2020).

El artículo 19 de la Convención sobre los Derechos del Niño (1989) (CDN, en adelante) establece que "los Estados Partes adoptarán todas las medidas legislativas, administrativas, sociales y educativas apropiadas para proteger al niño contra toda forma de perjuicio o abuso físico o mental, descuido o trato negligente, malos tratos o explotación, incluido el abuso sexual…". Evidentemente, dicho precepto incluye la protección de los menores contra el acoso y el ciberacoso en el entorno educativo ejercido por pares.

Así las cosas, la necesidad de especial protección del niño frente a cualquier clase de maltrato está presente en un nutrido número de artículos de la CDN (artículos 2, 11, 16, 19, 32, 33, 34, 35, 36, 37, 38 y 39, respectivamente).

No obstante, tal y como se señala en la web de Convivencia Escolar del Ministerio de Educación y Formación Profesional, la convivencia pacífica es la base sobre la que se construye cualquier estado democrático y de derecho. Todo sistema educativo moderno tiene en la convivencia un doble referente, por una parte, constituye una finalidad de la educación (artículo 2 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación) y por otra parte, no puede haber proceso educativo sin convivencia en las aulas y en las comunidades educativas a las que atienden los centros escolares.

La Ley Orgánica 8/2013, de 9 de diciembre, para la Mejora de la Calidad

Educativa (en adelante, LOMCE) señala la convivencia como un objetivo de todas y cada una de las etapas del Sistema Educativo Español. Estos objetivos por etapas quedan recogidos en el Plan Estratégico de Convivencia Escolar de la siguiente forma:

1º) la etapa de Educación Infantil considera entre sus objetivos el de adquirir progresivamente pautas elementales de convivencia y relación social, así como ejercitarse en la resolución pacífica de conflictos.

2º) la Educación Primaria introduce como finalidad facilitar el aprendizaje del hábito de la convivencia y como primer objetivo conocer y apreciar los valores y las normas de convivencia, aprender a obrar de acuerdo con ellas, prepararse para el ejercicio activo de la ciudadanía y respetar los derechos humanos, así como el pluralismo propio de una sociedad democrática.

3º) la Educación Secundaria Obligatoria establece como finalidad formar al alumnado para el ejercicio de sus derechos y obligaciones en la vida como ciudadanos, contemplando como objetivos de la misma asumir responsablemente sus deberes, conocer y ejercer sus derechos en el respeto a los demás, practicar la tolerancia, la cooperación y la solidaridad entre las personas y grupos, ejercitarse en el diálogo afianzando los derechos humanos como valores comunes de una sociedad plural y prepararse para el ejercicio de la ciudadanía democrática.

4º) la Formación Profesional establece entre sus objetivos que el sistema educativo contribuirá a que el alumnado consiga los resultados de aprendizaje que le permitan formarse en la prevención de conflictos y en la resolución pacífica de los mismos en todos los ámbitos de la vida personal, familiar y social, con especial atención a la prevención de la violencia de género.

5º) el Bachillerato considera el desarrollo de las capacidades que permitan al alumnado ejercer la ciudadanía democrática, prever y resolver pacíficamente los conflictos personales, familiares y sociales y velar por la igualdad efectiva de derechos y oportunidades entre hombres y mujeres, así como analizar y valorar críticamente las desigualdades existentes e impulsar la igualdad real y la no discriminación de las personas con discapacidad.

Por último, no podemos olvidar la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia (LOPINFAVIO, en adelante), en cuyo artículo 1 contempla que su objeto es "garantizar los derechos

fundamentales de los niños, niñas y adolescentes a su integridad física, psíquica, psicológica y moral frente a cualquier forma de violencia…" (p.68668).

Pero ¿Qué entiende la LOPINFAVIO por violencia?

> Toda acción, omisión o trato negligente que priva a las personas menores de edad de sus derechos y bienestar, que amenaza o interfiere su ordenado desarrollo físico, psíquico o social, con independencia de su forma y medio de comisión, incluida la realizada a través de las tecnologías de la información y la comunicación, especialmente la violencia digital (p.68669).

En este sentido, ¿Qué conductas engloba en su abanico la LOPINFAVIO?

Pues, entre otras, aglutina expresamente conductas tales como el maltrato físico, psicológico o emocional, el trato negligente, las amenazas, injurias y calumnias, el acoso escolar, el acoso sexual, el ciberacoso, la violencia de género, la extorsión sexual, la difusión pública de datos privados, etc.

Y, ¿qué finalidades persiguen las disposiciones de la LOPINFAVIO?

En síntesis, entre otras, podemos destacar las siguientes:

a) garantizar la implementación de medidas de sensibilización para el rechazo y eliminación de todo tipo de violencia sobre la infancia y la adolescencia, dotando a los poderes públicos, a los niños, niñas y adolescentes y a las familias, de instrumentos eficaces en todos los ámbitos, de las redes sociales e Internet, especialmente en el familiar, educativo, sanitario, de los servicios sociales, del ámbito judicial, de las nuevas tecnologías, del deporte y el ocio, de la Administración de Justicia y de las Fuerzas y Cuerpos de Seguridad.

b) establecer medidas de prevención efectivas frente a la violencia sobre la infancia y la adolescencia, mediante una información adecuada a los niños, niñas y adolescentes, la especialización y la mejora de la práctica profesional en los distintos ámbitos de intervención, el acompañamiento de las familias, dotándolas de herramientas de parentalidad positiva, y el refuerzo de la participación de las personas menores de edad.

c) establecer los protocolos, mecanismos y cualquier otra medida necesaria para la creación de entornos seguros, de buen trato e inclusivos para toda la infancia en todos los ámbitos desarrollados en esta ley en los que la persona menor de edad

> desarrolla su vida. Se entenderá como entorno seguro aquel que respete los derechos de la infancia y promueva un ambiente protector físico, psicológico y social, incluido el entorno digital. (pp. 68669-68670).

Asimismo, la LOPINFAVIO contempla un catálogo de derechos de los menores en sus artículos 9 a 14, ambos inclusive, que en síntesis son: derecho de información y asesoramiento, derecho a ser escuchados como víctimas, derecho a la atención integral, derecho a estar legitimados para defender sus derechos e intereses en todos los procedimientos judiciales que traigan causa de una situación de violencia y derecho a la asistencia jurídica gratuita, con independencia de sus recursos para pleitear.

Por otra parte, la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil (LOPJM, en adelante), dedica su capítulo II del título I a los derechos del menor, concretamente, a los derechos al honor, a la intimidad y a la propia imagen, al derecho a la información, al derecho a la libertad ideológica, al derecho de participación, asociación y reunión, al derecho a la libertad de expresión así como al derecho a ser oído y escuchado tanto en el ámbito familiar como en cualquier procedimiento administrativo, judicial o de mediación, en su caso.

No obstante, el derecho a la protección de datos de los menores en Internet se contempla en el artículo 92 de la LOPDGDD, que establece que:

> los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.
>
> Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales … (p. 119839).

En este sentido, la LOPDGDD contempla en su artículo 7 que el consentimiento del menor se podrá, únicamente, fundarse cuando sea mayor de 14 años, salvo excepciones. En el supuesto de menores de 14 años, el tratamiento de sus datos fundado en el consentimiento, "solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela" (p. 119802).

Por otra parte, la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia introdujo un nuevo capítulo III en el título I de la LOPJM, artículos 9 bis a 9 quinquies, dedicado a los deberes de los menores que teniendo en cuenta su edad y madurez, "deberán asumir y cumplir los deberes, obligaciones y responsabilidades inherentes o consecuentes a la titularidad y al ejercicio de los derechos que tienen reconocidos en todos los ámbitos de la vida, tanto familiar, escolar como social" (p. 64558).

Pero ¿Qué tipo de deberes se exigen a los menores en concreto? Básicamente, podríamos decir que son deberes relativos a los ámbitos familiar, escolar y social, respectivamente, es decir, los menores deben, entre otras obligaciones:

a) participar en la vida familiar respetando a sus progenitores y hermanos, así como a otros familiares.

b) respetar las normas de convivencia de los centros educativos, a los profesores y otros empleados de los centros educativos, así como al resto de sus compañeros, evitando situaciones de conflicto y acoso escolar en cualquiera de sus formas, incluyendo el ciberacoso.

c) respetar a las personas con las que se relacionan y al entorno en el que se desenvuelven (p. 64558).

II.3. Actuaciones del *Síndic de Greuges* de la Comunidad Valenciana en el ámbito de la violencia, acoso y ciberacoso en las escuelas.

El *Síndic de Greuges* de la Comunidad Valenciana es la figura homóloga del Defensor del Pueblo en la Comunidad Autónoma referenciada y que se encuentra regulada, actualmente, por la Ley 2/2021, de 26 de marzo, del *Síndic de Greuges* de la Comunidad Valenciana (LSGCV, en adelante).

El artículo 1 de la LSGCV establece que el *Síndic de Greuges* de la Comunidad Valenciana:

> se configura, de acuerdo con el Estatuto de Autonomía, como alto comisionado de las Corts Valencianes designado por estas para velar por la defensa de los derechos y las libertades reconocidos en el título I de la Constitución española, en el título II del Estatuto de Autonomía, así como por las normas de desarrollo correspondiente, y los instrumentos internacionales de protección de los derechos

humanos y en la Carta de Derechos Sociales de la Comunidad Valenciana.

(…) tiene la condición de defensor de los derechos de la infancia y de la adolescencia, sin detrimento de las funciones que correspondan al Ministerio Fiscal (p. 43685).

En este sentido, cabe destacar que, en la sede de la institución, el 10 de junio de 2015 se creó el Observatorio del Menor del *Síndic de Greuges* y entre sus objetivos se encuentran, entre otros: "Potenciar la figura del *Síndic de Greuges* como defensor de los derechos de la infancia y adolescencia entre este colectivo y profesionales del sector".

Posteriormente, en el informe anual del ejercicio 2016 que presentó el *Síndic de Greuges* ante las Cortes Valencianas, consta que durante ese año fueron muy frecuentes:

las noticias aparecidas en medios de comunicación de casos de menores de edad objeto de violencia, acoso o ciberacoso en sus escuelas, siendo identificado, por los/as componentes del Pleno del Observatorio del Menor del *Síndic de Greuges* como un problema de especial relevancia".

(...) dada la complejidad del asunto a tratar, además de los datos requeridos a las administraciones implicadas (principalmente Conselleria de Educación), se constituyó en el interior del Observatorio del Menor del *Síndic de Greuges*, un grupo de trabajo *ad hoc"* (p.60).

En este orden de cosas, con fecha 01/04/2022, el *Síndic de Greuges* procedió a la apertura de una queja de oficio[7] con el fin de investigar y supervisar las actuaciones de la administración en el ámbito de la violencia escolar en centros docentes, y con fecha 29/07/2022, el *Síndic de Greuges* emitió una resolución en la que acordó formular a la Conselleria de Educación, Cultura y Deporte de la Comunidad Valenciana cinco recomendaciones, de las que la administración a posteriori, acepto totalmente a excepción de dos que aceptó parcialmente, siendo éstas las siguientes:

-recomendamos la efectiva puesta en marcha de la figura del docente mediador o de equipos de mediación específicos para hacer frente a este tipo de conflictos en los que se de participación al alumnado así como la implementación de otros mecanismos para incentivar la resolución de los conflictos en el ámbito interno de los centros escolares, dotándolos de medios humanos y materiales necesarios para

[7] https://www.elsindic.com/actualidad/el-sindic-pide-a-educacion-medidas-mas-efectivas-para-atajar-el-acoso-escolar/

promover la participación de las familias en el proceso de detección y resolución de los conflictos.

-recomendamos la creación de aulas de convivencia para el tratamiento puntual e individualizado del alumno afectado por una medida correctora previsto en el Decreto 39/2008 de 4 de abril, del Consell sobre convivencia en los centros docentes no universitarios sostenidos con fondos públicos (*Síndic de Greuges*, 2022, p.4).

Desde una perspectiva político criminal, hechos como éste, evidencian, que la administración aprueba normativa que después tiene dificultades para poder cumplir, de manera que, a mi juicio deberían crearse organismos que ejerciesen de una especie de función de vigilantes del vigilante, es decir, evaluar y analizar el cumplimiento y eficacia normativa de la legislación estatal, autonómica y local, en su caso, de la administración.

Para el caso objeto de estudio que nos ocupa, se podría proponer la creación de un Observatorio de cumplimiento y eficacia normativa autonómica y local de la Comunidad Valenciana en el seno de la Institución del *Síndic de Greuges* o, en su caso, un grupo de trabajo exprofeso para desempeñar dicho cometido en el ámbito de la violencia, acoso y ciberacoso escolar, dentro del Observatorio del Menor referenciado.

II.4. Actuaciones de la Agencia Española de Protección de Datos relacionados con la difusión de imágenes grabadas de menores.

En virtud de los poderes de investigación y correctivos que el artículo 58 del RGPD otorga a cada autoridad de control, y en concordancia con lo dispuesto en el artículo 47 de la LOPDGDD, ante la formulación de una denuncia escrita en el ámbito que nos cupa admitida a trámite, la persona competente para resolver las actuaciones de investigación corresponde al Director o Directora de la Agencia Española de Protección de Datos.

En este orden de cosas, si navegamos por la página web de la Agencia Española de Protección de Datos https://www.aepd.es/es podemos encontrar varias resoluciones sobre denuncias interpuestas por padres, madres, representantes legales, etc., en las que sus hijos/as menores de edad han sido víctimas o, en su caso, presuntamente han difundido imágenes en las redes sociales sobre peleas y/o agresiones entre alumnos menores de edad pertenecientes a institutos de secundaria.

Ejemplo de dichas resoluciones son los procedimientos nº: E/01784/2020 y nº: E/09442/2019, respectivamente, en los que finalmente se acordó el archivo de las actuaciones.

Actualmente, la Agencia Española de Protección de datos (AEPD)[8] dispone de un canal prioritario para la retirada de contenidos sensibles que puede ser utilizado por cualquier ciudadano, habiéndose habilitado dos vías de accesibilidad. La primera para el público adulto en general, y la segunda para menores a partir de los 14 años de edad, con el objeto de que en el supuesto haber sido cibervíctimas puedan solicitar la retirada de contenidos sexuales o violentos publicados en Internet en abierto sin permiso de las personas que aparecen en ellos.

II.5 Cibercriminalidad social: Características, tipologías y tipificación penal.

Desde una perspectiva criminológica, podríamos decir que los cibercrímenes sociales constituyen una categoría que aglutina a todos aquellos que tienen como objetivo una persona individual, en cualquiera de los aspectos de su desarrollo personal como es el caso del acoso entre adolescentes, especialmente en el ámbito escolar. Actualmente, las TIC e Internet se encuentran en un proceso constante de evolución, existiendo muchas conductas criminales que se pueden llevar a cabo en el ciberespacio empleando como herramienta un ordenador, una tableta, un teléfono móvil, etc., junto a las redes sociales o programas de mensajería instantánea, en su caso.

La Instrucción 10/2005, de 6 de octubre, sobre el tratamiento del acoso escolar desde el sistema de justicia juvenil, contempla una definición generalizada de acoso escolar definiéndolo como "exposición de un alumno, de forma repetida y durante un tiempo, a acciones negativas que lleva a cabo otro u otros alumnos" (p.7).

La Orden 62/2014, de 28 de julio, de la Conselleria de Educación, Cultura y Deporte, por la que se actualiza la normativa que regula la elaboración de los planes de convivencia en los centros educativos de la Comunitat Valenciana y se establecen los protocolos de actuación e intervención ante supuestos de violencia escolar, contempla en su anexo I, la definición de la conducta de ciberacoso como: "acoso entre iguales en el entorno de las TIC, e incluye actuaciones de chantaje, vejaciones e insultos entre alumnos" (pp.19274-19275).

Por lo que respecta a las características del ciberacoso, dicha Orden, establece las

[8]https://www.aepd.es/canalprioritario/

siguientes:

a) agresión repetida y duradera en el tiempo.

b) intención de causar daño: no siempre se da en los primeros estadios del proceso.

c) suele existir contacto o relación previa en el mundo físico.

d) puede estar ligado o no a situaciones de acoso en la vida real.

e) usar medios TIC: sms, e-mail, teléfonos móviles, redes sociales, blogs, foros, salas de chats (p.19275).

No obstante, *Save The Children* en un informe de febrero de 2016, titulado "Yo a eso no juego. *Bullying* y *Ciberbullying* en la infancia", contempla tal y como sucede en el acoso escolar presencial u acoso *offline* que, en el ciberacoso u acoso *online*, los insultos son las conductas más frecuentes, seguidos de los rumores, las amenazas y la exclusión, respectivamente, en calidad tanto de víctima como de victimario o agresor, en su caso.

Pero, desde una perspectiva jurídica, ¿Qué tipificación penal tiene tanto el acoso como el ciberacoso escolar?

En principio como tipo básico se encontraría tipificado en el artículo 173.1 del Código Penal (CP, en adelante), y lo comete "el que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral" (p. 34008).

Sin embargo, debemos tener presente a tenor de lo establecido en el artículo 177, CP, que si además del atentado a la integridad moral, se produjere "lesión o daño a la vida, integridad física, salud, libertad sexual o bienes de la víctima o de un tercero", estaríamos ante un concurso de delitos, y "se castigarán los hechos separadamente con la pena que les corresponda por los delitos cometidos, excepto cuando aquél ya se halle especialmente castigado por la ley" (p.34008).

En los medios de comunicación, podemos observar casos graves de ciberacoso que han acabado con el fatídico final del suicidio de la víctima como es el caso de la canadiense de 16 años, Amanda Michelle Todd que sucedió en el año 2012.

Actualmente, la inducción al suicidio se encuentra tipificada en nuestro CP, concretamente, en su artículo 143.1, así como otras conductas tales como las amenazas y las coacciones que también recoge nuestra Constitución negativa.

Concretamente, el CP castiga en su artículo 169 al que:

amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones,

aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico (p.34007).

Y en su artículo 172.1 castiga al que, "sin estar legítimamente autorizado, impidiere a otro con violencia hacer lo que la ley no prohíbe, o le compeliere a efectuar lo que no quiere, sea justo o injusto" (p. 34008).

Así las cosas, dentro del ámbito de la cibercriminalidad social también existen otros tipos delictivos que debemos destacar, a parte del ciberacoso en el ámbito escolar que hemos abordado, y que son:

-*cyberstalking*: "consiste en una combinación de distintas formas de acecho a través de los medios que facilita la tecnología como el chat, foros, redes sociales, etc." (Miró, 2012, p. 89).

El CP recoge esta conducta en su artículo 172 ter.1 que la comete:

El que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

a) la vigile, la persiga o busque su cercanía física.

b) establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

c) mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

d) atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella, constituyendo un tipo agravado cuando la víctima se halle en una situación de especial vulnerabilidad por razón de su edad, enfermedad, discapacidad o por cualquier otra circunstancia.

e) utilice, sin consentimiento de su titular, la imagen de una persona para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la misma situación de acoso, hostigamiento o humillación (p.124239).

Desurmont (2009) distingue tres modalidades distintas de ejecución del *stalking*: individual, múltiple y organizativo (*gang-stalking*) que si las extrapolamos al ámbito del ciberespacio, podríamos decir que la primera sería la conducta típica generalizada y llevada a cabo por un solo victimario, y las dos siguientes serían las realizadas por más

de un victimario diferenciándose en que en el *cyberstalking* múltiple los ciberacosadores implicados no actúan de manera concertada, y en el organizativo sí y con una víctima como objetivo común.

En síntesis, bajo mi criterio personal y desde una perspectiva criminológica podríamos distinguir dos tipos de cyberstalking, uno individual o propiamente dicho y otro grupal (*gang-cyberstalking)*, actúen o no de manera organizada los *cyberstalkers*.

-*online grooming*: el ciberacoso sexual a menores, también conocido como *child grooming* o *cybergrooming*, "consiste en contactar con menores por medio de las redes sociales o de otras formas de comunicación como salas de chat, canales de mensajería instantánea o similares, para acercarse a ellos e intentar posteriormente un contacto sexual" (Miró, 2012, p. 96).

El CP entre los abusos y agresiones sexuales a menores de dieciséis años tipificados en los artículos 183 a 183 quater, contempla en su artículo 183 ter las conductas típicas de este ilícito penal, cometiéndose por:

> a) el que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento (p. 27120).

Tenemos que destacar que si el acercamiento del adulto victimario se obtiene mediante coacción, intimidación o engaño agravará las penas que se impongan, en su caso.

> b) el que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor (p. 27120).

Para Sedeño (2017), en el *online grooming* se pueden distinguir cuatro fases que se suceden en la comisión de este ilícito penal, y que son las siguientes:

1. fase de acercamiento: en esta fase el victimario (una persona adulta) selecciona una víctima menor de edad vulnerable por sentirse incomprendido/a familiar y/o socialmente, y procede a realizar el primer contacto virtual para fingir comprender su situación y ganarse su confianza (Miró, 2012).

2. fase de relación: en esta fase el victimario irá ganándose la confianza de la víctima consiguiendo fotos y/o vídeos íntimos (semidesnuda, desnuda, masturbándose, etc.) de ésta (Sedeño, 2017).

3. fase de seducción: en esta fase el victimario ha conseguido seducir a la víctima y si el menor deja de acceder a sus peticiones es amenazado con la difusión del material de carácter íntimo en internet, redes sociales, etc. (Sedeño, 2017).

4. fase de acoso: en esta fase se produce el verdadero ciberacoso sexual, accediendo la víctima menor de edad a los deseos sexuales del victimario por miedo (Sedeño, 2017).

-*sexting*:

> consiste en la realización, por parte de menores, de fotografías propias de desnudos completos o de partes desnudas y su envío, generalmente por medio de teléfono móvil, a otros, junto con textos obscenos y con la finalidad de conocer a personas o de enviar mensajes de amor o de odio (Miró, 2012, pp. 92-93).

En este sentido, Lenhart (2009, citado por Miró, 2012) distingue entre sexting activo y pasivo, consistiendo el primero en realizar "autofotos/vídeos en una postura sexy, provocativa o inapropiada" y el segundo en recibir "fotos/vídeos de personas de su entorno en una postura sexy, provocativa o inapropiada" (p.93).

Actualmente, la práctica del sexting en sí misma no se encuentra tipificada penalmente, siempre que la difusión de fotos y/o vídeos por parte del menor haya sido realizada voluntariamente. Sin embargo, si dicho material es difundido a terceros sin el consentimiento o autorización del afectado o afectada, en su caso, la situación ya cambia.

De hecho, el CP en su artículo 197.7 castiga al que:

> sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona (p. 27125).

Constituye un tipo agravado de este delito, cuando los hechos hubieran sido cometidos por:

> el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona

con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa (p. 27125).

En este sentido, cabe destacar que la LECrim contempla en su artículo 13 que:

> en la instrucción de delitos cometidos a través de internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación, el juzgado podrá acordar, como primeras diligencias, de oficio o a instancia de parte, las medidas cautelares consistentes en la retirada provisional de contenidos ilícitos, en la interrupción provisional de los servicios que ofrezcan dichos contenidos o en el bloqueo provisional de unos y otros cuando radiquen en el extranjero (p. 124236).

Por último, mencionaremos la violencia de género digital entre adolescentes o ciberviolencia de género, para lo que deberemos tener claro qué es lo que se entiende por violencia de género *stricto sensu*. Para ello, nos remitiremos a la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género que contempla su definición en su artículo 1, como "cualquier acto de violencia tanto físico, como psicológica, y ello incluye las agresiones a la libertad sexual, amenazas, coacciones o privación arbitraria de la libertad" (p.42168).

Asimismo, el objetivo de dicha ley es:

> actuar contra la violencia que, como manifestación de la discriminación, la situación de desigualdad y las relaciones de poder de los hombres sobre las mujeres, se ejerce sobre éstas por parte de quienes sean o hayan sido sus cónyuges o de quienes estén o hayan estado ligados a ellas por relaciones similares de afectividad, aun sin convivencia (p.42168).

En este sentido, la citada Orden 62/2014 define en su anexo IV la violencia de género como: "aquella que, como manifestación de la discriminación, la situación de desigualdad y las relaciones de poder de los hombres sobre las mujeres, se ejerce sobre ella por el hecho de serlo" (p.19280).

En España, según el Instituto Nacional de Estadística (INE) durante el año 2020 se registraron 29.215 mujeres víctimas de violencia de género de las que 514 eran menores de 18 años. En el mismo ejercicio, en cuanto a los victimarios o agresores de violencia de género menores de edad, se denunciaron a un total de 72 jóvenes.

Según Victoria Rosell, delegada del gobierno contra la violencia de género, en el mes de febrero de 2022, habían más de 850 adolescentes de 14 a 17 años con protección

policial por sufrir violencia de género[9].

Desde una perspectiva político criminal, el Observatorio Nacional de Tecnología y Sociedad (ONTSI, en adelante), ha recomendado la consideración expresa de la violencia de género digital como una forma de violencia de género en nuestro acervo normativo, así como: "la definición de nuevos tipos penales para abarcar todas las facetas de la violencia de género digital que actualmente no son denunciables por no ser constitutivas de delito" (Europapress, 2022).[10]

En este sentido, ¿estamos ante un panorama social que exige un cambio en la normativa o inclusión exprofeso de un problema real que se llama violencia de género digital?

En mi opinión, sí que lo es, y de hecho, la sociedad lo reclama a través de los medios de comunicación.

No obstante, con motivo del estudio realizado en la presente, nos centraremos en la violencia de género digital u *online* que forma parte del concepto amplio de ciberviolencia[11] y que el Consejo de Europa en 2018 la definió como:

> el uso de sistemas informáticos para causar, facilitar o amenazar con violencia contra las personas, que tiene como resultado, o puede tener como resultado, un daño o sufrimiento físico, sexual, psicológico o económico, y puede incluir la explotación de la identidad de la persona, así como de las circunstancias, características o vulnerabilidades de la persona[12] (ONTSI, 2022, p.6).

Así las cosas, a pesar de su semejanza con la violencia de género *offline*, para Cañas, E., Estévez, E., Marzo, J.C., y Piqueras, J.A. (2019, citado por Expósito, 2020), "características como el anonimato de los agresores o una mayor audiencia para la humillación, le otorgan identidad propia y puede acarrear consecuencias más negativas para quienes sufren las agresiones directas" (p.6).

Actualmente, en el marco de la violencia de género, el CP castiga en su artículo 147, apartado 1, al que:

---

[9] https://www.elespanol.com/mujer/actualidad/20220217/adolescentes-anos-proteccion-policial-sufrir-violencia-genero-delito/650935242_0.html

[10] https://www.europapress.es/epsocial/igualdad/noticia-observatorio-nacional-tecnologia-pide-considerar-violencia-genero-digital-ordenamiento-juridico-20220412173343.html

[11] Parlamento Europeo (2021). Report with recommendations to the Commission on combating gender-based violence: cyberviolence

[12] Consejo de Europa (2018). Mapping study on cyberviolence. Cybercrime Convention Committee (T-CY). Working Group on cyberbullying and other forms of violence, especially against women and children

por cualquier medio o procedimiento, causare a otro una lesión que menoscabe su integridad corporal o su salud física o mental, (...), siempre que la lesión requiera objetivamente para su sanidad, además de una primera asistencia facultativa, tratamiento médico o quirúrgico (p.27115).

En la comisión de este hecho resulta un tipo agravado atendiendo al resultado causado o riesgo producido, si la víctima "fuere menor de catorce años o persona con discapacidad necesitada de especial protección" (p. 68710), o la víctima fuere o hubiere "sido esposa, o mujer que estuviere o hubiere estado ligada al autor por una análoga relación de afectividad, aun sin convivencia" (p. 42174).

Otros preceptos penales para debemos destacar en materia de violencia de género, son los siguientes artículos:

a) artículo 153, que lo comete: el que por cualquier medio o procedimiento causare a otro menoscabo psíquico o una lesión de menor gravedad de las previstas en el apartado 2 del artículo 147, o golpeare o maltratare de obra a otro sin causarle lesión, cuando la ofendida sea o haya sido esposa, o mujer que esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia, o persona especialmente vulnerable que conviva con el autor (pp. 27115-27116).

b) artículos 171, apartado 4, y 172, apartado 2, respectivamente, que lo comete "el que de modo leve amenace o coaccione a quien sea o haya sido su esposa, o mujer que esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia" (pp. 42174-42175).

d) artículo 173, apartados 2 y 4, que lo comete "el que habitualmente ejerza violencia física o psíquica, o cause injuria o vejación injusta de carácter leve sobre quien sea o haya sido su cónyuge o sobre persona que esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia, así como quienes se dirijan a otra persona con expresiones, comportamientos o proposiciones de carácter sexual que creen a la víctima una situación objetivamente humillante, hostil o intimidatoria, sin llegar a constituir otros delitos de mayor gravedad. (...) (pp. 124239-124240).

Como hemos podido observar, desde una perspectiva político criminal podemos decir que se encuentra a faltar en nuestro ordenamiento jurídico, un desarrollo más amplio de la violencia de género digital que se plasme en determinados preceptos penales que

puedan abarcar otras casuísticas en este ámbito para que puedan ser perseguibles conforme a derecho.

Por último, y dentro del ámbito de la ciberviolencia por razón de sexo y/o género, en su caso, debemos hacer mención del artículo 510 del CP que castiga entre otras conductas a:

> quienes públicamente fomenten, promuevan o inciten directa o indirectamente al odio, hostilidad, discriminación o violencia contra un grupo, una parte del mismo o contra una persona determinada por razón de su pertenencia a aquél, por motivos racistas, antisemitas, antigitanos u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, aporofobia, enfermedad o discapacidad (p. 98068).

II.6 Responsabilidad del menor.

Los menores de edad están sujetos a diversas responsabilidades tales como la disciplinaria ejercida por la dirección del centro educativo donde estudie el o la menor, así como la administrativa, la civil y la penal, en su caso. No obstante, por el objeto de este estudio, y dado que nos interesan las acciones que puedan llevar a cabo los menores en el ámbito de la cibercriminalidad social, nos centraremos en la responsabilidad penal y civil de los menores.

II.6.1 Responsabilidad penal del menor.

Actualmente, la responsabilidad penal de los menores se aplica al rango etario de entre 14 a 18 años de edad, como consecuencia de la comisión de delitos que se contemplen en el Código Penal (CP, en adelante) así como en leyes especiales, se encuentra expresamente regulada en la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores (LORPEM, en adelante), que contiene medidas específicas a imponer a los menores que delinquen, en lugar de las penas que se recogen para personas mayores de edad en el CP.

En el supuesto de que el ilícito penal haya sido cometido por un menor de 14 años, la LORPEM en su artículo 3, contempla que no se le exigirá responsabilidad penal, sino que le serán de aplicación "las normas sobre protección de menores previstas en el Código Civil y demás disposiciones vigentes" (p.1426).

Desde una perspectiva policial la Instrucción 1/2017, de la Secretaría de Estado

de la Seguridad por la que se actualiza el protocolo de actuación policial con menores contempla que: "la intervención policial con menores de edad inferior a catorce años en el ámbito penal, infractores o no, será siempre de carácter protector administrativo" (p.6).

No obstante, la Ley de Enjuiciamiento Criminal (LECrim, en adelante) en su artículo 100 establece que: "de todo delito o falta nace acción penal para el castigo del culpable, y puede nacer también acción civil para la restitución de la cosa, la reparación del daño y la indemnización de perjuicios causados por el hecho punible" (p.861). Pero ¿Significa este precepto que no en todos los delitos se deriva responsabilidad civil? Efectivamente, puesto que para que nazca la responsabilidad civil derivada del delito tiene que haberse producido un daño, que en la casuística que nos ocupa, es decir, en el ámbito de la cibercriminalidad social, podríamos hablar, principalmente, de daños psíquicos y físicos, en su caso, a menores de edad.

II.6.2 Responsabilidad civil del menor.

La responsabilidad civil de un o una menor por la comisión de una infracción penal, en su caso, será tramitada en pieza separada y ejercitada por el Ministerio Fiscal, en virtud de lo establecido en los artículos 61 a 64 de la LORPEM, excepto en los siguientes casos: renuncia del perjudicado a la responsabilidad civil, ejercicio de la responsabilidad por el propio perjudicado y reserva de la acción por el perjudicado para ejercitarla por el Ministerio Fiscal según los preceptos del Código Civil y de la Ley de Enjuiciamiento Civil (pp. 1439-1440).

En este orden de cosas, hay que destacar que el artículo 61 de la LORPEM, establece que:

> cuando el responsable de los hechos cometidos sea un menor de dieciocho años, responderán solidariamente con él de los daños y perjuicios causados sus padres, tutores, acogedores y guardadores legales o de hecho, por este orden. Cuando éstos no hubieren favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada por el Juez según los casos (p.1439).

En este sentido, ¿Podríamos decir que es objetiva la responsabilidad solidaria mencionada? A mi entender sí que lo es puesto que se basa tanto en negligencias educativas, así como en el control y vigilancia del menor, es decir, que los padres y tutores responderán por culpa in educando y por culpa *in vigilando*, en su caso. Dichas responsabilidades las contempla el Código Civil (CC, en adelante) en su artículo 1903

que establece que “los padres son responsables de los daños causados por los hijos que se encuentren bajo su guarda y los tutores lo son de los perjuicios causados por los menores que están bajo su autoridad y habitan en su compañía” (pp.310-311).

No obstante, lo anterior no es óbice para que los padres y tutores puedan exonerarse de responsabilidad si acreditan que emplearon toda la diligencia exigible para prevenir el daño.

II.7 Responsabilidad penal de los profesores.

En el supuesto de que un profesor o profesora sea sabedor o conozca de la situación sufrida por un menor a su cargo y no realice ninguna acción para que cese, podría incurrir en un delito tipificado en el artículo 450.2 del C.P. (omisión de los deberes de impedir delitos o de promover su persecución), o un delito del artículo 195 del C.P. (omisión del deber de socorro), en su caso. De hecho, este deber de comunicación cualificado se contempla en la LOPINFAVIO en su artículo 16 a los profesores y profesoras, entre otras personas que, por razón de su cargo, profesión, oficio o actividad, tengan encomendada la asistencia, el cuidado, la enseñanza o la protección de niños, niñas o adolescentes, en su caso, y:

> tuvieran conocimiento o advirtieran indicios de la existencia de una posible situación de violencia de una persona menor de edad, deberán comunicarlo de forma inmediata a los servicios sociales competentes.
>
> Además, cuando de dicha violencia pudiera resultar que la salud o la seguridad del niño, niña o adolescente se encontrase amenazada, deberán comunicarlo de forma inmediata a las Fuerzas y Cuerpos de Seguridad y/o al Ministerio Fiscal.
>
> (…) O adviertan una posible infracción de la normativa sobre protección de datos personales de una persona menor de edad, deberán comunicarlo de forma inmediata a la Agencia Española de Protección de Datos” (pp. 68675-68676).

II.8 Responsabilidad civil de los centros docentes de enseñanza no superior.

En primer lugar, respecto a la responsabilidad civil el CC en sus artículos 1903 y 1904, establece que:

> las personas o entidades que sean titulares de un Centro docente de enseñanza no superior responderán por los daños y perjuicios que causen sus alumnos menores de edad durante los períodos de tiempo en que los mismos se hallen bajo el control o vigilancia del profesorado del Centro, desarrollando actividades escolares o

extraescolares y complementarias (p.311).

Asimismo, los titulares de los Centros docentes citados, "podrán exigir de los profesores las cantidades satisfechas, si hubiesen incurrido en dolo o culpa grave en el ejercicio de sus funciones que fuesen causa del daño" (p.311).

Seguidamente, cabe mencionar la responsabilidad patrimonial de los centros docentes públicos, que a tenor de lo establecido en los artículos 32 y siguientes de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que:

> los particulares tendrán derecho a ser indemnizados por las Administraciones Públicas correspondientes, de toda lesión que sufran en cualquiera de sus bienes y derechos, siempre que la lesión sea consecuencia del funcionamiento normal o anormal de los servicios públicos salvo en los casos de fuerza mayor o de daños que el particular tenga el deber jurídico de soportar de acuerdo con la Ley (p.89437).

Es decir, que para generarse dicha responsabilidad es necesario que como consecuencia del funcionamiento de la Administración se cause un daño y exista un nexo causal.

II.9 Perfiles cibercriminales y de cibervictimización sociales.

En el ámbito de la cibercriminalidad social no podemos establecer un único perfil del agresor o victimario puesto que la motivación delictiva es diferente o varía de unos delitos a otros.

Comenzaremos por una de las definiciones, entre otras, de perfil que contempla el Diccionario de la RAE siendo, concretamente, la siguiente: "conjunto de rasgos peculiares que caracterizan a alguien o algo" (RAE, 2020).

No obstante, Vicente Garrido (2012) define el perfil criminal como: "disciplina de la ciencia forense que se ocupa de analizar las huellas del comportamiento en una escena del crimen con objeto de proveer información útil a la policía para la captura de un delincuente desconocido" (p.20).

Si analizamos la definición referenciada, observamos un concepto importante a tener en cuenta, "escena del crimen", que para la casuística que no ocupa, sería el ciberespacio. En la escena del crimen, hemos de observar tanto el modus operandi como la firma del delincuente.

Para Vicente Garrido (2012), en su planteamiento de la definición genérica del

modus operandi señala que:

> la manera de comportarse un criminal lo constituyen sus elecciones y conductas por las que pretende consumar un delito. El modus operandi se refiere al cómo del delito. Esto es diferente del porqué del delito o motivación del delincuente, lo que se conoce como firma del delincuente (p.21).

En este sentido, el modus operandi de una persona que ciberacosa a otra, en sus diversas modalidades, con o sin implicación de otras personas en connivencia, ya sea compartiendo o difundiendo fotos y/o vídeos de carácter íntimo en redes sociales, reenviando emails con programas malignos (*malware*), etc., constituiría el cómo del delito.

Por lo que respecta, a la firma podríamos decir que, en términos generales, sería el ánimo de infligir o causar un daño psicológico a la víctima ya sea por diversión, despecho, motivos sentimentales, etc., aunque también podría buscar satisfacer una parafilia como es el caso de la pedofilia a través del *child grooming* u *online grooming*. (el porqué del delito).

Para Miró (2012) los perfiles criminales de los tres ciberdelitos sociales más llamativos es el siguiente:

1º) el *cybergroome*r: Internet ha supuesto un cambio tanto en el modus operandi de hacer grooming como en el perfil criminal del que comete el ilícito penal puesto que:

> Internet, en este sentido, es un vehículo utilizado por muchos sujetos para vencer el aislamiento social y comunicarse con otros. En segundo lugar, Internet aumenta el número potencial de víctimas a las que puede acceder un agresor. Además, Internet permite que el agresor realice una investigación del perfil de la víctima antes de decidir quién puede ser más vulnerable al ataque (Wolak, J; Finkelhor, D.; Mitchell, K.J., e Ybarra, M.L., 2010; citado por Miró, 2012).

En este orden de cosas, tenemos que destacar que según un estudio de Young (2005):

> las conductas sexuales *online* las ejecuta el agresor en el ambiente familiar y cómodo en casa o la oficina, lo que reduce la sensación de riesgo y permite incluso los comportamientos más aventureros (…) el ciberabusador que realiza grooming en los chats deriva sus fantasías sexuales de los desórdenes psicológicos motivados por la necesidad de escapar de la soledad, de la dificultad de las

> relaciones personales, de su baja autoestima, por lo que sí es consciente del significado de su conducta y del daño que puede infligir (…) el sujeto que realiza *grooming* a través de Internet, muchas veces no tiene una intención real de llevar a cabo sus fantasías, sino que las hace públicas generalmente de forma descarada, sin importarle que otros miembros del chat puedan sentirse ofendidos, reconociendo en la gran mayoría de los casos, que se trata de varones de edad avanzada con deseos de realizar fantasías sexuales con menores, etc. (pp. 254-255, citado por Miró, 2012).

En conclusión, podemos decir tal y como afirma Miró (2012) que, según los estudios referenciados, la persona que utiliza Internet para ocasionar molestias y realizar proposiciones a menores de edad, no es un pedófilo como norma generalizada, puesto que su objetivo no son niños sino adolescentes con experiencias sexuales en su haber, y con predisposición a tener más.

2º) el *cyberstalker*: según los estudios llevados a cabo por Bocij y McFarlen (2003), el perfil de los *cyberstalker*s es el siguiente:

> suelen ser hombres (84,6% de los hombres frente a 15,4% de mujeres) con una edad media de 41 años, aunque el rango de edad puede variar de 18 a 67 años. Respecto al estado civil de los agresores, la mayoría suelen ser solteros (52,3%) aunque también se pueden dar en menor medida casos de agresores casados (21,7%) o que estén separados o divorciados (17,3%). Suelen tener conocimientos medios (41%) y altos o muy altos (50%) informáticos. Finalmente, respecto a la ocupación, laboral, un 50% tienen trabajo, un 18,2% están en el paro y un 8,3% son estudiantes (p.257, citado por Miró, 2012).

En el estudio reseñado realizado por Bocij y Mc Farlen (2003, citado por Miró, 2012) distinguen cuatro tipos de *cyberstalkers*, con características y objetivos diferenciados, siendo éstos los siguientes:

a) vengativo *(vindicative*). Es el tipo más violento que, generalmente, posee antecedentes penales, conocimientos avanzados en las TIC y con un amplio abanico de modus operandi para acosar a sus víctimas. Asimismo, los autores del estudio opinan como consecuencia de las evidencias halladas y análisis de los mensajes que los *cyberstalkers* vengativos remitieron a sus víctimas, que es más que probable que presentasen alguna tipología de enfermedad mental.

b) integrado (*composed*). Su objetivo no es mantener relaciones sentimentales con sus víctimas sino molestarlas, poseen conocimientos avanzados de Internet y no suelen tener antecedentes penales ni historial psiquiátrico previo.

c) intimo (*intimate*). Su objetivo es mantener relaciones sentimentales con sus víctimas empleando como modus operandi el contacto por vía correo electrónico y las webs de citas, en su caso. Su nivel de conocimientos en el manejo de Internet es variable, desde básicos o elementales hasta avanzados o altos, según el caso.

d) colectivo (*collective*). En esta tipología la víctima es acosada por dos o más personas con conocimientos avanzados en informática, a través de medios telemáticos empleando técnicas muy diversas para conseguir su objetivo.

3º) El *cyberbully*: para Mason (2008) existen dos clases de perfil de los *cyberbullies*: "los proactivos que cometen su acción para conseguir un fin, y los reactivos, que agreden como respuesta a una provocación, agresión o amenaza" (p.258, citado por Miró, 2012).

Desde la perspectiva estadística, en lo atinente al porcentaje de ciberagresores podemos decir que varían según los estudios realizados, aunque destacaremos el llevado a cabo en España por el Defensor del Pueblo (2007) que arrojó un resultado de un 5,4%.

Según Ortega, Calmaestra y Mora-Merchán (2008), con relación al sexo de los ciberagresores "la mayoría de los estudios indican que son los chicos quienes más involucrados están en este tipo de conductas" (pp.258-259, citado por Miró, 2012).

No obstante, para Calvete, Orue, Estévez, Villardón y Padilla (2010), en los cursos que más se registran casos de *cyberbullying* son en segundo y tercero de la ESO como sucede en el *bullying* tradicional u *offline* (p.259, citado por Miró, 2012).

Por otra parte, con relación a la autoestima de los ciberagresores, Calmaestra (2011) apunta que "tienen una autoestima más elevada que las víctimas" (p.191), en concordancia con lo que ya postulaba Olweus (2005) en el caso del *bullying* tradicional u *offline* donde:

> además de no presentar problemas de autoestima, siente una fuerte necesidad de dominar y someter a otros estudiantes, son impulsivos e iracundos, carecen de empatía, suelen ser desafiantes y agresivos con los adultos incluidos los padres y los profesores y suelen presentar otro tipo de conductas antisociales como el

vandalismo (p.260, citado por Miró, 2012).

Por último, hemos de destacar que según Walrave y Wannes (2011) existen determinados factores que pueden favorecer o potenciar, en su caso, cometer ciberacoso o *cyberbullying*, encontrándose entre ellos "tener una percepción favorable sobre este tipo de conductas, ser usuarios frecuentes de Internet, tener acceso a un ordenador privado y hacer uso de él en dependencias poco vigilados y tener conocimientos específicos sobre las TIC" (p.260, citado por Miró, 2012).

En este orden de cosas, no podemos olvidar el perfil de las víctimas de los cibercrímenes sociales, que podríamos diferenciar entre las víctimas adultas y las menores de edad. Pero por el objeto del presente estudio nos centraremos en el perfil de las víctimas menores de edad nativos digitales.

Partiendo del caso del *cyberbullying,* para Garaigordobil (2011) "el porcentaje de menores que dicen haber sufrido algún tipo de conducta está entre el 20% y el 50%, reduciéndose entre un 2% y un 7% cuando la violencia sufrida es severa" (p.284, citado por Miró, 2012).

Para Miró (2012), en cuanto a la variable sociodemográfica género, existen discrepancias entre los estudios realizados. De hecho, algunos estudios contemplan la tendencia de los chicos a ser victimarios o agresores y a las chicas víctimas. Sin embargo, otros estudios no encuentran diferencia alguna.

Algo similar ocurre con la edad, hay estudios como el de Kowalski y Limber (2007), en los que se ha podido demostrar que mayor edad mayor probabilidad de victimización. Por otra parte, también hay estudios que, a contrario sensu, como los de Slonje y Smith (2008), hallaron evidencias de mayor riesgo en la franja de edad entre los 12 y 15 años, respectivamente, y otros estudios como los de Smith et al. (2008) no encontraron relación alguna entre víctima y edad.

Sin embargo, existen estudios como el de Li (2007) que evidencian que haber sido ciberacosador incrementa la posibilidad de ser víctima en un 70%, comparativamente, con los estudiantes que nunca habían sido víctimas de ciberacoso. A contrario sensu, los estudiantes que habían sido víctimas de ciberacoso tenían menos probabilidades de ser ciberacosadores que los estudiantes que no lo habían sido.

Según los estudios realizados por algunos autores, otros factores que se asocian al

incremento del riesgo de cibervictimización son, entre otros, los siguientes:

a) para Li (2007), la frecuencia de acceso a Internet, desde la perspectiva del ciberacosador.

b) para Patchin e Induja (2006), la frecuencia de participación en actividades en línea.

c) para Juvonen y Gross (2008), la frecuencia de utilización de la mensajería instantánea y las webcams.

d) para Vandebosh y Van Cleemput (2009), tener unos padres poco implicados en Internet.

e) para Mitchell, Finkelhor y Wolak (2007), "la relación existente entre el anonimato que puede brindar Internet y la victimización por ciberacoso en el ámbito escolar" (citado por Miró, 2012).

f) para Wolak, Finkelhor, Mitchell e Ybarra (2008), realizar envíos directos de información personal a personas desconocidas.

Por último, en lo atinente al perfil de las víctimas de *grooming*, sobre la base del estudio realizado por Wolak et al. (2008), podemos destacar que "el 99% de las víctimas de intentos de ataques sexuales a través de Internet comprendía edades entre los 13 a los 17 años, quedando el 1% para las víctimas de 12 años" (p.113).

En conclusión, podemos observar cómo las actividades cotidianas de los menores juegan un papel primordial en su mayor o menor riesgo, en su caso, de victimización en el ciberespacio, y más concretamente, las asociadas a la privacidad, que para Miró (2012) "constituyen un elemento decisivo en la selección del agresor de la víctima del ciberataque" (p.288).

II.10 Protocolo de actuación e intervención ante supuesto de violencia escolar en la Comunidad Valenciana.

Actualmente, Orden 62/2014, de 28 de julio, de la Conselleria de Educación, Cultura y Deporte, por la que se actualiza la normativa que regula la elaboración de los planes de convivencia en los centros educativos de la Comunidad Valenciana y se establecen los protocolos de actuación e intervención ante supuestos de violencia escolar, contempla en sus anexos I y IV, un protocolo de actuación ante el acoso y/o ciberacoso, así como un protocolo de actuación ante una situación de violencia de género, respectivamente.

Pero, desde la perspectiva municipal, ¿Qué puede hacer un ayuntamiento para contribuir a la prevención, actuación e intervención protocolaria ante la detección de supuestos de violencia escolar en el ámbito del ciberacoso y/o la violencia de género, entre otras problemáticas?

Los ayuntamientos pueden contribuir aprovechando su potestad reglamentaria y de autoorganización que le atribuye el ordenamiento jurídico para aprobar una ordenanza en aras a proteger a los menores como han hecho otras poblaciones de la Comunidad Valenciana como por ejemplo Rafelbuñol (Valencia) a través de su Ordenanza de la Comisión de Protección a la Infancia y Adolescencia, publicada en el BOP de Valencia nº199, de fecha 14 de octubre de 2021.[13]

En la Ordenanza referenciada tomada como ejemplo se regulan, entre otras cosas, los ámbitos familiar, escolar y social de intervención con menores en el municipio de Rafelbuñol, la coordinación y colaboración entre las entidades públicas, incluyendo protocolos, así como el desarrollo de la figura del agente tutor.

En conclusión, desde una óptica criminológica preventiva, el ejemplo de Rafelbuñol debería ser tomado por muchas más poblaciones como es el caso de Vinaròs que carece de este tipo de Ordenanza municipal y que a mi parecer constituiría una herramienta de trabajo muy valiosa para prevenir, combatir e intervenir entre otras casuísticas, en aquellas relacionadas con el ciberacoso y violencia de género digital en el ámbito escolar, en su caso.

Pero ¿quiénes deben ser los agentes sociales que deben intervenir en la prevención

[13]file:///C:/Users/HOME/Downloads/Ordenan%C3%A7a%20protecci%C3%B3%20inf%C3%A0ncia%20i%20adolesc%C3%A8ncia%20cast.pdf

y detección de situaciones de riesgo?

Para Muñoz Ruiz (2016), "la lucha contra el acoso y el ciberacoso requiere la intervención conjunta y coordinada de distintas instancias: la familia, la comunidad educativa y los servicios de protección de menores" (p.84).

CAPÍTULO III: CIBERCRIMINALIDAD ECONÓMICA EN EL ÁMBITO DE LOS AUTÓNOMOS Y MICROPYMES DE LA CIUDAD DE VINAROS.

III.1 Concepto de cibercrimen económico.

> El cibercrimen económico es definido por Miró (2012) como:
> 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 un fraude, como otros que no son más que un acto preparatorio de los ciberataques defraudatorios finales" (p.301).

III.2 ¿Qué es un trabajador autónomo?

Su definición legal se contempla en la Ley 20/2007, de 11 de julio, del Estatuto del trabajo autónomo, como: "personas físicas que realicen de forma habitual, personal, directa, por cuenta propia y fuera del ámbito de dirección y organización de otra persona, una actividad económica o profesional a título lucrativo, den o no ocupación a trabajadores por cuenta ajena" (p.29968).

III.3 ¿Qué es una microempresa (micropyme)?

Para saber conforme a derecho que se entiende por microempresa o micropyme, nos hemos de dirigir al Reglamento (UE) nº 651/2014 de la Comisión, de 17 de junio de 2014, que la define como "una empresa que ocupa a menos de 10 personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los 2 millones de euros" (p.70).

III.4 Cibercriminalidad económica: características y tipologías.

Para Miró (2012), el cibercrimen económico abarca tanto a los ciberataques delictivos que afectan individualmente al patrimonio de personas como al sistema económico con relación a las transacciones comerciales por Internet y a otros bienes jurídicos como la intimidad, seguridad de los sistemas, etc., con la particularidad de que

todos ellos tienen un objetivo final común, es decir, la obtención de un beneficio económico.

Para poder conseguir dicho objetivo, los ciberdelincuentes necesitan realizar, previamente, una cadena de ciberataques distinguiéndose para ello, dos tipos de cibercrímenes económicos que Miró (2012) clasifica en "mediales o instrumentales, y económicos en sentido estricto, siendo los primeros actos preparatorios de estos últimos" (p.119). Ver tabla 4.

Tabla 4. *Tipos de cibercrímenes económicos.*

Cibercrímenes económicos mediales	*Hacking*
	Infecciones de *malware* destructivo
	Infecciones de *malware* intrusivo
	Envío de *spam*
	Spoofing e *identify theft*
	Uso de *spyware (sniffers, keyloggers)*
	Ataques Dos
Cibercrímenes económicos puros	*Phishing*
	Auction fraud (ciberfraudes)
	Scam
	Extorsión
	Revelación de secretos de empresa

Fuente: Miró (2012, p.119)

Del abanico de cibercrímenes económicos referenciados, comenzaremos en primer lugar por saber, ¿qué se entiende por *hacking*?

Sedeño (2017) lo define como "conjunto de acciones que garantizan y permiten acceder ilegalmente a determinados sistemas informáticos o programas, vulnerando las medidas de seguridad" (p.32)

En este sentido, podemos distinguir dos tipos o clases de *hacking*, el *white hat hacking* y el *black hat hacking*, respectivamente.

El primero, también conocido como hacking blanco (Miró, 2012) tiene como objetivo "acceder al sistema o a sus datos e información, pero sin ningún propósito de sabotaje o utilización posterior de la información" (p.54).

El segundo también conocido como *cracking* tiene por objetivo "realizar cualquier tipo de daño al sistema, a los elementos que él contiene, o a su titular al adquirir, eliminar o modificar información del mismo" (p.54).

No obstante, el *hacking* se encuentra tipificado en nuestro CP, concretamente, en su Título X, capítulo I que lleva por rúbrica "del descubrimiento y revelación de secretos", artículos 197 a 201, castigándose, entre otros supuestos, al que:

> a) para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación.
>
> b) se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.
>
> c) sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero (pp. 27124-27125).

Asimismo, es necesario matizar que el CP también castiga en su artículo 197 ter, el desarrollo y adquisición de software de *hacking* para cometer alguno de los delitos reseñados.

Por otra parte, el CP en sus artículos 248 y 249[14], respectivamente, contempla, en términos generales, cualquier tipo de estafa o ciberestafa, abarcando por consiguiente los delitos tecnológicos de *phishing*, suplantaciones de identidad, *scam*, estafas piramidales, etc.

Concretamente, el artículo 249 castiga en su apartado 1.a), la manipulación de sistemas informáticos con el fin de cometer ciberestafas como el *pharming* cuyo modus operandi según Sedeño (2017) se caracteriza por "la manipulación del servidor DNS con

[14] Modificados por L.O. 14/2022, de 22 de diciembre, de transposición de directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la Unión Europea, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso.

el objetivo de conseguir que las páginas (web lícitas) que visitan los usuarios, no sean las verdaderas u originales, siendo imitaciones (web ficticia) creadas con la finalidad primordial de conseguir datos e información personal" (p.115), así como todas aquellas relacionadas con programas informáticos maliciosos o *malware* destinados a robar datos bancarios, u análogos.

El apartado 2. a) de dicho precepto indica expresamente que está penado fabricar, importar, obtener, poseer, transportar, comerciar, etc., en su caso, dispositivos, instrumentos o datos o programas informáticos destinados a la perpetración de estafas.

Por último, los apartados 1.b) y 2.b) del artículo referenciado, contemplan el uso fraudulento de tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo, como es la práctica del *skimming* o clonado de tarjetas de crédito directamente desde los cajeros de entidades bancarias, así como sus sustracción, apropiación o adquisición, en su caso, para la comisión de estafas.

En relación con los cibercrímenes económicos en sentido estricto o puro, es necesario que abordemos uno de los modus operandi habituales para la comisión de ciberestafas, es decir, el *phishing*.

Sedeño (2017) define el *phishing* como "tipo de estafa informática que utiliza la ingeniería social para conseguir unos enormes ingresos y ganancias, de manera ilícita e ilegal" (p.102).

Existen numerosas modalidades de *phishing* como es *vishing* y el s*mishing* que son muy parecidas, radicando la diferencia en que en el *phishing* los ciberdelincuentes envían un mensaje suplantando a una entidad legítima empleando el correo electrónico, redes sociales o aplicaciones de mensajería instantánea, en su caso. En el *vishing* los ciberdelincuentes utilizan las llamadas telefónicas para cometer la estafa y en el *smishing* emplean los SMS. No obstante, en el supuesto de que estas modalidades de ciberataque se centren en una persona en concreto estaríamos hablando de *spear phishing* (OSI, 2020).

Asimismo, tenemos que destacar que estos ciberataques basados en la ingeniería social "en ocasiones, traen consigo un enlace a una web fraudulenta, que ha podido ser suplantada, fingiendo ser un enlace legítimo, o bien se trata de un archivo adjunto malicioso para infectarnos con *malware*" (OSI, 2020, p.8).

Por último, tenemos que mencionar la tipificación penal consistente en ocasionar daños y/o destrucción de información de datos y sistemas de información, contemplada

en los artículos 264 y siguientes del CP, y lo comete el que "por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave" (p.27133).

Constituye un tipo agravado de este delito cuando los daños ocasionados fueran considerados de especial gravedad, afecten a numerosos sistemas informáticos, se dirijan contra servicios públicos vitales, infraestructuras críticas, o cuando se utilicen las credenciales de un tercero, entre otros.

También se contempla como delito en el artículo 264 ter del CP, la creación, adquisición o distribución de software destinado a realizar ataques contra equipos informáticos, así como la revelación de contraseñas a terceros con fines destructivos.

En este orden de cosas, desde la perspectiva del cibercrimen económico, debemos tener presente que los autónomos y las microempresas también están expuestos a sufrir ciberataques motivo por el que deben aprender a proteger sus recursos y tomar medidas preventivas de ciberseguridad puesto que también manejan datos sensibles de sus clientes y proveedores. Pero ¿por qué tipo de incidentes se pueden ver afectados?

Pues bien, en función de su origen según el INCIBE (2017), los incidentes se pueden clasificar en "errores y fallos no intencionados, ataques intencionados, desastres naturales y de origen industrial" (p.9). Ver tabla 5.

Tabla 5. *Tipos de incidentes en función de su origen.*

Errores y fallos no intencionados	-Errores de los usuarios, del administrador o de configuración. -Deficiencias en la organización. -Alteración de la información. -Introducción de información incorrecta. -Degradación de la información. -Destrucción de información. -Divulgación de información.
Ataques intencionados	-Manipulación de la configuración. -Suplantación de la identidad del usuario. -Abuso de privilegios de acceso. -Acceso no autorizado.

	-Interceptación de información (escucha). -Modificación de la información. -Introducción de falsa información. -Destrucción de información. -Divulgación de información. -Ingeniería social.
Desastres naturales	-Fuego (por un rayo). -Daños por agua (desbordamiento de un rio). -Otros desastres naturales (tornados).
Incidentes de origen industrial	-Fuego, agua. -Desastres industriales. -Contaminación mecánica o electromagnética. -Avería de origen físico o lógico. -Corte del suministro eléctrico.

Fuente: INCIBE (2017, p.10)

Para el INCIBE (2017), "la ciberseguridad afecta en mayor o menor medida a los negocios en función de su dependencia de la tecnología" (p.15), motivo por el que en función de la dependencia de las TIC (utilización de teléfono móvil, ordenador con conexión a internet, uso de programas informáticos, servicios en la nube, página web, tienda online, etc.) en el desarrollo de la actividad económica que lleven a cabo los autónomos y microempresas, en su caso, constituirá un factor a tener presente y que les permitirá analizar los riesgos a los que están expuestos (ver tabla 6).

Tabla 6. *Grado dependencia de las TIC de autónomos y microempresas.*

Grado dependencia TIC	Descripción
Bajo	Usan las TIC principalmente para la gestión diaria de las actividades internas del negocio.
Moderado	Dependen de las TIC para el desarrollo y lanzamiento de productos y servicios y para la comunicación con proveedores y clientes a través de Internet.
Alto	Las TIC son el pilar básico que permite el desarrollo del negocio en su totalidad.

Fuente: INCIBE (2017)

Otro factor para tener en cuenta por parte de los autónomos y microempresas es que deben proteger la información correspondiente al ejercicio de sus actividades económicas y todo aquello que la contiene, es decir, teléfonos móviles, ordenadores, memorias USB, discos, software, página web, tienda online, bases de datos de clientes, productos, contratos de trabajo, etc.

De hecho, el Consejo de Ministros con fecha 22 de marzo de 2022 aprobó un Plan Nacional de Ciberseguridad de cuyas principales actuaciones, entre otras, podemos destacar el impulso de la ciberseguridad de pymes, micropymes y autónomos, así como promover un mayor nivel de cultura de ciberseguridad.[15]

En este sentido, los regentes de los comercios, establecimientos públicos y microempresas, en su caso, deben tener presente que no toda la información mencionada tiene la misma importancia, razón por la que debe ser clasificada identificando los activos de información concretos de su negocio tanto la que tengan en formato digital como en otros formatos físicos, según sea información sensible o no, en su caso.

Pero ¿cómo podemos proteger la información independientemente de su formato?

Una opción sencilla sería guardando la información física bajo llave y la información lógica cifrada, puesto que, en caso de pérdida o sustracción de información sensible o crítica, así como la necesaria para el desarrollo del negocio, en su caso, podríamos correr el riesgo de que la información fuese utilizada para cometer ciberdelitos, ser vendida en la *Deep Web*, etc., sin perjuicio de poder sufrir una pérdida de competitividad, un deterioro de la imagen o reputación y/o ser sancionados por la Agencia Española de Protección de Datos.

Respecto a este último extremo, hay que destacar que la LOPDGDD en su artículo 73, contempla como falta grave "la falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del RGPD", así como "la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado, en su caso" (p.119831).

15 https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2022/refc20220329_corregidav02.aspx#ciberseguridad

En este orden de cosas, a mi juicio, dado que las cuantías pecuniarias de las sanciones son bastante elevadas es conveniente contratar un seguro de riesgos cibernéticos para proteger nuestro patrimonio si nuestro grado de dependencia tecnológica es moderado o alto, en su caso.

A colación, como ejemplo, podemos citar la sentencia nº188/2922, de 15 de febrero, de la Sala de lo Contencioso-Administrativo del Tribunal Supremo.[16]

III.5 Riesgos, vulnerabilidades y amenazas para los autónomos y microempresas.

Cada negocio tiene unas características y unos activos de información a proteger particulares por lo que la evaluación de riesgos puede variar de unas empresas a otras, es decir, una peluquería tendrá unos ciberriesgos diferentes a los de una asesoría jurídica en función de su grado de dependencia a las TIC.

En la tabla 7 podemos observar un listado de los principales riesgos existentes para la mayoría de los negocios, así como el impacto que ocasionan en éstos.

Tabla 7. *Principales riesgos y su impacto para autónomos y microempresas.*

Riesgo	Impacto
Robo de información privilegiada o esencial.	-Pérdida de ventaja competitiva / comercial.
Intrusiones en sistemas y acceso a información sensible o confidencial.	-Acceso a la información y los datos de mi negocio a través de intrusiones difíciles de detectar. -Exponer datos / información confidencial. -Impacto reputacional /pérdida de imagen.
No ser capaces de restaurar la situación después de un incidente (Resiliencia).	-Tener una situación desventajosa en un tiempo alargado acentúa el daño (más pérdidas por inactividad). No poder restaurar la situación debidamente pone en riesgo la

[16] https://confilegal.com/20220224-el-supremo-obliga-a-las-empresas-a-establecer-un-sistema-de-doble-verificacion-que-garantice-que-aceptaron-la-politica-de-privacidad/

https://amp.expansion.com/juridico/sentencias/2022/02/23/621683f7468aebd1178b456e.html#aoh=16457219801434&csi=0&referrer=https%3A%2F%2Fwww.google.com&amp_tf=De%20%251%24s

	continuidad de nuestra actividad, con la consiguiente pérdida económica y de imagen.
Estar expuesto a ciberdelincuentes.	-Pérdidas económicas por robo/fraude. -Impacto reputacional.
Ataques a la marca (redes sociales).	-Pérdidas de clientes. -Impacto reputacional.
Estar expuesto a un ciberataque de denegación de servicio.	-Interrumpir el servicio tanto interno como a cliente (pérdida de ventas). -Impacto reputacional. -Incumplimiento normativo o contractual y posibles sanciones.

Fuente: INCIBE (2017)

En este orden de cosas, a parte de los riesgos cibernéticos vistos, los autónomos y microempresas deben conocer cuáles son sus vulnerabilidades y las amenazas a las que se enfrentan en un mundo laboral cada vez más dependiente de las tecnologías conectado a internet. Para ello, en primer lugar, tendremos que saber qué significan ambos conceptos.

El INCIBE (2017) define vulnerabilidad en términos generales como: "una debilidad que puede poner en peligro la información y comprometer el buen desarrollo de nuestra actividad profesional" (p.32), y una amenaza como "todo elemento que aprovecha una vulnerabilidad para atentar contra la seguridad de un activo de información" (p.35), citando algunos ejemplos de tipos de vulnerabilidades como las que podemos observar en la tabla 8.

Tabla 8. *Tipos de vulnerabilidades por su origen.*

Tipo de vulnerabilidad	Descripción
Error en la gestión de recursos	Una aplicación permite que se consuman un exceso de recursos afectando a la disponibilidad de los mismos.
Error de configuración	Problema de configuración de software o de los servidores web. Este error puede provocar la inutilización de páginas web a través de ataques

	de denegación de servicio (DoS).
Validación de entrada	Fallo en la validación de datos introducidos en aplicaciones que puede ser una vía de acceso de un ataque.
Salto de directorio	Fallo en la depuración de un programa, en la validación de caracteres especiales que permite el acceso a directorios o subdirectorios no deseados.
Factor humano	Negligencias causadas generalmente por la falta de formación y concienciación. Ejemplo: apuntar las contraseñas en notas adhesivas.
Permisos, privilegios y/o control de acceso	Fallos en la protección y gestión de permisos que permiten el control de acceso.

Fuente: INCIBE (2017)

Una vez vistas las principales vulnerabilidades que podemos tener, ahora abordaremos las amenazas más habituales tanto externas como internas en el ámbito de los autónomos y microempresas, pudiendo citar, entre otras, las siguientes que podemos observar en las tablas 9 y 10, respectivamente.

Tabla 9. *Principales amenazas externas para autónomos y microempresas.*

Amenazas	Descripción
Malware	También llamado código malicioso, es el software diseñado para tener acceso a los sistemas informáticos específicos, robar información o interrumpir las operaciones del ordenador. Hay otros tipos de malware: como los virus, gusanos y troyanos, que se diferencian por la forma en que operan o se propagan.
Rasomware	Es un *malware* que bloquea o codifica los datos o funciones de los equipos a cambio de un pago para desbloquearlos.
Botnets	Es una red, automatizada y distribuida de ordenadores previamente comprometidos (infectados) que, controlados remotamente, realizan acciones maliciosas de forma simultánea, como el envío de *spam* o ataques de denegación de servicio distribuido (DDoS).
Exploit	Es un programa que aprovecha una vulnerabilidad de un sistema informático en beneficio propio. Los llamados exploit de día cero

	(*zero-day*) son aquellos que todavía no se han hecho públicos y, por tanto, no disponen de soluciones de seguridad que eviten la vulnerabilidad.
Ataques DoS y DDoS	Se entiende como denegación de servicio (DoS) a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. El ataque consiste en saturar con miles de peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso. Un método más sofisticado es el ataque de denegación de servicio distribuido (DDoS), mediante el cual miles de peticiones son enviadas, de forma coordinada desde varios equipos (pertenecientes a una *botnet*), que están siendo utilizados para este fin sin el conocimiento de sus legítimos dueños.
Phishing	Es un método de ataque que busca obtener información personal o confidencial de los usuarios a través de medios electrónicos (email, WhatsApp, mensajería instantánea, etc.) donde se intenta convencer a un usuario de que el autor es auténtico, pero con la intención de obtener información confidencial. Los mensajes de *phishing* han mejorado notablemente, cada vez son más sofisticados y personalizados. Lo más novedoso de este tipo de ataques es el uso combinado del correo electrónico y del teléfono. Se usa este engaño (llamado ingeniería social) para obtener información que de otra forma no facilitaríamos.

Fuente: INCIBE (2017)

Tabla 10. *Principales amenazas internas para autónomos y microempresas.*

Amenazas por agentes internos	Descripción
Malintencionados	Los usuarios internos malintencionados pueden ocasionar daños considerables por su capacidad de acceso interno a nuestro negocio o empresa como por ejemplo: empleados descontentos o despedidos cuyas credenciales no se han eliminado y si tenían permisos como administradores con privilegios.
Engañados	Los usuarios internos pueden ser engañados por

	terceros (ciberdelincuentes) para proporcionar datos o contraseñas que no deberían compartir.
Descuidados	Un usuario interno descuidado puede realizar acciones como, simplemente, presionar la tecla equivocada y borrar o modificar información esencial de manera no intencionada.

Fuente: INCIBE (2017)

En este orden de cosas, debemos tener presente que tanto las vulnerabilidades de nuestros negocios como las amenazas incrementarán el riesgo de que podamos ser víctima del cibercrimen económico, por lo tanto, ¿qué medidas preventivas podemos implementar para proteger los activos de información de nuestros negocios y minimizar su impacto en caso de ser víctima de un ciberincidente?

Siguiendo las recomendaciones de INCIBE (2017), podemos destacar, entre otras, las contempladas en el siguiente decálogo preventivo de medidas que podemos observar en la tabla 11.

Tabla 11. *Medidas preventivas de ciberincidentes.*

Medidas preventivas	Descripción
Antivirus	Usar antivirus en los ordenadores y teléfonos móviles.
Actualizaciones	Actualizar el sistema operativo, antivirus y aplicaciones de internet.
Formación de empleados.	Formar a los empleados y aumentar su nivel de concienciación en ciberseguridad.
Spam	No abrir spam y desecharlo de inmediato.
Contraseñas	Usar contraseñas seguras con mayúsculas, números y caracteres combinados.
Copias de seguridad	Realizar copias de seguridad de los archivos que no queramos perder y consideremos importantes.
Aplicaciones	Descargar sólo aplicaciones de confianza de lugares oficiales y con el consentimiento de la empresa.

Uso de conexiones	Utilizar únicamente conexiones bluetooth, wifi y función GPS cuando sea necesario.
Interactuación en redes sociales	Evitar contactar con personas de origen dudoso.
Tratamiento de la información sensible y/o personal	Velar por el buen uso de la información sensible y personal de la organización y sus empleados. Controlar su acceso y cifrar la información. Establecer protocolos de ciberseguridad.

Fuente: INCIBE (2017)

En este orden de cosas, teniendo en cuenta las medidas preventivas mencionadas en la tabla 11, ¿sería segura para una empresa utilizar contraseñas como "12345", "123456" o "123456789"? La respuesta es sencilla, y es que no al tratarse de contraseñas poco robustas y ser fácilmente *hackeables*, pero lamentablemente, según un estudio anual realizado por NordPass durante el año 2021, las contraseñas referenciadas fueron las más utilizadas.[17]

Para Paul Ducklin (2022) investigador principal de la empresa de ciberseguridad Sophos, debemos evitar el empleo de contraseñas demasiado fáciles y repetitivas, en su caso, y acostumbrarnos a utilizar gestores de contraseñas que nos proporcionaran contraseñas más seguras y robustas.

Por último, no podemos olvidar la inteligencia artificial que también es una herramienta utilizada por el cibercrimen para cometer estafas, a través de modus operandi tales como la suplantación de voz (*Vishing)*, la falsificación de imágenes y vídeos, en su caso, etc. De hecho, según Sandra de Pedro (2020) la startup Lyrebird durante el año 2019, consiguió desarrollar un algoritmo capaz de imitar la voz de cualquier persona e incluso aprender a hablar de la misma manera[18].

No obstante, no debemos demonizar los avances tecnológicos en el campo de la inteligencia artificial puesto que también pueden sernos útiles desde una perspectiva de la ciberseguridad ayudándonos a identificar vulnerabilidades e identificar riesgos, automatizando respuestas ante ciberamenazas y a recuperarnos ante ciberincidentes.[19]

[17] https://www.redseguridad.com/actualidad/dia-mundial-de-la-contrasena-casi-un-millon-de-espanoles-utiliza-la-combinacion-12345-como-contrasena_20220505.html
[18] https://gaptain.com/blog/inteligencia-artificial-la-nueva-arma-de-los-cibercriminales/
[19] https://www.realinstitutoelcano.org/analisis/la-ciberseguridad-y-su-relacion-con-la-inteligencia-artificial/

En síntesis, en aras de prevenir problemas presentes y futuros en el ámbito de la inteligencia artificial y protegernos, entre otros, del cibercrimen económico, en su caso, de manera que podamos ejercer sobre la misma un control de los ciberriesgos derivados, para González Rus (2022) tal y como contempla en su recensión del libro de Javier Valls Prieto, Inteligencia artificial, Derechos Humanos y bienes jurídicos, en concordancia con el contenido de dicha obra literaria, deja patente que, obligatoriamente, se "ha de contar con mecanismos de control técnico, autorregulaciones, regulación y control administrativo y, en último término, intervención penal" (p.7).

Precisamente, en el ámbito penal, según Morillas Fernández (2023) deberá concretarse quién deberá responder por "las consecuencias jurídicas derivadas de la actuación de un sistema de inteligencia artificial, debiendo recurrir a criterios que permitan verificar cómo y por qué se ha producido el fallo correspondiente o bien la existencia de una voluntad criminal" (p.79), en su caso.

Para ello, Valls Prieto (2022) considera en función de la relación y control existente respecto a la inteligencia artificial una responsabilidad derivada diferente que clasifica en tres grupos o niveles de imputación:

> El primero sería el compuesto por desarrolladores y fabricantes del producto que lo diseñan y mandan al mercado. El segundo estaría constituido por los profesionales que utilizan estos sistemas inteligentes para realizar una parte de su trabajo y que van a interaccionar con la máquina de forma diferente a como lo realizarían los desarrolladores de este. El tercer grupo lo constituirían los usuarios finales, en muchos casos consumidores del mismo (p.24).

III.6 Perfiles cibercriminales y de cibervictimización económicos.

En el marco de la cibercriminalidad económica, no hay un perfil exprofeso de cibercriminal tal y como postulan Pinguelo y Muller (2011) para los que "éstos adquieren distintas formas en su intento de robar, engañar y destruir" (p.121).

Los últimos estudios de perfilación criminal cifran entre los veinte y veinticinco años, la media de edad de los cibercriminales económicos, pudiendo pertenecer a cualquier estrato o clase social, y tener conocimientos básicos o elevados de informática, en su caso, ser estudiante en la universidad, no tener trabajo y poseer ordenador

constituyendo un blanco perfecto para las captaciones de las bandas organizadas que les ofrecen la oportunidad de ganar dinero fácilmente (Miró, 2012).

Según Miró (2012) podemos distinguir los siguientes perfiles de victimarios del cibercrimen económico:

a) Hackers-crackers: personas con conocimientos informáticos cuyo modus operandi consiste en acceder mediante las TIC de manera ilícita a sistemas o redes. La motivación del primero sería en esencia conseguir un reto tecnológico y del segundo cometer una actividad delictiva con la finalidad de obtener un beneficio económico. Pueden actuar tanto individualmente como colectivamente en bandas organizadas, en su caso. La línea divisoria entre ambos es muy fina, y en la práctica la traspasan habitualmente. No obstante, Miró (2012) destaca que, en la actualidad, los hackers-crackers "ya no son expertos informáticos, sino que también comienzan a realizar tales actividades usuarios, generalmente jóvenes, con conocimientos básicos de informática que aprovechan programas y aplicaciones sencillas para realizar sus incursiones (*scriptkiddies*) (p.236).

b) *Insiders*: Para INCIBE (2017) son empleados o exempleados, en su caso, así como personal temporal o proveedores que tienen a han tenido alguna relación con la empresa. Su motivación suele ser siempre similar: venganza, motivos financieros, etc., o simplemente pueden realizar acciones maliciosas por desconocimiento.

Pinguelo y Muller (2011) destacan que, aunque los ataques de los *insiders* son menos frecuentes que los externos, su porcentaje de conseguir con éxito sus objetivos es superior al pasar desapercibidos y tener acceso a la información de la organización o empresa.

c) Organizaciones criminales: Para Miró (2012), empíricamente, está demostrado que la mayoría de los ciberataques externos son ejecutados por grupos organizados de cibercriminales, de los que podemos diferencias dos grupos:

> Las organizaciones tradicionales (mafia siciliana, mafias rusas, tríadas chinas o yakuzas, etc.) que suman a sus múltiples actividades la realización de delitos por medio de Internet, y aquellas otras ciberbandas organizadas o conjunto de crackers que se organizan como grupo criminal y cuyo único ámbito de actuación es el ciberespacio (Miró, 2012, p.241).

d) Cibermulas: como señala Choo (2008), son colaboradores del cibercrimen, es decir, colaboradores necesarios o cómplices, en su caso, cuyo cometido consiste en remitir por medios seguros de transmisión como Wester Union o MoneyGram, los beneficios económicos de Internet a los autores del delito o a los responsables de los grupos organizados tradicionales, quedándose como contraprestación un porcentaje como ganancia corriendo el riesgo de ser detenidos (citado por Miró, 2012, p.244).

Por otra parte, en lo atinente a las víctimas del cibercrimen económico, pondremos nuestra atención en los autónomos y microempresas, así como en sus empleados, clientes y proveedores en su caso, al interactuar en las compraventas por Internet, páginas web, correo electrónico, etc.

En este sentido, según un estudio realizado por Prat, Holfreter y Reisig (2010), "realizar compras *online* incrementa la posibilidad de ser objetivo de un ciberfraude en un 377%" (p. 281).

Para Miró (2012) lo que incrementa el riesgo de ser una potencial cibervíctima económica no es la acción de comprar *online* en sí, sino lo que va supeditado a la misma, es decir, cuando al pagar online tecleamos nuestros datos bancarios personales.

En este orden de cosas, el INCIBE (2021) alertó a autónomos y microempresas con una nueva campaña de ciberestafas mediante la técnica del phishing que consistía en enviar por correo electrónico facturas falsas a clientes de Iberdrola suplantando su identidad, con el objeto de engañar y conseguir que abonasen una supuesta factura de la compañía eléctrica.

Por último, cabe destacar que por parte del Grupo de Delitos Tecnológicos de la Unidad Técnica de Policía Judicial de la Guardia Civil (2021), se alertó a través de los medios de comunicación para que tanto los regentes como los clientes de restaurantes, bares, etc., extremasen las precauciones ante una estafa consistente en suplantar los códigos QR de sus cartas de menú. Al parecer, los ciberdelincuentes pegan un código QR malicioso encima del auténtico u original del establecimiento con el objeto de obtener datos personales de sus víctimas. No obstante, para Ana Gómez (2022), responsable de cultura de seguridad del banco BBVA, esta estafa es una modalidad de phishing que es conocida como QRishing.

III.7 Los autónomos y micropymes en el marco de la Criminología Empresarial.

En primer lugar, debemos tener claro en *stricto sensu* ¿qué es la Criminología Empresarial?

Para Alejandro Zapata (2017) "es el área de la criminología encargada de intervenir en empresas o instituciones de la iniciativa privada con el objetivo de implementar estrategias preventivas del delito a fin de proteger su patrimonio" (p.25).

En este orden de cosas, la Criminología Empresarial o también conocida como Criminología Corporativa o Preventiva, en el ámbito de la esfera de la digitalización de los negocios, nos permitirá detectar y evitar ciberriesgos potenciales y también nos ayudará a orientarnos sobre qué políticas preventivas podemos implementar para evitar o reducir las posibilidades, en su caso, de ser cibervíctimas, puesto que la protección total en ciberseguridad no existe, tal y como postula Faustino (2021), *managing* director de Nexllence.[20]

En conclusión, las microempresas, regentes autónomos de establecimientos, comercios y otros pequeños negocios de la ciudad de Vinaròs, deben tener presente que ante los ciberriesgos que nos acechan, pueden contar con una aliada muy poderosa para protegerse, la Criminología Preventiva, Empresarial o Corporativa.

III.8 Responsabilidad por culpa *in vigilando* del empresario.

La culpa *in vigilando* empresarial se contempla en nuestro ordenamiento jurídico en el artículo 1903 con relación al artículo 1902 del Código Civil que establecen que:

> el que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado (...) no sólo por los actos u omisiones propios, sino por los de aquellas personas de quienes se debe responder (...) lo son igualmente los dueños o directores de un establecimiento o empresa respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones (pp. 310-311).

En este sentido, la digitalización de las microempresas y/o de los negocios que regentan los autónomos en la ciudad de Vinaròs ha de ser extensiva tanto a la prevención de riesgos como de ciberriesgos laborales, en su caso.

[20] https://revistas.eleconomista.es/digital/2021/septiembre/la-proteccion-total-en-ciberseguridad-no-existe-AJ8975398

Para Fernández Moreno (2020), director ejecutivo de 720º CH Riesgos, Consultora Integral de Riesgos, "debe considerarse de vital importancia para las Organizaciones la incorporación de la tecnología a la prevención, procedimientos y sistemas dotados de inteligencia que permita abordar la detección del riesgo de forma precoz y actuar proactivamente frente a él" [21]

Sin embargo, para INCIBE (2017) debemos tener presente que los empleados constituyen el eslabón más importante en ciberseguridad.[22]

En conclusión, para reducir o minimizar los ciberriesgos tanto las microempresas como los autónomos que regentan pequeños negocios en Vinaròs deberán cumplir con lo establecido en el artículo 19 de la Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales que establece que:

> en cumplimiento del deber de protección, el empresario deberá garantizar que cada trabajador reciba una formación teórica y práctica, suficiente y adecuada, en materia preventiva, tanto en el momento de su contratación, cualquiera que sea la modalidad o duración de ésta, como cuando se produzcan cambios en las funciones que desempeñe o se introduzcan nuevas tecnologías o cambios en los equipos de trabajo (...) (p.32597).

III.9 Plan de prevención del delito para autónomos y microempresas.

La adopción de medidas de cumplimiento normativo también conocidas como *compliance* penal, es obligatoria para todas las empresas, incluidas las microempresas y trabajadores autónomos. En estas dos últimas, el administrador y director de cumplimiento normativo o *compliance officer* suele ser una única persona, a tenor de lo establecido en el artículo 31 bis, apartado 3 del CP.

En este sentido, el artículo 31 bis del CP, apartado 2.1ª, contempla que el órgano de administración es quien ha de implantar el Plan de Prevención de Delitos. Dicho precepto, en su apartado 1.b), castiga a la empresa por la omisión del debido control, en su caso.

Por otra parte, la Circular 1/2016, de 22 de enero, sobre la responsabilidad penal

[21] https://prevencionar.com/2020/04/22/las-nuevas-tecnologias-y-la-responsabilidad-por-culpa-in-vigilando/
[22] https://www.incibe.es/protege-tu-empresa/blog/el-eslabon-mas-importante-ciberseguridad-tus-empleados

de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015, de la Fiscalía General del Estado, contempla en su apartado 5.1, que "en puridad, los modelos de organización y gestión o *corporate compliance programs* no tienen por objeto evitar la sanción penal de la empresa sino promover una verdadera cultura ética empresarial" (p.20).[23]

En este orden de cosas, entre sus conclusiones, concretamente en la 20ª, dicha Circular establece que:

> la cláusula de exención de la responsabilidad de la persona jurídica que incorpora el apartado 2 del art. 31 bis constituye una causa de exclusión de la punibilidad, a modo de excusa absolutoria, cuya carga probatoria incumbe a la persona jurídica, que deberá acreditar que los modelos de organización y gestión cumplían las condiciones y requisitos legales (p.33).

En virtud de los argumentos de derecho expuestos, podemos comprobar la importancia que tiene para las microempresas y trabajadores autónomos tengan un Plan de Prevención de Delitos porque el tamaño de la empresa no exime de que se tenga que cumplir con lo establecido en el ordenamiento jurídico.

Por lo que respecta a los delitos imputables a las personas jurídicas, la Circular reseñada, orientativamente, contempla entre otros de la parte especial del CP, los siguientes: el delito de descubrimiento y revelación de secretos y allanamiento informático del artículo 197 quinquies; estafas del artículo 251 bis; daños informáticos del art 264 quater; delitos de odio y enaltecimiento del artículo 510 bis, etc.

Por último, destacar que para garantizar la efectividad de la implantación del Plan de Prevención de Delitos en el seno de las microempresas y negocios de los trabajadores autónomos, según la guía *compliance* para pymes de la Confederación Canaria de Empresarios (2019), se deberá entregar copia del mismo a sus empleados así como otra información relevante, en su caso, con acuse de recibo, así como formarlos, periódicamente, "a las acciones que realicen o puedan ocasionar actividades delictivas en el seno de la empresa, dependiendo del departamento" (p. 69).

[23] https://www.boe.es/buscar/doc.php?id=FIS-C-2016-00001

PARTE II: ANÁLISIS EMPÍRICO DEL ESTUDIO CRIMINOLÓGICO

I. HIPOTESIS Y OBJETIVOS.

I.1 Hipótesis y objetivos estudio de cibercriminalidad social.

La primera parte del estudio tiene como objetivos generales, por una parte, realizar un análisis de los ciberriesgos sociales de los menores que cursan la ESO en los centros educativos públicos Instituto Leopoldo Querol e Instituto Sanchis y Vilaplana así como en los centros educativos concertados Nuestra Señora de la Divina Providencia y Nuestra Señora de la Consolación, respectivamente, de la ciudad de Vinaròs, desde una perspectiva criminológica como víctima y/o victimario, en su caso.; y por otra parte, determinar cuáles son las actividades de uso rutinario de las TIC que pueden incrementar o disminuir el riesgo de ser víctima de un ciberdelito.

Para alcanzar estos dos objetivos generales, se proponen los siguientes específicos:

a) identificar los factores de riesgo y de protección asociados al uso de las TIC para poder conocer ¿qué pasa?, ¿por qué pasa?, y ¿qué tenemos que hacer para que los menores aprendan a prevenir el cibercrimen y educadores y padres puedan protegerles de tal amenaza, en su caso?

b) analizar la relación existente entre las actividades de uso rutinario de las TIC con las distintas modalidades de ciberacoso.

c) conocer y analizar la frecuencia con la que protagonizan los menores participan que cursan la ESO determinados hechos o conductas relacionadas con las distintas modalidades de ciberacoso como víctima o victimario, en su caso.

d) analizar las variables sociodemográficas de los participantes.

e) conocer y analizar a quién comunicarían los menores participantes determinados hechos o conductas relacionadas con las distintas modalidades de ciberacoso, en el caso de observarlas y/o protagonizarlas como víctima o victimario, en su caso.

f) conocer y analizar qué actividades preventivas propondrían los menores participantes frente a determinados hechos o conductas relacionadas con las distintas modalidades de ciberacoso.

A partir de los planteamientos referenciados, se han formulado las siguientes cinco hipótesis, basadas en la teoría o enfoque de la oportunidad delictiva de Felson y Clarke (1998) de las actividades rutinarias o teoría de las actividades cotidianas de los menores que cursan la ESO en su interacción con las TIC en el ciberespacio.

La primera de las hipótesis está basada en que los menores que dedican más tiempo en sus actividades diarias a Internet, redes sociales, envío de WhatsApp, emails, juegos online, utilización de webcam, etc., tienen mayor probabilidad de ser víctimas, sin perjuicio de las tecnoadicciones que puedan adquirir, en su caso, y repercusión en la salud que puedan tener.

En lo atinente a las tecnoadicciones hay que destacar que la Comunidad de Madrid ha sido pionera en poner en funcionamiento el primer centro público para tratar adicciones a las nuevas tecnologías tanto a menores de edad (de 12 a 17 años) como personas adultas mayores de 18 años. Dicho centro, se llama Centro Integral de Prevención e Investigación en Adicciones Comportamentales, AdCom Madrid, y se encuentra en el hospital público Gregorio Marañón.[24]

Por lo tanto, la formulación de la primera hipótesis sería la siguiente:

1ª) la probabilidad de riesgo de cibervictimización de los menores aumenta cuando la frecuencia de interacción con las TIC en Internet es mayor.

La segunda de las hipótesis se encuentra relacionada con la privacidad en el ciberespacio, es decir, sobre la base de la asociación del incremento del riesgo de cibervictimización con la acción de realizar envíos directos de información personal, fotos, vídeos, etc., a personas desconocidas o conocidas, en su caso, en Internet.

De manera que, la formulación de la segunda hipótesis sería la siguiente:

2ª) la probabilidad de riesgo de cibervictimización de los menores aumenta cuando la frecuencia de envíos directos de información personal, fotos, vídeos, etc., a personas desconocidas o conocidas, en su caso, en Internet.

La tercera de las hipótesis se basa en las respuestas a la pregunta de a quién comunicarían los menores participantes determinados hechos o conductas relacionadas con las distintas modalidades de ciberacoso, en el caso de observarlas y/o protagonizarlas

[24] https://www.mujerymadrehoy.com/primer-centro-publico-para-tratar-las-adicciones-a-las-nuevas-tecnologias/

como víctima o victimario, en su caso, y su relación con la probabilidad de riesgo de cibervictimización, puesto que juegan un papel muy importante en poner freno al ciberacoso.

Siguiendo este postulado, la tercera hipótesis quedaría formulada de la siguiente manera:

3ª) la probabilidad de riesgo de cibervictimización de los menores aumenta si para ellos carecen de importancia o normalizan, en su caso, determinadas conductas relacionadas con las distintas modalidades de ciberacoso que puedan observar y/o protagonizar como víctima o victimario, en su caso.

La cuarta hipótesis está basada en las respuestas a la pregunta sobre qué actividades preventivas propondrían los menores participantes frente a determinados hechos o conductas relacionadas con las distintas modalidades de ciberacoso, y su relación con la probabilidad de riesgo de cibervictimización, puesto que juegan un rol vital en poner freno al ciberacoso.

Siguiendo este postulado, la cuarta hipótesis quedaría formulada de la siguiente manera:

4ª) la probabilidad de riesgo de cibervictimización de los menores aumenta si para ellos carecen de importancia o normalizan, en su caso, determinadas conductas relacionadas con las distintas modalidades de ciberacoso que se puedan prevenir, en su caso, con su interacción para ponerle freno.

La quinta hipótesis está basada en la relación existente entre el control y vigilancia parental de los menores y la probabilidad de riesgo de cibervictimización en situaciones tales como tener el ordenador ubicado en su habitación donde el control de los padres será menor o en una zona común de la casa donde puedan estar más supervisados, en su caso.

Siguiendo este postulado, la quinta hipótesis quedaría formulada de la siguiente manera:

5ª) la probabilidad de riesgo de cibervictimización de los menores aumenta si el control parental es menor en la supervisión de sus interacciones con las TIC.

I.2 Hipótesis y objetivos estudio de cibercriminalidad económica.

La segunda parte del estudio tiene como objetivos generales, por una parte, realizar un análisis de los ciberriesgos laborales y económicos, en su caso, a los que están expuestos los autónomos, regentes de comercios y establecimientos públicos, así como micropymes de la ciudad de Vinaròs, de manera que podamos averiguar la probabilidad y/o riesgo que tienen de ser víctimas de la cibercriminalidad económica desde una perspectiva conjunta o global con relación a los 100 participantes de la muestra; y por otra parte, determinar cuáles son las actividades de uso rutinario de las TIC que pueden incrementar o disminuir el riesgo de ser víctima de un ciberdelito económico, la importancia de poseer o no, en su caso, conocimientos de ciberseguridad, así como determinadas conductas realizadas en el ámbito del ciberespacio, que nos permita poder identificar factores de riesgo y de protección, en su caso.

Para alcanzar estos dos objetivos generales, se proponen los siguientes específicos:

a) identificar los factores de riesgo y de protección asociados al uso de las TIC para poder conocer ¿qué pasa?, ¿por qué pasa?, y ¿qué deberían hacer los autónomos, regentes de comercios y establecimientos públicos, así como micropymes de la ciudad de Vinaròs para aprender a prevenir el cibercrimen económico y protegerse de tal amenaza, en su caso?

b) analizar la relación existente entre las actividades de uso rutinario de las TIC y la mayor o menor probabilidad de riesgo de cibervictimización económica, en su caso, de los autónomos, regentes de comercios y establecimientos públicos, así como micropymes de la ciudad de Vinaròs.

c) conocer y analizar la frecuencia con la que los autónomos, regentes de comercios y establecimientos públicos, así como micropymes de la ciudad de Vinaròs, protagonizan determinados hechos o conductas relacionadas con un mayor o menor riesgo de cibervictimización económica, en su caso.

d) analizar las variables sociodemográficas de los participantes.

e) conocer y analizar los conocimientos de los autónomos, regentes de comercios y establecimientos públicos, así como micropymes de la ciudad de Vinaròs, sobre diversas tecnologías biométricas aplicadas a la ciberseguridad con el fin de proteger la

información confidencial de teléfonos móviles, ordenadores, tabletas, etc.

A partir de los planteamientos referenciados, se han formulado las tres siguientes hipótesis, basadas en la teoría o enfoque de la oportunidad delictiva de Felson y Clarke (1998) de las actividades rutinarias o teoría de las actividades cotidianas de los autónomos, regentes de comercios y establecimientos públicos, así como micropymes de la ciudad de Vinaròs, en su interacción con las TIC en el ciberespacio.

La primera de las hipótesis está basada en que los autónomos, regentes de comercios y establecimientos públicos, así como micropymes de la ciudad de Vinaròs que se encuentren más digitalizadas y por ende, dediquen más tiempo en sus actividades diarias a interactuar en Internet, redes sociales, envío de WhatsApp, emails, etc., tienen mayor probabilidad de ser víctimas, sin perjuicio de las tecnoadicciones que puedan adquirir, en su caso, y repercusión en la salud que puedan tener.

Por lo tanto, la formulación de la primera hipótesis sería la siguiente:

1ª) la probabilidad de riesgo de cibervictimización de los autónomos, regentes de comercios y establecimientos públicos, así como micropymes de la ciudad de Vinaròs aumenta cuando mayor es su digitalización y mayor es la frecuencia de interacción con las TIC en Internet.

La segunda de las hipótesis se encuentra relacionada con la seguridad de la información en ordenadores, tabletas, teléfonos móviles, pendrives, etc., con conexión a Internet, es decir, sobre la base de la asociación del incremento del riesgo de cibervictimización económica con la perdida, sustracción o infección por *malware*, en su caso, de información confidencial y/o sensible, contenida en dispositivos como los reseñados, por parte de los autónomos, regentes de comercios y establecimientos públicos, así como micropymes de la ciudad de Vinaròs.

De manera que, la formulación de la segunda hipótesis sería la siguiente:

2ª) la probabilidad de riesgo de cibervictimización económica de los autónomos, regentes de comercios y establecimientos públicos, así como micropymes de la ciudad de Vinaròs, aumenta cuando mayor es la frecuencia de perdida, sustracción o infección por *malware*, de información confidencial y/o sensible, en su caso, contenida en dispositivos como ordenadores, teléfonos móviles, pendrives, etc.

La tercera de las hipótesis se basa en el seguimiento de pautas recomendadas de

ciberseguridad como: utilizar los servicios de almacenamiento en la nube, realizar copias de seguridad, cifrar la información confidencial, cuidado de la imagen digital, etc., por parte de los autónomos, regentes de comercios y establecimientos públicos, así como micropymes de la ciudad de Vinaròs, en sus interacciones con las TIC en las actividades cotidianas de administración, gestión y relación con clientes, proveedores, etc.

Siguiendo este postulado, la tercera hipótesis quedaría formulada de la siguiente manera:

3ª) la probabilidad de riesgo de cibervictimización económica de los autónomos, regentes de comercios y establecimientos públicos, así como micropymes de la ciudad de Vinaròs aumenta si no realizan en sus actividades cotidianas, un seguimiento de determinadas pautas recomendadas de ciberseguridad, carecen de conocimientos para ello, o no les dan importancia, en su caso, a determinadas conductas en su interacción con las TIC.

II. MÉTODO.

II.1 Muestra estudio cibercriminalidad social.

La muestra del estudio está compuesta por 436 menores de una población total de 1.243 alumnos de la ESO, de los cuales 198 son chicos (45%) y 238 son chicas (55%), de edades comprendidas entre los 11 y los 17 años, todos ellos alumnos de los cursos de 1º a 4º de la ESO de los cuatro centros que participaron en el estudio. El único criterio de exclusión ha sido la negativa a participar en el estudio.

Los resultados arrojados han aportado evidencias empíricas sobre el ciberriesgo existente para los menores que cursan la ESO en la ciudad de Vinaròs, de ser víctima o victimario, en su caso, de la cibercriminalidad social.

II.2 Muestra estudio cibercriminalidad económica.

Para poder realizar el estudio, se han entrevistado un total de 130 comercios o establecimientos públicos y/o micropymes, en su caso, de aproximadamente un total de 575 de actividades económicas de comercios tradicionales, establecimientos públicos y/o micropymes de Vinaròs. El único criterio de exclusión ha sido la negativa a participar en el estudio, participando finalmente 100 de ellos.

Los resultados obtenidos han aportado evidencias empíricas sobre el ciberriesgo existente para los regentes de los establecimientos públicos y del comercio tradicional,

así como de micropymes de la ciudad de Vinaròs, de ser víctima de la cibercriminalidad económica.

Las diversas actividades económicas desarrolladas por los 100 participantes de la muestra, las podemos observar en la Figura nº8.

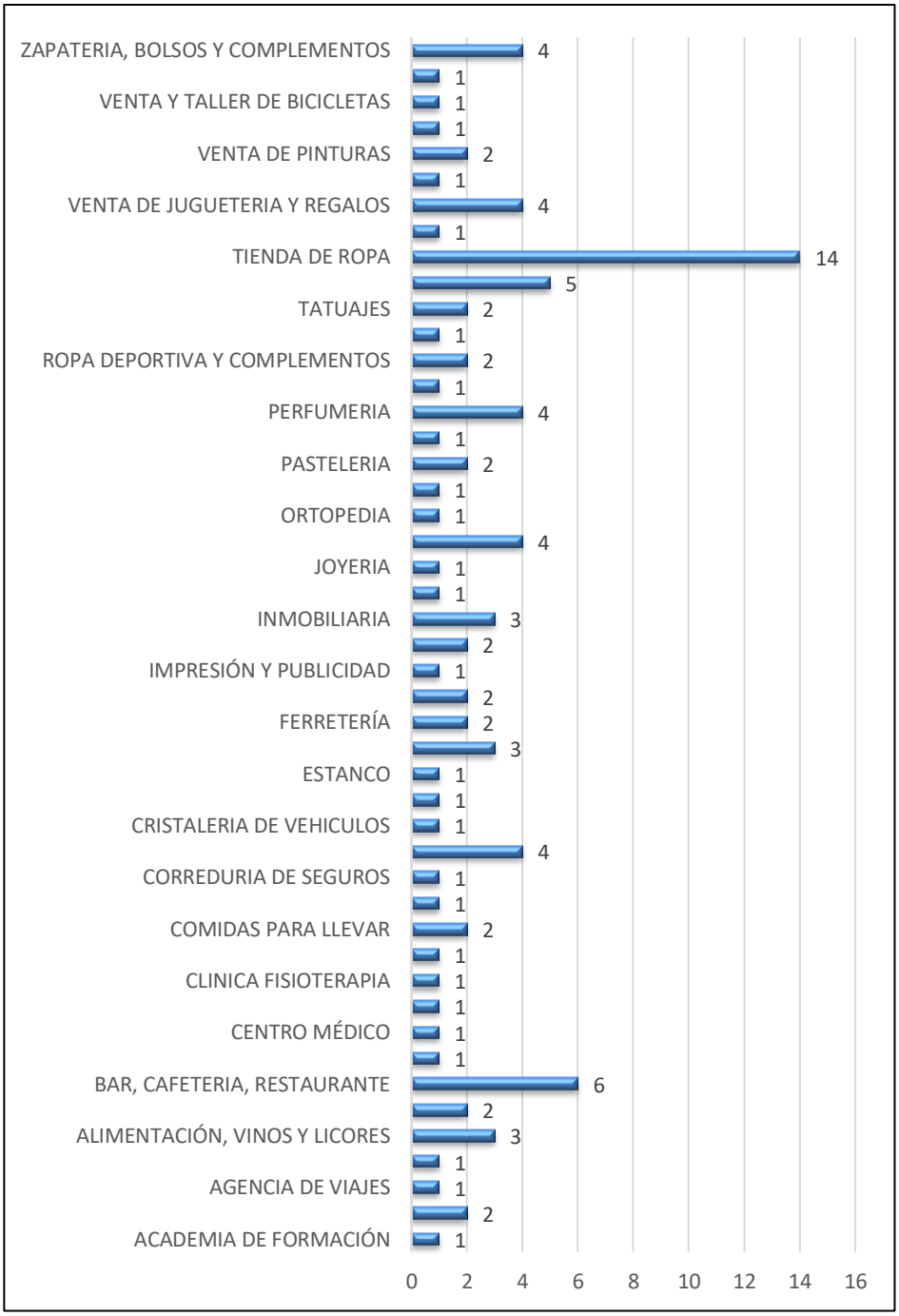

Figura 8. Actividades económicas de los participantes en la muestra

II.3. Material estudio cibercriminalidad social.

Para la primera parte del estudio se ha empleado una encuesta voluntaria, individual y anónima de victimización *ad hoc* como instrumento de elaboración propia basado en parte, en el cuestionario de ciberbullying de Garaigordobil y Fernández-Tomé (2011) citado por González (2015), que se han pasado en horario escolar por parte del investigador entre los menores que cursan la ESO de los cuatro centros educativos siguientes: Colegio Nuestra Señora de la Consolación, Colegio Nuestra Señora Divina Providencia, IES José Vilaplana e IES Leopoldo Querol, respectivamente, con el objeto de determinar cuáles son las actividades de uso cotidiano de las TIC que pueden incrementar o disminuir el riesgo de ser víctima de cibercrímenes sociales.

En otras palabras, se pretende medir la cibercriminalidad que afecta a los menores adolescentes de Vinaròs, cómo identificar los factores de riesgo y de protección asociados al uso de las TIC para poder conocer qué pasa, por qué pasa y qué tenemos que hacer para que los jóvenes aprendan a prevenir el cibercrimen y los educadores y los padres puedan protegerles de tal amenaza.

En lo atinente a los datos obtenidos de los participantes, han sido tratados con confidencialidad y anonimato teniendo en cuenta lo establecido en la normativa vigente en materia de protección de datos de carácter personal.

Asimismo, por parte del investigador y a petición de los centros educativos objeto de estudio, se han impartido unas charlas informativas sobre *cyberbullying*, *online grooming*, *sexting*, *sextorsion* y violencia de género 2.0 (*cyberstalking)*, respectivamente, apoyadas con una presentación de PowerPoint, formulando determinadas preguntas al colectivo del alumnado del aula donde se impartía la charla, para comprobar si habían entendido lo conceptos básicos, los riesgos en la red y cómo prevenirlos, en su caso.

II.4 Material estudio cibercriminalidad económica.

Para la segunda parte del estudio se ha utilizado una encuesta voluntaria, individual y anónima de victimización *ad hoc* en la que se ha entrevistado por parte del investigador a los regentes de los comercios, establecimientos públicos y/o microempresas, en su caso, sobre interacción o hábitos de uso de las TIC y otros hábitos de actividades cotidianas, conocimientos de ciberseguridad, así como hechos o conductas realizados en el ámbito del ciberespacio, de manera que mediante la relación de las respuestas marcadas con una "X", poder identificar factores de riesgo y de protección, en

su caso.

En este sentido, el cuestionario reseñado, es un instrumento de elaboración propia basado en parte en el contenido de la guía de privacidad y seguridad en Internet de OSI (2016), así como en la encuesta que forma parte de la tesis doctoral de Guilabert (2014) de la Universidad de Murcia.

Por lo que respecta a los datos obtenidos de los participantes, han sido tratados con confidencialidad y anonimato teniendo en cuenta lo establecido en la normativa vigente en materia de protección de datos de carácter personal.

III. PROCEDIMIENTO.

III.1. Aplicación de la escala de valoración de riesgos de VIOGEN a la cibercriminalidad social.

Basándome en los niveles de riesgos de la Instrucción 4/2019, de la Secretaria de Estado de Seguridad, por la que se establece un nuevo protocolo para la valoración policial del nivel de riesgo de violencia de género (Viogén), he realizado un análisis de los ciberriesgos a los que están expuestos los menores de la ciudad de Vinaròs que cursan la ESO, así como de la probabilidad y/o riesgo que tienen de ser víctimas o victimarios, en su caso, de la cibercriminalidad social.

En este sentido, la Ley 4/2015, de 27 de abril, del Estatuto de la víctima del delito en su Disposición Final Primera, modifica la Ley de Enjuiciamiento Criminal (LECrim, en adelante) a efectos de la transposición de algunas de las disposiciones contenidas en la Directiva 2012/29/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos, y entre otros preceptos se modifica el artículo 282 de la LECrim que establece que:

> cuando las víctimas entren en contacto con la Policía Judicial, cumplirá con los deberes de información que prevé la legislación vigente. Asimismo, llevarán a cabo una valoración de las circunstancias particulares de las víctimas para determinar provisionalmente qué medidas de protección deben ser adoptadas para garantizarles una protección adecuada, sin perjuicio de la decisión final que corresponderá adoptar al Juez o Tribunal (p.36590).

No obstante, cabe matizar que la Policía Local es Policía Judicial al ser miembro

de las Fuerzas y Cuerpos de Seguridad a tenor de lo establecido en el artículo 2 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad (LOFCS, en adelante). En consecuencia, participa en el ejercicio de funciones de Policía Judicial en la forma establecida en el artículo 53.1 apartado e) en concordancia el artículo 29. 2 de la LOFCS.

Pero ¿Qué entendemos por Policía Judicial? Si acudimos a nuestra Carta Magna y leemos que dice su artículo 126, podríamos definirla como un órgano auxiliar del Poder Judicial y del Ministerio Fiscal de los que depende en sus funciones de averiguación del delito y descubrimiento y aseguramiento del delincuente, en los términos que la ley establezca.

Asimismo, según el artículo 1 del Real Decreto 769/1987, de 19 de junio, sobre regulación de la Policía Judicial, "las funciones generales de la Policía Judicial corresponden a todos los miembros de las Fuerzas y Cuerpos de Seguridad, cualquiera que sea su naturaleza y dependencia [...]" (p.18989).

Centrándonos en la Instrucción 4/2019, de la Secretaria de Estado de Seguridad, por la que se establece un nuevo protocolo para la valoración policial del nivel de riesgo de violencia de género (Ley Orgánica 1/2004) referenciada, la evaluación de ciberriesgos de los menores que cursan la ESO en la ciudad de Vinaròs como víctima y/o victimario, en su caso, se ha llevado a cabo, principalmente, a través de los 20 ítems sobre determinados hechos o conductas que aparecen en la encuesta de victimización *ad hoc*, y en función de los resultados arrojados se ha realizado una valoración policial de los niveles de riesgo (VPR), clasificándolos de la siguiente manera: NO APRECIADO, BAJO, MEDIO, ALTO Y EXTREMO, teniendo también en cuenta el análisis de otros ítems relacionados con la interacción de los menores y las TIC.

En lo atinente a los 20 ítems reseñados, hay que matizar que a través de éstos se han evaluado los ciberriesgos a los que se exponen los menores de la ciudad de Vinaròs que cursan la ESO, desde una perspectiva criminológica tanto de la víctima como del victimario, en su caso. Concretamente, la evaluación de los riesgos de los menores de ser víctima y/o victimario, en su caso, se ha realizado:

a) ciberacoso: mediante los ítems 1, 2, 5, 6, 7, 8, 9, 10, 11, 12, 13 ,14 y 15, respectivamente.
b) *sexting*: mediante los ítems 3 y 4, respectivamente.

c) *child grooming*: mediante el item 16.

d) violencia de género digital: mediante los ítems 17 a 20, respectivamente.

Respecto a la evaluación de los riesgos de los menores de ser víctima y/o victimario, en su caso, de sexting, se ha hecho a través de los ítems 3 y 4, respectivamente.

La escala de frecuencia tipo Likert en la que los menores participantes protagonizan los hechos o conductas, en su caso, presenta en la encuesta de victimización cinco posibles respuestas:

1=NUNCA: Cero veces.

2=POCAS VECES: Una o dos ocasiones o veces en un año.

3=ALGUNAS VECES: Tres o cuatro ocasiones o veces en un año.

4=MUCHAS VECES: Desde cinco hasta diez ocasiones o veces en un año.

5=SIEMPRE: Habitualmente o con mucha frecuencia (diez o más veces) en un año.

A los hechos o conductas de los ítems número 1 al 20, respectivamente, se les ha aplicado a los resultados obtenidos un factor de ponderación que va del número 1 al número 5.

En la encuesta de victimización, también hay 12 preguntas o ítems para marcar con la respuesta de “SI” o “NO”, con respuesta cerrada o de multirrespuesta, en su caso, que hacen referencia a la interacción o hábitos de uso de las TIC y otros hábitos de actividades cotidianas de los menores.

En lo que respecta a las contestaciones de la encuesta de victimización, se han analizado, y se han evaluado de manera tanto individual (por curso de la ESO) como generalizada o global sobre la base de la puntuación total obtenida para los cuatro cursos de la ESO de cada uno de los cuatro centros educativos objeto de estudio, y su inclusión en un rango de nivel de riesgo de las tablas 4 y 5, respectivamente, cosa que ha permitido valorar los ciberriesgos de los menores que cursan la ESO en la ciudad de Vinaròs de poder ser víctimas o victimarios, en su caso.

Tabla 12. *Niveles de riesgo individualizado para los cuatro cursos de la ESO*

Nivel riesgo	Valoración policial del riesgo (VPR)	Probabilidad victima/ victimario	Medidas de autoprotección recomendadas
200-400	No apreciada	Muy Baja	-Formación e información en ciberseguridad sobre uso seguro TIC y RRSS.
400-600	Baja	Baja	-Formación e información en ciberseguridad sobre uso seguro TIC y RRSS.
600-800	Media	Media	-Formación e información en ciberseguridad sobre uso seguro TIC y RRSS.
800-1000	Alta	Alta	-Formación e información en ciberseguridad sobre uso seguro TIC y RRSS. -Aplicación plan de seguridad con medidas de autoprotección y/o mediación policial, en su caso.
1000-1200	Extrema	Muy Alta	-Formación e información en ciberseguridad sobre uso seguro TIC y RRSS. -Aplicación plan de seguridad con medidas de autoprotección y/o mediación policial, en su caso.

Tabla 13. *Niveles de riesgo generalizado para los cuatro cursos de la ESO*

Nivel riesgo	Valoración policial del riesgo (VPR)	Probabilidad victima/ victimario	Medidas de autoprotección recomendadas
2000-2400	No apreciada	Muy Baja	- Formación e información en ciberseguridad sobre uso seguro TIC y RRSS.
2400-2800	Baja	Baja	- Formación e información en ciberseguridad sobre uso seguro TIC y RRSS.
2800-3200	Media	Media	- Formación e información en ciberseguridad sobre uso seguro TIC y RRSS.
3200-3600	Alta	Alta	- Formación e información en ciberseguridad sobre uso seguro TIC y RRSS. -Aplicación plan de seguridad con medidas de autoprotección y/o mediación policial, en su caso.
3600-4000	Extrema	Muy Alta	- Formación e información en ciberseguridad sobre uso seguro TIC y RRSS. -Aplicación plan de seguridad con medidas de autoprotección y/o mediación policial, en su caso.

En este orden de cosas, si de la puntuación del nivel del riesgo individualizado y/o generalizado obtenida resulta una valoración policial de riesgo (VPR) no apreciado, bajo o medio en su caso, deberíamos considerar que la probabilidad de que los menores (chicos o chicas) sean víctimas o victimarios, en su caso, es muy baja, baja o media, según el caso, pero si la valoración policial de riesgo (VPR) es alto o extremo, en su caso, deberíamos considerar el hecho importante, cosa que nos obligaría a tomar medidas de carácter inmediato o a la mayor brevedad posible.

Pero ¿qué medidas de autoprotección concretas se recomiendan para cada nivel de riesgo en función de la VPR?

Básicamente, en el supuesto de que el resultado de la valoración policial del riesgo sea no apreciado, bajo o medio se proponen medidas informativas y formativas en materia de ciberseguridad sobre el uso seguro de las tecnologías de la información y comunicación y redes sociales para los menores, pero si el resultado de dicha valoración fuese alto o extremo, adicionalmente además de la formación en ciberseguridad reseñada, se propondría la aplicación de un plan de seguridad con medidas de autoprotección personal generalizadas y/o mediación policial, en su caso, para los menores del curso o cursos que hayan arrojado el resultado preocupante.

En el supuesto de que algún alumno o alumna decidiera denunciar cualquier hecho delictivo junto con sus padres o, en su caso lo comunicase individualmente a los miembros de las Fuerzas y Cuerpos de Seguridad, se actuaría conforme a derecho en estos casos. Si el hecho está relacionado con la violencia de género digital, y la víctima no quisiera denunciar se aplicaría el protocolo cero en violencia de género en virtud de la Instrucción 5/2021, de la Secretaria de Estado de Seguridad, por la que se establece el protocolo de primer contacto policial con víctimas de violencia de género en situación de desprotección (protocolo cero).

III.2. Aplicación de la escala de evaluación de riesgos en prevención de riesgos laborales y de análisis de riesgos del INCIBE a la cibercriminalidad económica.

El procedimiento utilizado en el estudio que nos ocupa está basado en una combinación de dos escalas que he diseñado, en primer lugar, tenemos la escala de evaluación de riesgos en prevención de riesgos laborales del Instituto Nacional de Seguridad e Higiene en el Trabajo[25] y, en segundo lugar, un modelo de escala para análisis de riesgos del INCIBE[26].

La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, en su artículo 14 contempla que:

> en cumplimiento del deber de protección. el empresario deberá garantizar la seguridad y la salud de los trabajadores a su servicio en todos los aspectos relacionados con el trabajo. A estos efectos. en el marco de sus responsabilidades. el empresario realizara la prevención de los riesgos laborales mediante la adopción de cuantas medidas sean necesarias para la protección de la seguridad y la salud de los trabajadores (p.32596).

En este sentido, y dado que las personas que regentan los comercios, establecimientos públicos y/o microempresas de la muestra objeto de estudio suelen ser propietarios y trabajadores al mismo tiempo y/o tienen asalariados, en su caso (hasta un máximo de nueve empleados), y la gran mayoría poseen en sus negocios ordenador con conexión a internet, y así como teléfono móvil, mediante la combinación de las dos escalas reseñadas que aparecen en la tabla 6, ha permitido analizar su nivel de ciberriesgos o riesgos de cibervictimización, de acuerdo con la probabilidad estimada y a sus consecuencias esperadas (impacto) tanto para el trabajador como para el empresario y por ende a la empresa.

[25] https://www.insst.es/documents/94886/96076/Evaluacion_riesgos.pdf/1371c8cb-7321-48c0-880b-611f6f380c1d

[26] INCIBE (2016). *Manual curso de ciberseguridad para micropymes y autónomos*. Recuperado de https://www.incibe.es/formacion/ciberseguridad-para-micropymes-y-autonomos

Tabla 14. *Escala de riesgos, probabilidad e impacto (fuente INSHT e INCIBE)*

		Consecuencias (impacto)		
		Bajo (1)	Medio (2)	Alto (3)
Probabilidad	Baja (1)	Riesgo trivial (1)	Riesgo tolerable (2)	Riesgo moderado (3)
	Media (2)	Riesgo tolerable (2)	Riesgo moderado (4)	Riesgo importante (6)
	Alta (3)	Riesgo moderado (3)	Riesgo importante (6)	Riesgo intolerable (9)

La evaluación de ciberriesgos o riesgos de cibervictimización, se ha realizado a partir de 20 ítems, principalmente, teniendo en cuenta además el resto de los ítems de la encuesta para el estudio global.

La escala de frecuencia tipo Likert en la que los participantes protagonizan los hechos o conductas, en su caso, presenta en la encuesta de victimización cinco posibles respuestas:

1=NUNCA: Cero veces.

2=POCAS VECES: Una o dos ocasiones o veces en un año.

3=ALGUNAS VECES: Tres o cuatro ocasiones o veces en un año.

4=MUCHAS VECES: Desde cinco hasta diez ocasiones o veces en un año.

5=SIEMPRE: Habitualmente o con mucha frecuencia (diez o más veces) en un año.

A los hechos o conductas de los ítems número 1 al 13, respectivamente, se les ha aplicado a los resultados obtenidos un factor de ponderación que va del número 1 al número 5, y a los ítems número 14 hasta el 20, respectivamente, se les ha aplicado un factor de ponderación del número 5 al número 1.

En la encuesta de victimización, también hay 18 preguntas o ítems para marcar con la respuesta de "SI" o "NO", de los que 9 hacen referencia a la interacción o hábitos de uso de las TIC y otros hábitos de actividades cotidianas, y los 9 restantes versan

sobre determinados conocimientos de ciberseguridad, concretamente, sobre los posibles conocimientos de los participantes sobre tecnologías biométricas.

En lo que respecta a las contestaciones de la encuesta de victimización, se han analizado, y se han evaluado de manera generalizada o global sobre la base de la puntuación total obtenida, y su inclusión en un rango de nivel de riesgo, cosa que nos permitirá estimar el riesgo de cibervictimización de los regentes empleados y/o empresarios y por consiguiente de los comercios, establecimientos públicos o micropymes, en su caso, (autónomos y/o microempresas o micropymes) tanto desde una perspectiva de la prevención de riesgos laborales como del daño, pérdida o perjuicio económico que pudieran sufrir.

En este orden de cosas, si la estimación del riesgo generalizado resulta menor o igual a 4, deberíamos considerarlo tolerable o moderado, en su caso, pero si es mayor de 4, deberíamos considerarlo importante o intolerable, cosa que nos obligaría a tomar medidas de carácter inmediato o a corto plazo (máximo tres meses). Dichas medidas preventivas, serían de dos tipos:

1º) medidas planificadas consistentes en información y formación de los trabajadores autónomos, regentes de comercios y establecimientos públicos, y microempresas, así como de sus empleados, en su caso, en buenas prácticas en ciberseguridad sobre el uso seguro de las TIC, redes sociales, correo electrónico, seguridad en dispositivos móviles, reputación o imagen digital, interacciones seguras con proveedores y clientes, etc.

2º) procedimientos y establecimiento de pautas y obligaciones para los trabajadores en el ámbito de ciberseguridad, administración de accesos de los usuarios, clasificación de la información y cumplimiento de políticas de empresa.

IV. RESULTADOS.

IV.1 Resultados estudio de cibercriminalidad social.

Los resultados obtenidos de los cuatro centros educativos objeto de estudio han sido los siguientes:

a)-Nuestra Señora de la Consolación: de un total de 126 alumnos matriculados de la ESO, se ha tomado una muestra de este centro educativo de 109 alumnos encuestados que han participado voluntariamente, de los que un 55% son chicas y un 45% son chicos,

de 11 a 16 años, correspondientes a los cursos de 1º a 4º de la ESO, tal y como podemos observar en la tabla 15 y figura 9, respectivamente.

Concretamente, de 1º de la ESO la media de edad es 12,30 años; de 2º de la ESO es de 13,41 años; de 3º ESO es de 14,64 años y de 4º ESO es 15,22 años.

Tabla 15. *Edad y género de los menores participantes de la ESO de N. Sª Consolación.*

Curso académico	Edades	Chicos	Chicas	
1º ESO	11-13	17	10	27
2º ESO	13-15	10	17	27
3º ESO	14-16	12	16	28
4º ESO	15-16	10	17	27
	Totales	49	60	109

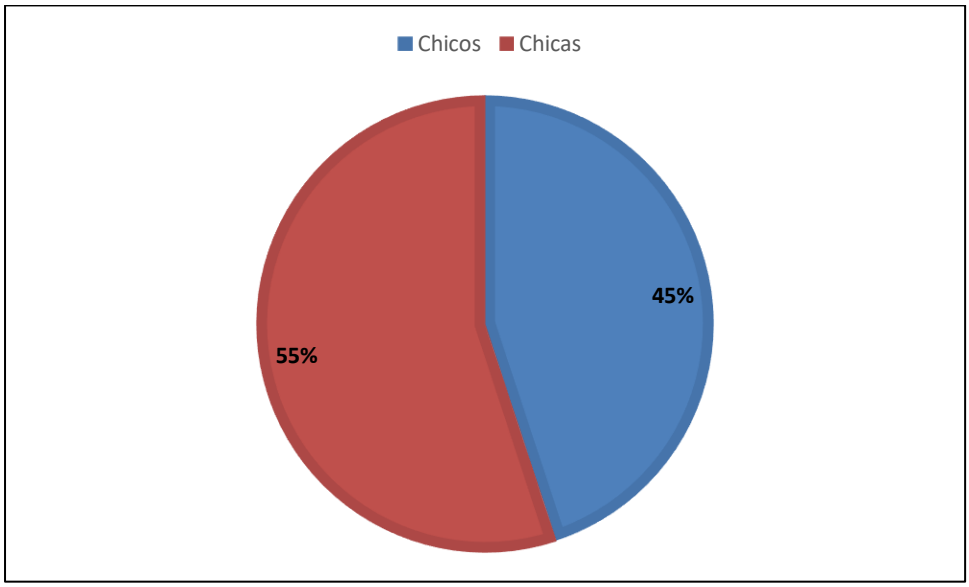

Figura 9. Porcentaje total participantes por género de la ESO de N. Sª Consolación.

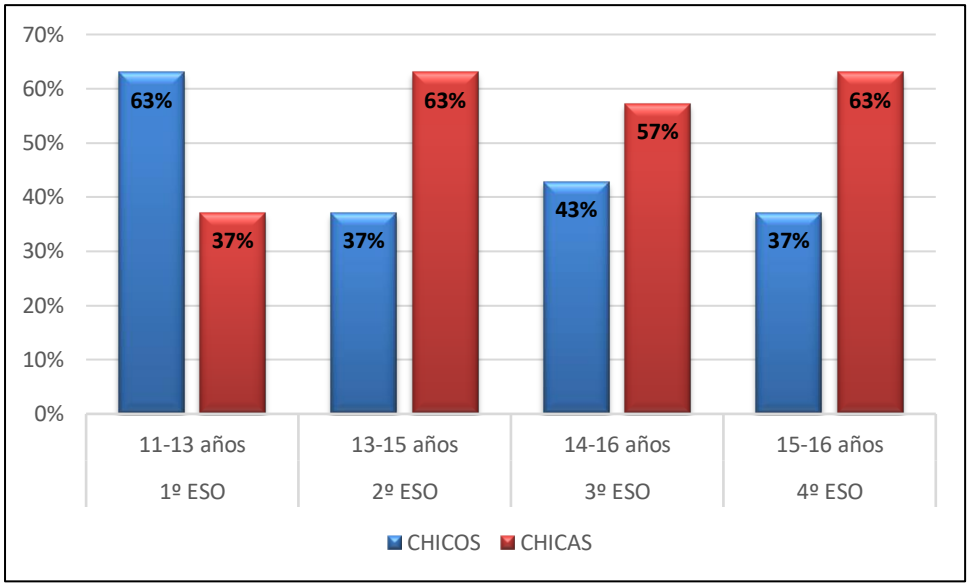

Figura 10. Menores de la ESO de N. Sª de la Consolación por curso académico y género.

El curso académico que más chicos hay es 1ºESO y en el que menos 4º ESO. Sin embargo, con relación a las chicas, podemos destacar que el curso que menos hay es 1º ESO y en el resto de los cursos su representación es mayor que la de los chicos, tal y como podemos apreciar en la figura 10.

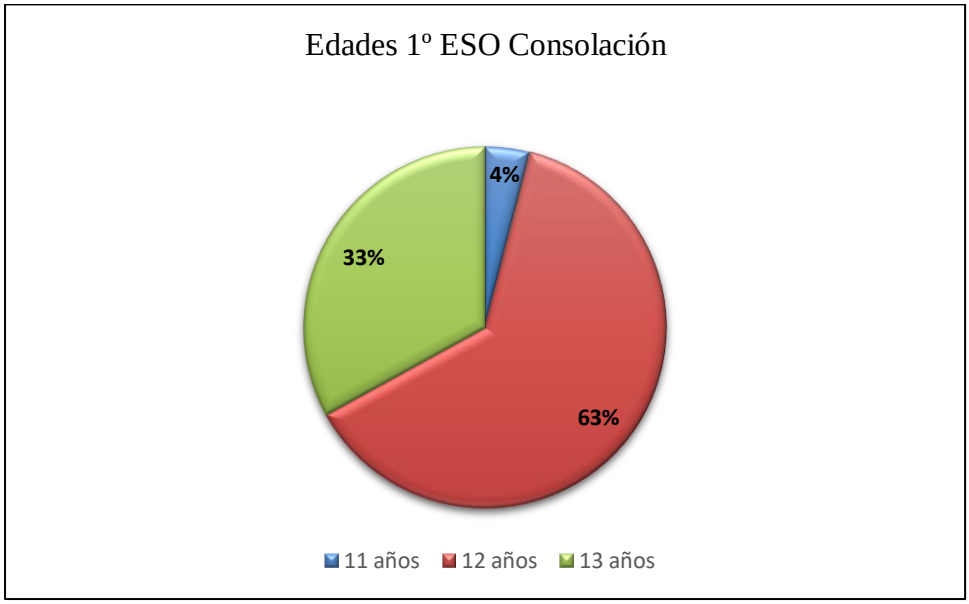

Figura 11. Edades menores de 1º ESO de N. Sª de la Consolación.

En la figura 11, podemos apreciar que dentro del rango de edad de los menores participantes en el presente estudio correspondientes al curso de 1º de la ESO de N. Sª de la Consolación, la mayoría tiene 12 años, es decir, un 63%, mientras que tan solo un 4% tiene 11 años y el 33% restante tiene 13 años.

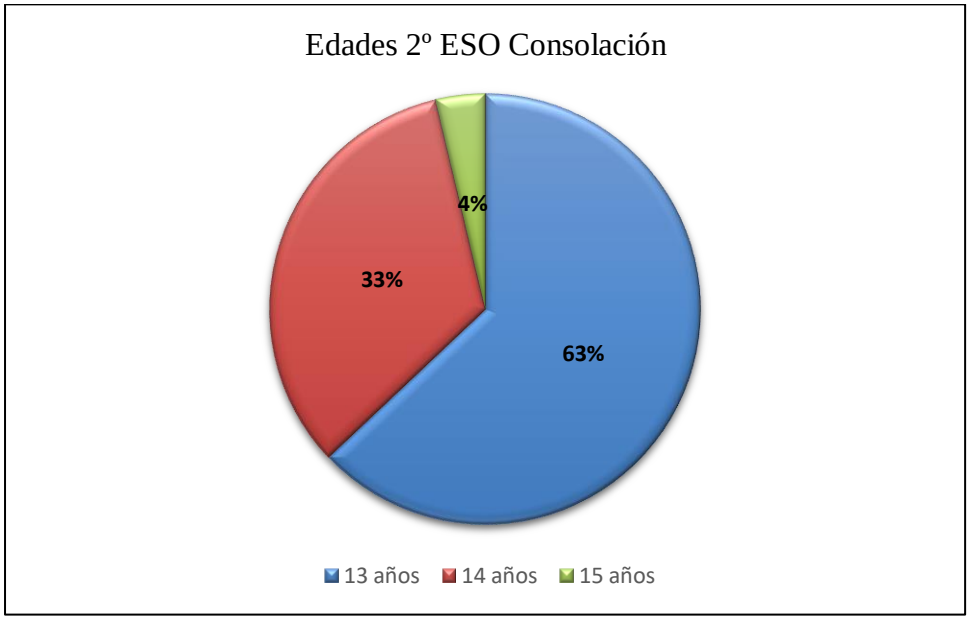

Figura 12. Edades menores de 2º ESO de N. Sª de la Consolación.

En la figura 12, podemos destacar que del curso 2º de la ESO de N. Sª de la Consolación, la mayoría tiene 13 años, es decir, un 63%, mientras que tan solo un 4% tiene 15 años y el 33% restante tiene 14 años.

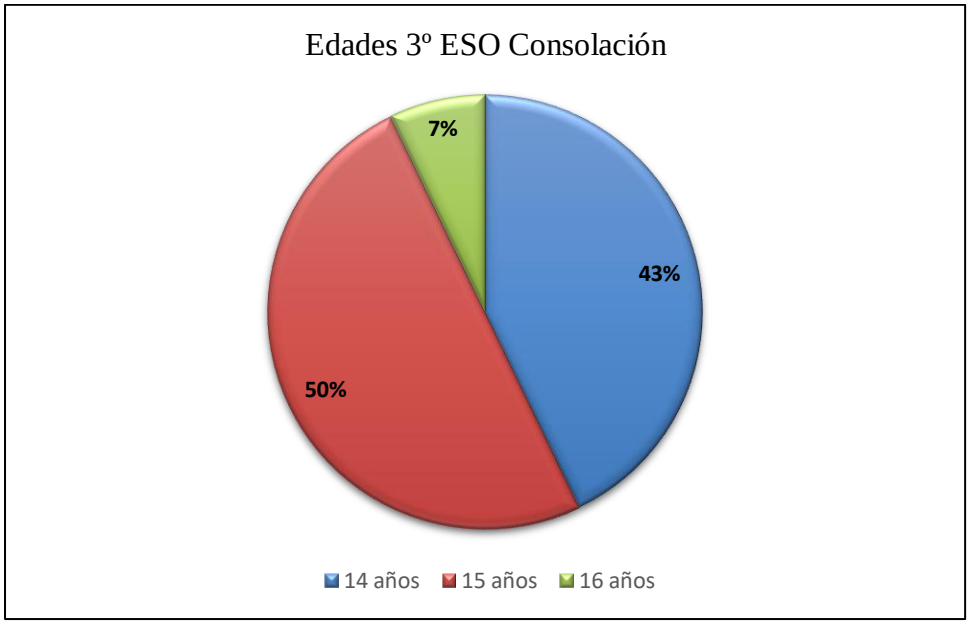

Figura 13. Edades menores de 3º ESO de N. Sª de la Consolación.

En la figura 13, podemos observar que del curso 3º de la ESO de N. Sª de la Consolación, la mayoría tiene 15 años, es decir, un 50%, mientras que tan solo un 7% tiene 16 años y el 43% restante tiene 14 años.

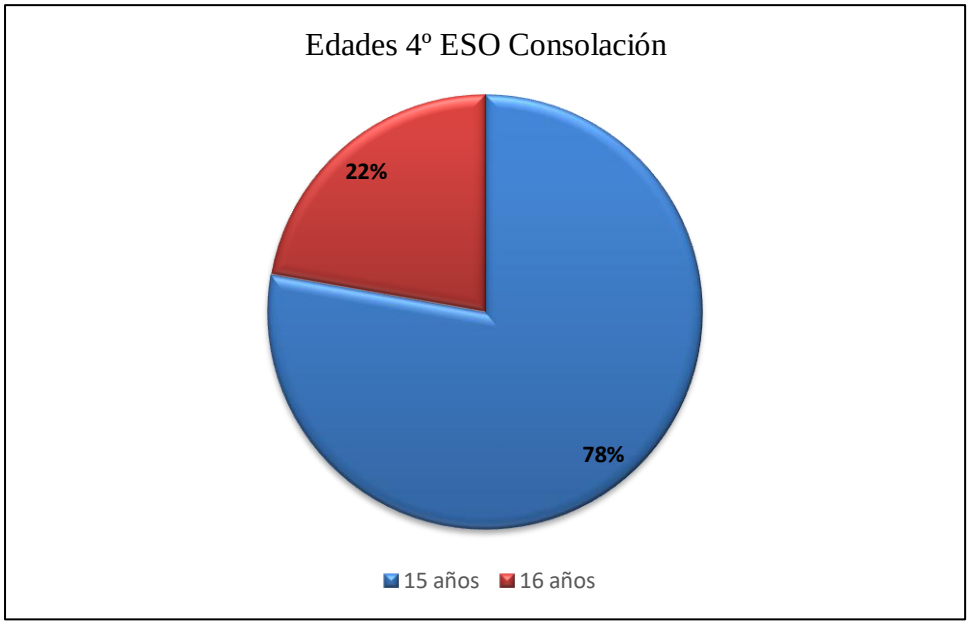

Figura 14. Edades menores de 4º ESO de N. Sª de la Consolación.

En la figura 14, podemos observar que del curso 4º de la ESO de N. Sª de la Consolación, un 78% tiene 15 años mientras que el 22% restante tiene 16 años.

Por otra parte, con relación a la interacción con las TIC de los menores que cursan la ESO en el centro educativo Consolación, en la encuesta de victimización social figuraban en la primera página, diez ítems con opción de respuesta "SI o "NO", así como otras preguntas con respuestas cerradas, en su caso, obteniéndose los resultados que a continuación se detallan en las tablas 16 a 19, respectivamente, así como los representados gráficamente en las figuras 15 a 54, ambas inclusive.

Tabla 16. *Resultados interacción TIC menores de 1º ESO N. Sª Consolación.*

Ítems interacciones TIC menores 1º ESO	SI	NO
Tengo ordenador en casa	26	1
Tengo webcam	18	9
Tengo teléfono móvil	27	0
Guardo información personal en el teléfono móvil	17	10
Tengo cuenta de correo electrónico	27	0
Utilizo programas de mensajería instantánea	27	0
Utilizo redes sociales	21	6
Utilizo blogs, foros en Internet	9	18

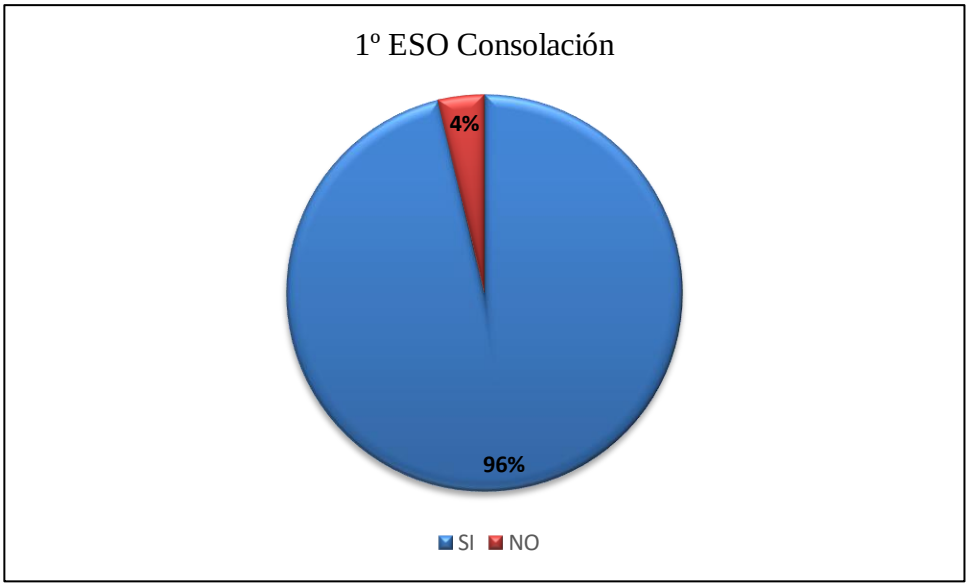

Figura 15.¿Tienes ordenador en casa?

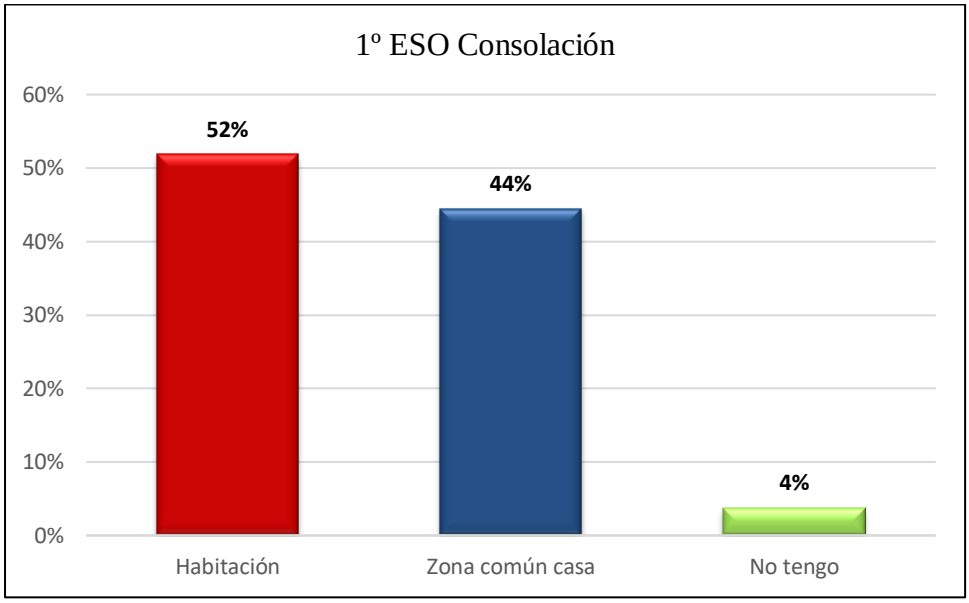

Figura 16. ¿Dónde tienes ubicado tu ordenador?

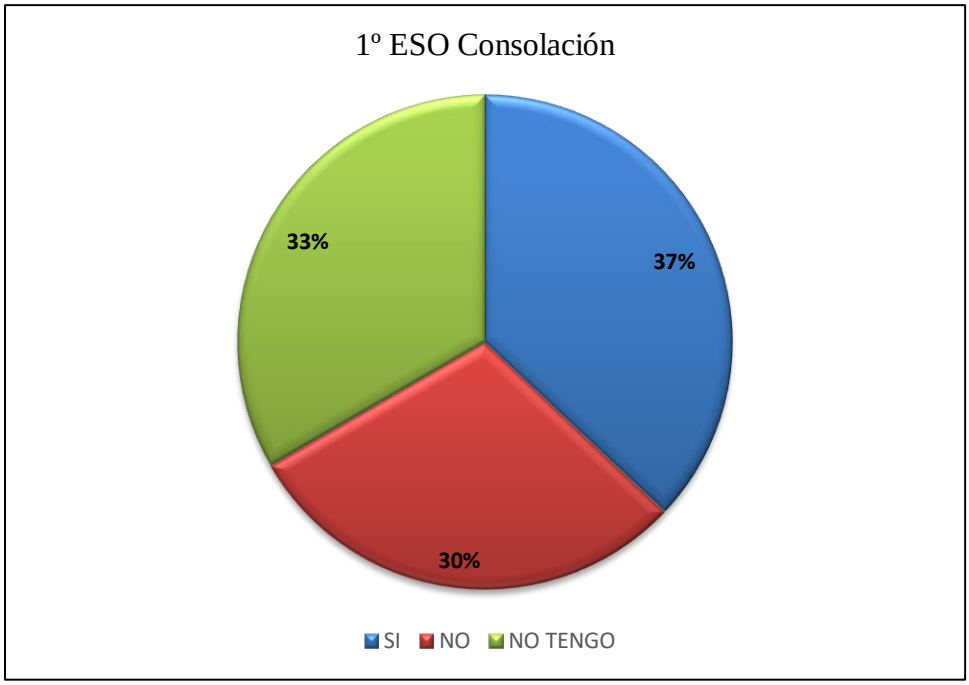

Figura 17. ¿Tapas la webcam cuando no la utilizas?

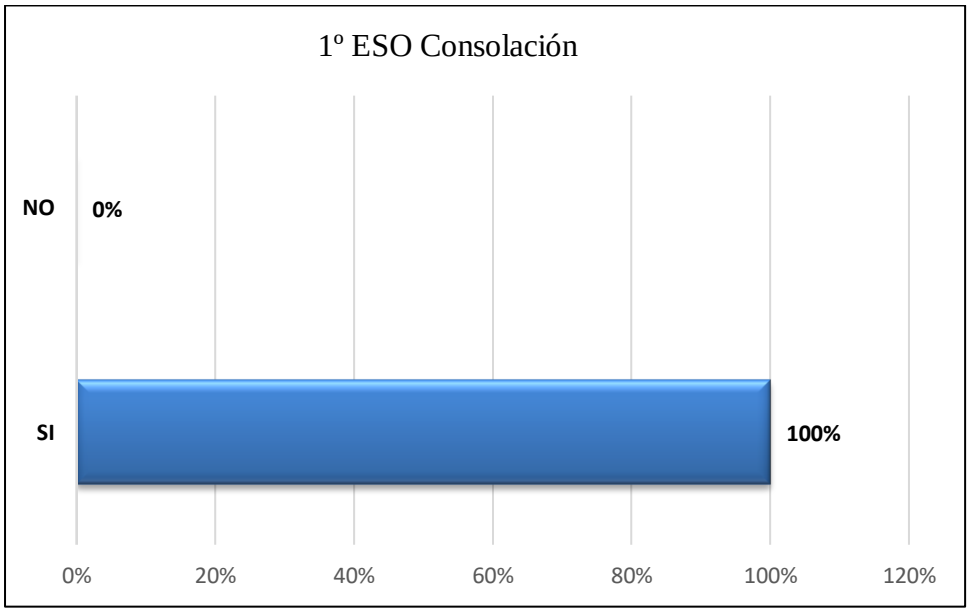

Figura 18. ¿Tienes teléfono móvil?

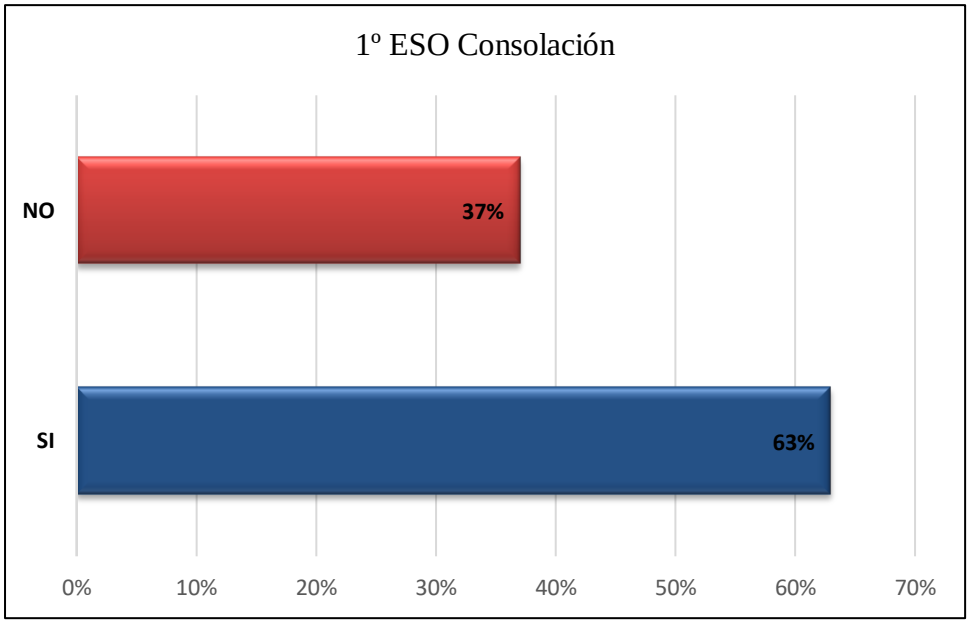

Figura 19. ¿Guardas información personal en tu teléfono móvil?

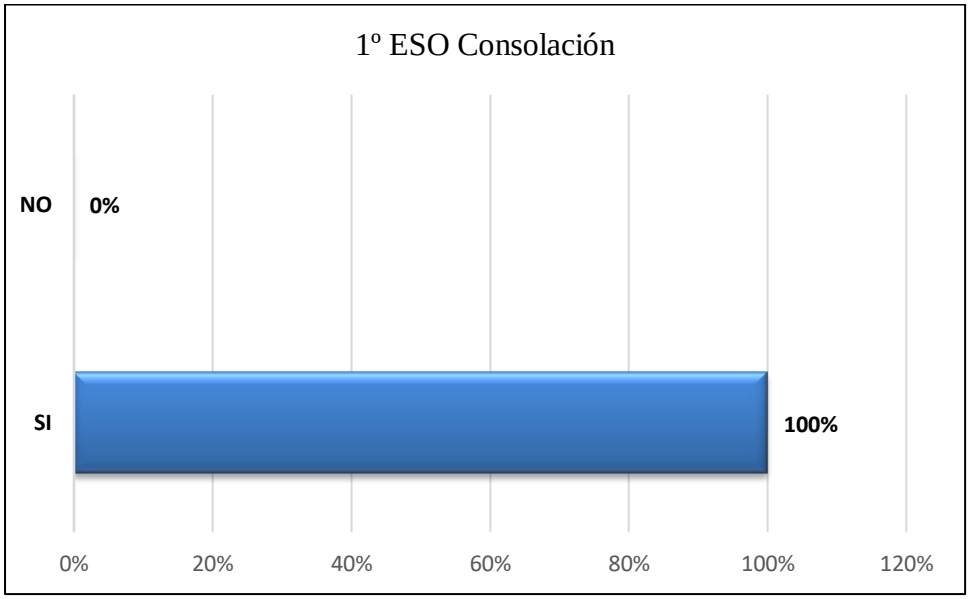

Figura 20. ¿Tienes cuenta de correo electrónico?

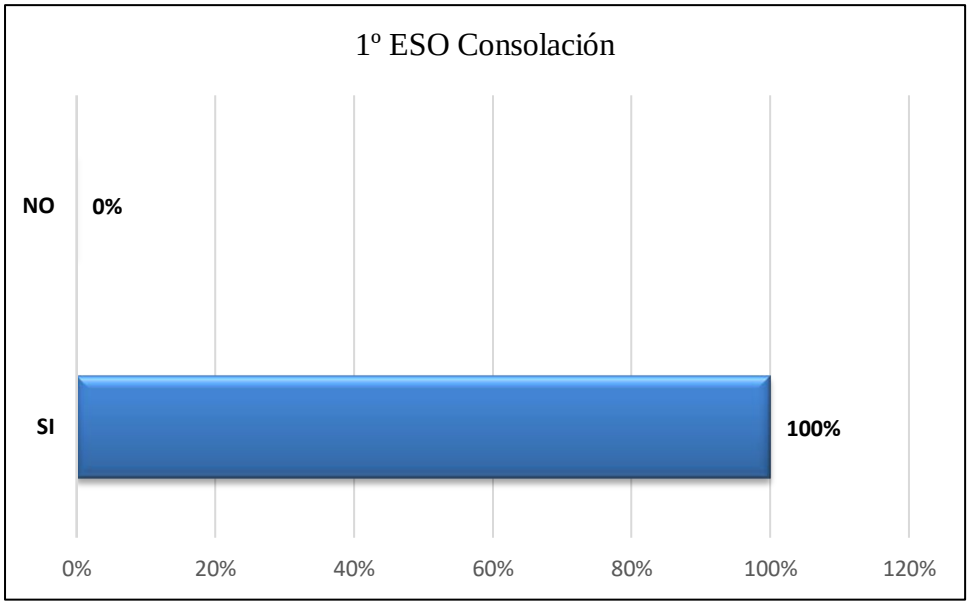

Figura 21. ¿Utilizas programas de mensajería instantánea?

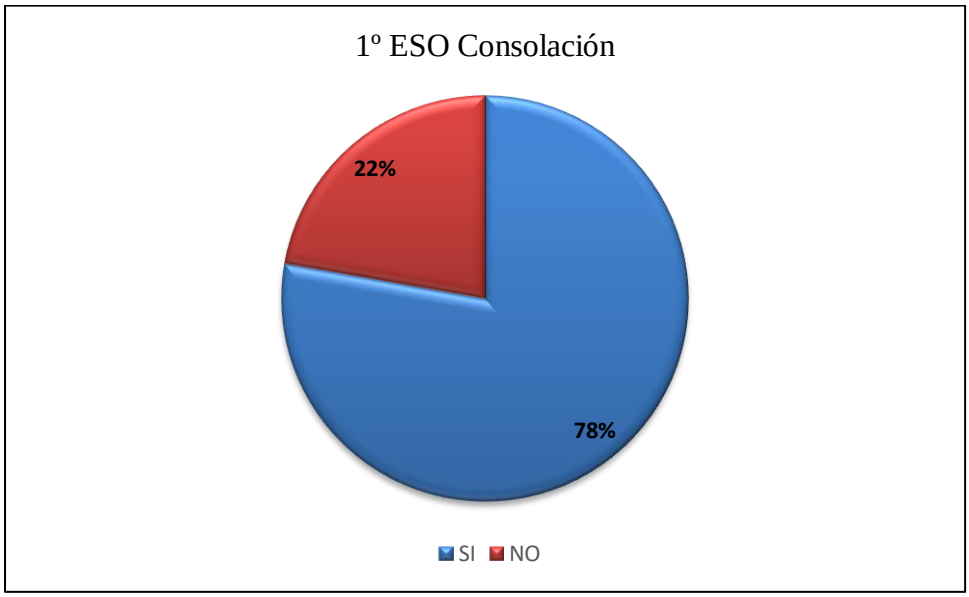

Figura 22. ¿Utilizas redes sociales?

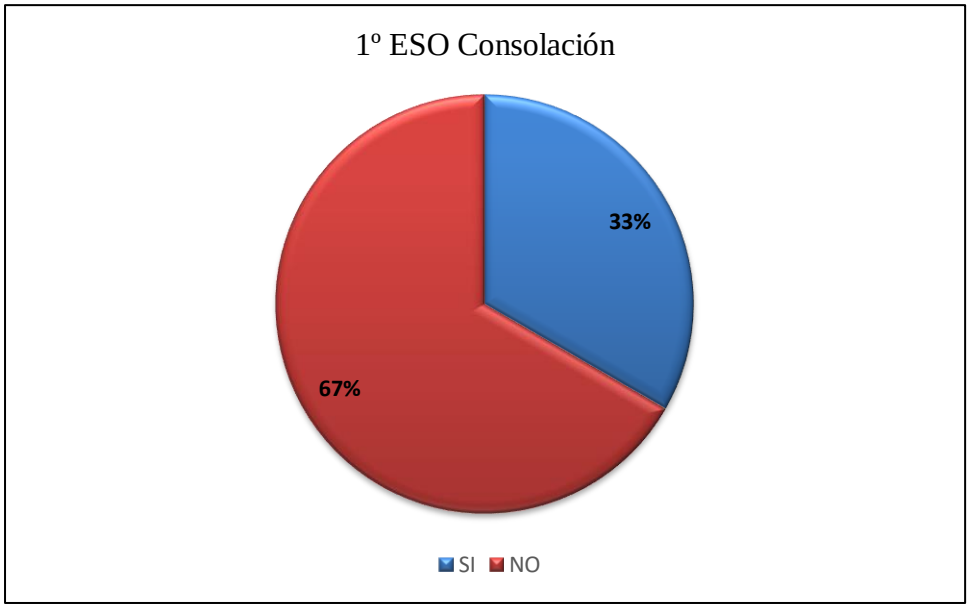

Figura 23. ¿Utilizas blogs, foros en Internet?

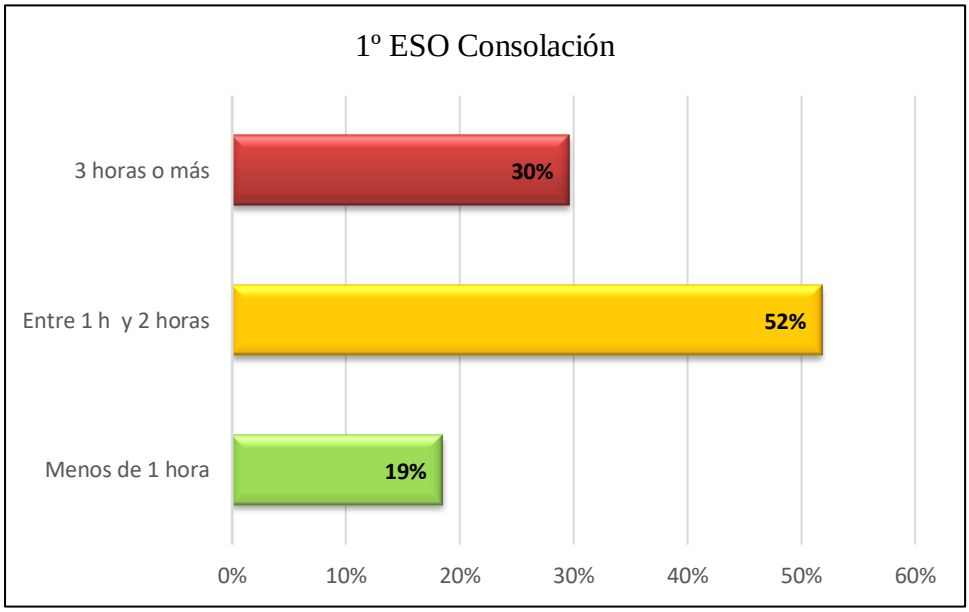

Figura 24. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Tabla 17. *Resultados interacción TIC menores de 2º ESO N. Sª Consolación*.

Ítems interacciones TIC menores 2º ESO	SI	NO
Tengo ordenador en casa	27	0
Tengo webcam	26	1
Tengo teléfono móvil	27	0
Guardo información personal en el teléfono móvil	24	3
Tengo cuenta de correo electrónico	27	0
Utilizo programas de mensajería instantánea	27	0
Utilizo redes sociales	26	1
Utilizo blogs, foros en Internet	9	18

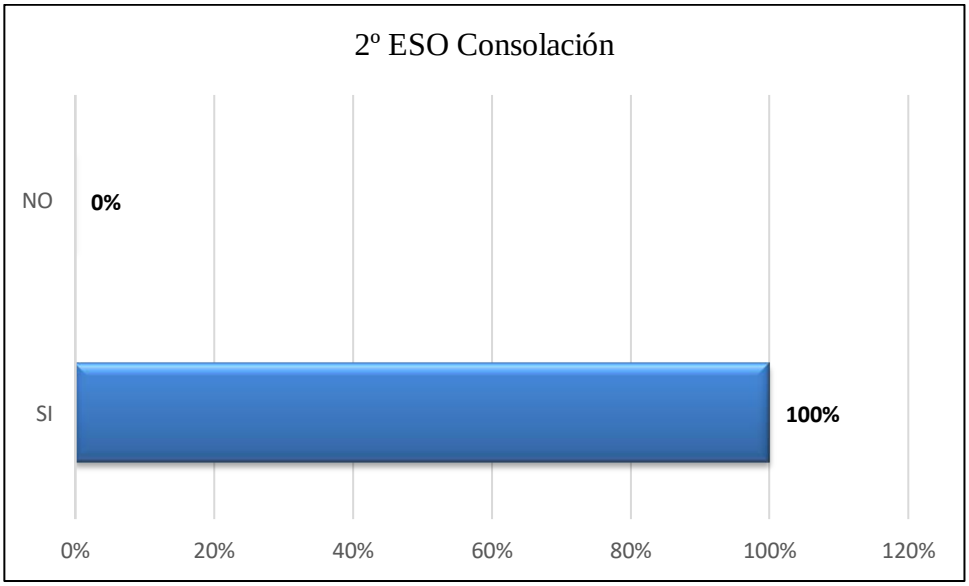

Figura 25. ¿Tienes ordenador en casa?

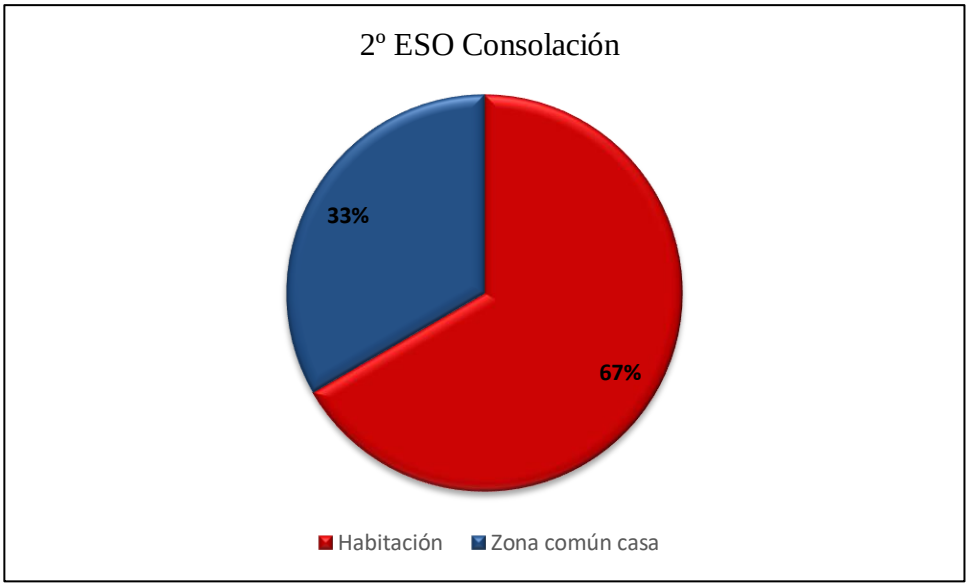

Figura 26. ¿Dónde tienes ubicado tu ordenador?

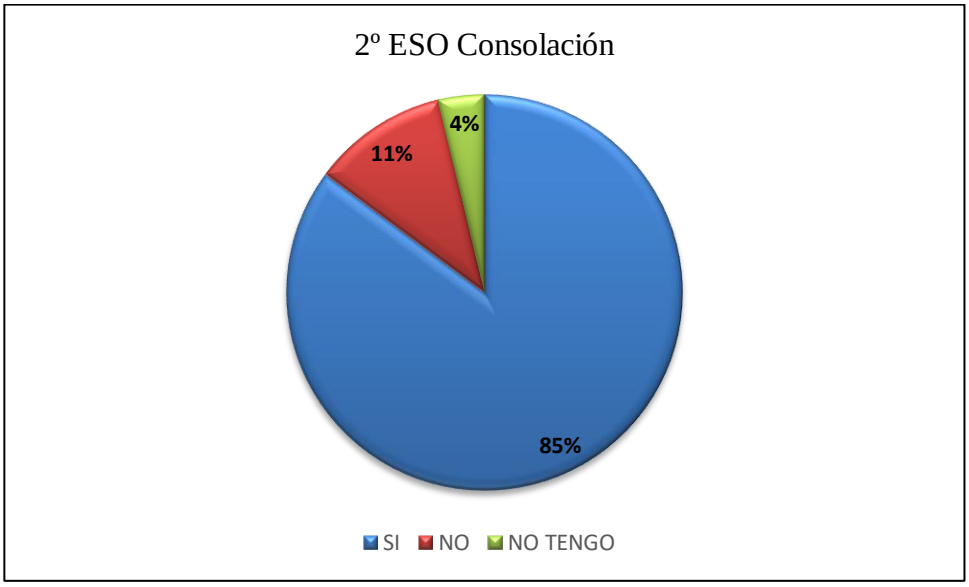

Figura 27. ¿Tapas la webcam cuando no la utilizas?

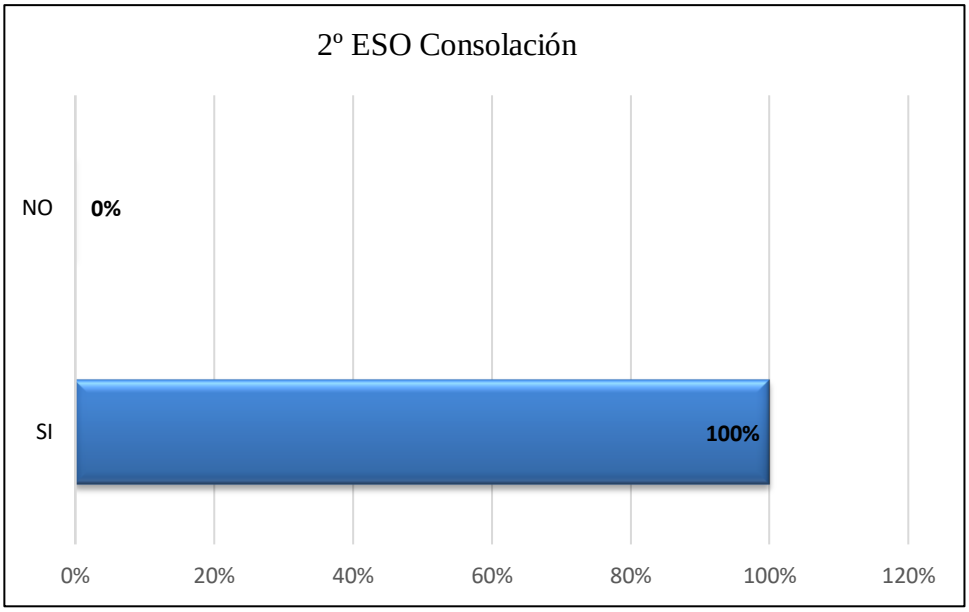

Figura 28. ¿Tienes teléfono móvil?

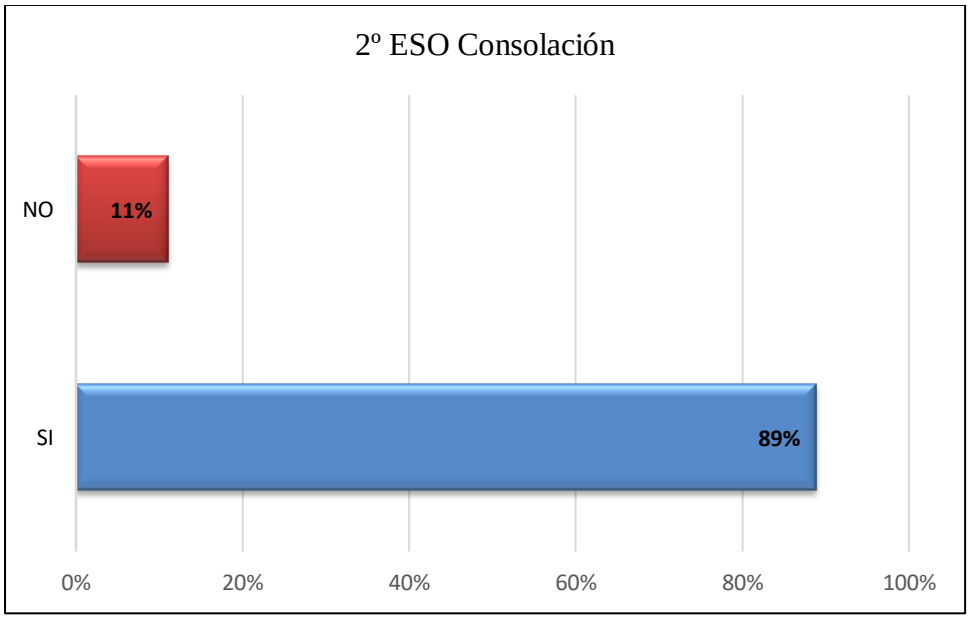

Figura 29. ¿Guardas información personal en tu teléfono móvil?

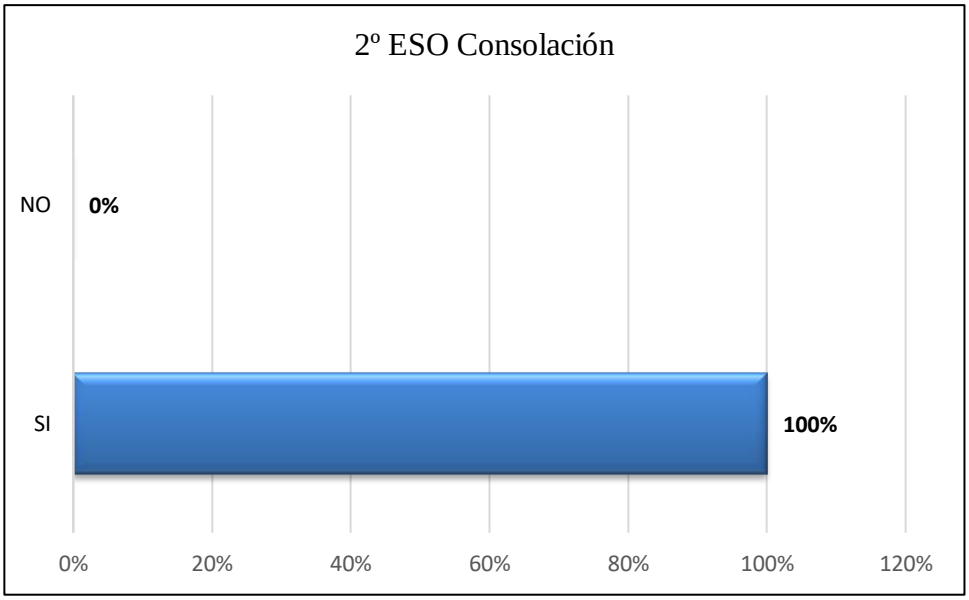

Figura 30. ¿Tienes cuenta de correo electrónico?

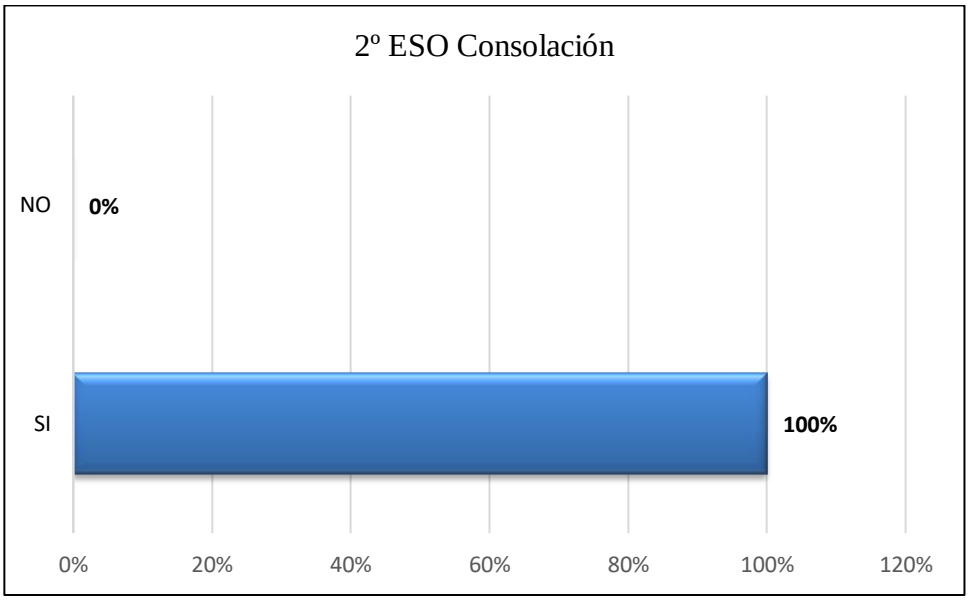

Figura 31. ¿Utilizas programas de mensajería instantánea?

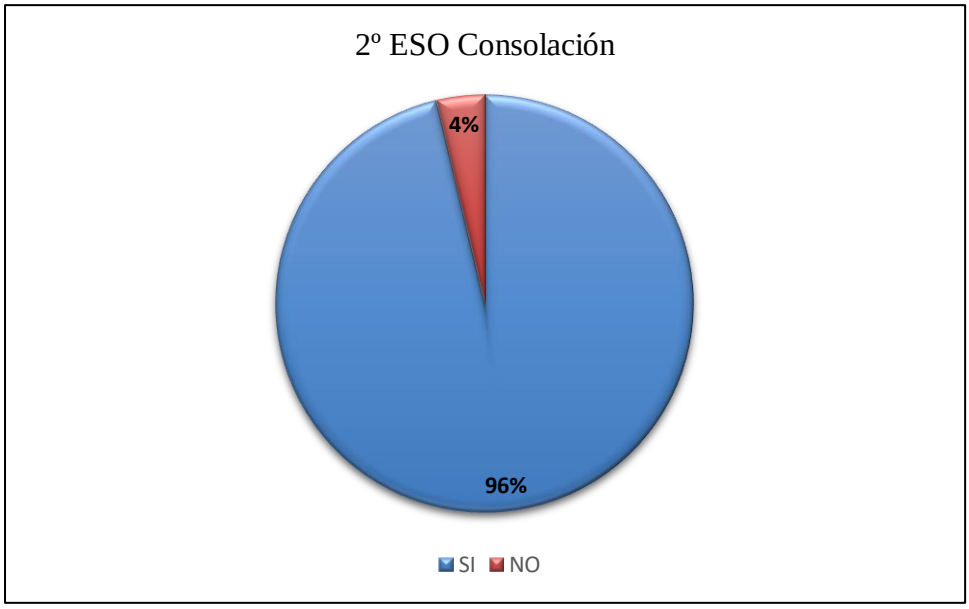

Figura 32. ¿Utilizas redes sociales?

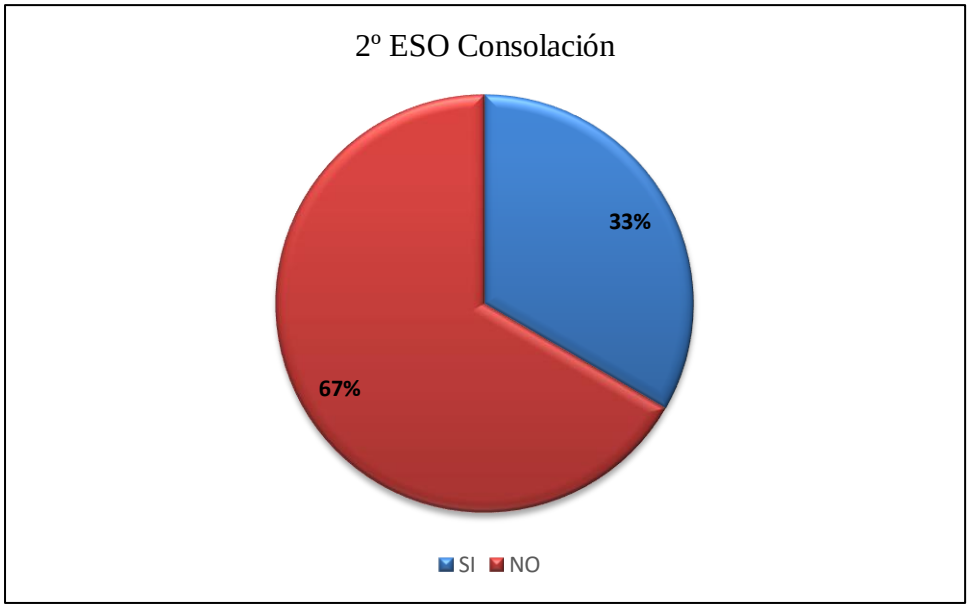

Figura 33. ¿Utilizas blogs, foros en Internet?

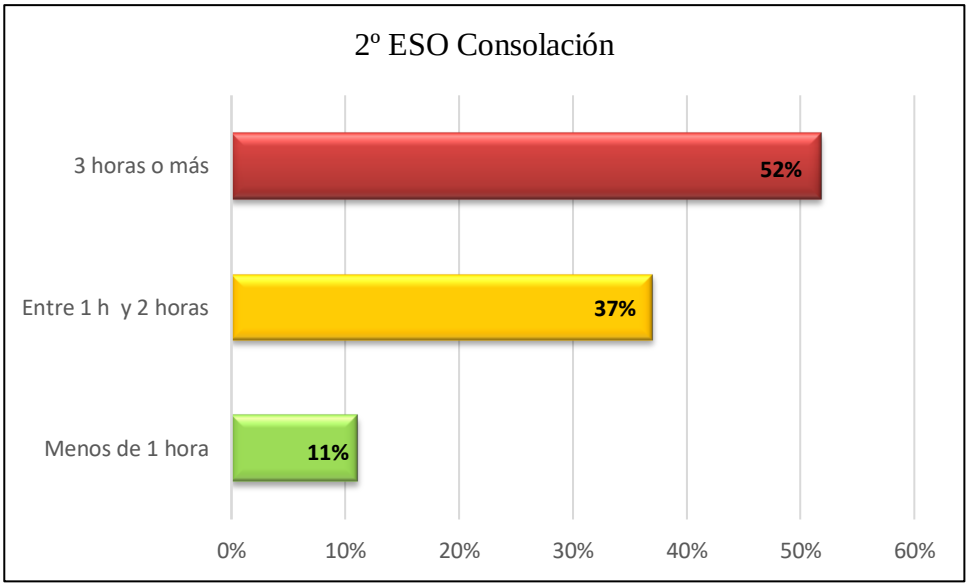

Figura 34. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Tabla 18. *Resultados interacción TIC menores de 3º ESO N. Sª Consolación*.

Ítems interacciones TIC menores 3º ESO	SI	NO
Tengo ordenador en casa	28	0
Tengo webcam	21	7
Tengo teléfono móvil	28	0
Guardo información personal en el teléfono móvil	21	7
Tengo cuenta de correo electrónico	28	0
Utilizo programas de mensajería instantánea	27	1
Utilizo redes sociales	24	4
Utilizo blogs, foros en Internet	18	10

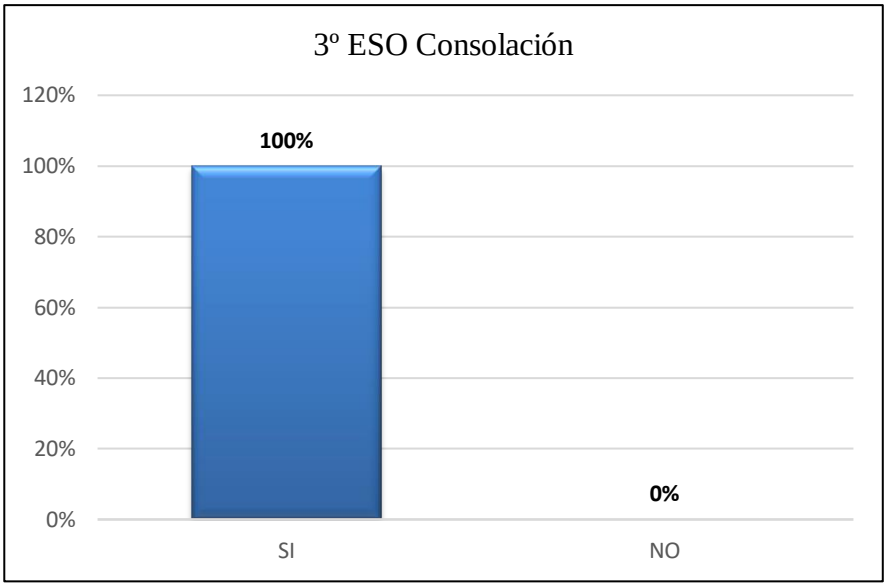

Figura 35. ¿Tienes ordenador en casa?

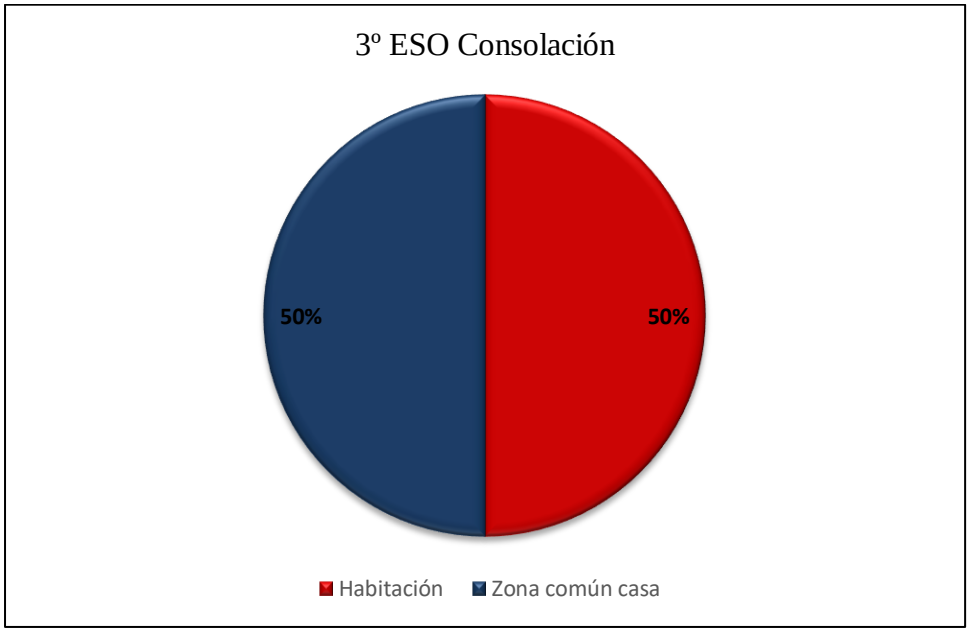

Figura 36. ¿Dónde tienes ubicado tu ordenador?

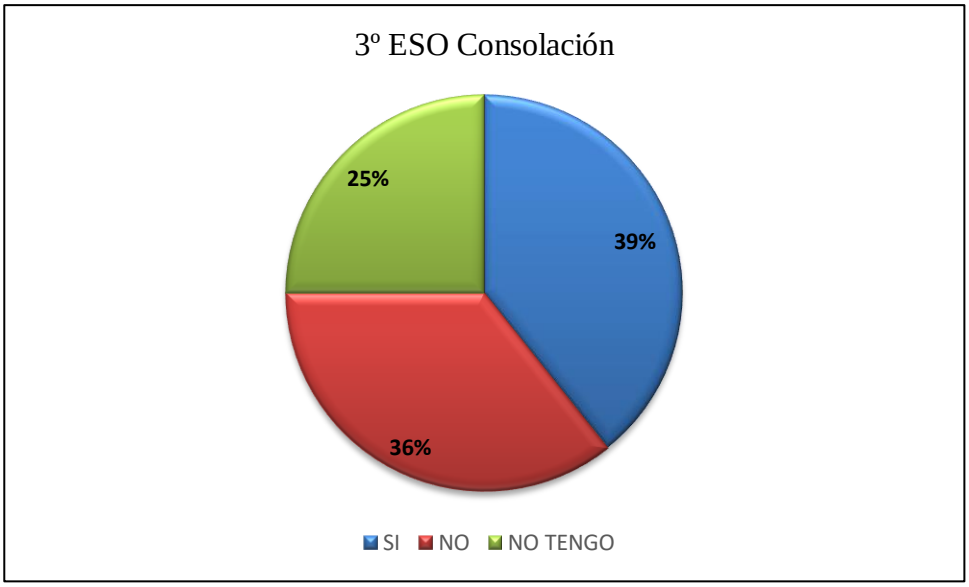

Figura 37. ¿Tapas la webcam cuando no la utilizas?

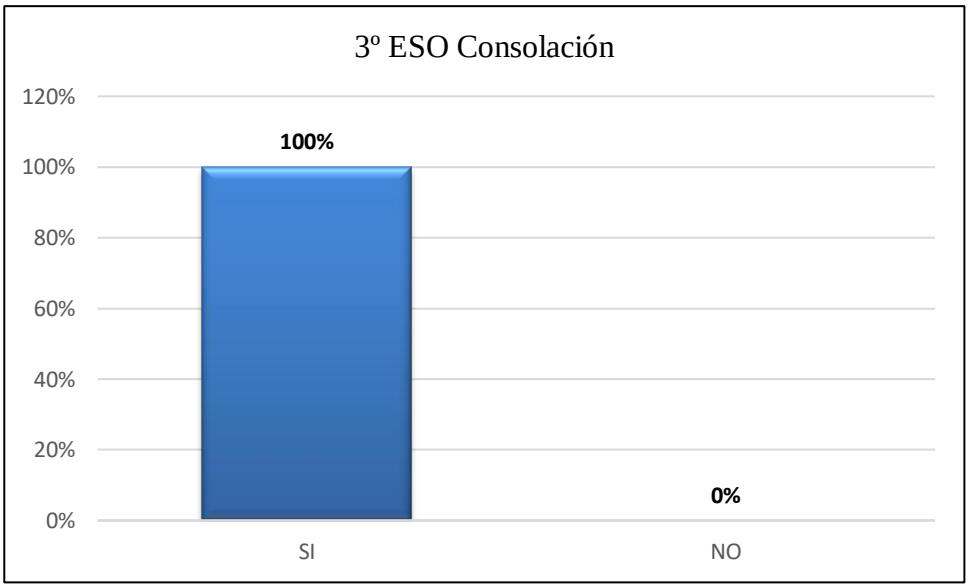

Figura 38. ¿Tienes teléfono móvil?

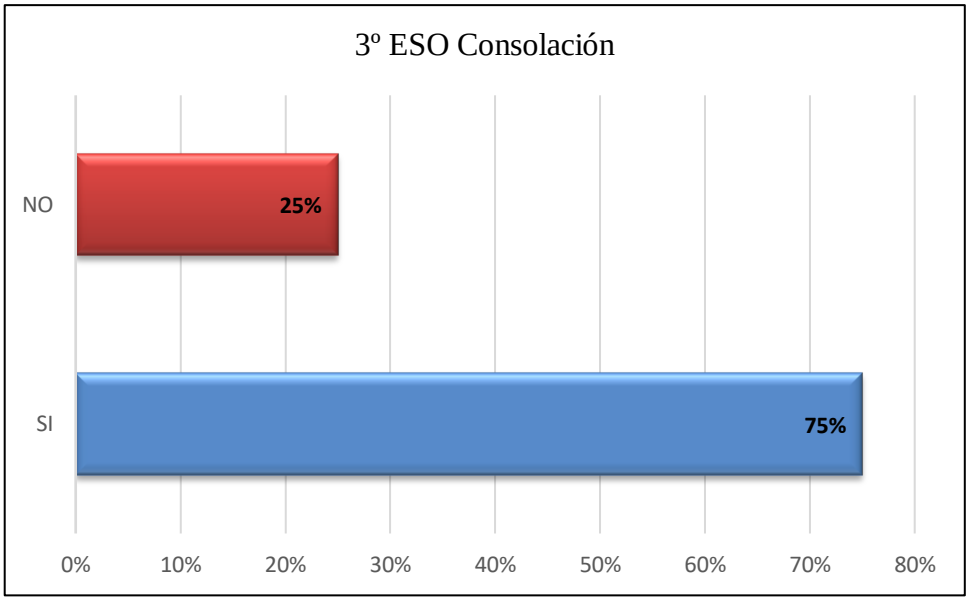

Figura 39. ¿Guardas información personal en tu teléfono móvil?

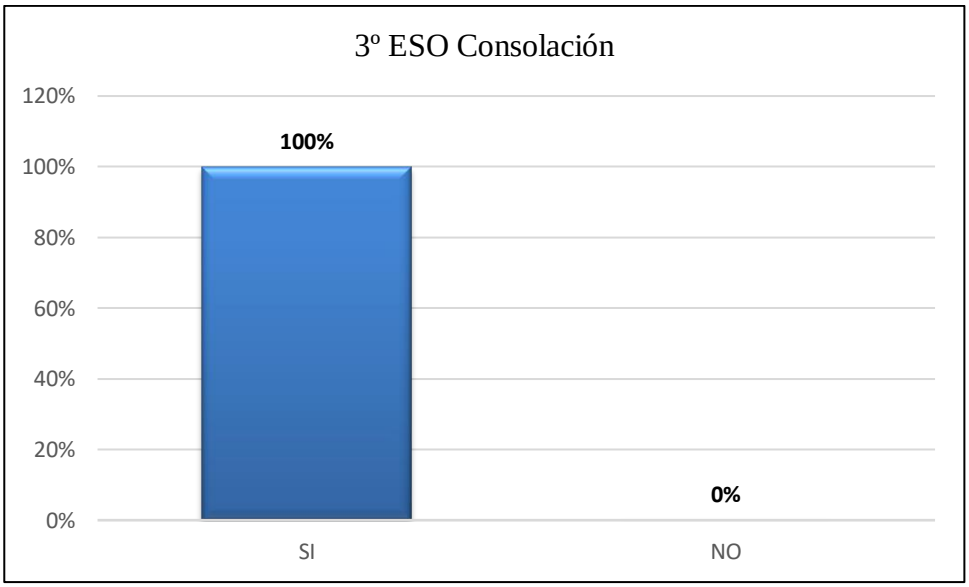

Figura 40. ¿Tienes cuenta de correo electrónico?

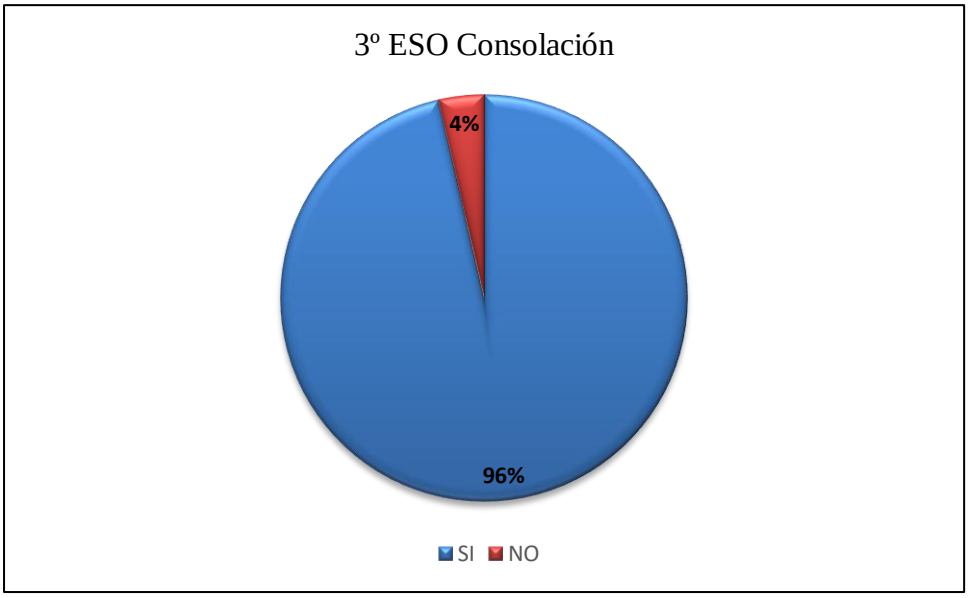

Figura 41. ¿Utilizas programas de mensajería instantánea?

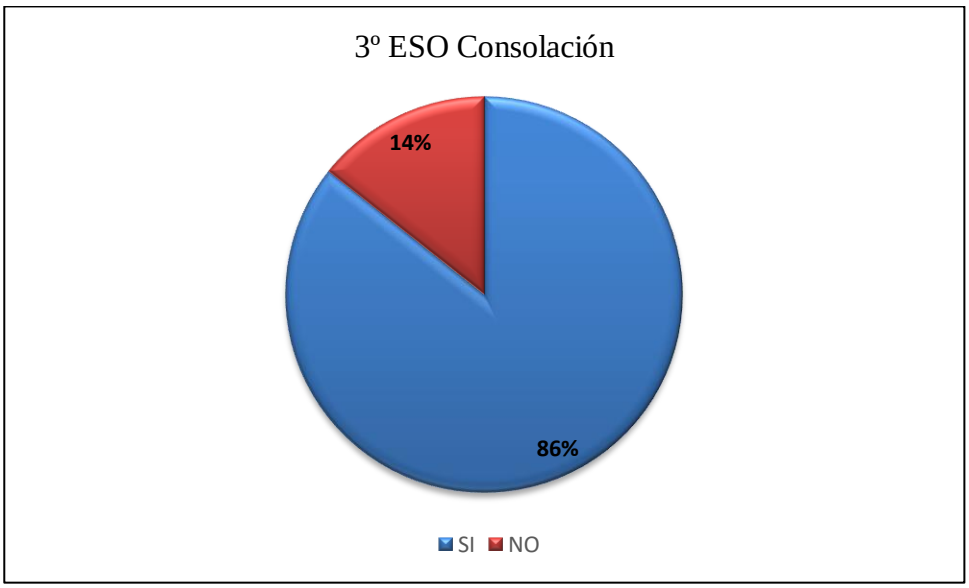

Figura 42. ¿Utilizas redes sociales?

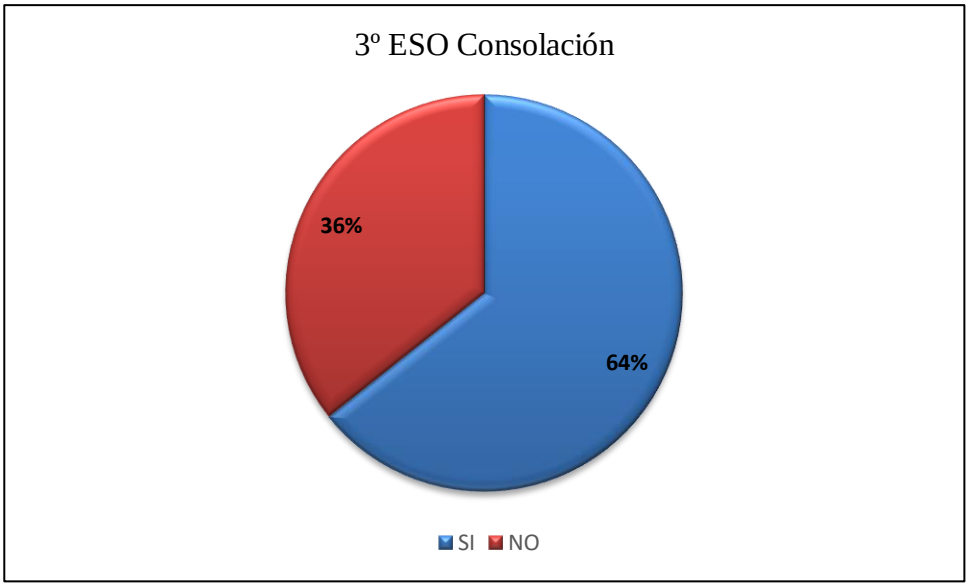

Figura 43. ¿Utilizas blogs, foros en Internet?

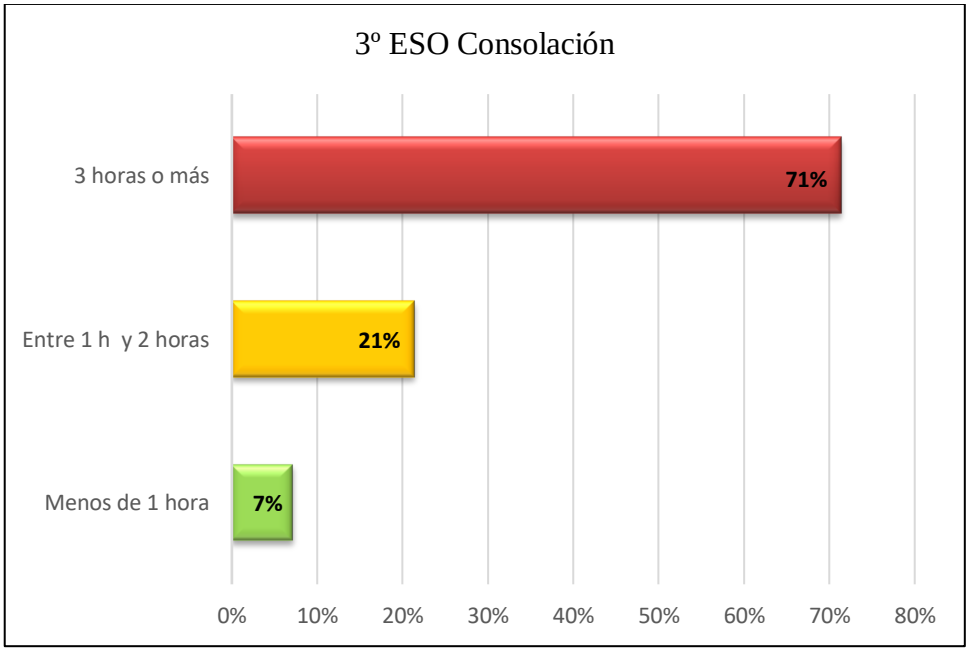

Figura 44. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Tabla 19. *Resultados interacción TIC menores de 4º ESO N. Sª Consolación.*

Ítems interacciones TIC menores 4º ESO	SI	NO
Tengo ordenador en casa	26	1
Tengo webcam	23	4
Tengo teléfono móvil	27	0
Guardo información personal en el teléfono móvil	21	6
Tengo cuenta de correo electrónico	27	0
Utilizo programas de mensajería instantánea	25	2
Utilizo redes sociales	23	4
Utilizo blogs, foros en Internet	9	18

Figura 45. ¿Tienes ordenador en casa?

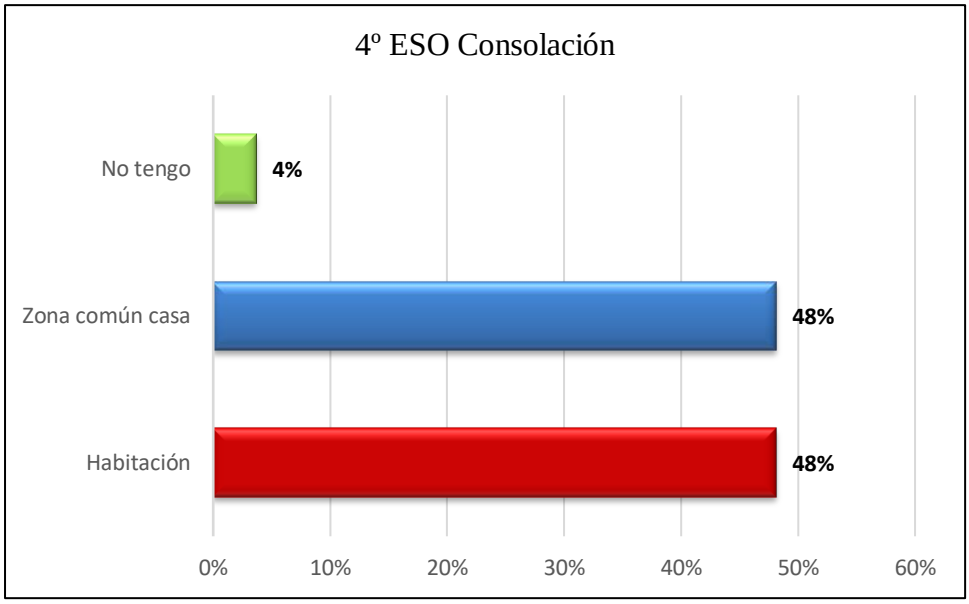

Figura 46. ¿Dónde tienes ubicado tu ordenador?

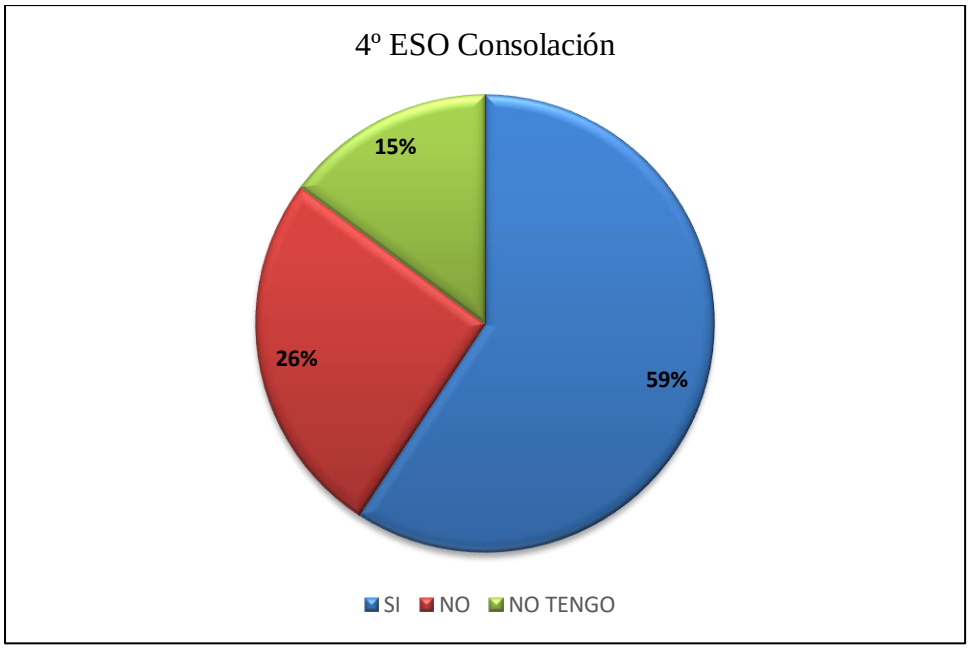

Figura 47. ¿Tapas la webcam cuando no la utilizas?

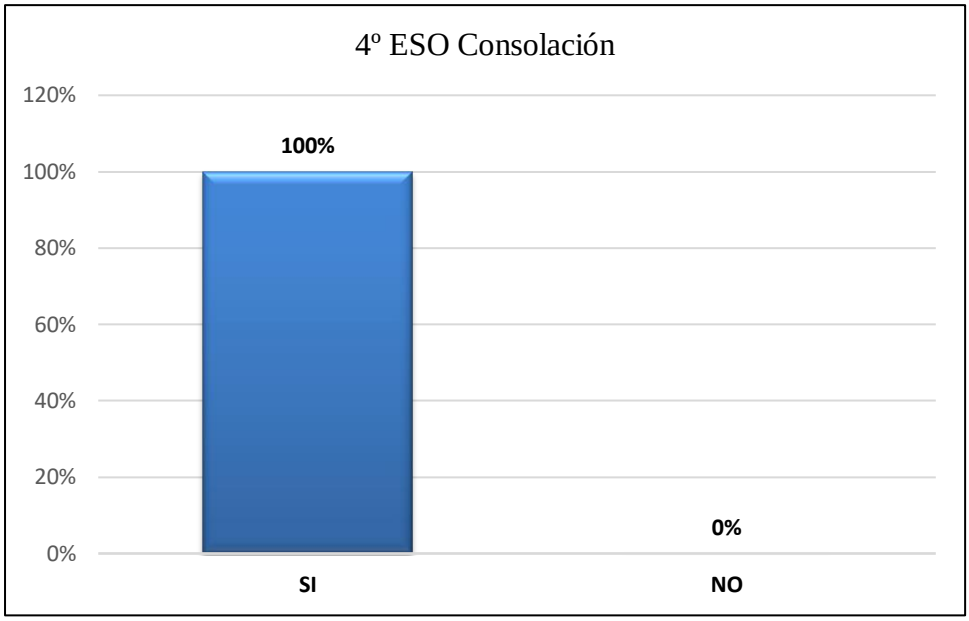

Figura 48. ¿Tienes teléfono móvil?

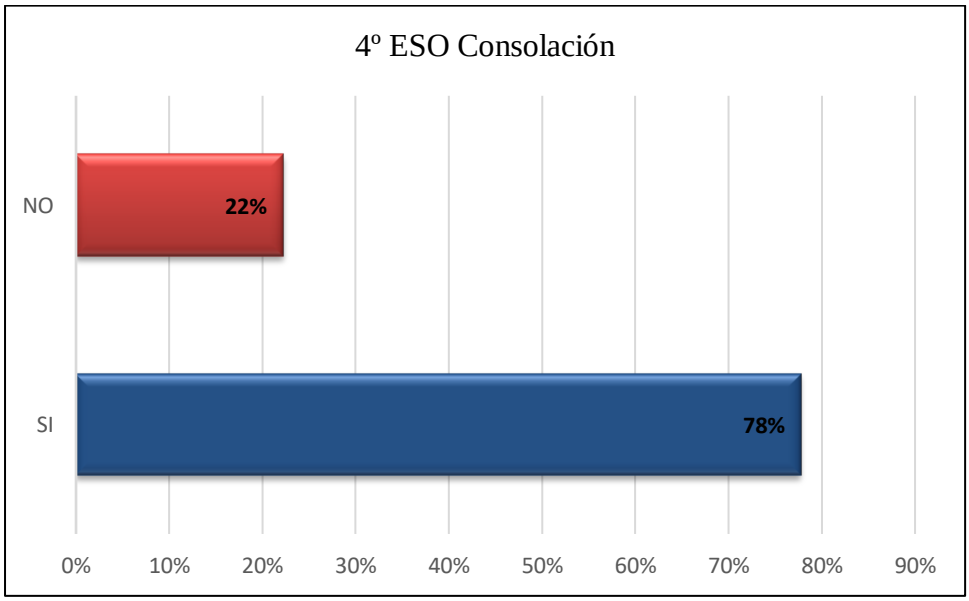

Figura 49. ¿Guardas información personal en tu teléfono móvil?

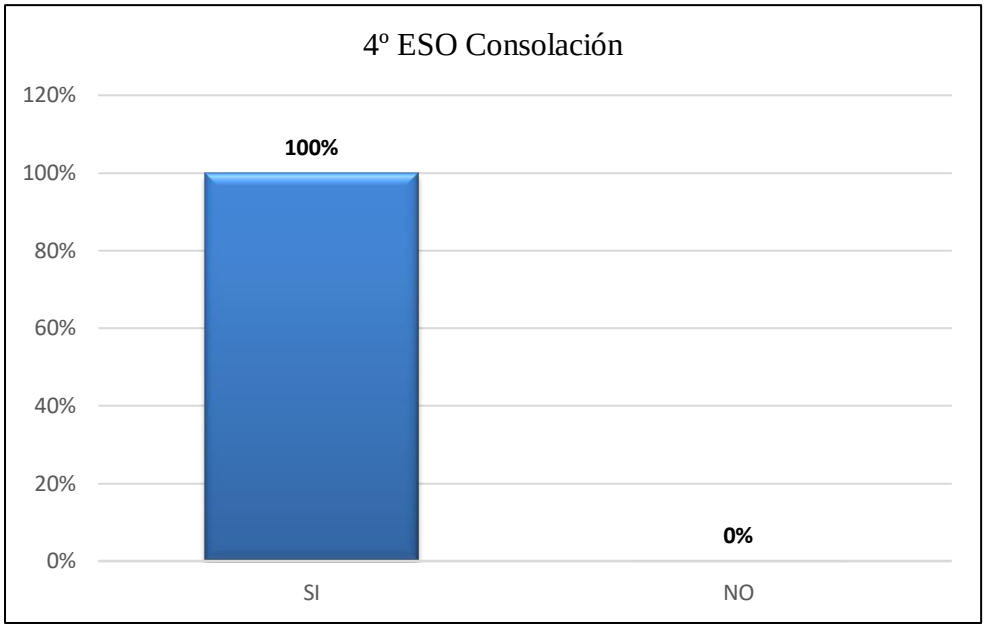

Figura 50. ¿Tienes cuenta de correo electrónico?

Figura 51. ¿Utilizas programas de mensajería instantánea?

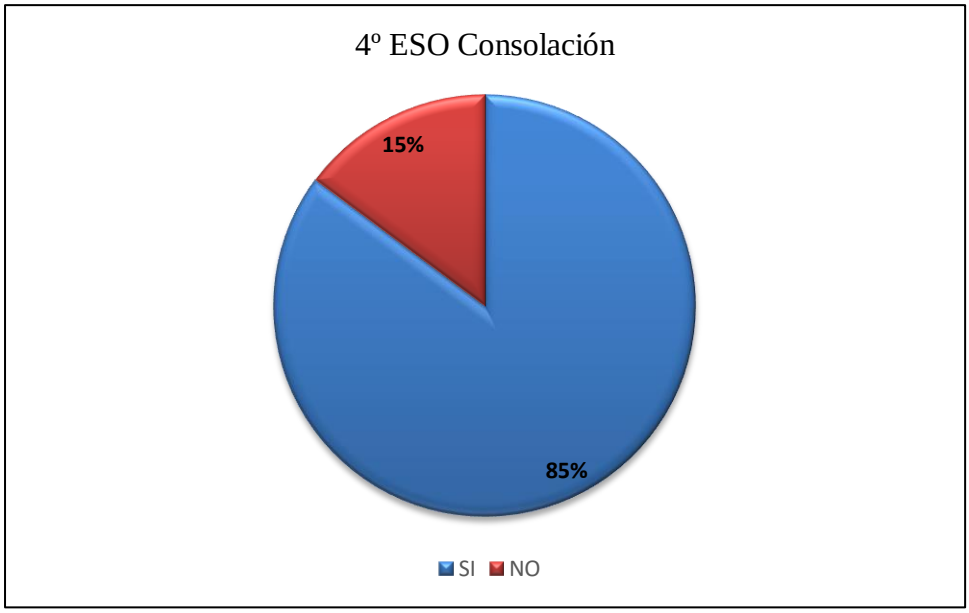

Figura 52. ¿Utilizas redes sociales?

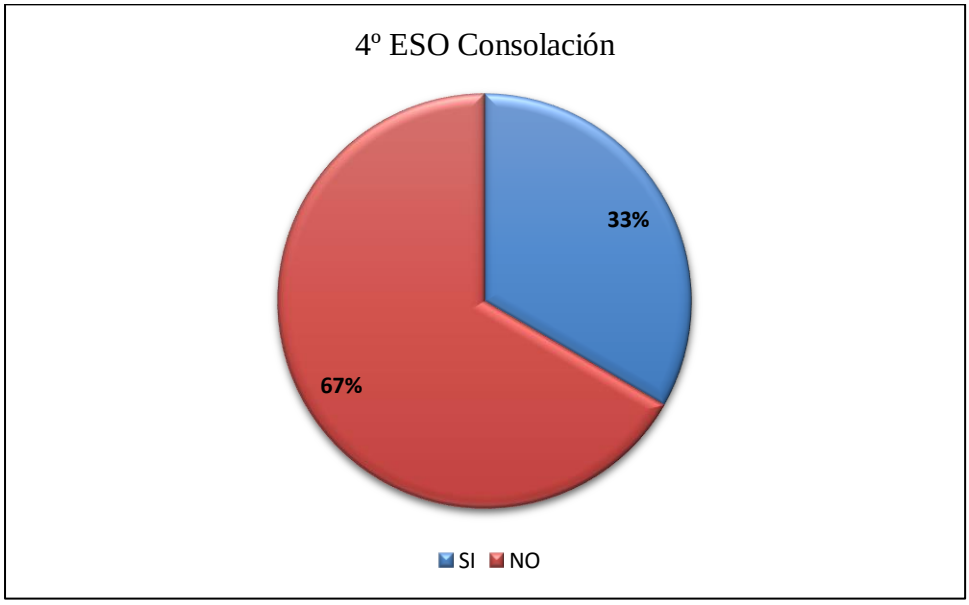

Figura 53. ¿Utilizas blogs, foros en Internet?

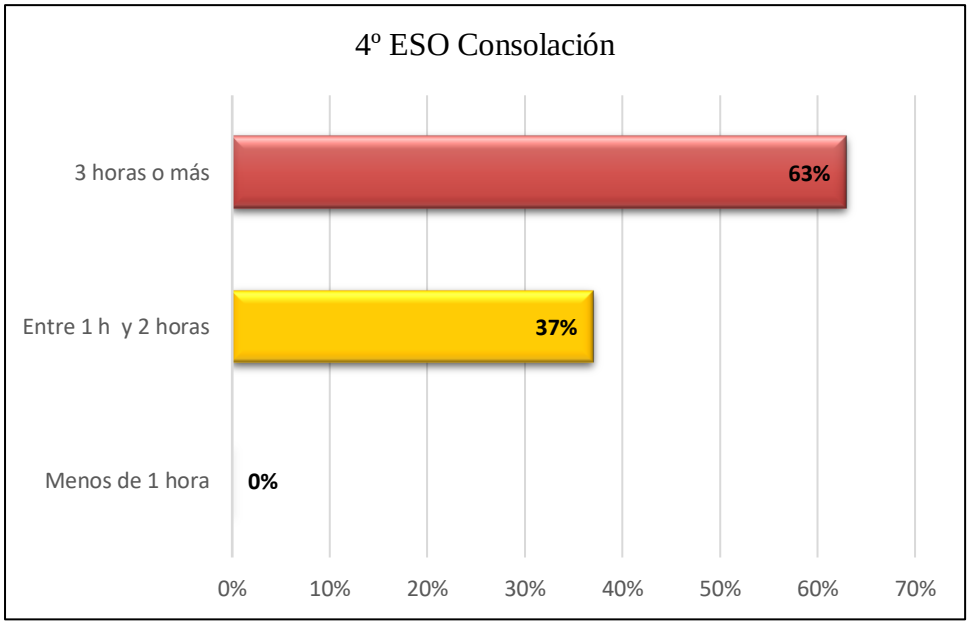

Figura 54. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

A continuación, podemos observar en las tablas 20 a 59 y figuras 55 a 74, respectivamente, los resultados obtenidos a las contestaciones de los 20 ítems, de escala frecuencia tipo Likert (de 1 a 5), relacionadas con hechos o conductas de los menores participantes de 1º a 4º de la ESO del centro educativo Consolación, que han servido para valorar los ciberriesgos a los que están expuestos tanto desde la perspectiva criminológica de la víctima como del victimario de ciberacoso, sexting, online grooming y violencia de género digital, en su caso.

1. ¿Has realizado mensajes y/o llamadas ofensivas a través de teléfono móvil y/o Internet?

Tabla 20. *Ítem. 1. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	79%	85%
2	Pocas veces	0%	0%	21%	15%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 21. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han realizado mensajes y/o llamadas ofensivas a través de teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,21	0,418	1	2
4º ESO	1,15	0,362	1	2

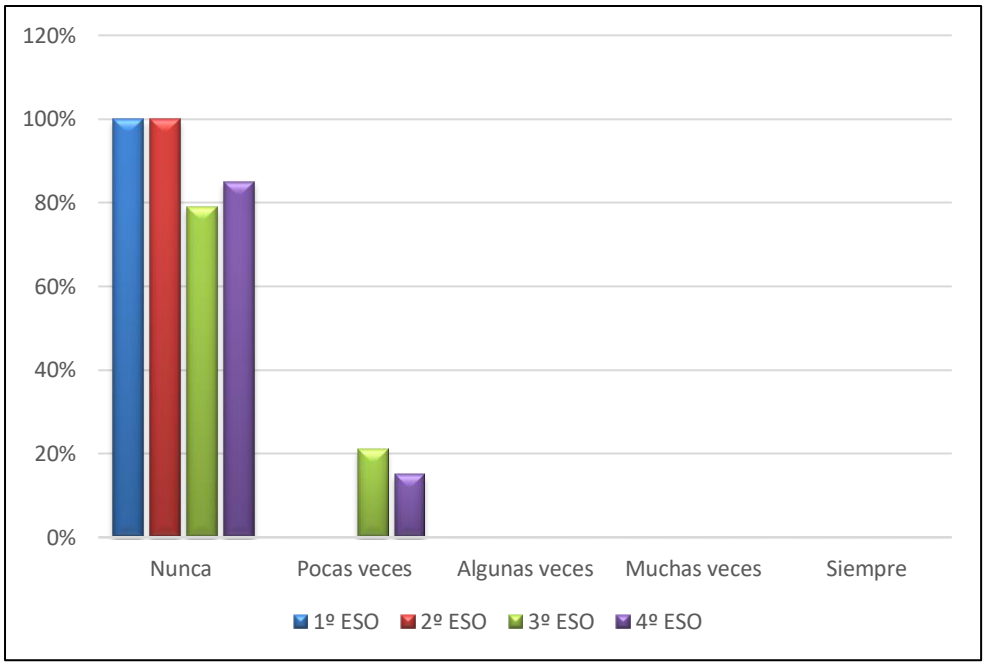

Figura 55. Ítem 1. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

2. ¿Has colgado en Internet una pelea, agresión o burla que ha sido grabada?

Tabla 22. *Ítem. 2. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	89%	100%
2	Pocas veces	0%	0%	11%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 23. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han colgado en Internet una pelea, agresión o burla que ha sido grabada.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,11	0,315	1	2
4º ESO	1	0	1	1

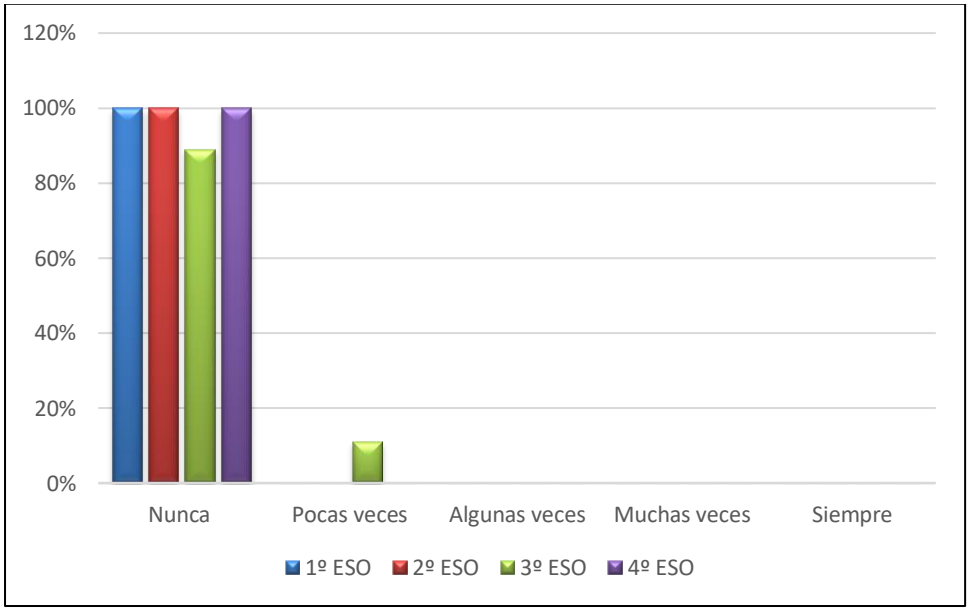

Figura 56. Ítem 2. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

3. ¿Has realizado comportamientos de tipo sexual a través de la webcam?

Tabla 24. *Ítem. 3. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	96%	96%
2	Pocas veces	0%	0%	0%	4%
3	Algunas veces	0%	0%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 25. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han realizado comportamientos de tipo sexual a través de la webcam.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,07	0,378	1	3
4º ESO	1,04	0,192	1	2

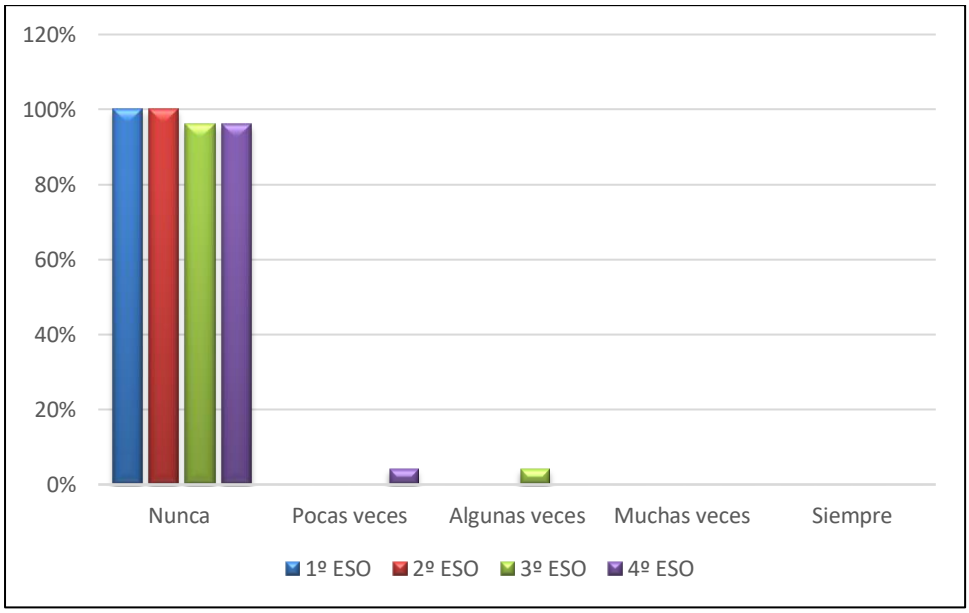

Figura 57. Ítem 3. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

4. ¿Has difundido vídeos y/o fotos privadas o comprometidas vía teléfono móvil o Internet?

Tabla 26. *Ítem. 4. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	93%	96%	96%
2	Pocas veces	0%	7%	4%	0%
3	Algunas veces	0%	0%	0%	4%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 27. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han difundido vídeos y/o fotos privadas o comprometidas vía teléfono móvil o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,07	0,267	1	2
3º ESO	1,04	0,189	1	2
4º ESO	1,07	0,385	1	3

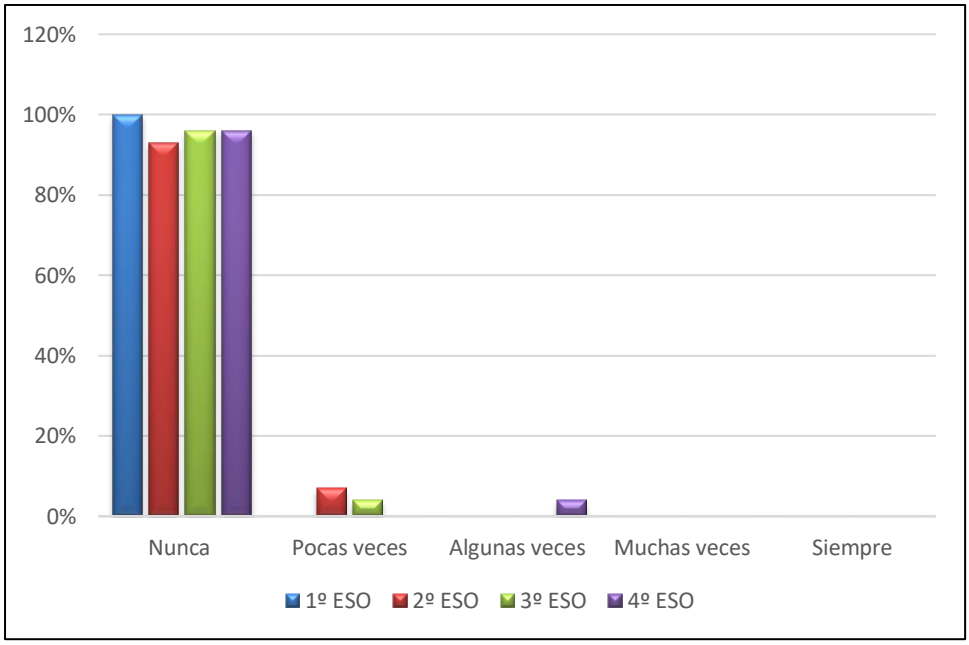

Figura 58. Ítem 4. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

5. ¿Has colgado vídeos y/o fotos robadas en Internet o difundirlos a través del teléfono móvil?

Tabla 28. *Ítem. 5. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	93%	85%	89%	85%
2	Pocas veces	7%	15%	7%	7%
3	Algunas veces	0%	0%	4%	4%
4	Muchas veces	0%	0%	0%	4%
5	Siempre	0%	0%	0%	0%

Tabla 29. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han colgado vídeos y/o fotos robadas en Internet o difundido a través del teléfono móvil.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,07	0,267	1	2
2º ESO	1,15	0,362	1	2
3º ESO	1,14	0,448	1	3
4º ESO	1,26	0,712	1	4

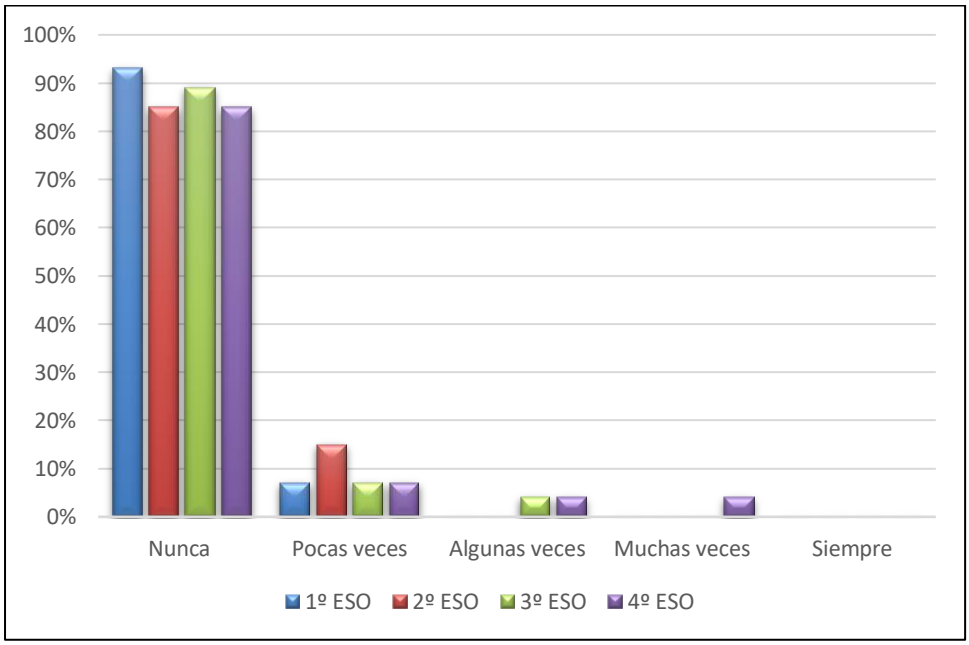

Figura 59. Ítem 5. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

6. ¿Has realizado llamadas anónimas para asustar o intimidar?

Tabla 30. *Ítem. 6. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	81%	70%	75%	70%
2	Pocas veces	11%	22%	18%	19%
3	Algunas veces	7%	4%	7%	11%
4	Muchas veces	0%	4%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 31. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han realizado llamadas anónimas para asustar o intimidar.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,26	0,594	1	3
2º ESO	1,41	0,747	1	4
3º ESO	1,32	0,612	1	3
4º ESO	1,41	0,694	1	3

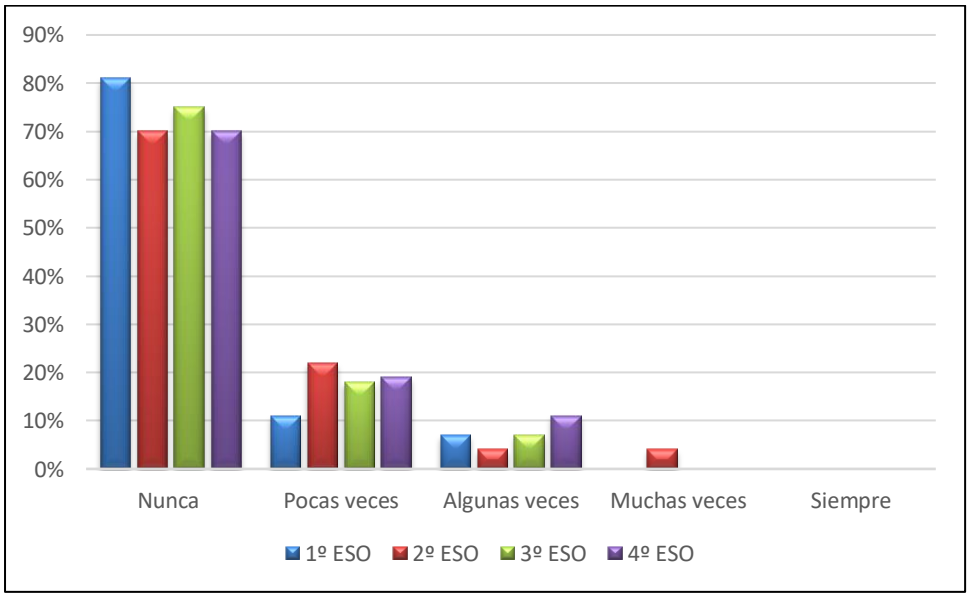

Figura 60. Ítem 6. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

7. ¿Has realizado amenazas o chantajes a través de mensajes y/o llamadas?

Tabla 32. *Ítem. 7. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	93%	100%	96%	93%
2	Pocas veces	7%	0%	4%	7%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 33. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han realizado amenazas o chantajes a través de mensajes y/o llamadas.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,07	0,267	1	2
2º ESO	1	0	1	1
3º ESO	1,04	0,189	1	2
4º ESO	1,07	0,267	1	2

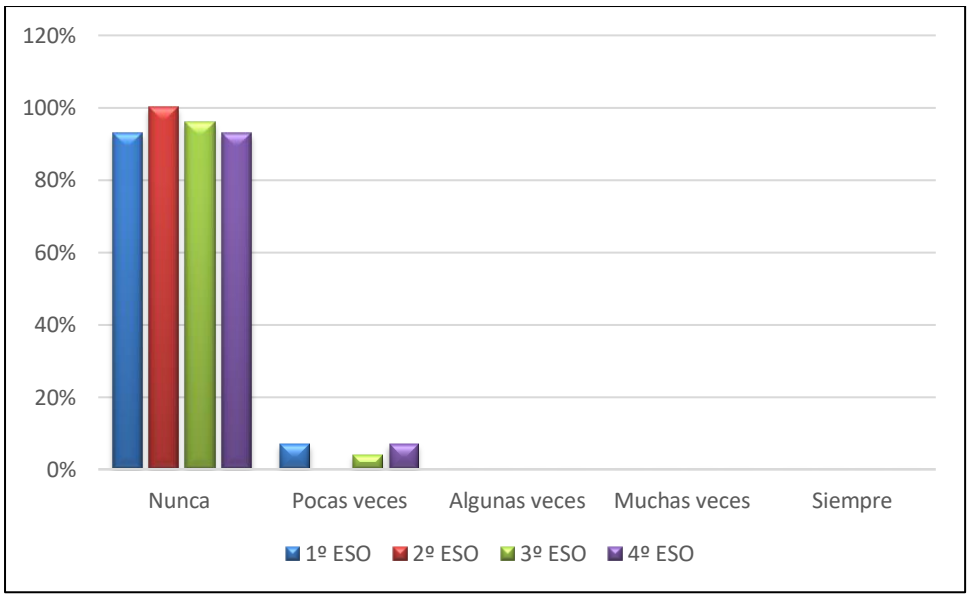

Figura 61. Ítem 7. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

8. ¿Has acosado sexualmente a través de teléfono móvil y/o Internet?

Tabla 34. *Ítem. 8. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	100%	100%
2	Pocas veces	0%	0%	0%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 35. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han acosado sexualmente a través de teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1	0	1	1
4º ESO	1	0	1	1

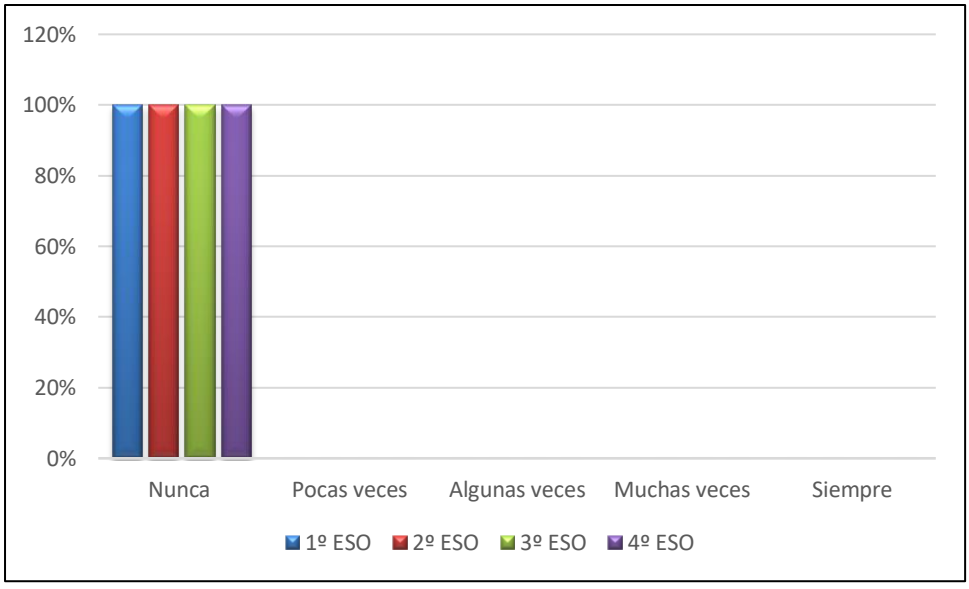

Figura 62. Ítem 8. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

9. ¿Has suplantado a una persona para difamar, mentir o contar sus secretos?

Tabla 36. *Ítem. 9. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	96%	89%	96%
2	Pocas veces	0%	0%	11%	0%
3	Algunas veces	0%	4%	0%	4%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 37. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han suplantado a una persona para difamar, mentir o contar sus secretos.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,07	0,385	1	3
3º ESO	1,11	0,315	1	2
4º ESO	1,07	0,385	1	3

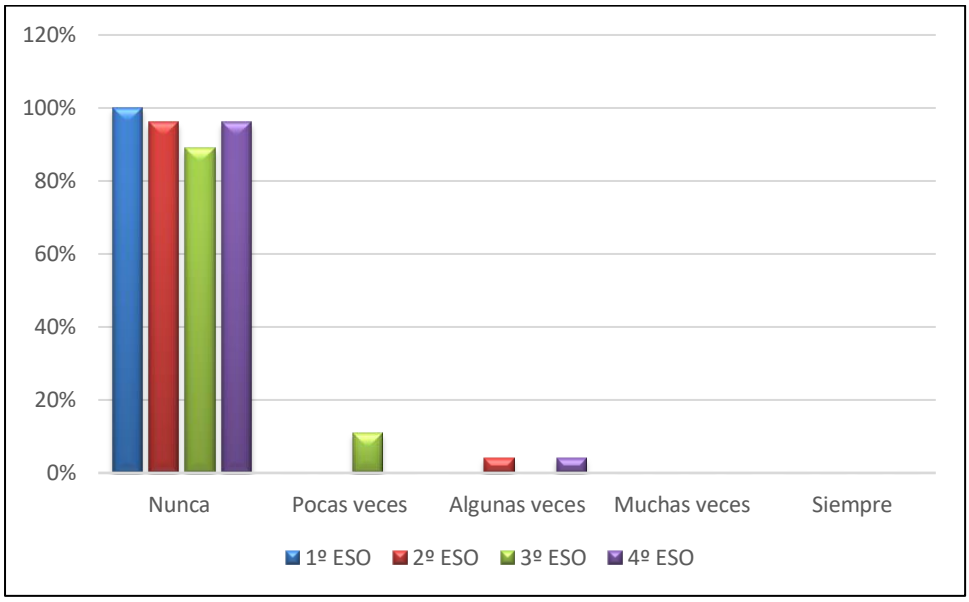

Figura 63. Ítem 9. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

10. ¿Has robado la contraseña a una persona?

Tabla 38. *Ítem. 10. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	96%	96%	93%	93%
2	Pocas veces	4%	0%	4%	7%
3	Algunas veces	0%	4%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 39. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han robado la contraseña a una persona.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,04	0,192	1	2
2º ESO	1,07	0,385	1	3
3º ESO	1,11	0,416	1	3
4º ESO	1,07	0,267	1	2

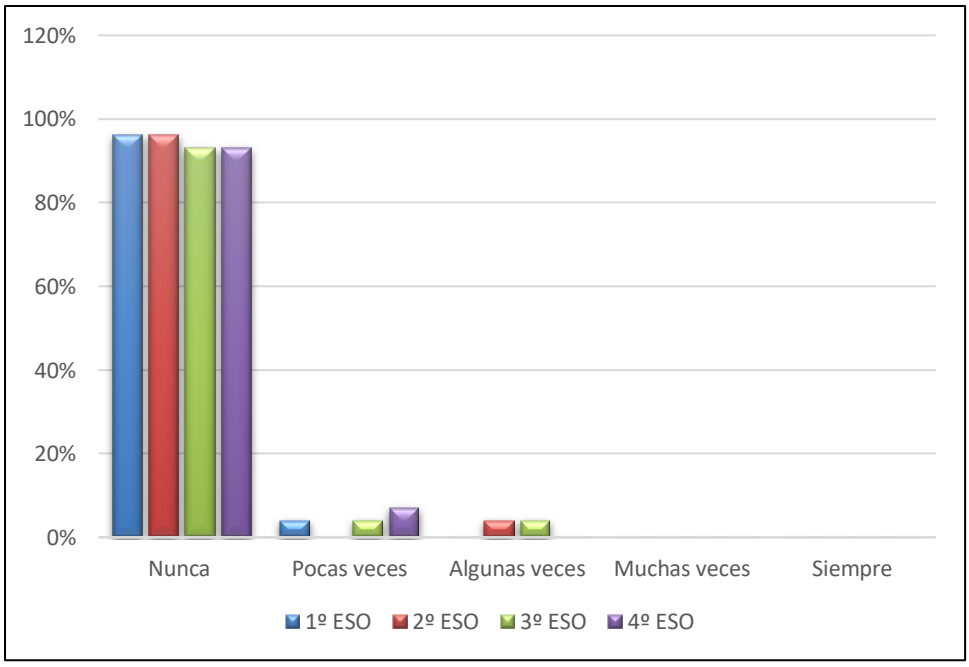

Figura 64. Ítem 10. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

11. ¿Has trucado fotos y vídeos para difundirlos y humillar vía teléfono móvil y/o Internet?

Tabla 40. *Ítem. 11. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	96%	93%	93%
2	Pocas veces	0%	4%	4%	7%
3	Algunas veces	0%	0%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 41. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han trucado fotos y vídeos para difundirlos y humillar vía teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,04	0,192	1	2
3º ESO	1,11	0,416	1	3
4º ESO	1,07	0,267	1	2

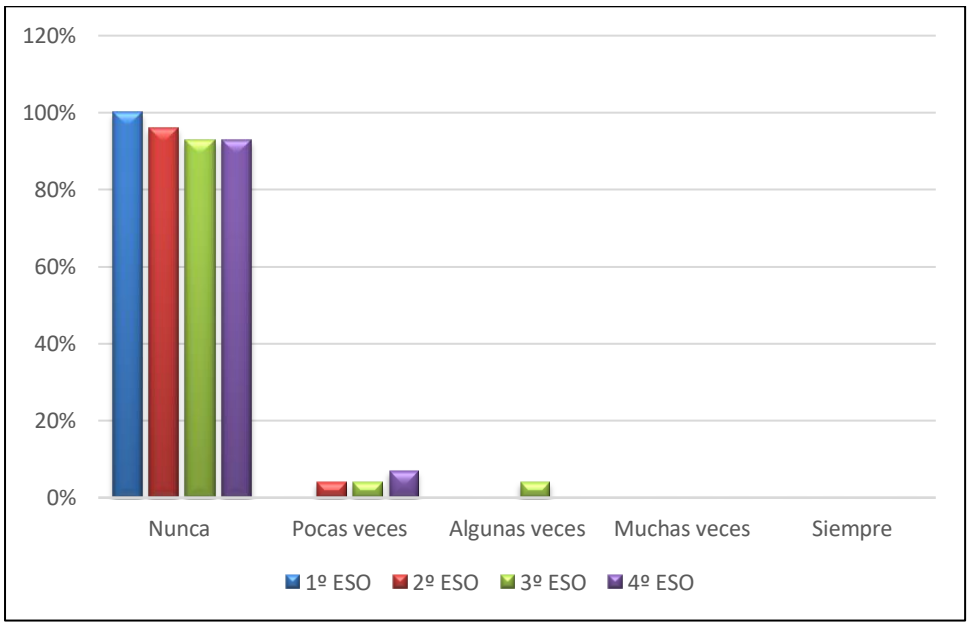

Figura 65. Ítem 11. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

12. ¿Has acosado a alguien para aislarle de sus contactos en las redes sociales?

Tabla 42. *Ítem. 12. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	96%	96%	100%
2	Pocas veces	0%	4%	4%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 43. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han acosado a alguien para aislarle de sus contactos en las redes sociales.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,04	0,192	1	2
3º ESO	1,04	0,189	1	2
4º ESO	1	0	1	1

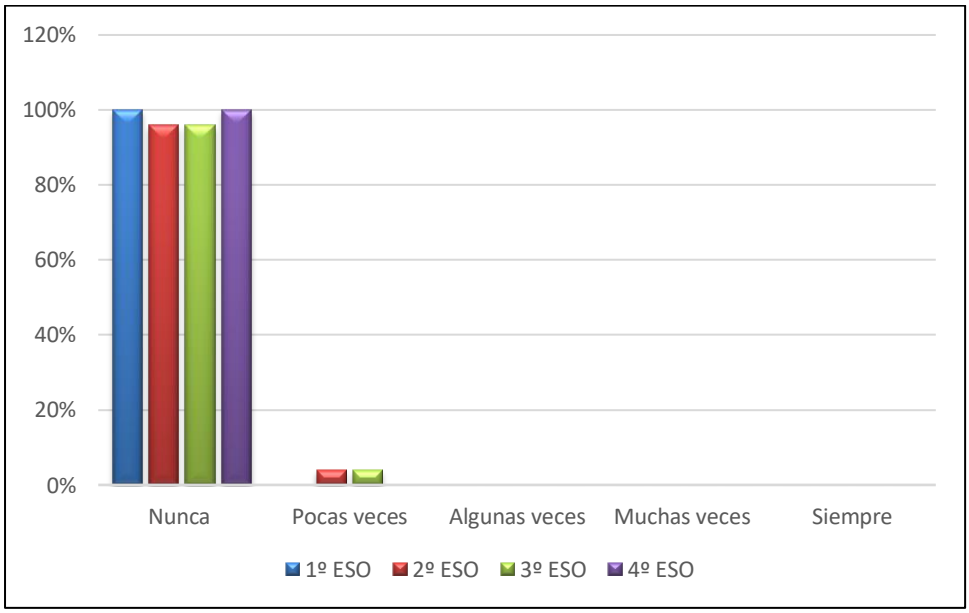

Figura 66. Ítem 12. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

13. ¿Has chantajeado a cambio de no divulgar información íntima vía teléfono y/o Internet?

Tabla 44. *Ítem. 13. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	96%	96%	93%	100%
2	Pocas veces	4%	4%	4%	0%
3	Algunas veces	0%	0%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 45. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han chantajeado a cambio de no divulgar información íntima vía teléfono y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,04	0,192	1	2
2º ESO	1,04	0,192	1	2
3º ESO	1,11	0,416	1	3
4º ESO	1	0	1	1

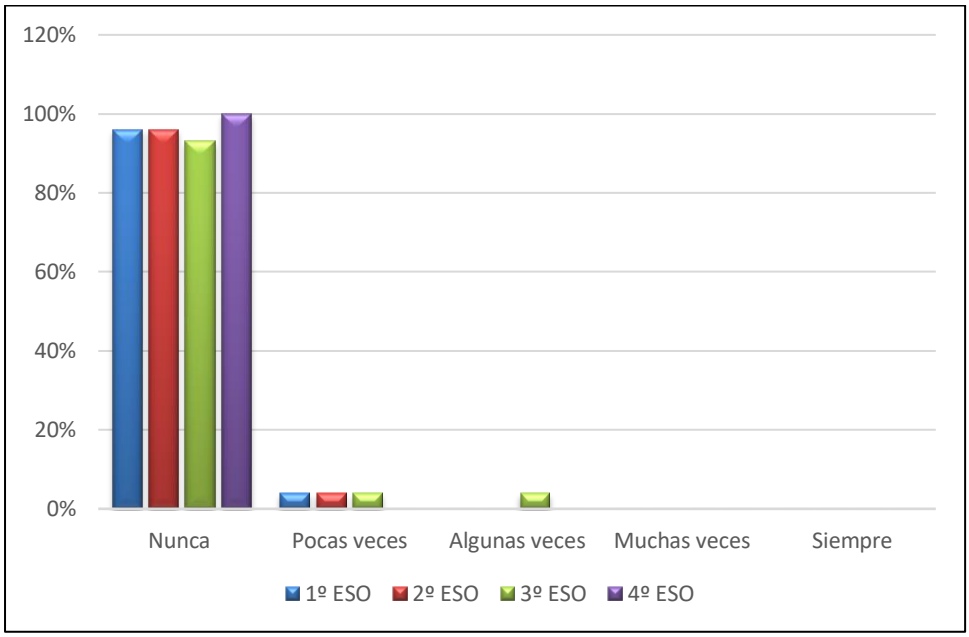

Figura 67. Ítem 13. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

14. ¿Has amenazado de muerte a alguien a través de teléfono móvil y/o Internet?

Tabla 46. *Ítem. 14. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	96%	96%	100%
2	Pocas veces	0%	4%	4%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 47. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han amenazado de muerte a alguien a través de teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,04	0,192	1	2
3º ESO	1,04	0,189	1	2
4º ESO	1	0	1	1

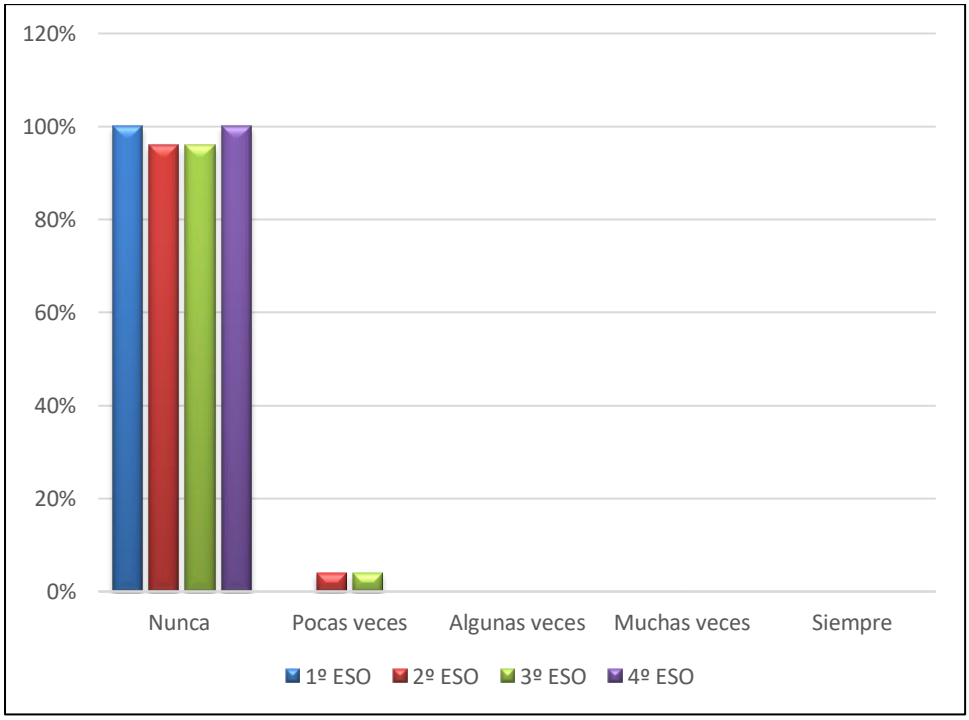

Figura 68. Ítem 14. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

15. ¿Has difundido y/o difamado con rumores para hacer daño vía teléfono móvil y/o internet?

Tabla 48. *Ítem. 15. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	96%	96%	96%	96%
2	Pocas veces	4%	4%	0%	4%
3	Algunas veces	0%	0%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 49. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han difundido y/o difamado con rumores para hacer daño vía teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,04	0,192	1	2
2º ESO	1,04	0,192	1	2
3º ESO	1,07	0,378	1	3
4º ESO	1,04	0,192	1	2

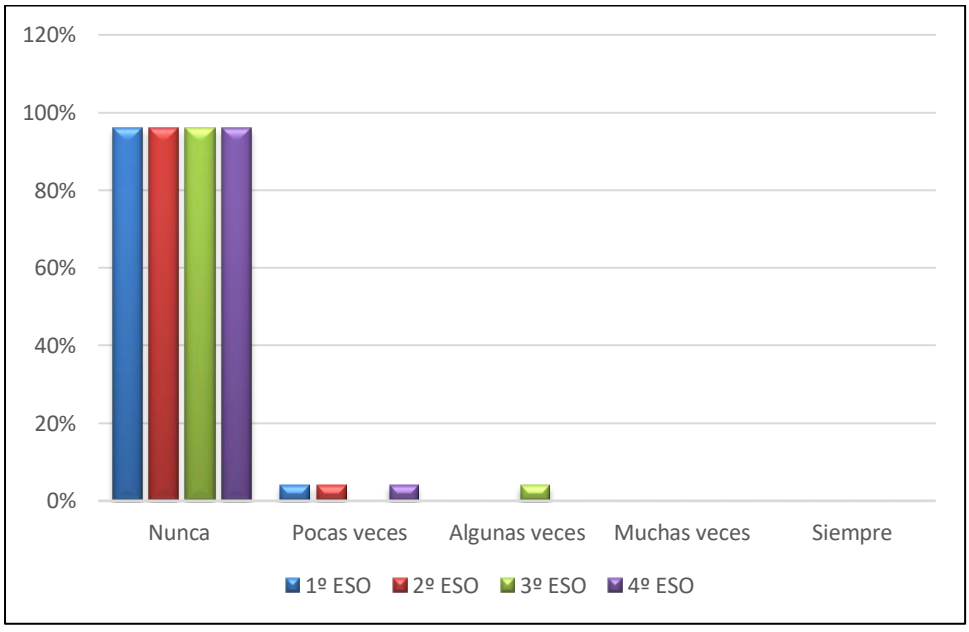

Figura 69. Ítem 15. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

16. ¿Has contactado con un adulto que se ha ganado tu confianza en las redes sociales?

Tabla 50. *Ítem. 16. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	93%	89%	86%	81%
2	Pocas veces	4%	4%	4%	11%
3	Algunas veces	4%	7%	7%	4%
4	Muchas veces	0%	0%	4%	0%
5	Siempre	0%	0%	0%	4%

Tabla 51. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han contactado con un adulto que se ha ganado su confianza en las redes sociales.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,11	0,424	1	3
2º ESO	1,19	0,557	1	3
3º ESO	1,29	0,582	1	4
4º ESO	1,33	0,877	1	5

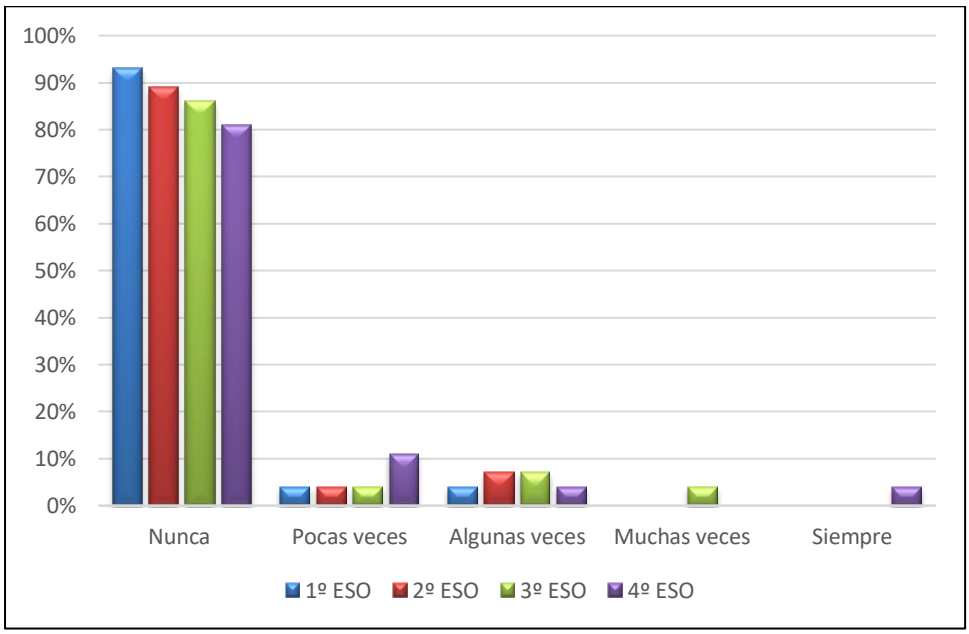

Figura 70. Ítem 16. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

17. ¿Controlas los amigos/as en redes sociales, mensajes, WhatsApp, etc., de tu pareja?

Tabla 52. *Ítem. 17. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	89%	71%	78%
2	Pocas veces	0%	7%	21%	7%
3	Algunas veces	0%	4%	4%	15%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	4%	0%

Tabla 53. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han controlado los amigos/as en redes sociales, mensajes, WhatsApp, etc., de su pareja.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,15	0,456	1	3
3º ESO	1,43	0,879	1	5
4º ESO	1,37	0,742	1	3

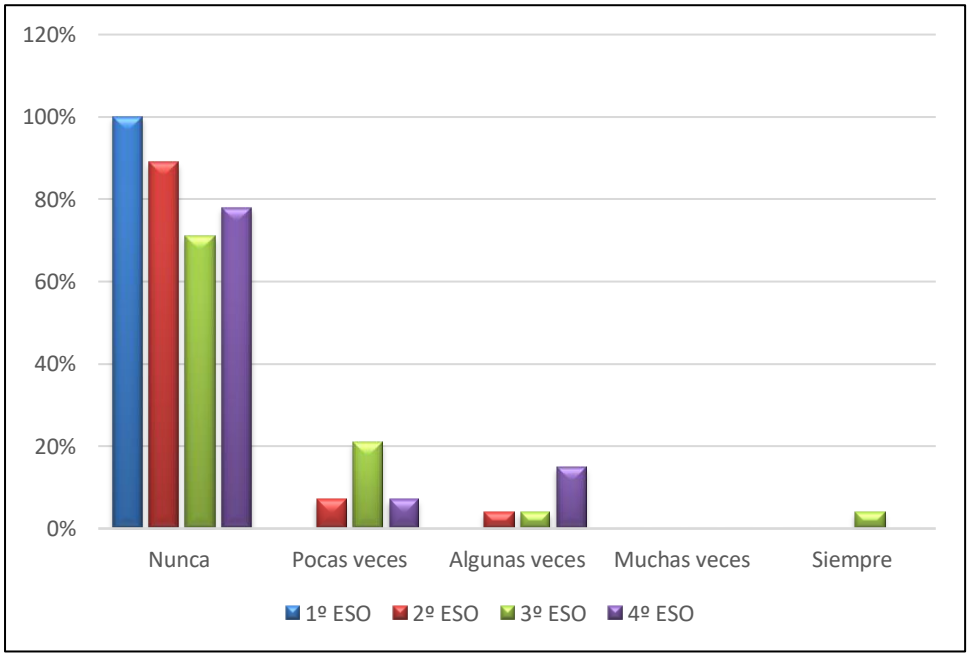

Figura 71. Ítem 17. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

18. ¿Has pedido a tu pareja que retire fotos o comentarios de redes sociales, WhatsApp, etc.?

Tabla 54. *Ítem. 18. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	89%	89%	78%
2	Pocas veces	0%	7%	7%	15%
3	Algunas veces	0%	0%	4%	7%
4	Muchas veces	0%	4%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 55. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han pedido a su pareja que retire fotos o comentarios de redes sociales, WhatsApp, etc.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,19	0,622	1	4
3º ESO	1,14	0,448	1	3
4º ESO	1,30	0,609	1	3

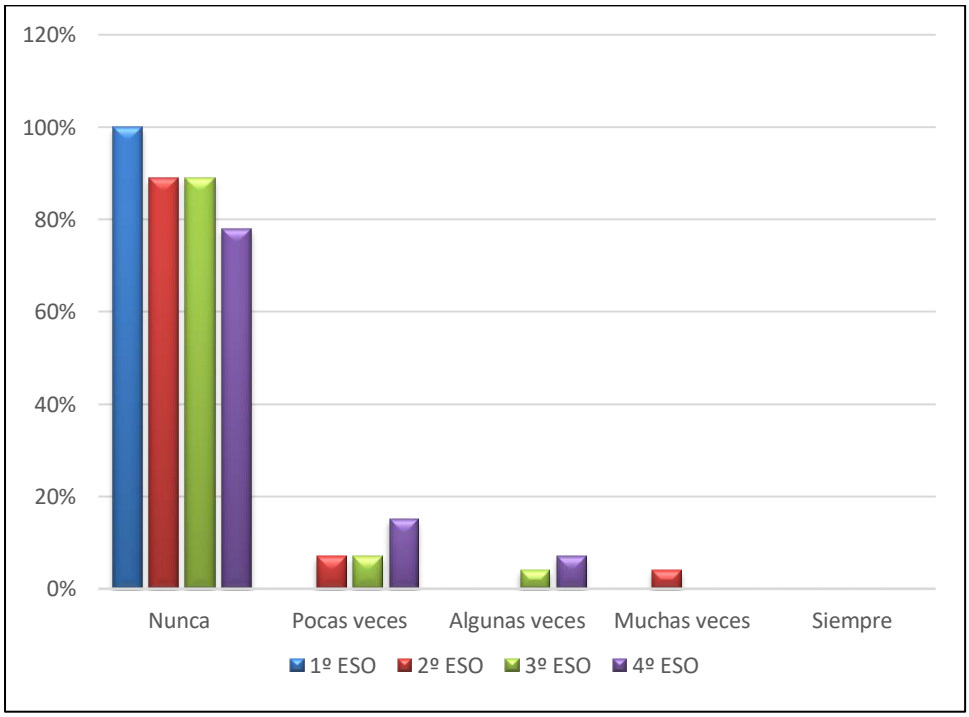

Figura 72. Ítem 18. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

19. ¿Has pedido a tu pareja que suprima o borre a amigos/as en redes sociales, etc.?

Tabla 56. *Ítem. 19. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	96%	93%	89%
2	Pocas veces	0%	4%	4%	7%
3	Algunas veces	0%	0%	4%	4%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 57. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han pedido a su pareja que suprima o borre a amigos/as en redes sociales, etc.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,04	0,192	1	2
3º ESO	1,11	0,416	1	3
4º ESO	1,15	0,456	1	3

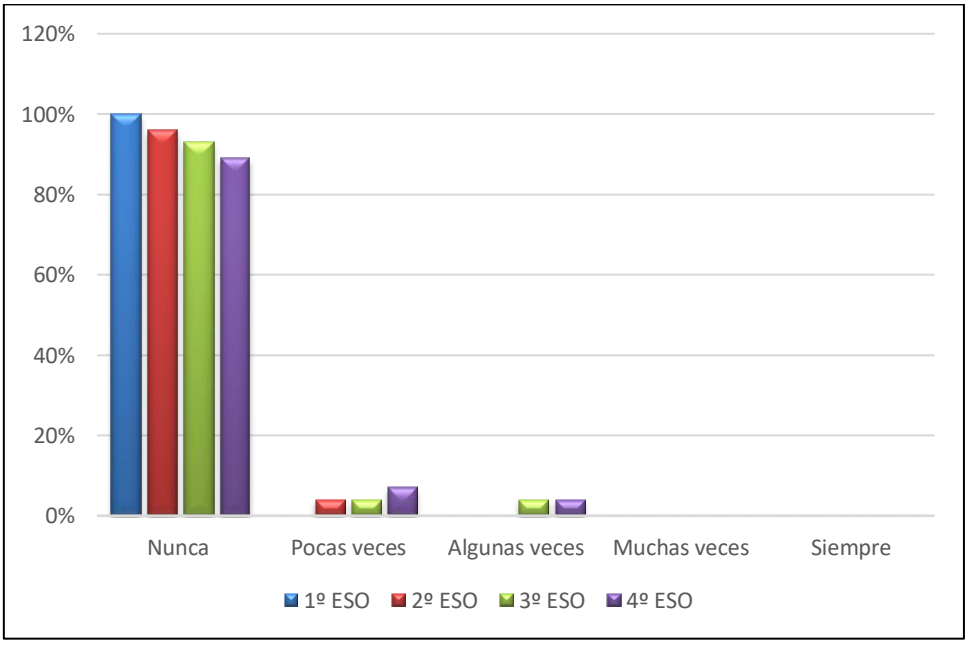

Figura 73. Ítem 19. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

20. ¿Has obligado a tu pareja a realizar comportamientos de tipo sexual a través de la webcam?

Tabla 58. *Ítem. 20. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	96%	100%
2	Pocas veces	0%	0%	4%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 59. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Consolación han obligado a su pareja a realizar comportamientos de tipo sexual a través de la webcam.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,04	0,189	1	2
4º ESO	1	0	1	1

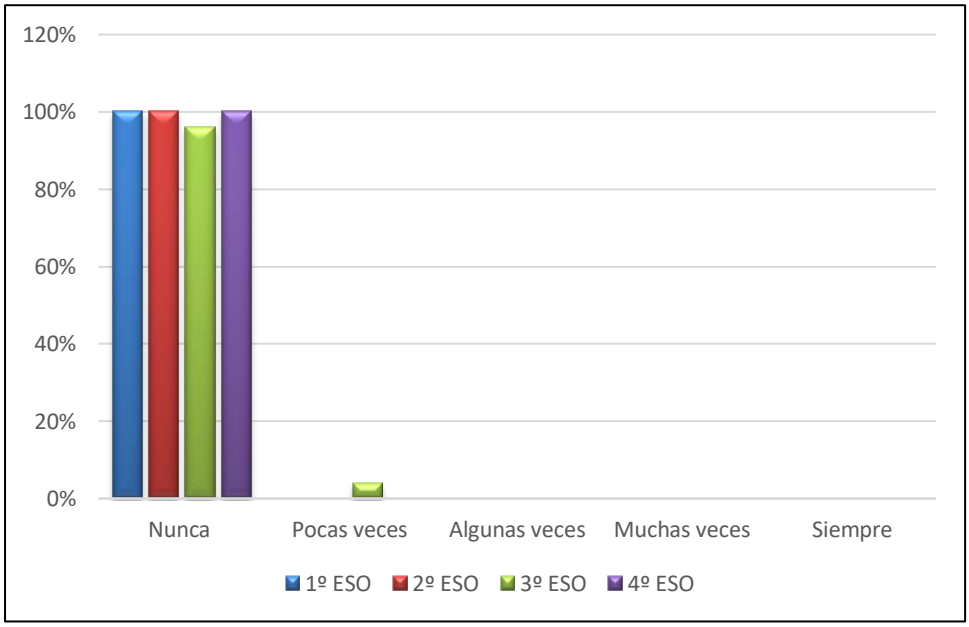

Figura 74. Ítem 20. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Consolación.

En la tabla 60 y figura 75, podemos apreciar que, de los 109 menores participantes, 49 chicos y 60 chicas, respectivamente, de los cursos 1º a 4º de la ESO de la Consolación, con relación a la pregunta de a quién comunicarían los hechos o conductas reseñados en los ítems 1 a 20, ambos inclusive, en el caso de observarlos y/o protagonizarlos, en primer lugar, la mayoría contestaron que lo participarían a sus padres, en segundo lugar, a sus compañeros, en tercer lugar, a sus profesores y, por último, a nadie.

Tabla 60. *Resultados sobre a quién comunicarían los observadores, víctimas y/o victimarios, en su caso, alguno de los hechos o conductas mencionados (Consolación).*

	Colegio N. Sª de la Consolación			
Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Compañeros	18%	22%	31%	23%
Padres	63%	64%	44%	77%
Profesores	13%	11%	20%	0%
A nadie	5%	3%	4%	0%

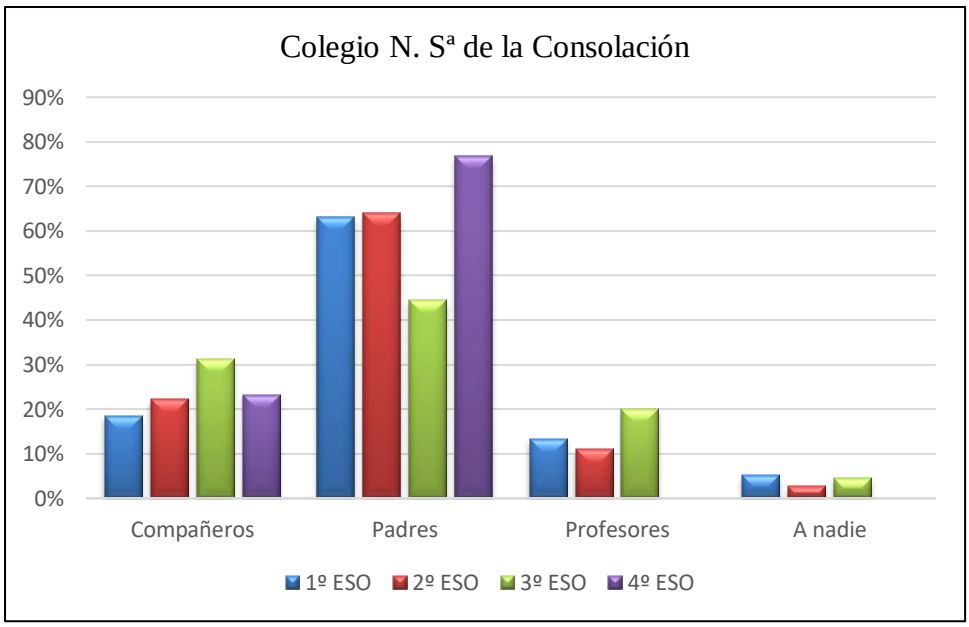

Figura 75. Comparativa de resultados de 1º a 4º de la ESO Consolación (tabla 60).

A continuación, en las figuras 76 a 79, podemos observar por cursos de la ESO del Colegio Consolación los resultados porcentuales obtenidos en las contestaciones a la pregunta mencionada por parte de los menores que han participado en este estudio criminológico social.

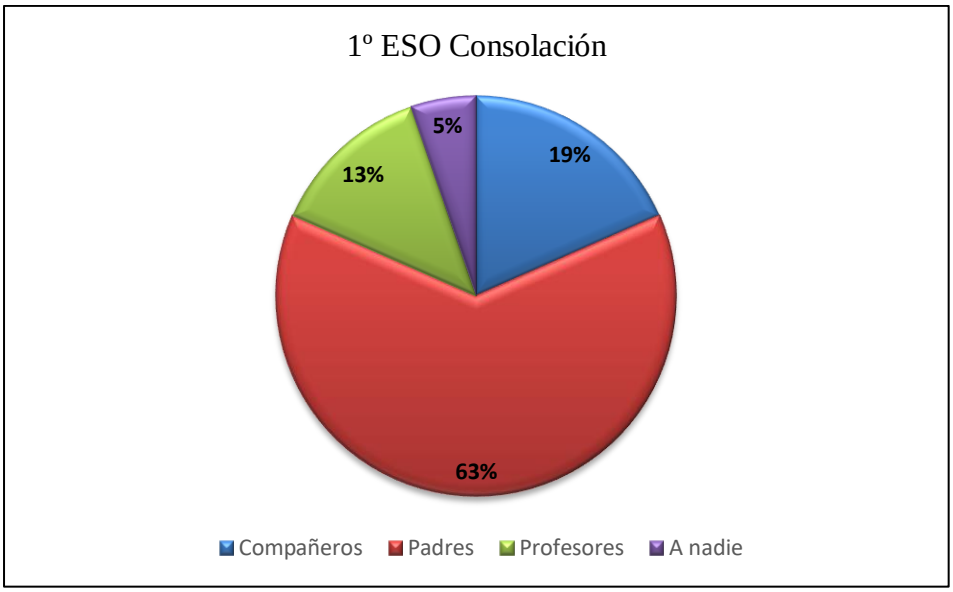

Figura 76. -1º ESO Consolación: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

Figura 77. -2º ESO Consolación: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

Figura 78. -3º ESO Consolación: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

Figura 79. -4º ESO Consolación: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

Por otra parte, en lo atinente a los resultados arrojados respecto a la pregunta sobre qué actividades preventivas propondrían frente a hechos o conductas de ciberacoso, y que se han plasmado en la tabla 61 y en las figuras 80 a 84, respectivamente, podemos destacar que los alumnos del Colegio Consolación del curso de 1º de la ESO, mayoritariamente (un 45% frente a un 26%), optaría por comunicarlo a personas adultas antes que denunciarlo a la policía. Sin embargo, los alumnos de 4º de la ESO son más partidarios de denunciar a la policía (un 35% frente a un 27%) que comunicar los hechos a adultos.

Curiosamente, respecto a la opción de respuesta de mediación con el ciberacosador, los resultados obtenidos oscilan del 2% al 4%, constituyendo una evidencia de que, en general, el alumnado de la ESO participante no cree en esta figura para prevenir, abordar y resolver conflictos con el ciberacosador, a pesar de que se contempla en el artículo 10 de la Orden 62/2014, de 28 de julio, de la Conselleria de Educación, Cultura y Deporte, por la que se actualiza la normativa que regula la elaboración de los planes de convivencia en los centros educativos de la Comunitat Valenciana y se establecen los protocolos de actuación e intervención ante supuestos de violencia escolar.

Por último, podemos destacar que un porcentaje muy minoritario del alumnado participante de la ESO, concretamente, entre un 0% y un 6%, marcó como respuesta ignorar el ciberacoso.

Tabla 61. *Resultados sobre las propuestas que hacen los menores participantes para evitar hechos o conductas de ciberacoso (Consolación).*

	Colegio N. Sª de la Consolación			
Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Comunicar adultos	45%	33%	34%	27%
Denunciar a la policía	26%	35%	31%	35%
Ignorar ciberacoso	6%	0%	3%	0%
Mediar con el ciberacosador	4%	4%	3%	2%
Pedir ayuda	19%	22%	25%	33%
Otras	0%	6%	3%	4%

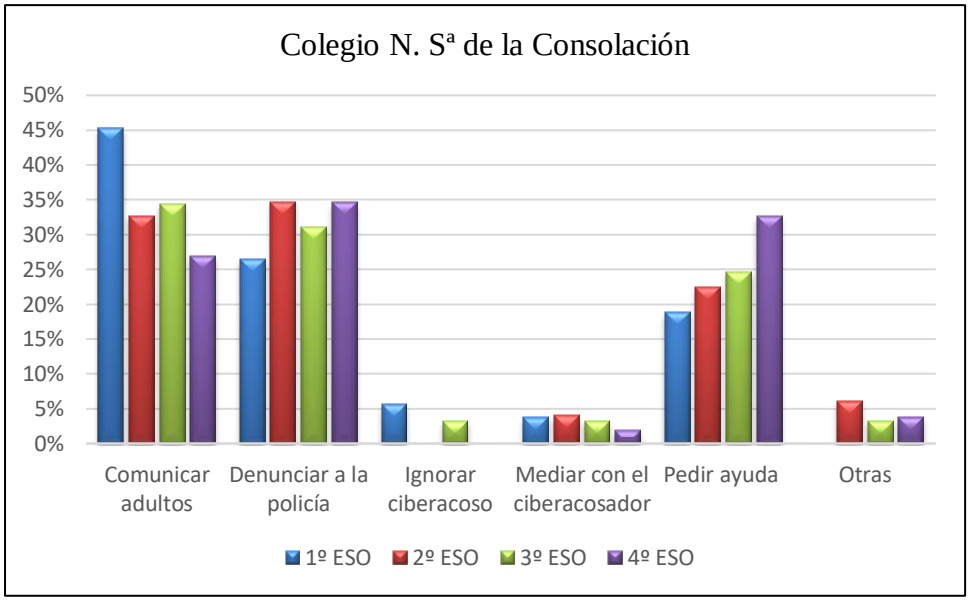

Figura 80. Comparativa de resultados 1º a 4º de la ESO Consolación (tabla 61).

Figura 81. -1º ESO Consolación: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

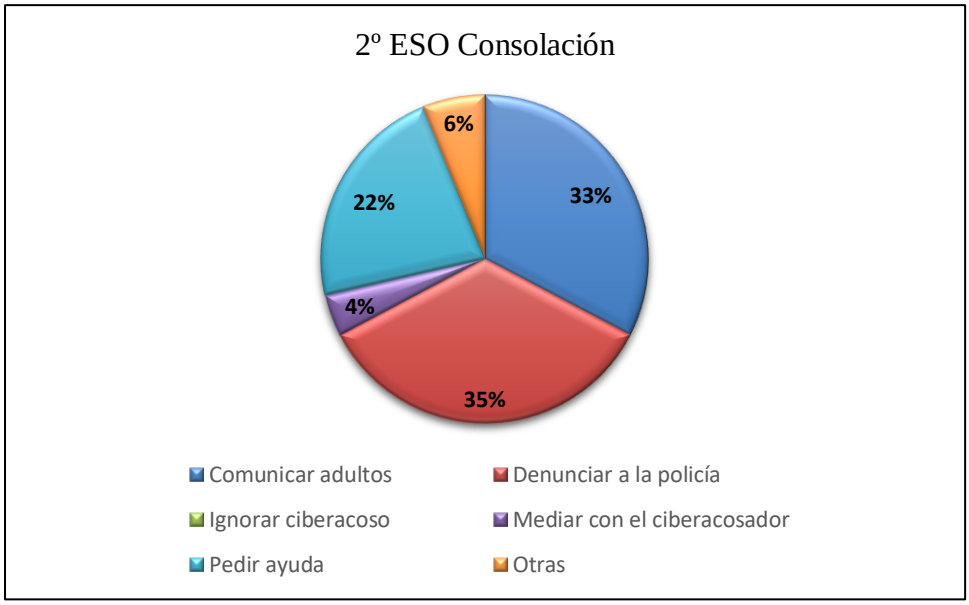

Figura 82. -2º ESO Consolación: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

Figura 83. -3º ESO Consolación: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

Figura 84. -4º ESO Consolación: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

b)-Nuestra Señora Divina Providencia: de un total de 125 alumnos matriculados de la ESO, se ha tomado una muestra de este centro educativo de 109 alumnos encuestados que han participado voluntariamente, de los que un 49% son chicas y un 51% son chicos, de 12 a 17 años, correspondientes a los cursos de 1º a 4º de la ESO, tal y como podemos observar en la tabla 62 y figura 85, respectivamente.

Concretamente, de 1º de la ESO la media de edad es 12,35 años; de 2º de la ESO es 13,78 años; de 3º ESO es de 14,46 años y de 4º ESO es 15,36 años.

Tabla 62. *Edad y género de los menores participantes de la ESO de N. Sª Divina Providencia.*

Curso académico	Edades	Chicos	Chicas	
1º ESO	12-14	12	19	31
2º ESO	13-16	18	9	27
3º ESO	14-17	10	16	26
4º ESO	15-16	16	9	25
	Totales	56	53	109

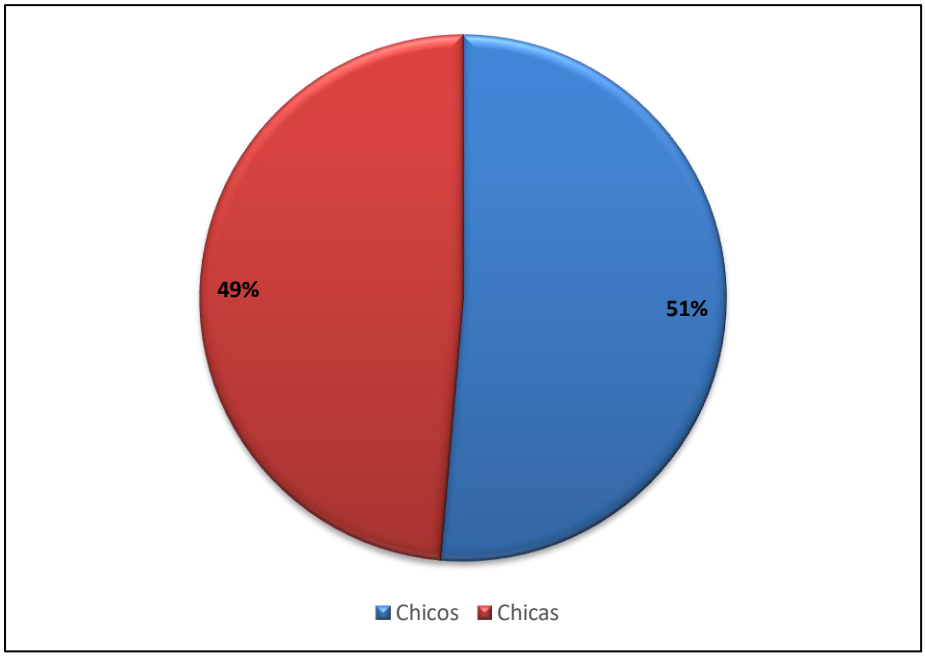

Figura 85. Porcentaje total participantes por género de la ESO de N. Sª Divina Providencia.

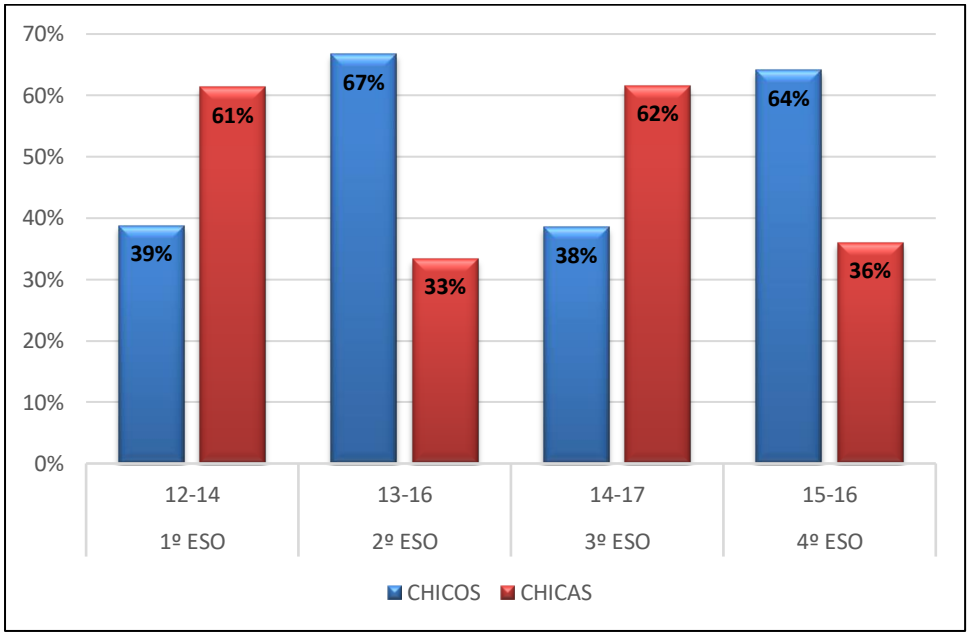

Figura 86. Menores de la ESO de N. Sª de la Divina Providencia por curso académico y género.

El curso académico que más chicos hay es 2º ESO y en el que menos 3º ESO. Sin embargo, con relación a las chicas, podemos destacar que el curso que menos hay es 2º ESO y en los cursos cuya representación es mayor que la de los chicos, son 1º y 3º de la ESO, respectivamente, tal y como podemos apreciar en la figura 86.

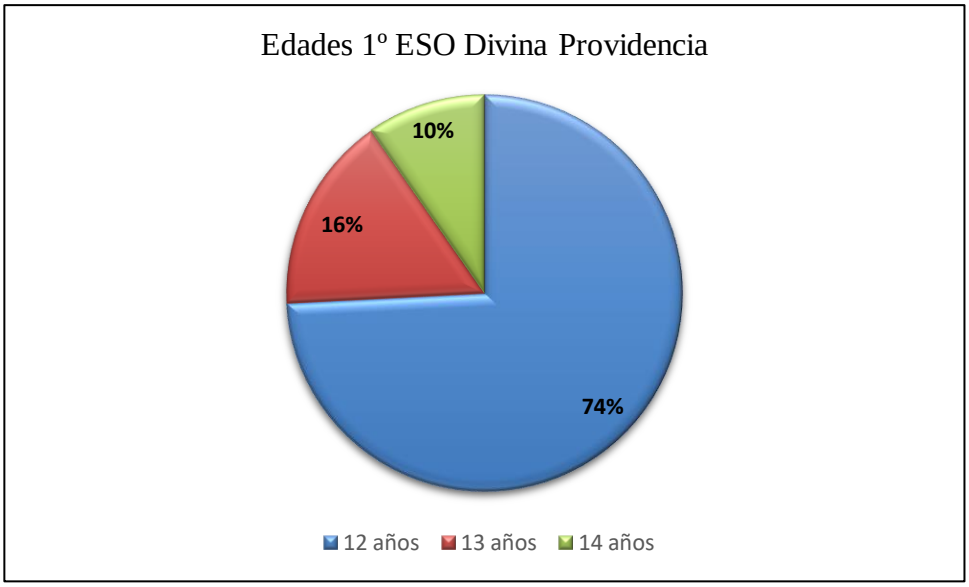

Figura 87. Edades menores de 1º ESO de N. Sª de la Divina Providencia.

En la figura 87, podemos apreciar que dentro del rango de edad de los menores participantes en el presente estudio correspondientes al curso de 1º de la ESO de N. Sª de la Divina Providencia, la mayoría tiene 12 años, es decir, un 74%, mientras que un 16% tiene 13 años y el 10% restante tiene 14 años.

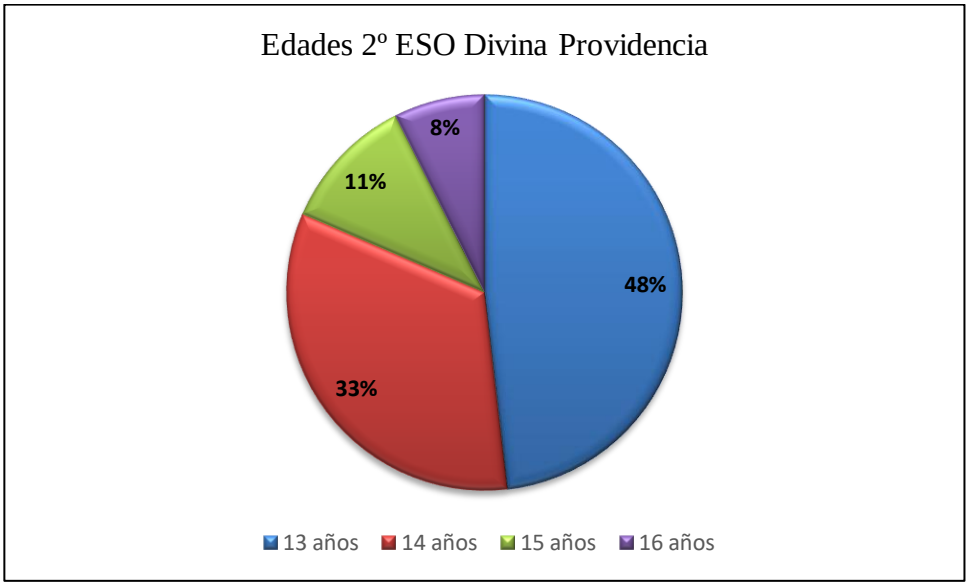

Figura 88. Edades menores de 2º ESO de N. Sª de la Divina Providencia.

En la figura 88, podemos destacar que del curso 2º de la ESO de N. Sª de la Divina Providencia, la mayoría de los participantes tiene 13 años, es decir, un 48%, mientras que una minoría del 8% tiene 16 años y el resto tiene 14 (33%) y 15 años (11%), respectivamente.

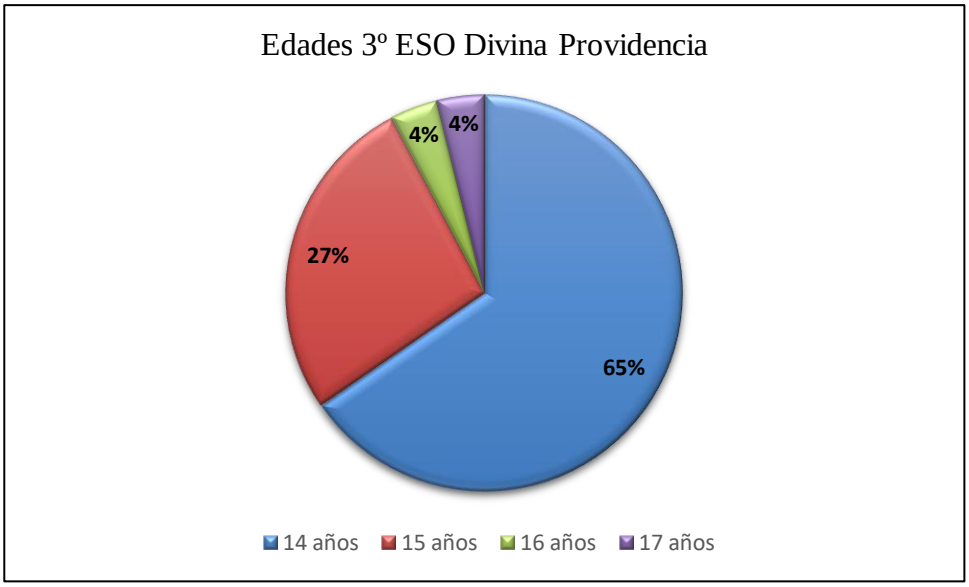

Figura 89. Edades menores de 3º ESO de N. Sª de la Divina Providencia.

En la figura 89, podemos observar que del curso 3º de la ESO de N. Sª de la Divina Providencia, la mayoría tiene 14 años, es decir, un 65%, mientras que tan solo un 4% tiene 16 años y 17 años, respectivamente, y el 27% restante tiene 15 años.

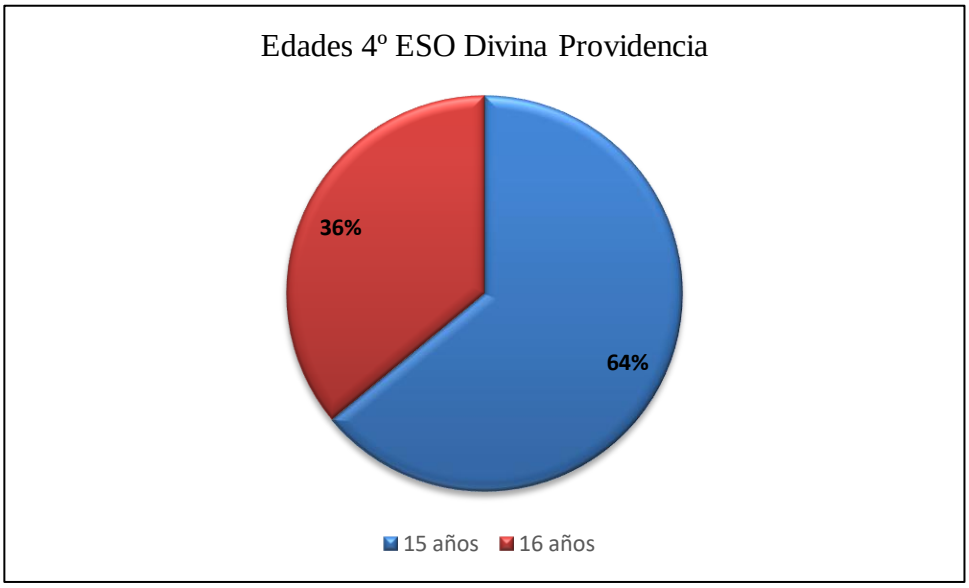

Figura 90. Edades menores de 4º ESO de N. Sª de la Divina Providencia.

En la figura 90, podemos observar que del curso 4º de la ESO de N. Sª de la Divina Providencia, un 64% tiene 15 años mientras que el 36% restante tiene 16 años.

Por otra parte, con relación a la interacción con las TIC de los menores que cursan la ESO en el centro educativo Divina Providencia, en la encuesta de victimización social figuraban en la primera página, diez ítems con opción de respuesta "SI o "NO", así como otras preguntas con respuestas cerradas, en su caso, obteniéndose los resultados que a

continuación se detallan en las tablas 63 a 66, respectivamente, así como los representados gráficamente en las figuras 91 a 130, ambas inclusive.

Tabla 63. *Resultados interacción TIC menores de 1º ESO N. Sª Divina Providencia.*

Ítems interacciones TIC menores 1º ESO	SI	NO
Tengo ordenador en casa	30	1
Tengo webcam	20	11
Tengo teléfono móvil	28	3
Guardo información personal en el teléfono móvil	16	15
Tengo cuenta de correo electrónico	27	4
Utilizo programas de mensajería instantánea	29	2
Utilizo redes sociales	27	4
Utilizo blogs, foros en Internet	10	21

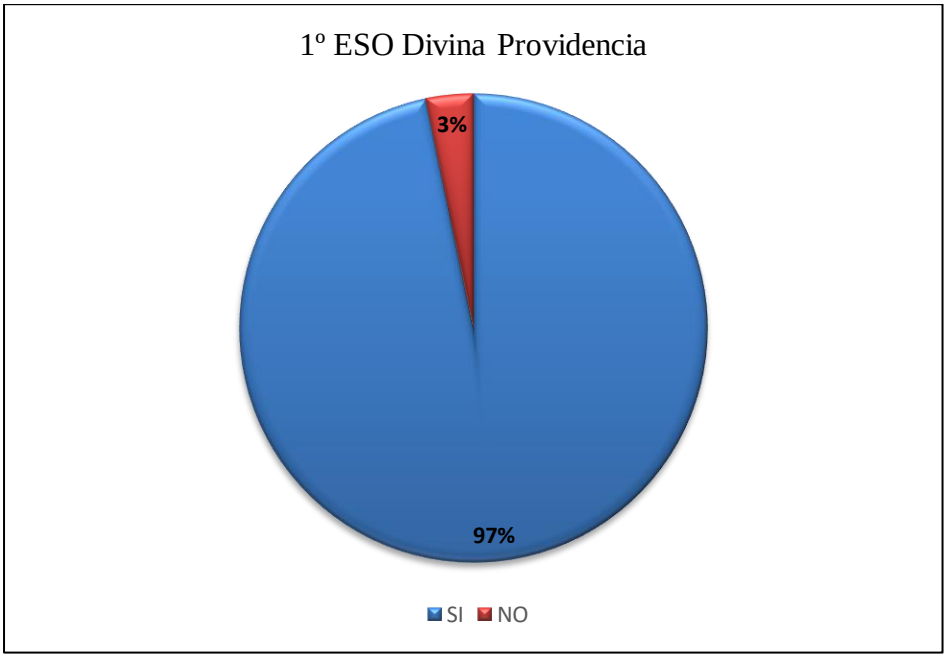

Figura 91. ¿Tienes ordenador en casa?

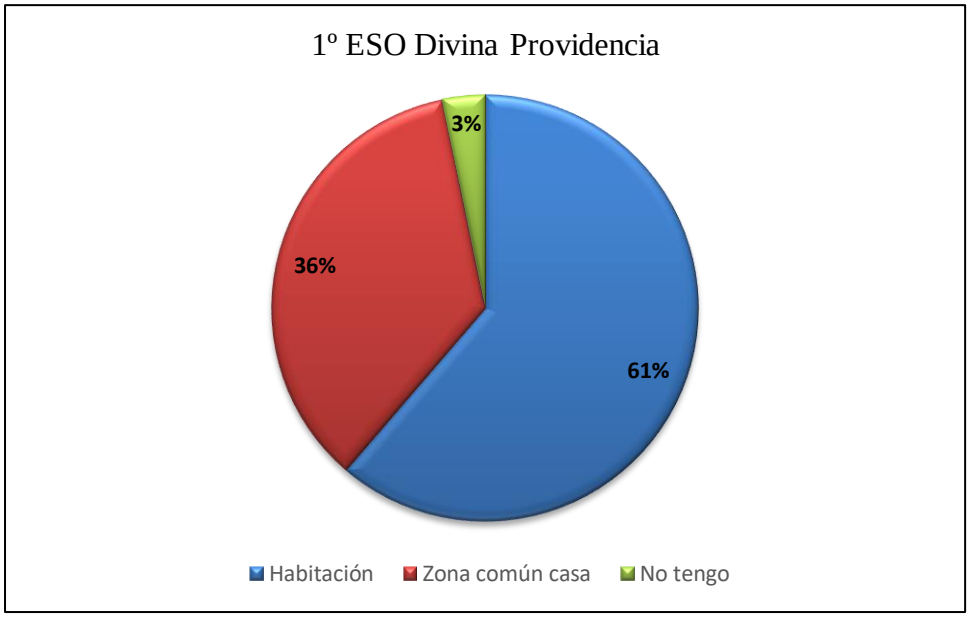

Figura 92. ¿Dónde tienes ubicado tu ordenador?

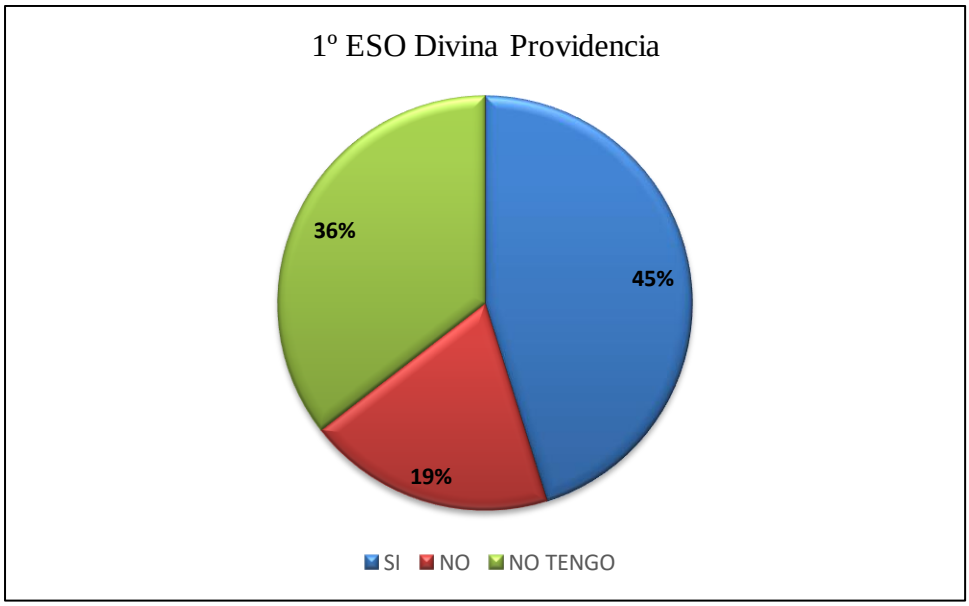

Figura 93. ¿Tapas la webcam cuando no la utilizas?

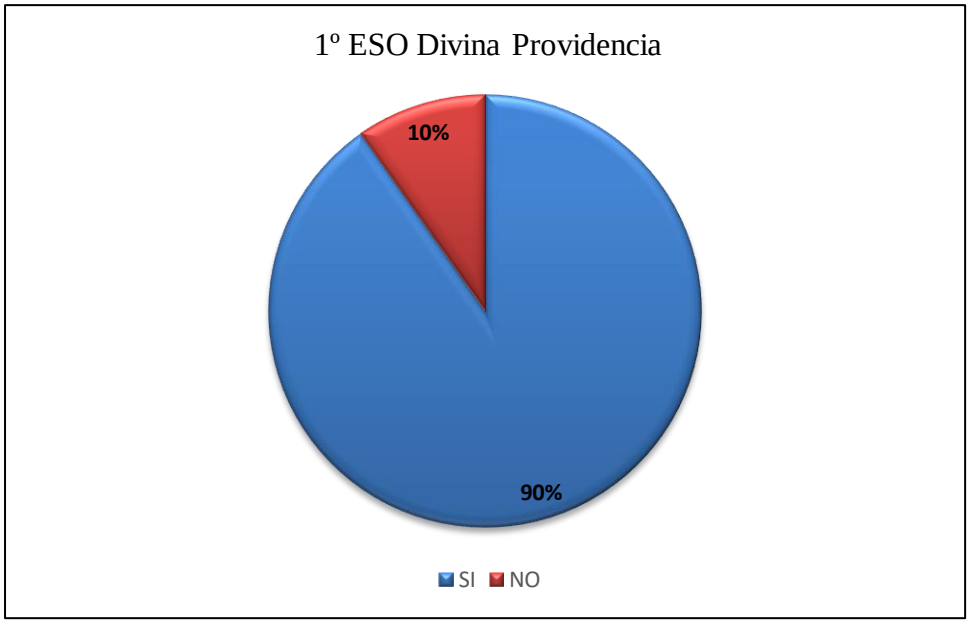

Figura 94. ¿Tienes teléfono móvil?

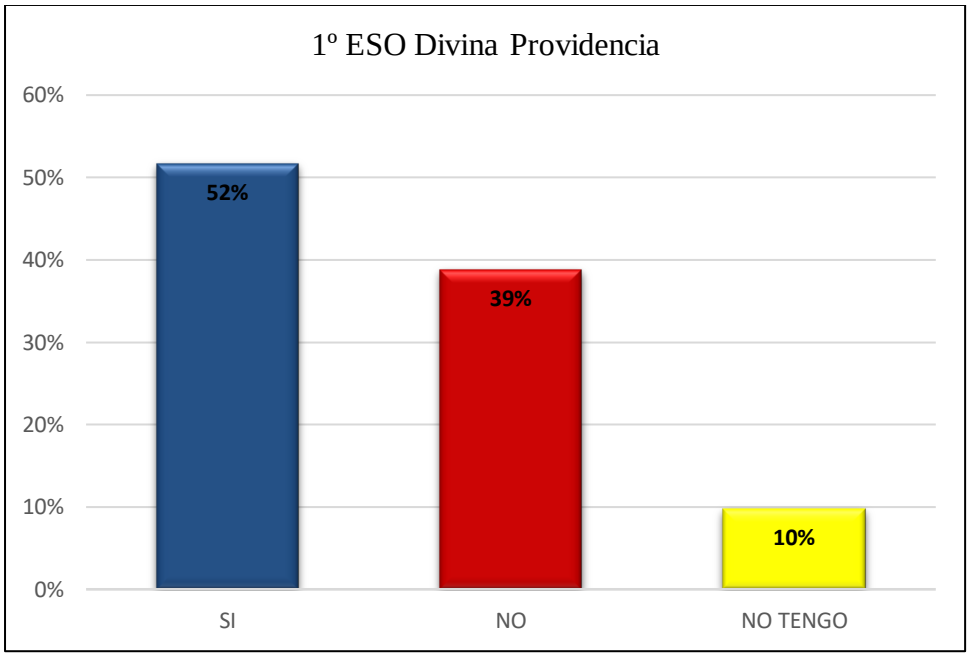

Figura 95. ¿Guardas información personal en tu teléfono móvil?

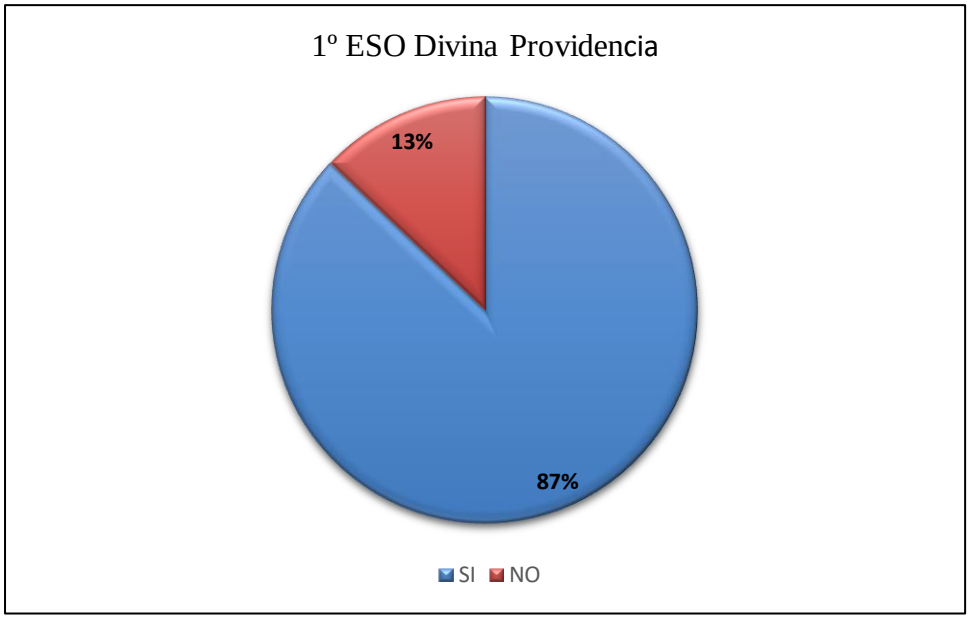

Figura 96. ¿Tienes cuenta de correo electrónico?

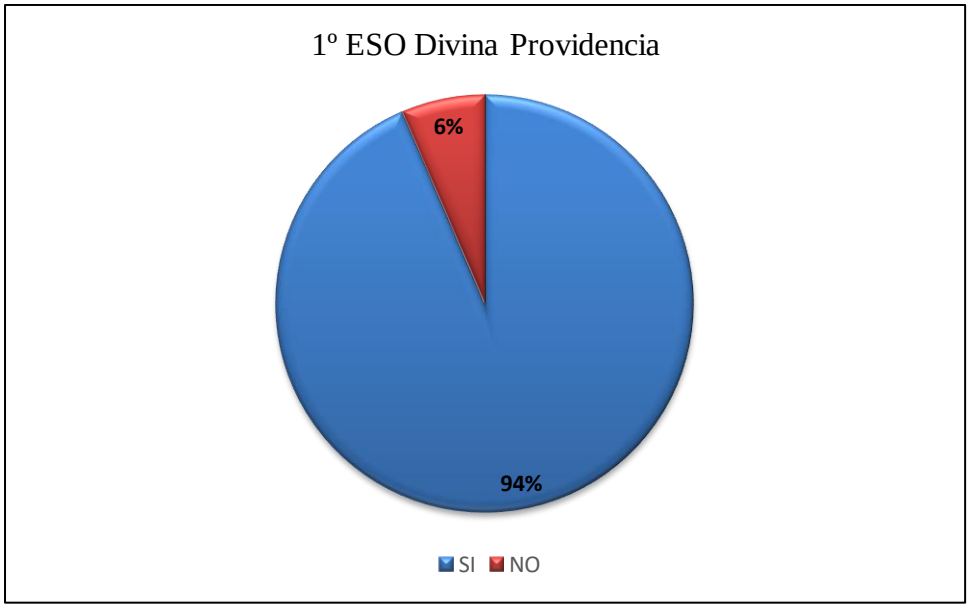

Figura 97. ¿Utilizas programas de mensajería instantánea?

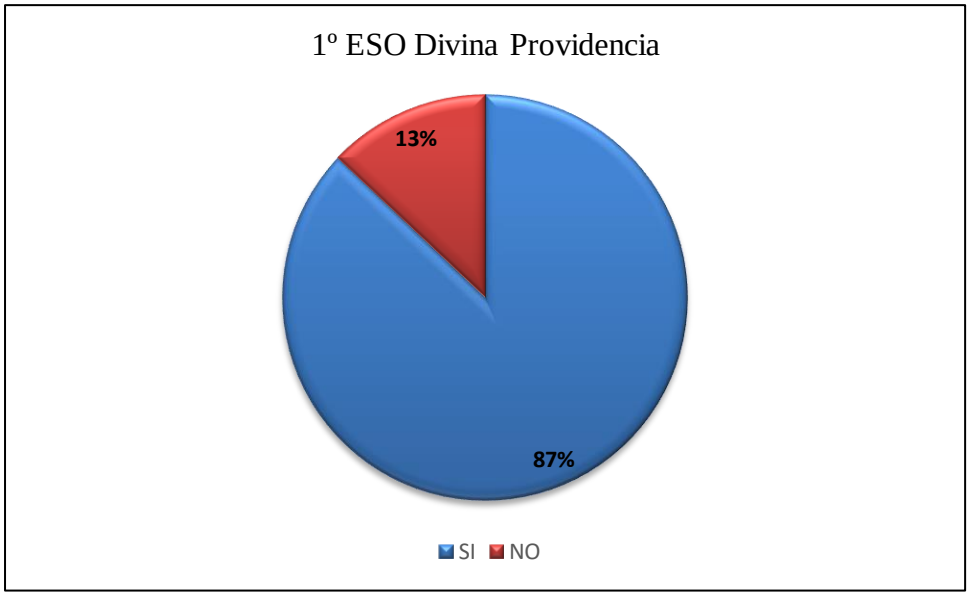

Figura 98. ¿Utilizas redes sociales?

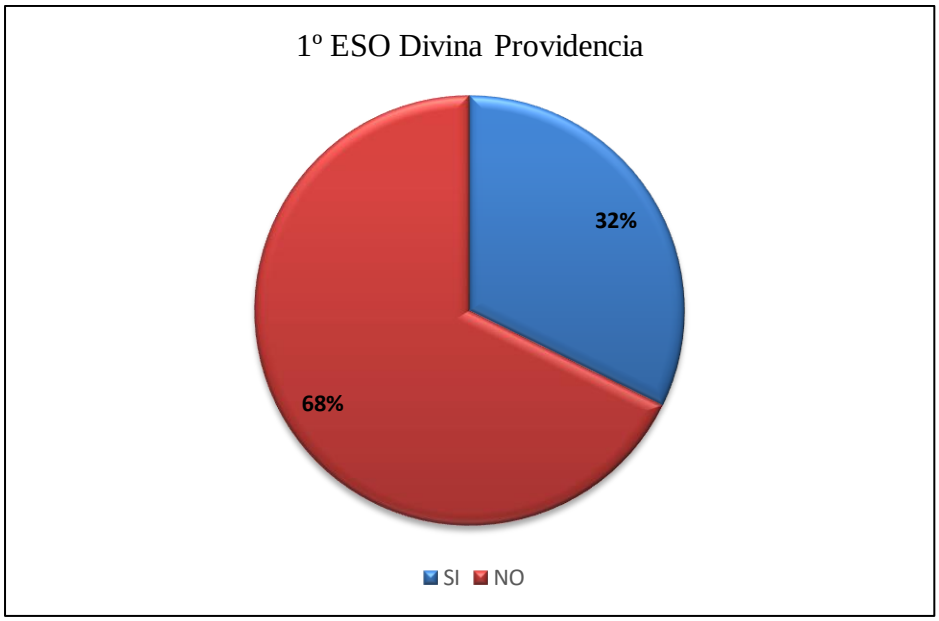

Figura 99. ¿Utilizas blogs, foros en Internet?

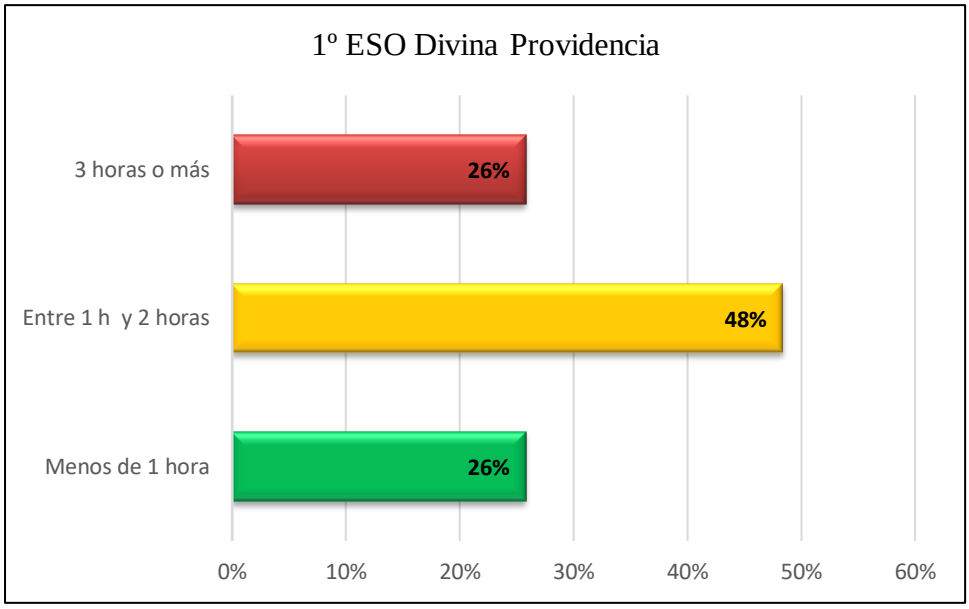

Figura 100. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Tabla 64. *Resultados interacción TIC menores de 2º ESO N. Sª Divina Providencia.*

Ítems interacciones TIC menores 2º ESO	SI	NO
Tengo ordenador en casa	24	3
Tengo webcam	16	11
Tengo teléfono móvil	27	0
Guardo información personal en el teléfono móvil	17	10
Tengo cuenta de correo electrónico	25	2
Utilizo programas de mensajería instantánea	27	0
Utilizo redes sociales	24	3
Utilizo blogs, foros en Internet	11	16

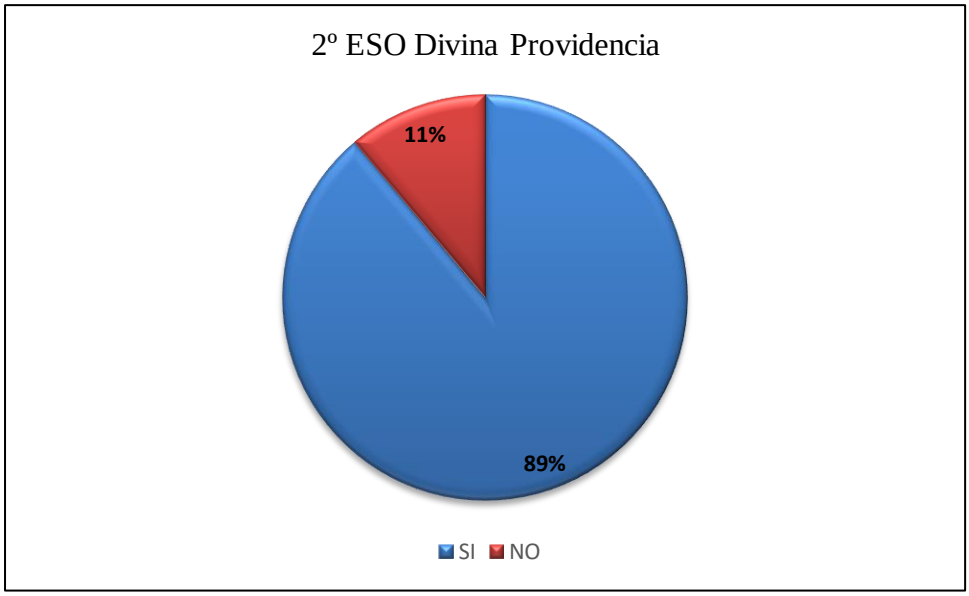

Figura 101. ¿Tienes ordenador en casa?

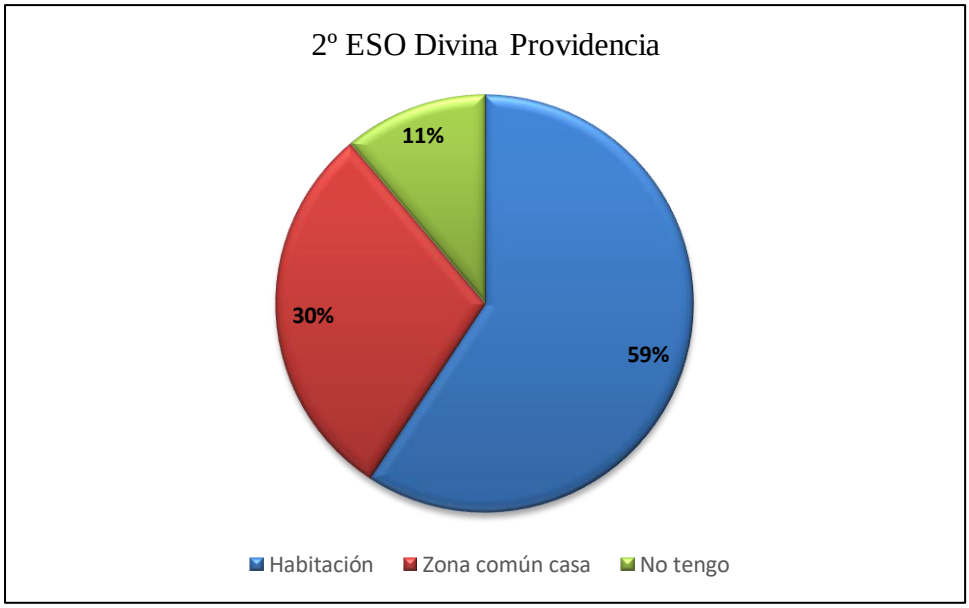

Figura 102. ¿Dónde tienes ubicado tu ordenador?

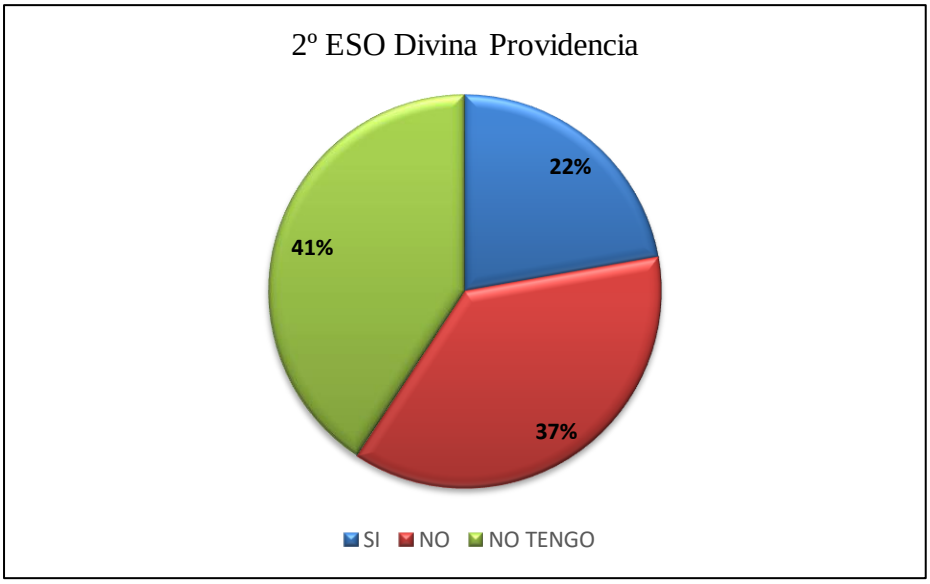

Figura 103. ¿Tapas la webcam cuando no la utilizas?

Figura 104. ¿Tienes teléfono móvil?

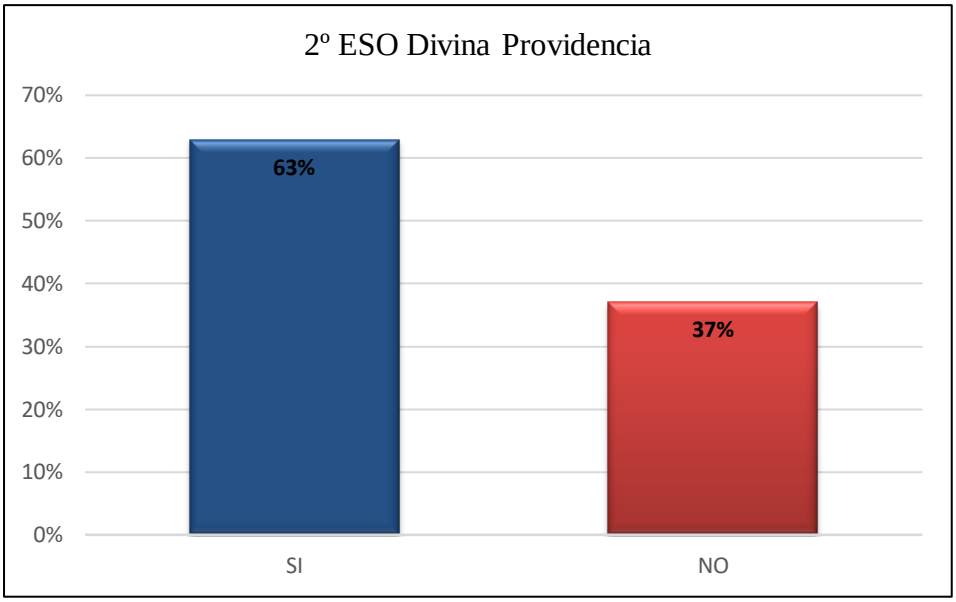

Figura 105. ¿Guardas información personal en tu teléfono móvil?

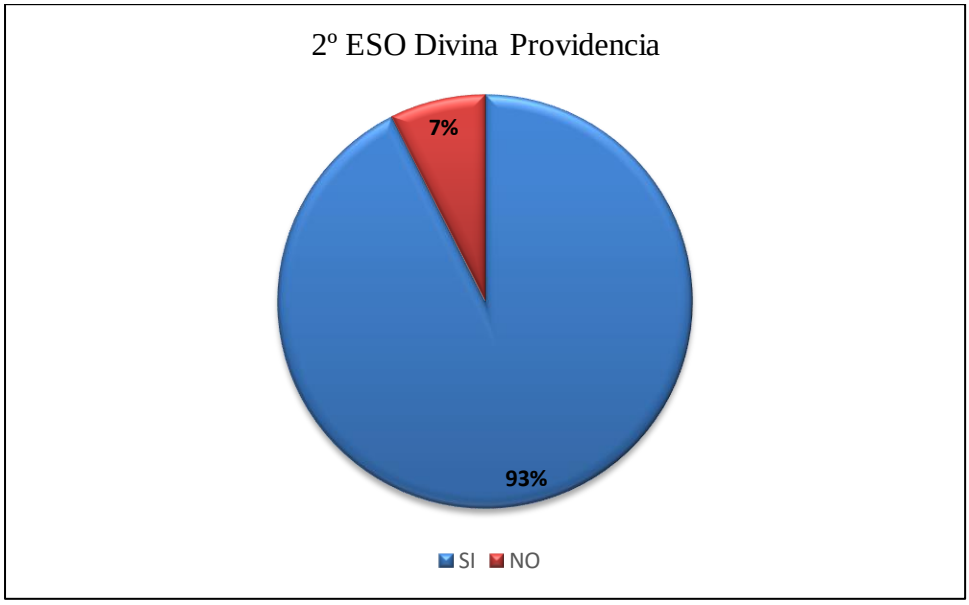

Figura 106. ¿Tienes cuenta de correo electrónico?

Figura 107. ¿Utilizas programas de mensajería instantánea?

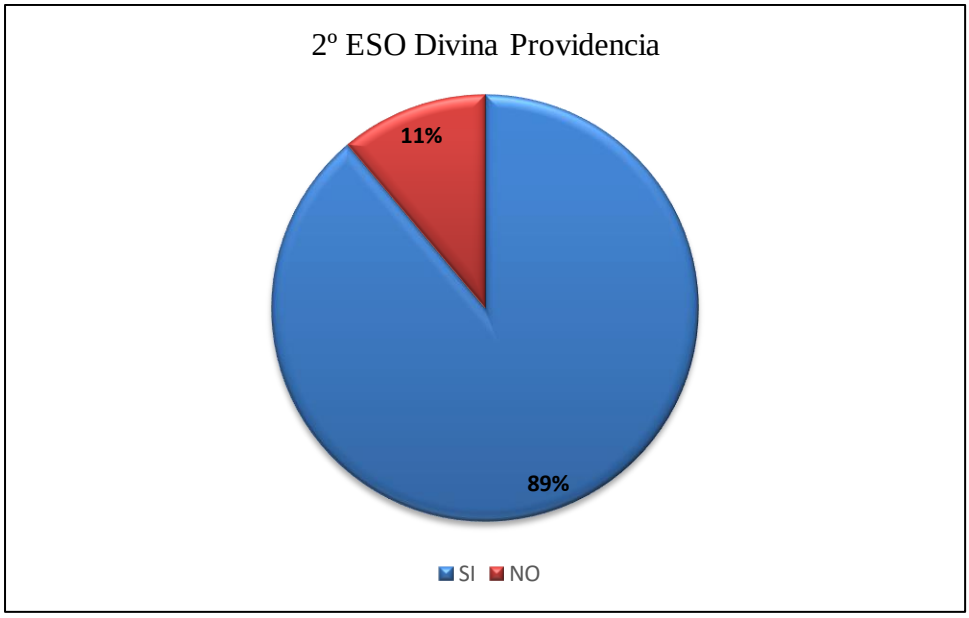

Figura 108. ¿Utilizas redes sociales?

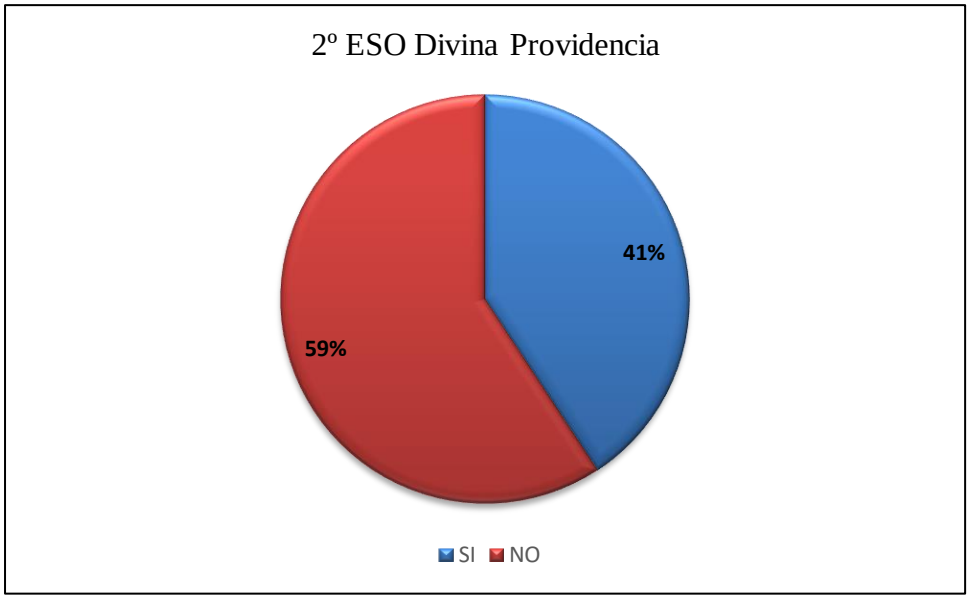

Figura 109. ¿Utilizas blogs, foros en Internet?

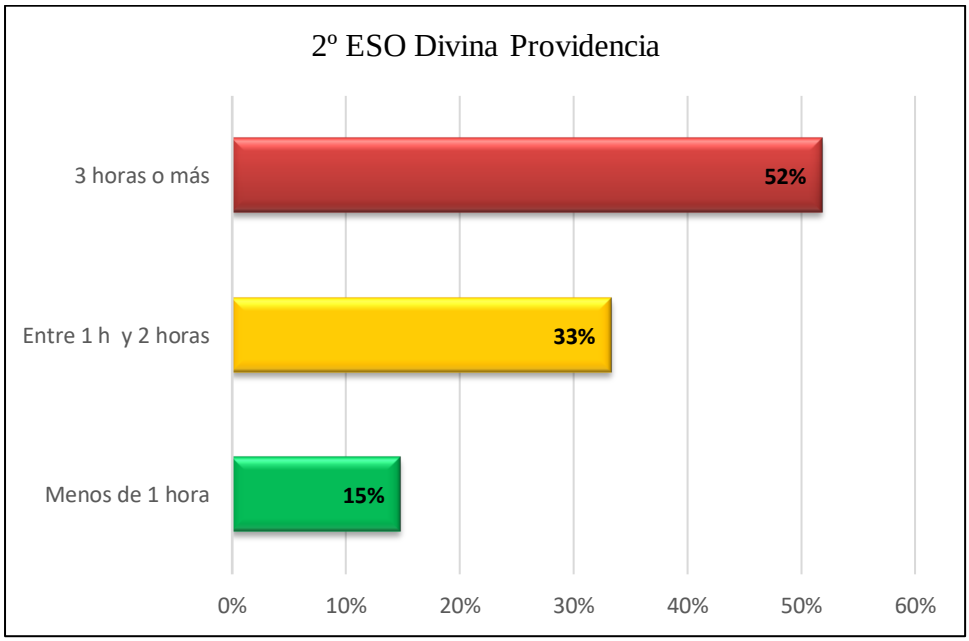

Figura 110. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Tabla 65. *Resultados interacción TIC menores de 3º ESO N. Sª Divina Providencia.*

Ítems interacciones TIC menores 3º ESO	SI	NO
Tengo ordenador en casa	26	0
Tengo webcam	17	9
Tengo teléfono móvil	26	0
Guardo información personal en el teléfono móvil	23	3
Tengo cuenta de correo electrónico	25	1
Utilizo programas de mensajería instantánea	26	0
Utilizo redes sociales	20	6
Utilizo blogs, foros en Internet	4	22

Figura 111. ¿Tienes ordenador en casa?

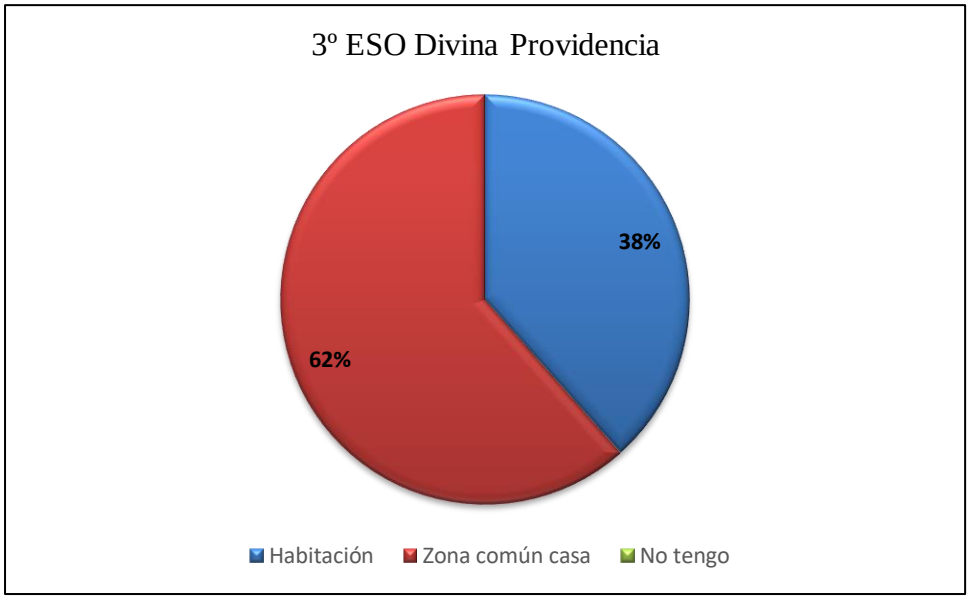

Figura 112. ¿Dónde tienes ubicado tu ordenador?

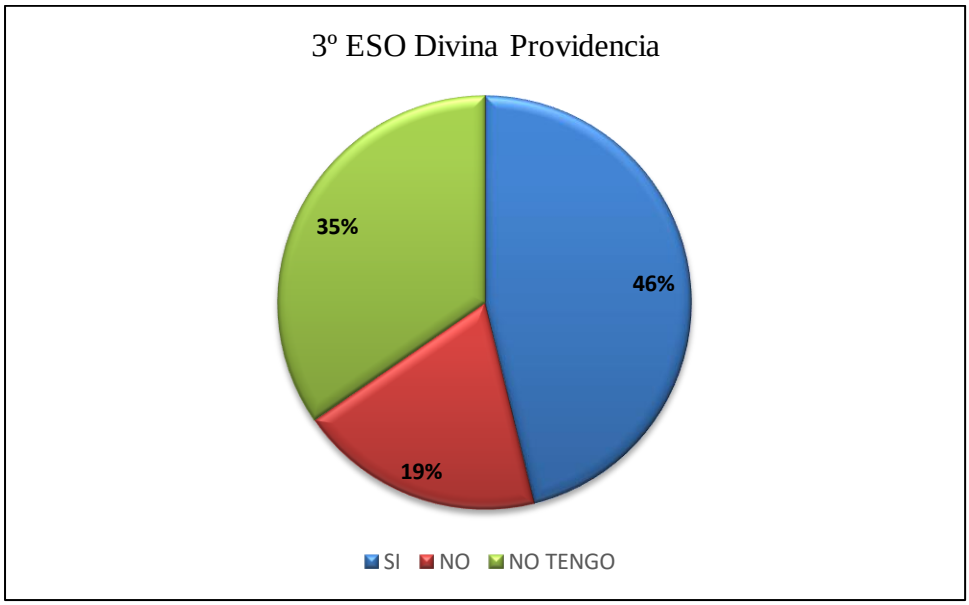

Figura 113. ¿Tapas la webcam cuando no la utilizas?

Figura 114. ¿Tienes teléfono móvil?

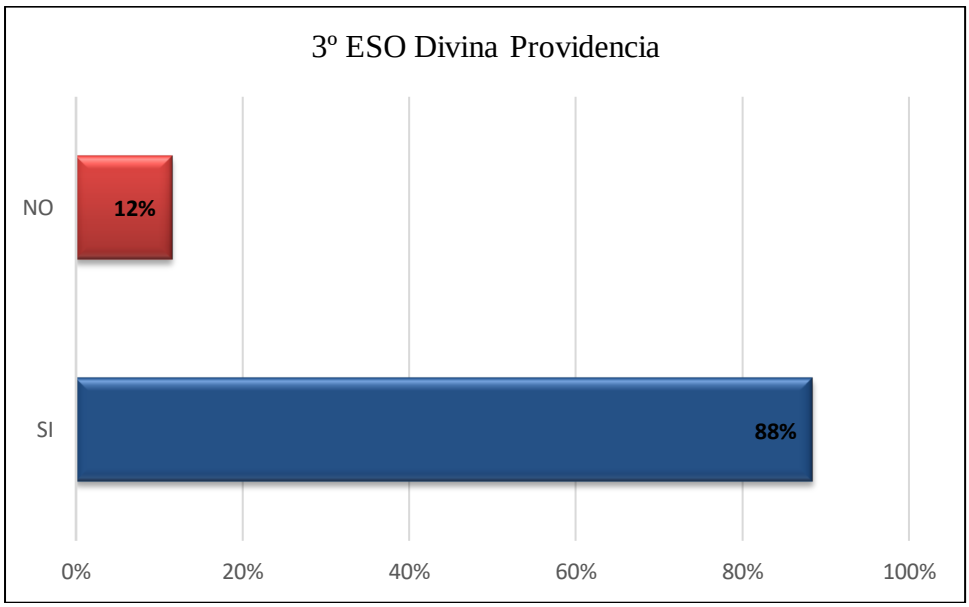

Figura 115. ¿Guardas información personal en el teléfono móvil?

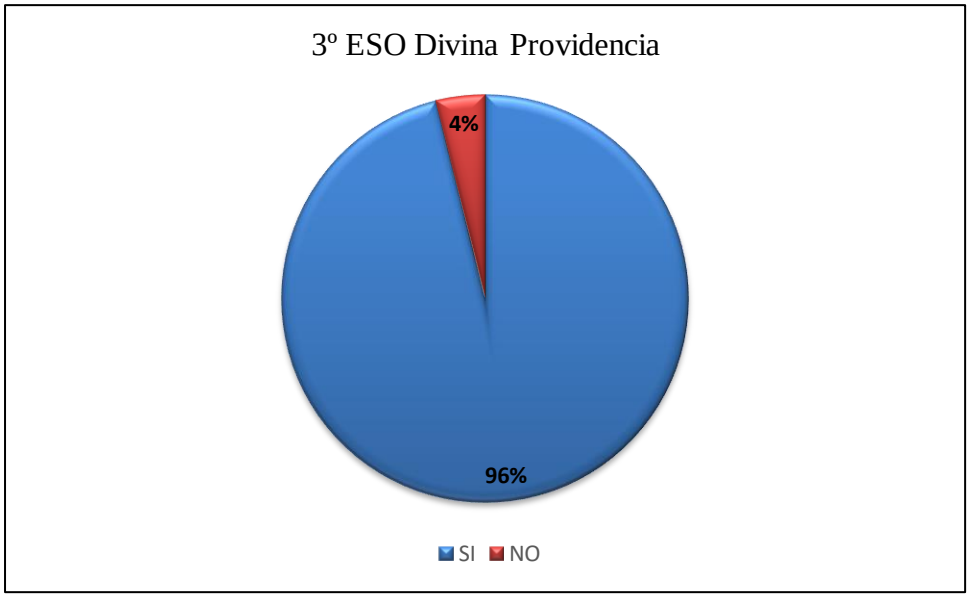

Figura 116. ¿Tienes cuenta de correo electrónico?

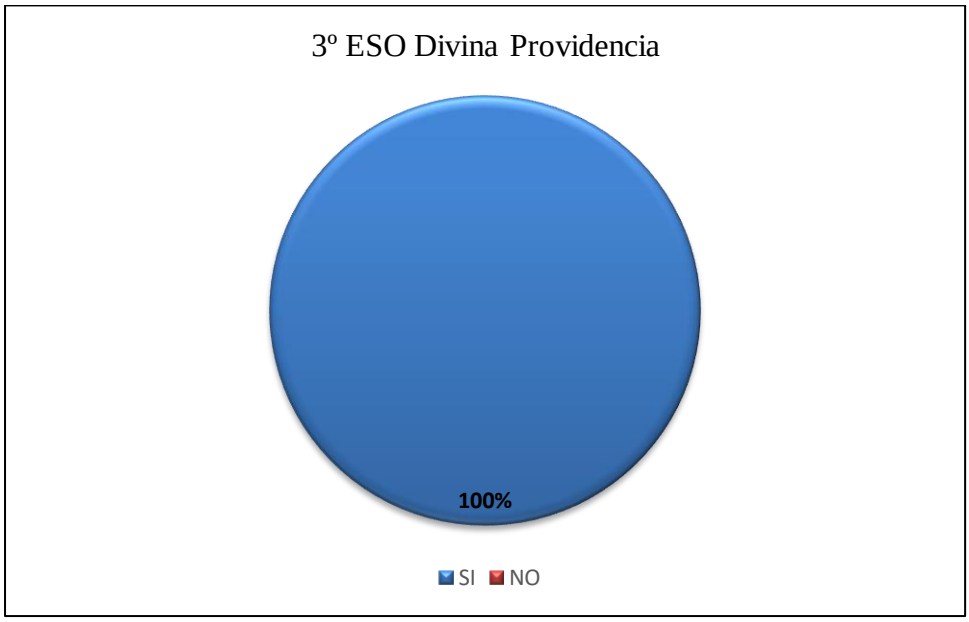

Figura 117. ¿Utilizas programas de mensajería instantánea?

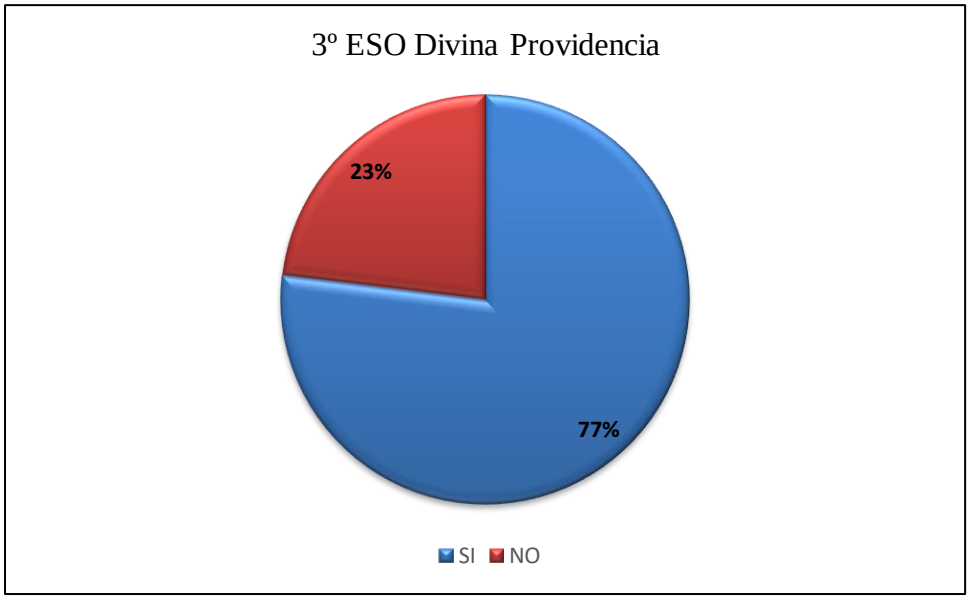

Figura 118. ¿Utilizas redes sociales?

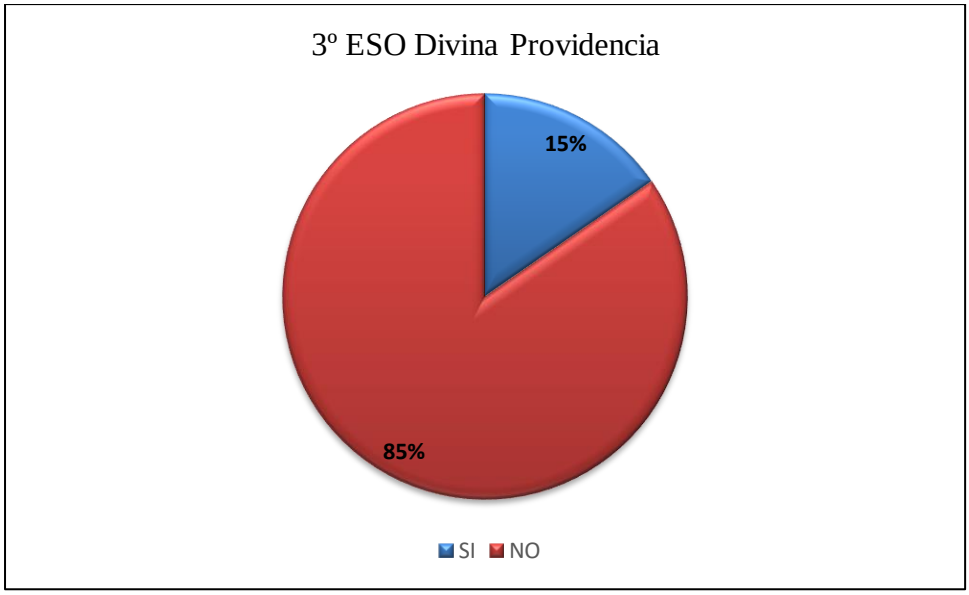

Figura 119. ¿Utilizas blogs, foros en Internet?

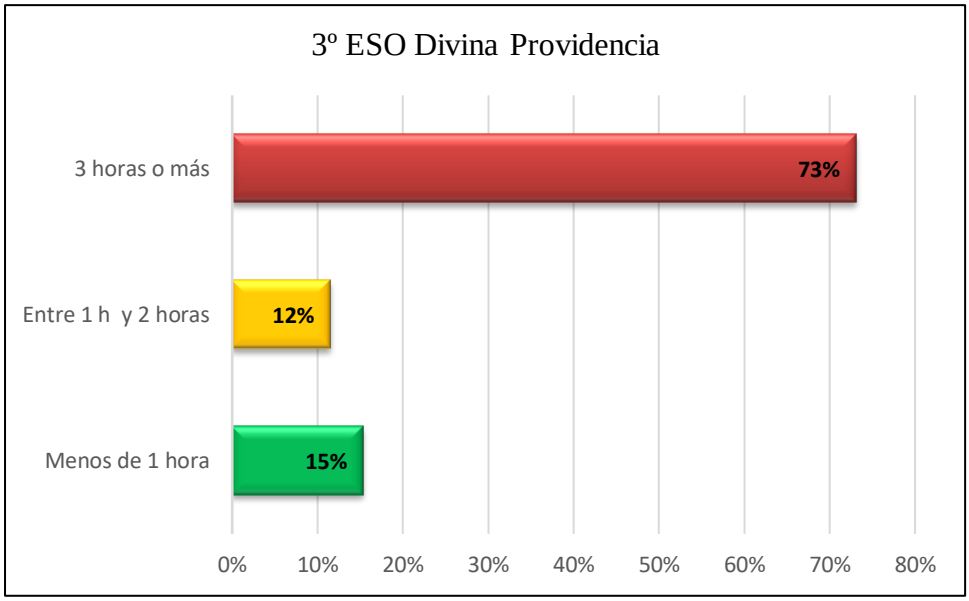

Figura 120. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Tabla 66. *Resultados interacción TIC menores de 4º ESO N. Sª Divina Providencia*.

Ítems interacciones TIC menores 4º ESO	SI	NO
Tengo ordenador en casa	24	1
Tengo webcam	18	7
Tengo teléfono móvil	25	0
Guardo información personal en el teléfono móvil	19	6
Tengo cuenta de correo electrónico	25	0
Utilizo programas de mensajería instantánea	25	0
Utilizo redes sociales	22	3
Utilizo blogs, foros en Internet	17	8

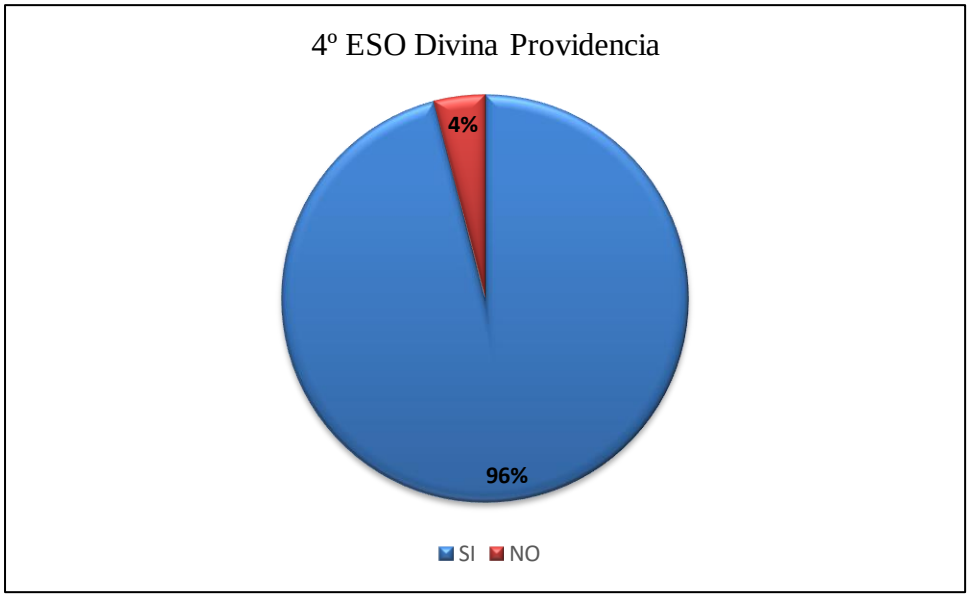

Figura 121. ¿Tienes ordenador en casa?

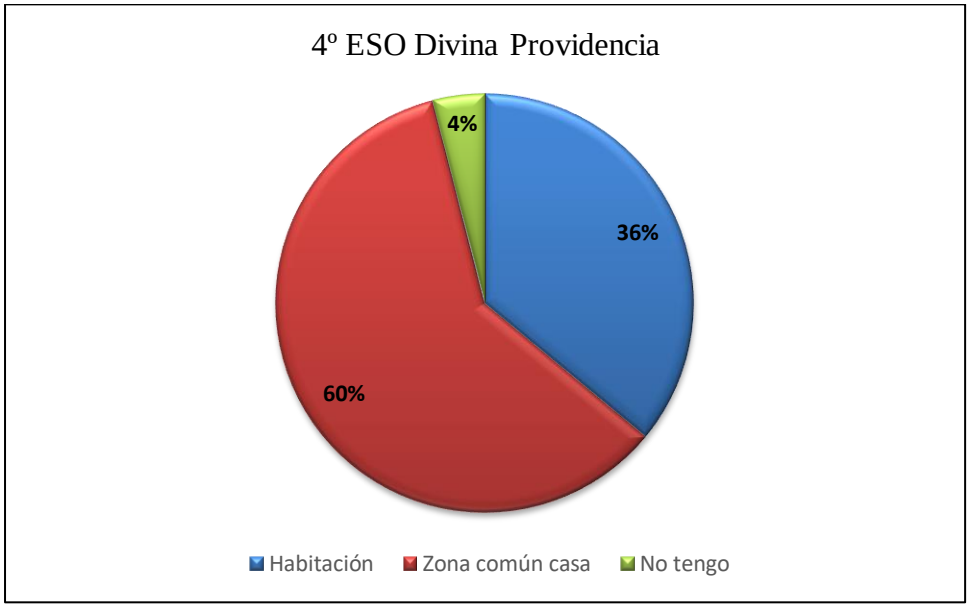

Figura 122. ¿Dónde tienes ubicado el ordenador?

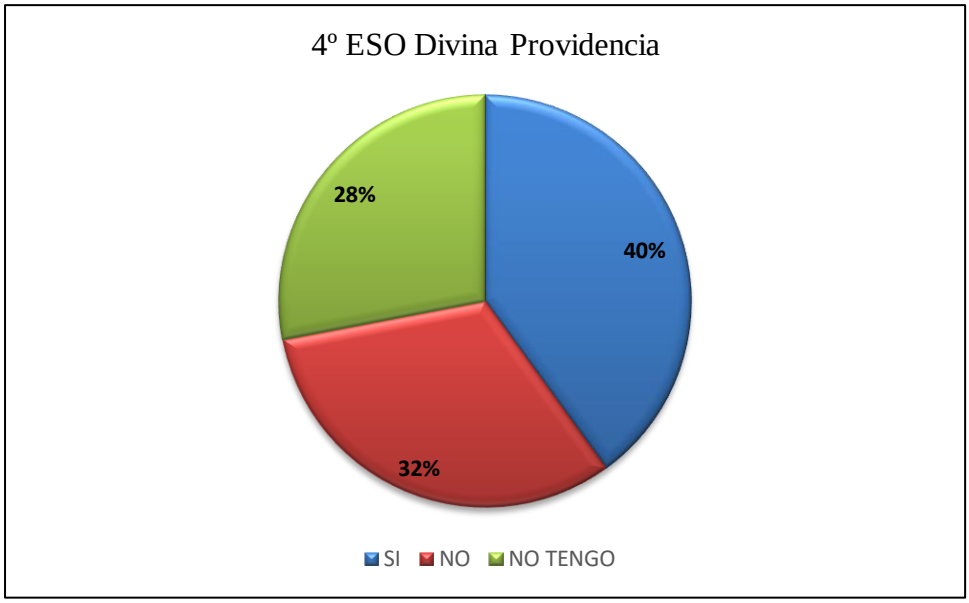

Figura 123. ¿Tapas la webcam cuando no la utilizas?

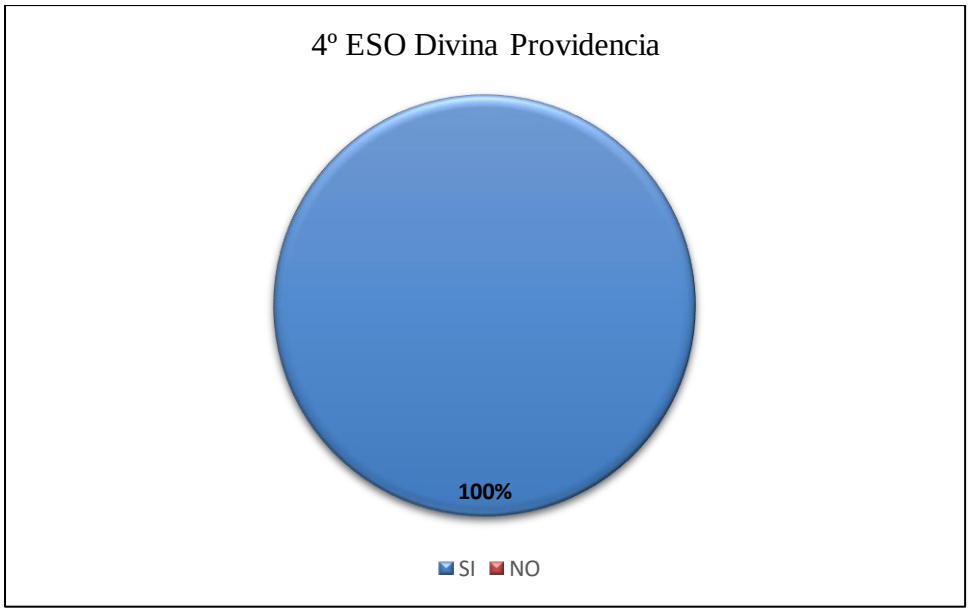

Figura 124. ¿Tienes teléfono móvil?

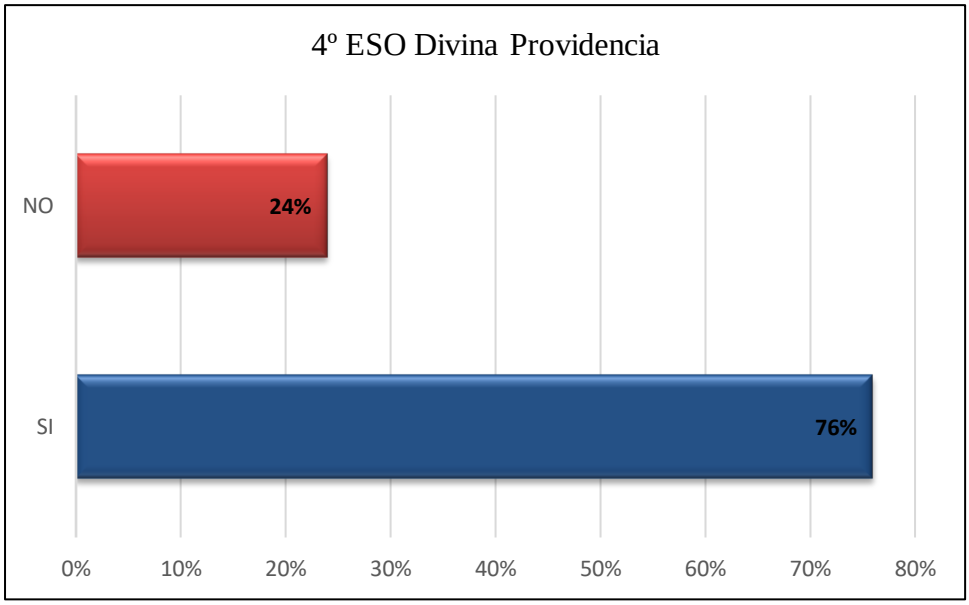

Figura 125. ¿Guardas información personal en el teléfono móvil?

Figura 126. ¿Tienes cuenta de correo electrónico?

Figura 127. ¿Utilizas programas de mensajería instantánea?

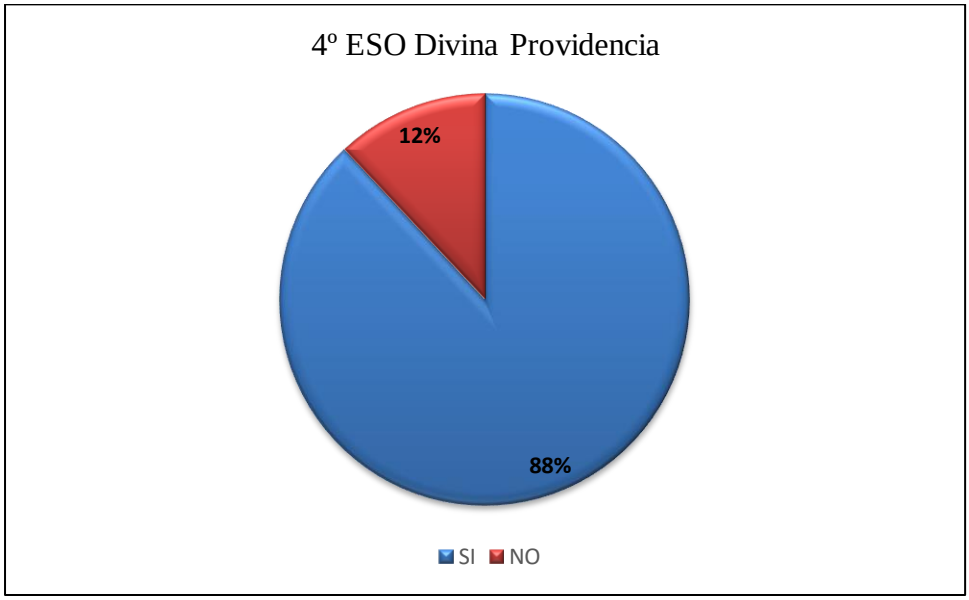

Figura 128. ¿Utilizas redes sociales?

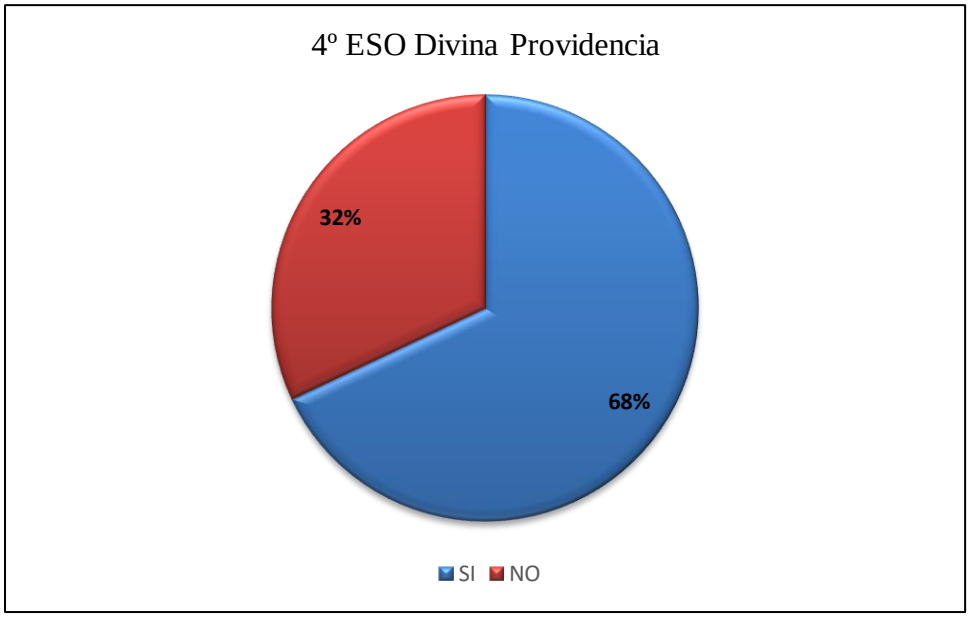

Figura 129. ¿Utilizas blogs, foros en Internet?

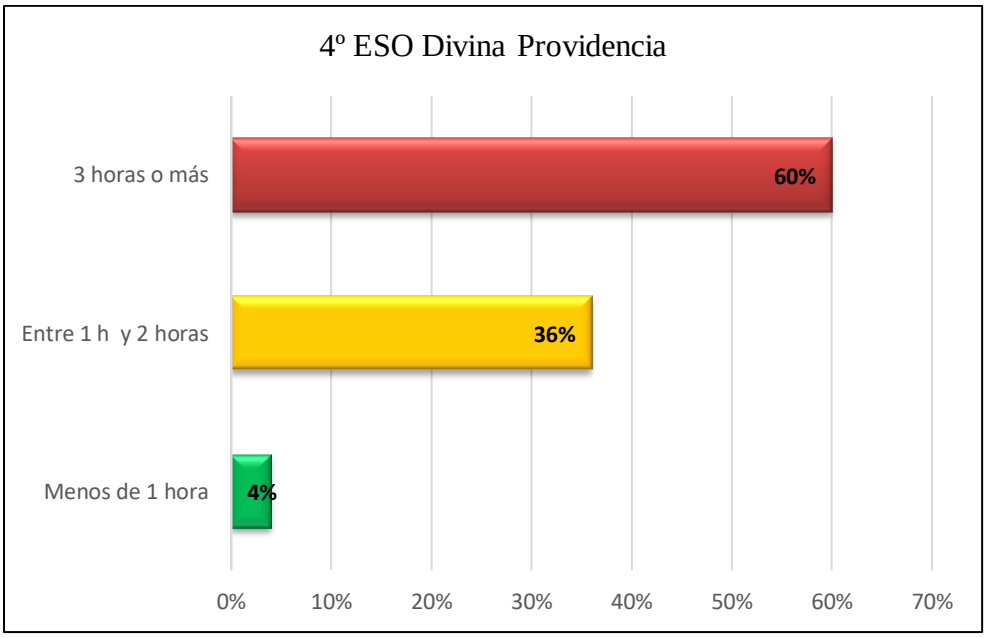

Figura 130. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

A continuación, podemos observar en las tablas 67 a 106 **y** figuras 131 a 150, respectivamente, los resultados obtenidos a las contestaciones de los 20 ítems, de escala frecuencia tipo Likert (de 1 a 5), relacionadas con hechos o conductas de los menores participantes de 1º a 4º de la ESO del centro educativo Divina Providencia, que han servido para valorar los ciberriesgos a los que están expuestos tanto desde la perspectiva criminológica de la víctima como del victimario de ciberacoso, sexting, online grooming y violencia de género digital, en su caso.

1. ¿Has realizado mensajes y/o llamadas ofensivas a través de teléfono móvil y/o internet?

Tabla 67. *Ítem. 1. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	90%	85%	77%	72%
2	Pocas veces	6%	4%	19%	20%
3	Algunas veces	0%	11%	0%	8%
4	Muchas veces	0%	0%	4%	0%
5	Siempre	3%	0%	0%	0%

Tabla 68. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han realizado mensajes y/o llamadas ofensivas a través de teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,19	0,749	1	5
2º ESO	1,26	0,656	1	3
3º ESO	1,31	0,679	1	4
4º ESO	1,36	0,638	1	3

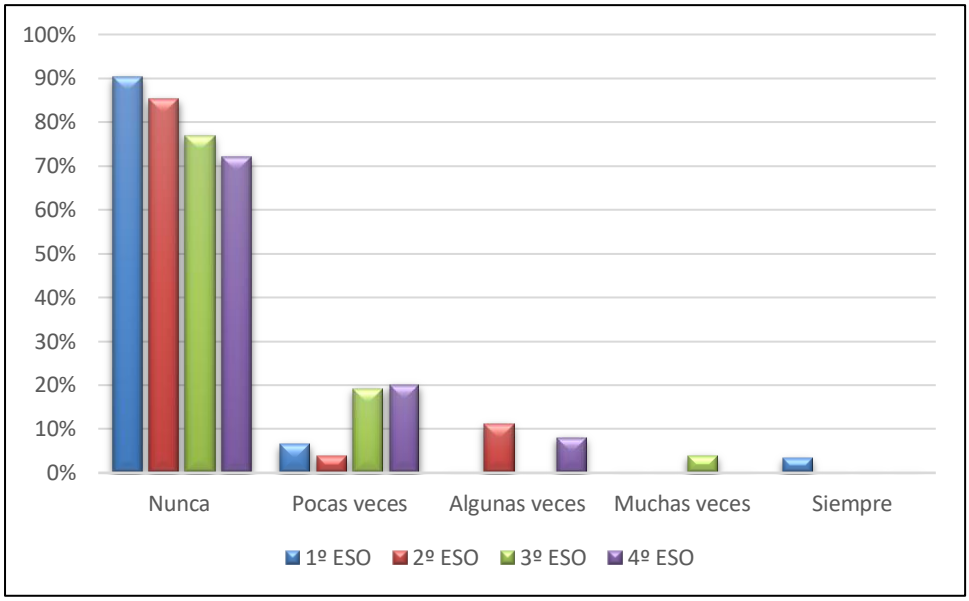

Figura 131. Ítem 1. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

2. ¿Has colgado en Internet una pelea, agresión o burla que ha sido grabada?

Tabla 69. *Ítem. 2. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	100%	100%
2	Pocas veces	0%	0%	0%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 70. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han colgado en Internet una pelea, agresión o burla que ha sido grabada.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1	0	1	1
4º ESO	1	0	1	1

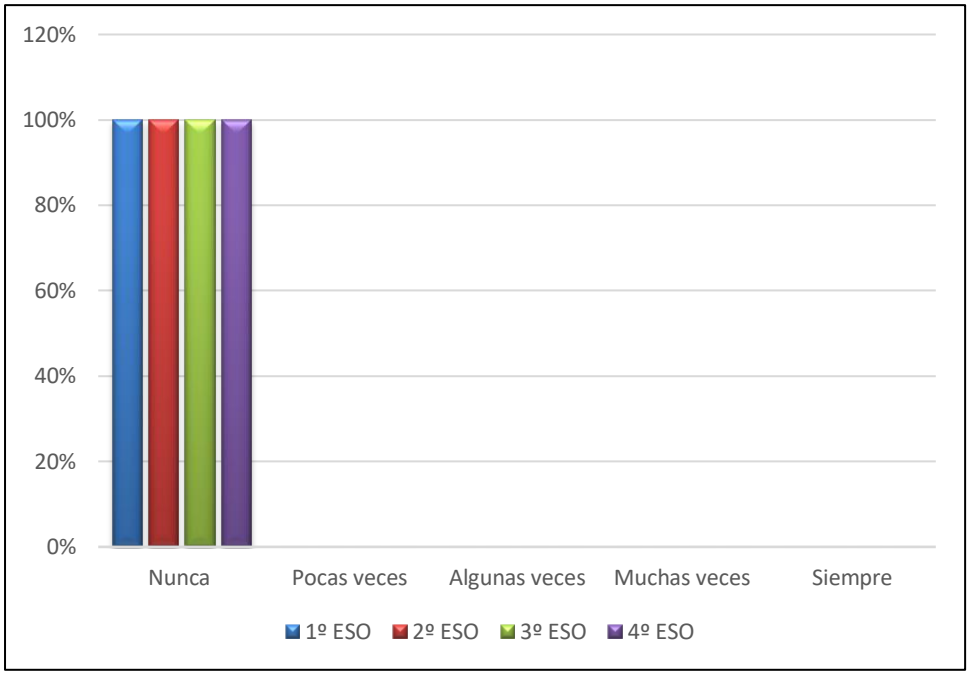

Figura 132. Ítem 2. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

3. ¿Has realizado comportamientos de tipo sexual a través de la webcam?

Tabla 71. *Ítem. 3. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	88%	100%
2	Pocas veces	0%	0%	8%	0%
3	Algunas veces	0%	0%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 72. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han realizado comportamientos de tipo sexual a través de la webcam.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,15	0,464	1	3
4º ESO	1	0	1	1

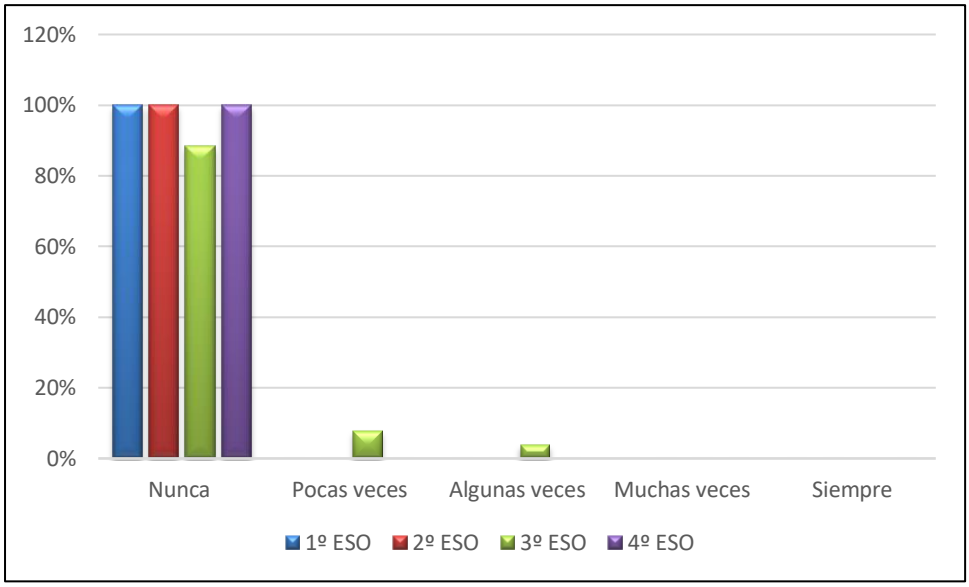

Figura 133. Ítem 3. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

4. ¿Has difundido vídeos y/o fotos privadas o comprometidas vía teléfono móvil o Internet?

Tabla 73. *Ítem. 4. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	94%	96%	85%	68%
2	Pocas veces	3%	4%	8%	8%
3	Algunas veces	3%	0%	8%	24%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 74. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han difundido vídeos y/o fotos privadas o comprometidas vía teléfono móvil o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,10	0,396	1	3
2º ESO	1,04	0,192	1	2
3º ESO	1,23	0,587	1	3
4º ESO	1,56	0,870	1	3

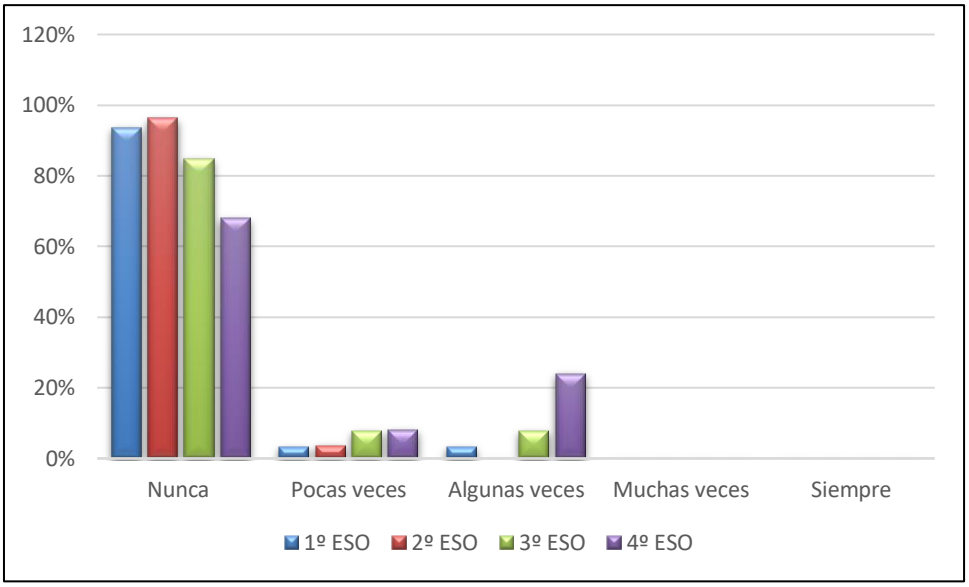

Figura 134. Ítem 4. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

5. ¿Has colgado vídeos y/o fotos robadas en Internet o difundido a través del teléfono móvil?

Tabla 75. *Ítem. 5. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	96%	77%	80%
2	Pocas veces	0%	4%	12%	12%
3	Algunas veces	0%	0%	8%	8%
4	Muchas veces	0%	0%	4%	0%
5	Siempre	0%	0%	0%	0%

Tabla 76. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han colgado vídeos y/o fotos robadas en Internet o difundirlos a través del teléfono móvil.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,04	0,192	1	2
3º ESO	1,38	0,804	1	4
4º ESO	1,28	0,614	1	3

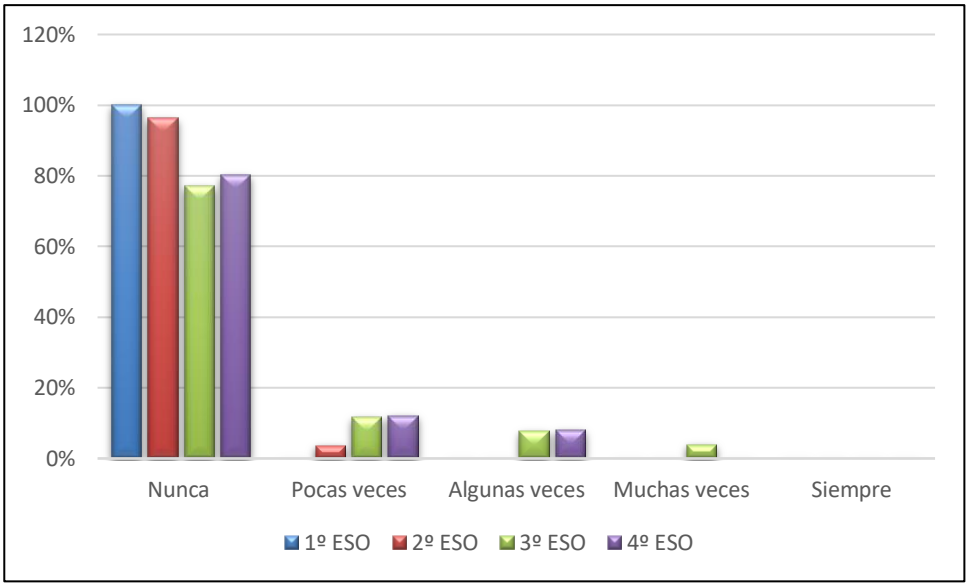

Figura 135. Ítem 5. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

6. ¿Has realizado llamadas anónimas para asustar o intimidar?

Tabla 77. *Ítem. 6. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	90%	70%	81%	76%
2	Pocas veces	10%	15%	15%	24%
3	Algunas veces	0%	11%	0%	0%
4	Muchas veces	0%	4%	4%	0%
5	Siempre	0%	0%	0%	0%

Tabla 78. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han realizado llamadas anónimas para asustar o intimidar.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,10	0,301	1	2
2º ESO	1,48	0,849	1	4
3º ESO	1,27	0,667	1	4
4º ESO	1,24	0,436	1	2

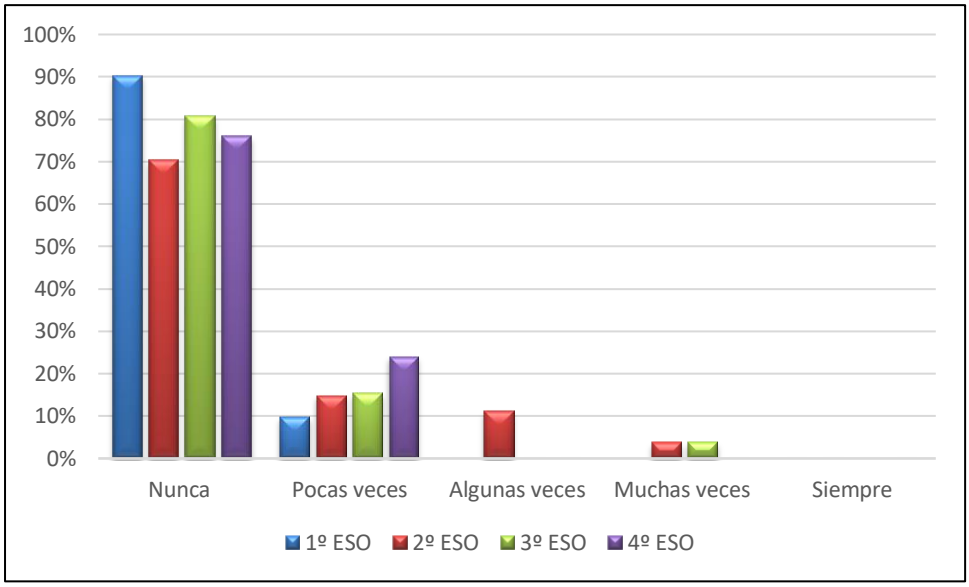

Figura 136. Ítem 6. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

7. ¿Has realizado amenazas o chantajes a través de mensajes y/o llamadas?

Tabla 79. *Ítem. 7. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	94%	100%	92%	84%
2	Pocas veces	6%	0%	4%	16%
3	Algunas veces	0%	0%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 80. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han realizado amenazas o chantajes a través de mensajes y/o llamadas.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,06	0,250	1	2
2º ESO	1	0	1	1
3º ESO	1,12	0,431	1	3
4º ESO	1,16	0,374	1	2

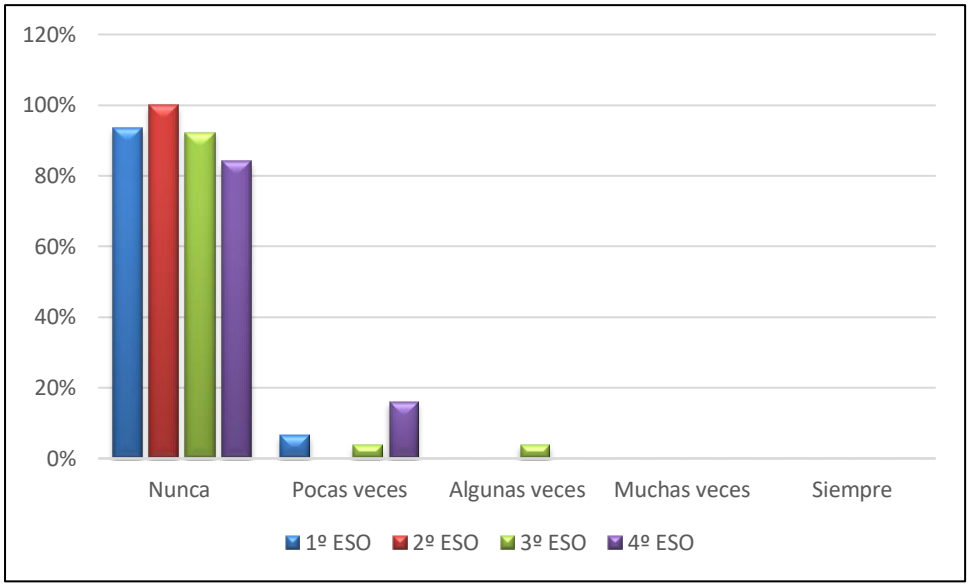

Figura 137. Ítem 7. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

8. ¿Has acosado sexualmente a través de teléfono móvil y/o Internet?

Tabla 81. *Ítem. 8. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	94%	100%	92%	84%
2	Pocas veces	6%	0%	4%	16%
3	Algunas veces	0%	0%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 82. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han acosado sexualmente a través de teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,06	0,250	1	2
2º ESO	1	0	1	1
3º ESO	1,12	0,431	1	3
4º ESO	1,16	0,374	1	2

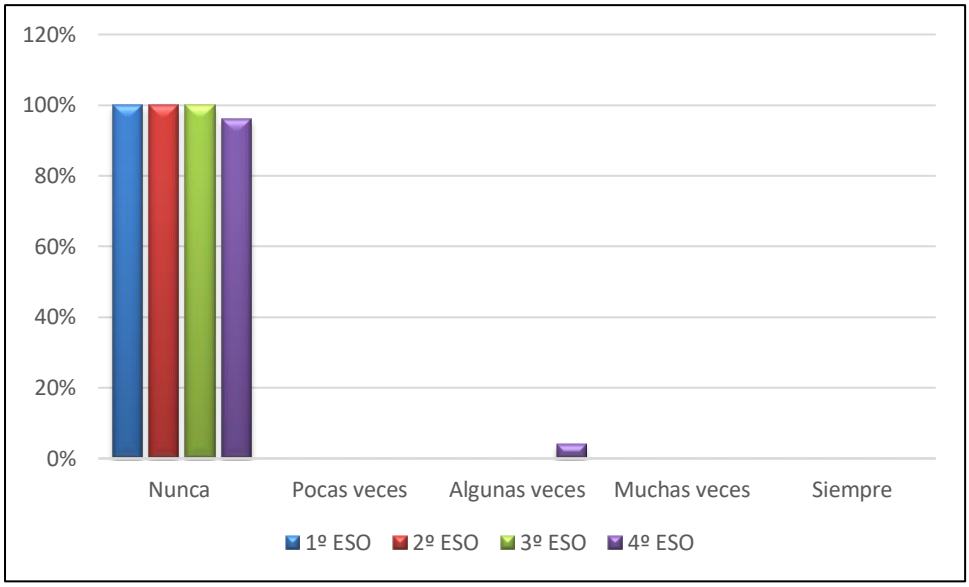

Figura 138. Ítem 8. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

9. ¿Has suplantado a una persona para difamar, mentir o contar sus secretos?

Tabla 83. *Ítem. 9. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	92%	92%
2	Pocas veces	0%	0%	8%	4%
3	Algunas veces	0%	0%	0%	4%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 84. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han suplantado a una persona para difamar, mentir o contar sus secretos.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,08	0,272	1	2
4º ESO	1,12	0,440	1	3

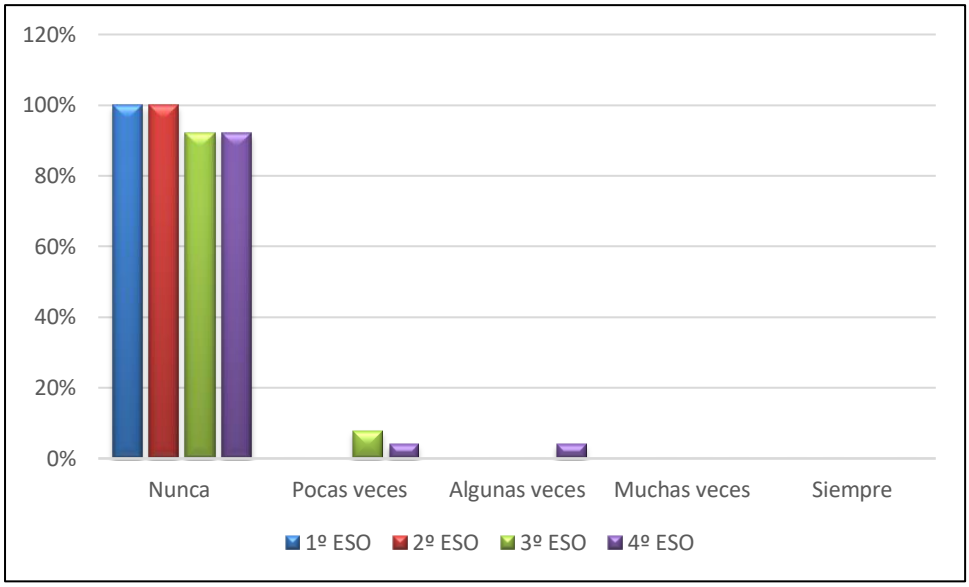

Figura 139. Ítem 9. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

10. ¿Has robado la contraseña a una persona?

Tabla 85. *Ítem. 10. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	90%	93%	96%	92%
2	Pocas veces	10%	4%	4%	0%
3	Algunas veces	0%	4%	0%	8%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 86. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han robado la contraseña a una persona.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,10	0,301	1	2
2º ESO	1,11	0,424	1	3
3º ESO	1,04	0,196	1	2
4º ESO	1,16	0,554	1	3

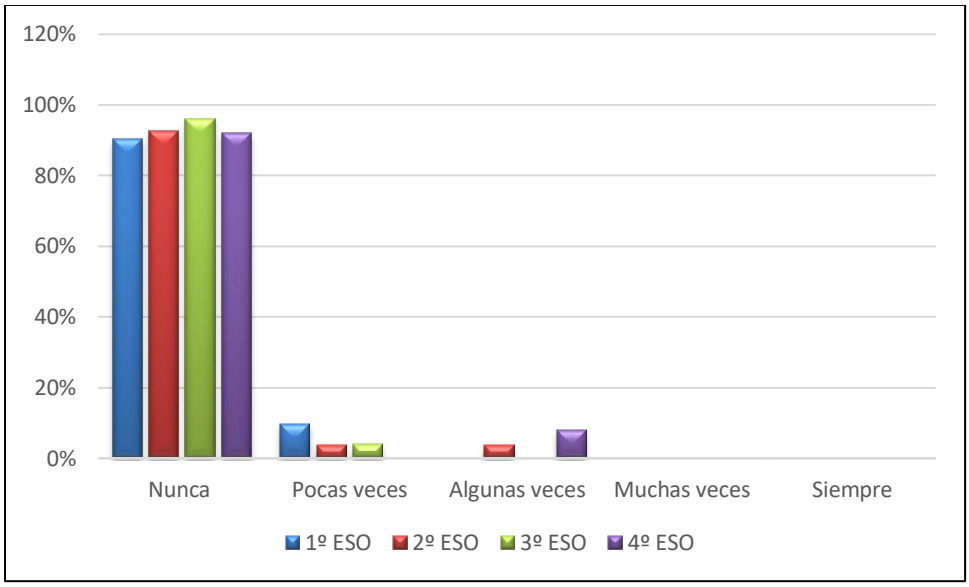

Figura 140. Ítem 10. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

11. ¿Has trucado fotos y vídeos para difundirlos y humillar vía teléfono móvil y/o Internet?

Tabla 87. *Ítem. 11. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	96%	96%
2	Pocas veces	0%	0%	4%	4%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 88. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han trucado fotos y vídeos para difundirlos y humillar vía teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,04	0,196	1	2
4º ESO	1,04	0,200	1	2

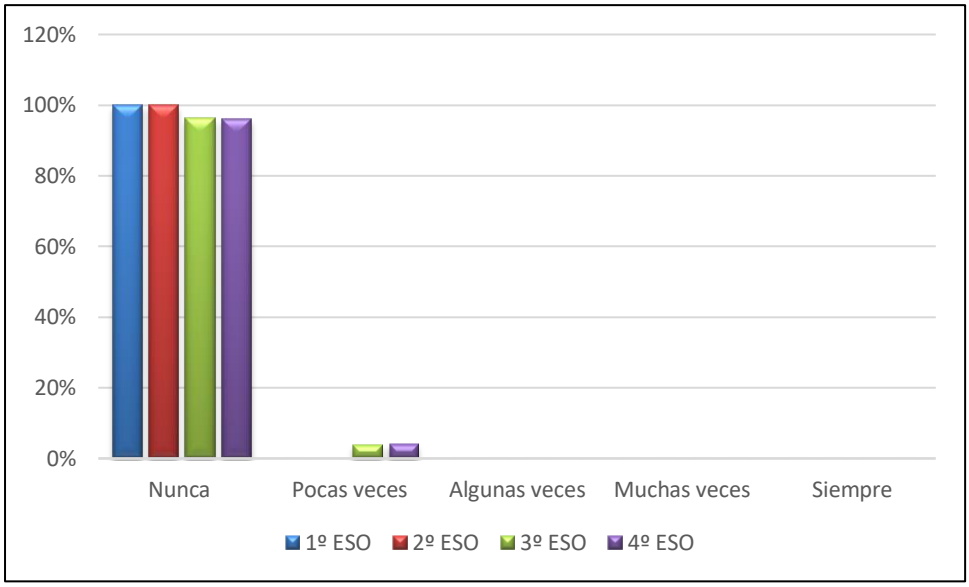

Figura 141. Ítem 11. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

12. ¿Has acosado a alguien para aislarle de sus contactos en las redes sociales?

Tabla 89. *Ítem. 12. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	100%	92%
2	Pocas veces	0%	0%	0%	8%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 90. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han acosado a alguien para aislarle de sus contactos en las redes sociales.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1	0	1	1
4º ESO	1,08	0,277	1	2

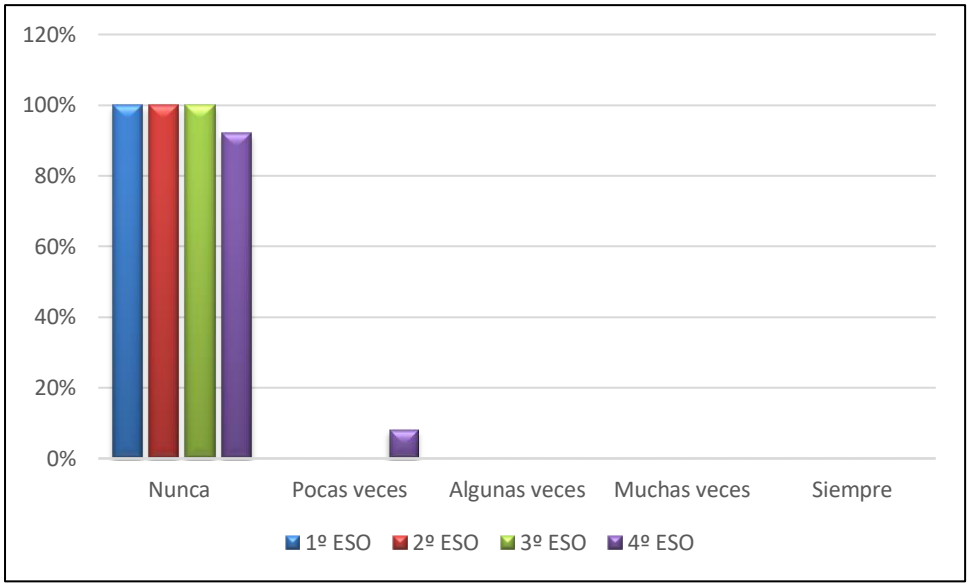

Figura 142. Ítem 12. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

13. ¿Has chantajeado a cambio de no divulgar información íntima vía teléfono y/o Internet?

Tabla 91. *Ítem. 13. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	93%	88%	80%
2	Pocas veces	0%	0%	12%	16%
3	Algunas veces	0%	4%	0%	4%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	4%	0%	0%

Tabla 92. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han chantajeado a cambio de no divulgar información íntima vía teléfono y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,22	0,847	1	5
3º ESO	1,12	0,326	1	2
4º ESO	1,24	0,523	1	3

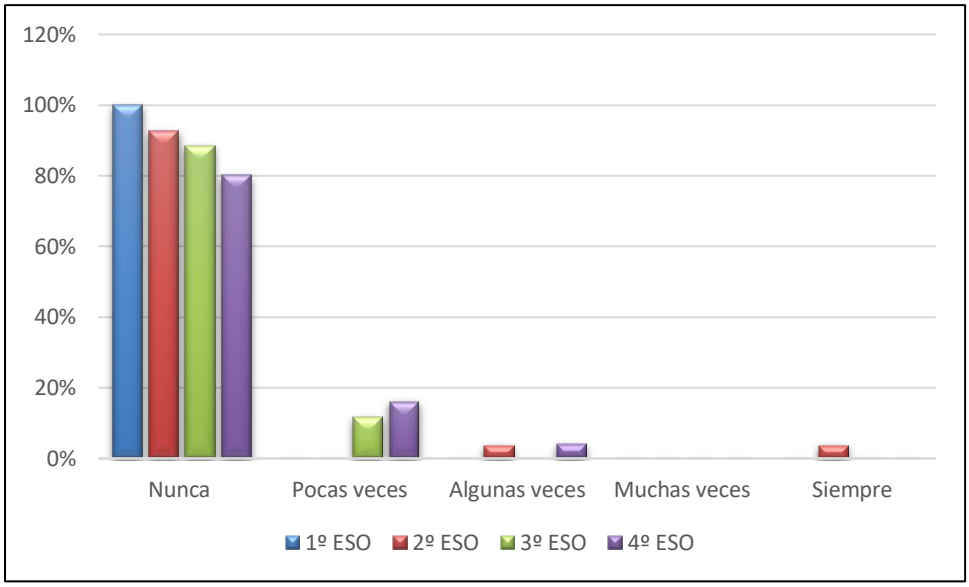

Figura 143. Ítem 13. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

14. ¿Has amenazado de muerte a alguien a través de teléfono móvil y/o Internet?

Tabla 93. *Ítem. 14. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	100%	100%
2	Pocas veces	0%	0%	0%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 94. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han difundido y/o difamado con rumores para hacer daño vía teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1	0	1	1
4º ESO	1	0	1	1

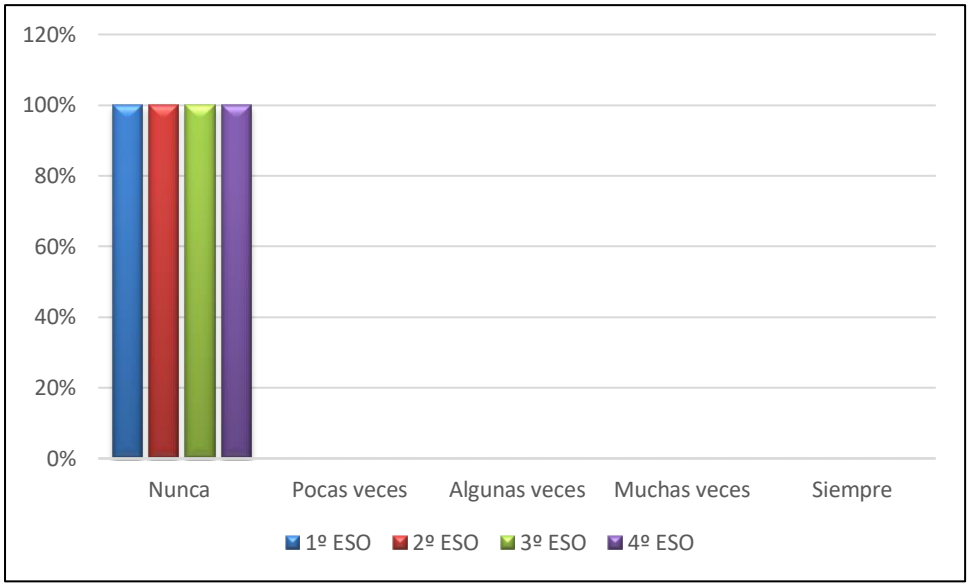

Figura 144. Ítem. 14. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

15. ¿Has difundido y/o difamado con rumores para hacer daño vía teléfono móvil y/o Internet?

Tabla 95. *Ítem. 15. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	85%	92%
2	Pocas veces	0%	0%	15%	8%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 96. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han difundido y/o difamado con rumores para hacer daño vía teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,15	0,368	1	2
4º ESO	1,08	0,277	1	2

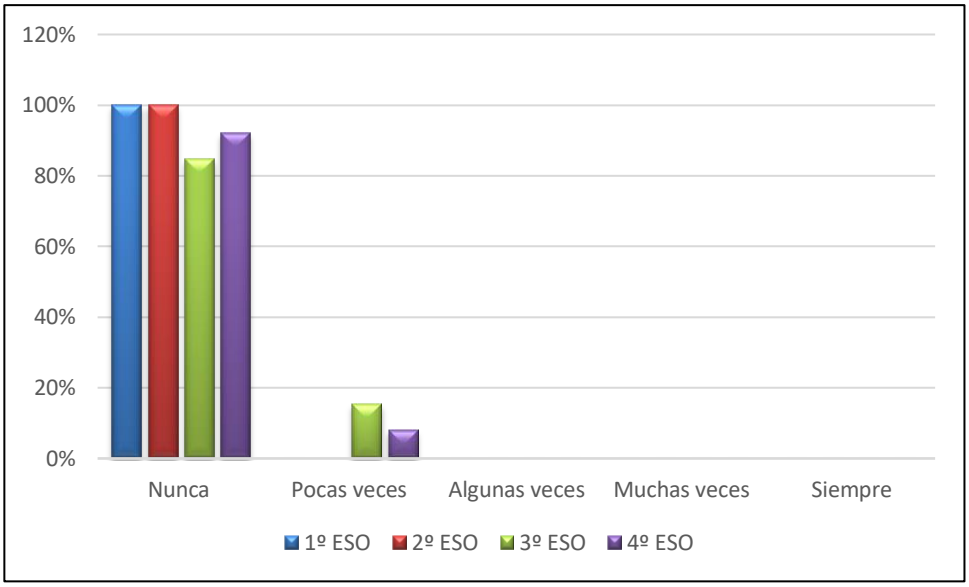

Figura 145. Ítem. 15. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

16. ¿Has contactado con un adulto que se ha ganado tu confianza en las redes sociales?

Tabla 97. *Ítem. 16. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	97%	81%	77%	80%
2	Pocas veces	3%	15%	8%	16%
3	Algunas veces	0%	0%	15%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	4%	0%	4%

Tabla 98. Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han contactado con un adulto que se ha ganado su confianza en las redes sociales.

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,03	0,180	1	2
2º ESO	1,30	0,823	1	5
3º ESO	1,38	0,752	1	3
4º ESO	1,32	0,852	1	5

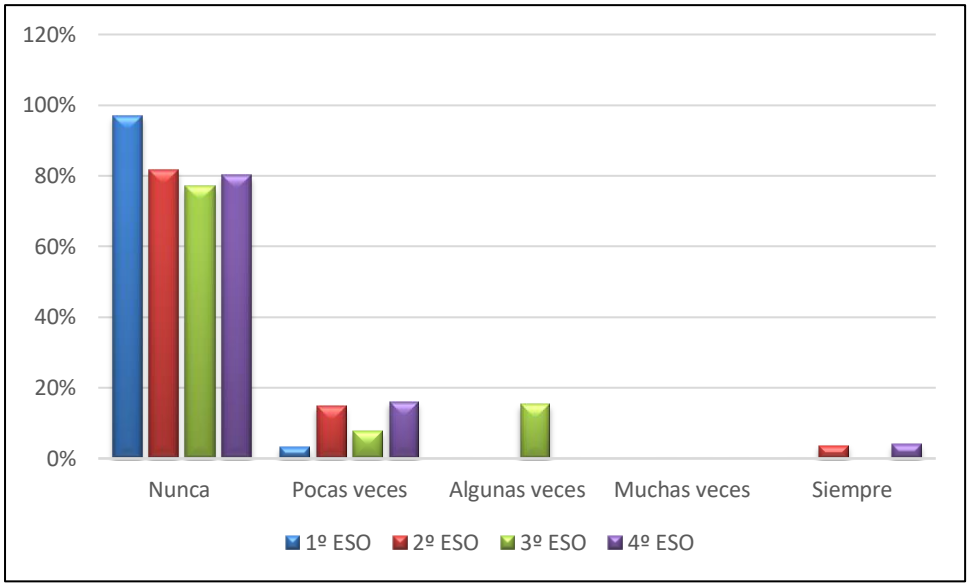

Figura 146. Ítem. 16. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

17. ¿Controlas los amigos/as en redes sociales, mensajes, WhatsApp, etc., de tu pareja?

Tabla 99. *Ítem. 17. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	87%	89%	65%	80%
2	Pocas veces	6%	11%	19%	8%
3	Algunas veces	3%	0%	8%	8%
4	Muchas veces	3%	0%	8%	0%
5	Siempre	0%	0%	0%	4%

Tabla 100. Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han controlado los amigos/as en redes sociales, mensajes, WhatsApp, etc., de su pareja.

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,23	0,669	1	4
2º ESO	1,11	0,320	1	2
3º ESO	1,58	0,945	1	4
4º ESO	1,40	0,957	1	5

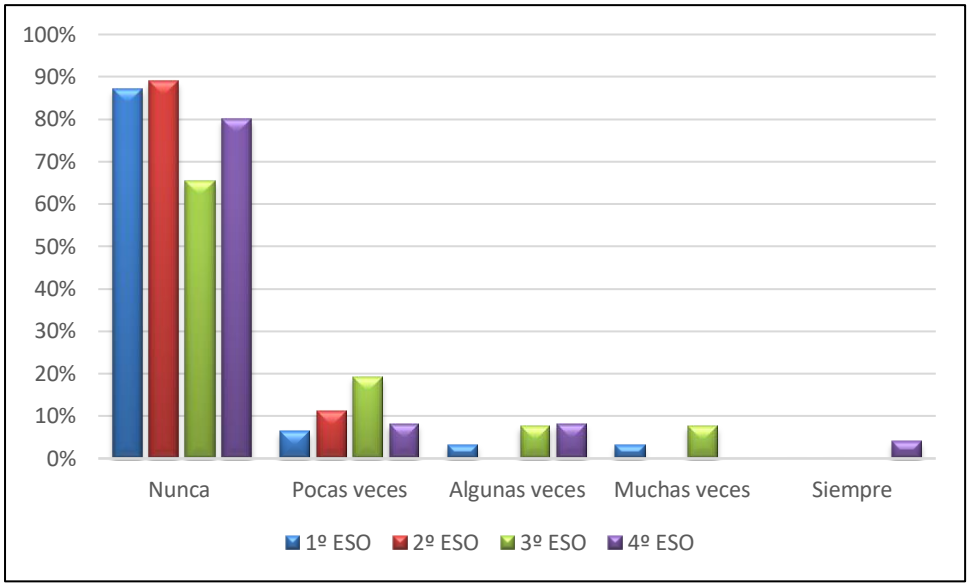

Figura 147. Ítem. 17. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

18. ¿Has pedido a tu pareja que retire fotos o comentarios de redes sociales, WhatsApp, etc.?

Tabla 101. *Ítem. 18. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	94%	85%	69%	88%
2	Pocas veces	3%	7%	8%	8%
3	Algunas veces	3%	4%	8%	0%
4	Muchas veces	0%	0%	15%	0%
5	Siempre	0%	4%	0%	4%

Tabla 102. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han pedido a su pareja que retire fotos o comentarios de redes sociales, WhatsApp, etc.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,10	0,396	1	3
2º ESO	1,30	0,869	1	5
3º ESO	1,69	1,158	1	4
4º ESO	1,24	0,831	1	5

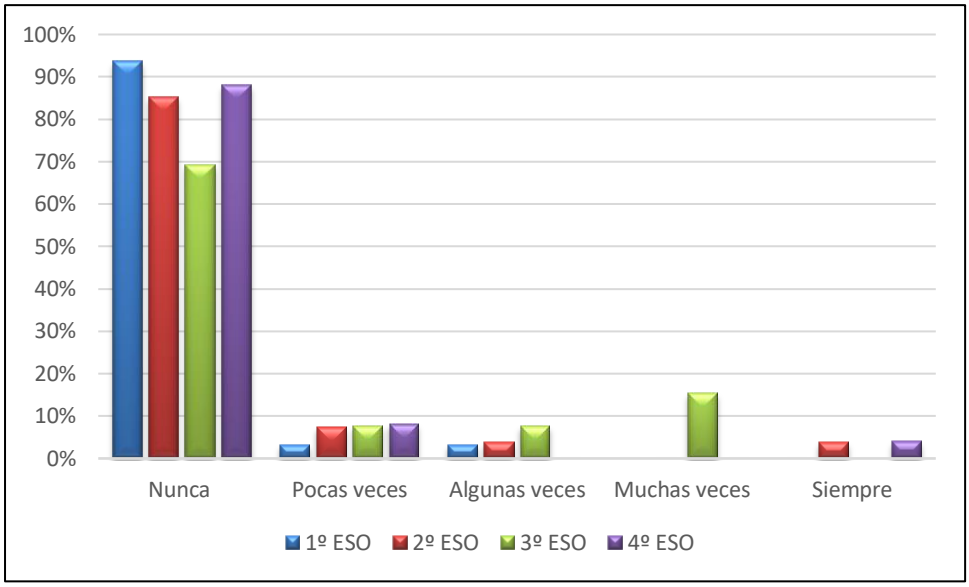

Figura 148. Ítem. 18. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

19. ¿Has pedido a tu pareja que suprima o borre a amigos/as en redes sociales, etc.?

Tabla 103. *Ítem. 19. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	94%	100%	85%	96%
2	Pocas veces	3%	0%	8%	0%
3	Algunas veces	3%	0%	4%	0%
4	Muchas veces	0%	0%	4%	0%
5	Siempre	0%	0%	0%	4%

Tabla 104. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han pedido a su pareja que suprima o borre a amigos/as en redes sociales, etc.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,10	0,396	1	3
2º ESO	1	0	1	1
3º ESO	1,27	0,724	1	4
4º ESO	1,16	0,800	1	5

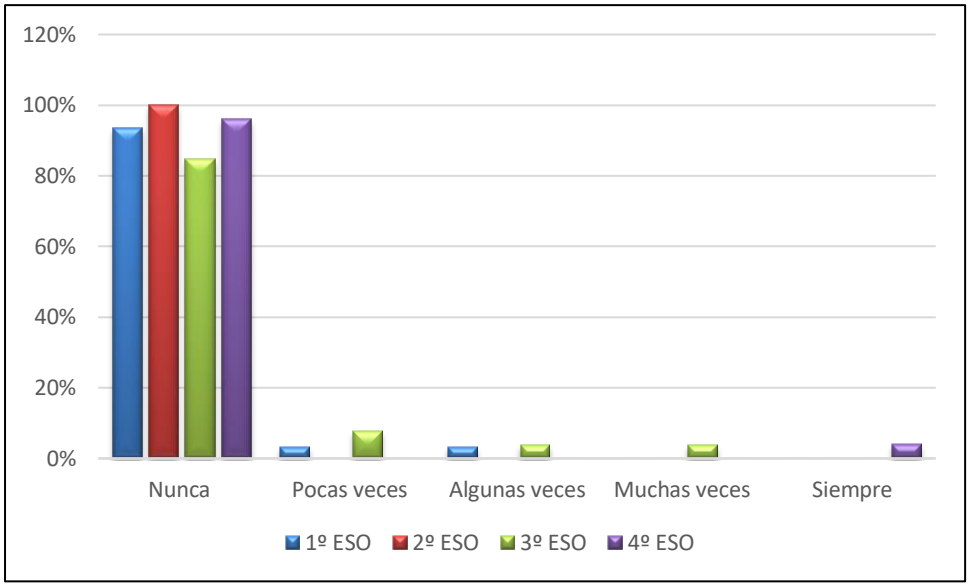

Figura 149. Ítem. 19. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

20. ¿Has obligado a tu pareja a realizar comportamientos de tipo sexual a través de la webcam?

Tabla 105. *Ítem. 20. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	100%	96%
2	Pocas veces	0%	0%	0%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	4%

Tabla 106. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO de la Divina Providencia han obligado a su pareja a realizar comportamientos de tipo sexual a través de la webcam.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1	0	1	1
4º ESO	1,16	0,800	1	5

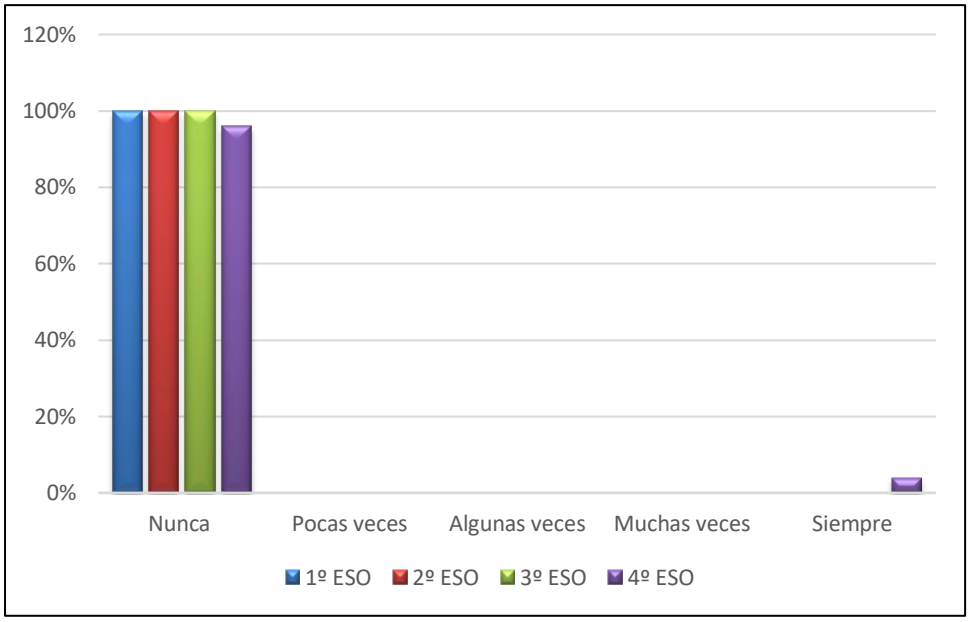

Figura 150. Ítem. 20. Contestaciones alumnos de 1º a 4º ESO de N. Sª de la Divina Providencia.

En la tabla 107 y figura 151, podemos apreciar que, de los 109 menores participantes, 56 chicos y 53 chicas, respectivamente, de los cursos 1º a 4º de la ESO de la Divina Providencia, con relación a la pregunta de a quién comunicarían los hechos o conductas reseñados en los ítems 1 a 20, ambos inclusive, en el caso de observarlos y/o protagonizarlos, en primer lugar, la mayoría contestaron que lo participarían a sus padres, en segundo lugar, a sus compañeros salvo los de 1º ESO que lo comunicarían antes a sus profesores, en tercer y cuarto lugar existen discrepancias entre los cursos, por ejemplo, podemos destacar que los de 3º y 4º de la ESO no lo comunicarían a nadie y como última opción lo harían a sus profesores.

Tabla 107. *Resultados sobre a quién comunicarían los observadores, víctimas y/o victimarios, en su caso, alguno de los hechos o conductas mencionados (Divina Providencia).*

	Colegio N. Sª de la Divina Providencia			
Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Compañeros	14%	27%	34%	19%
Padres	57%	49%	43%	52%
Profesores	25%	16%	9%	13%
A nadie	4%	8%	14%	16%

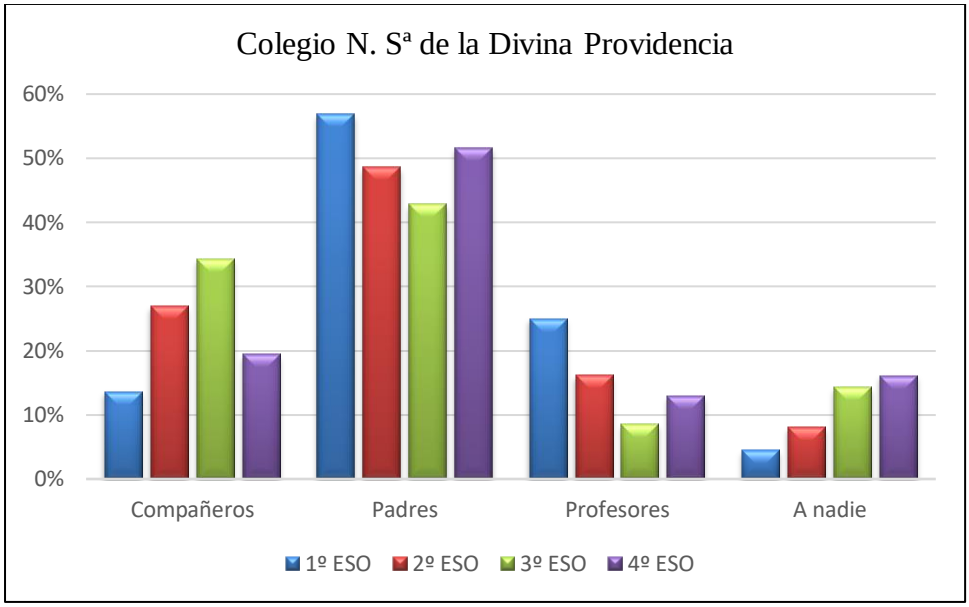

Figura 151. Comparativa de resultados de 1º a 4º de la ESO Divina Providencia (tabla 107).

A continuación, en las figuras 152 a 155, podemos observar por cursos de la ESO del Colegio Divina Providencia los resultados porcentuales obtenidos en las contestaciones a la pregunta mencionada por parte de los menores que han participado en este estudio criminológico social.

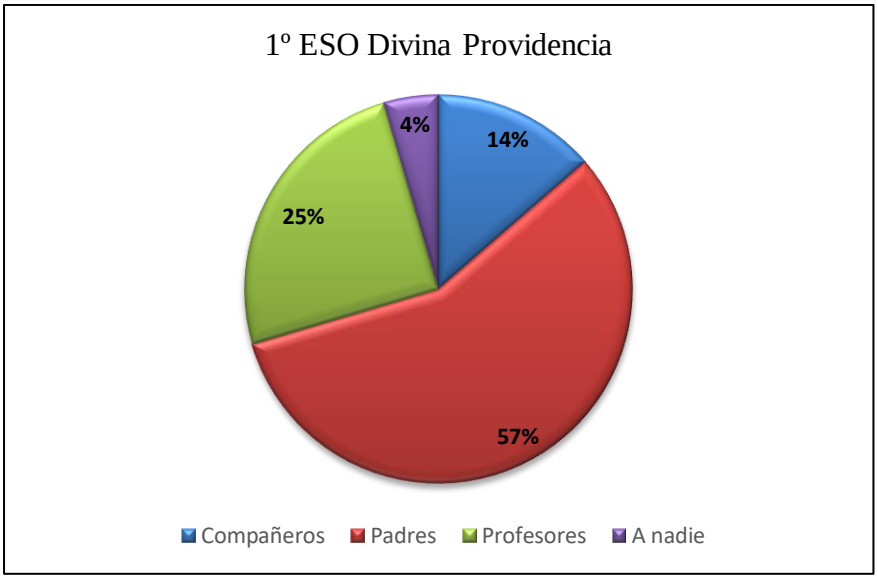

Figura 152. -1º ESO Divina Providencia: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

Figura 153. -2º ESO Divina Providencia: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

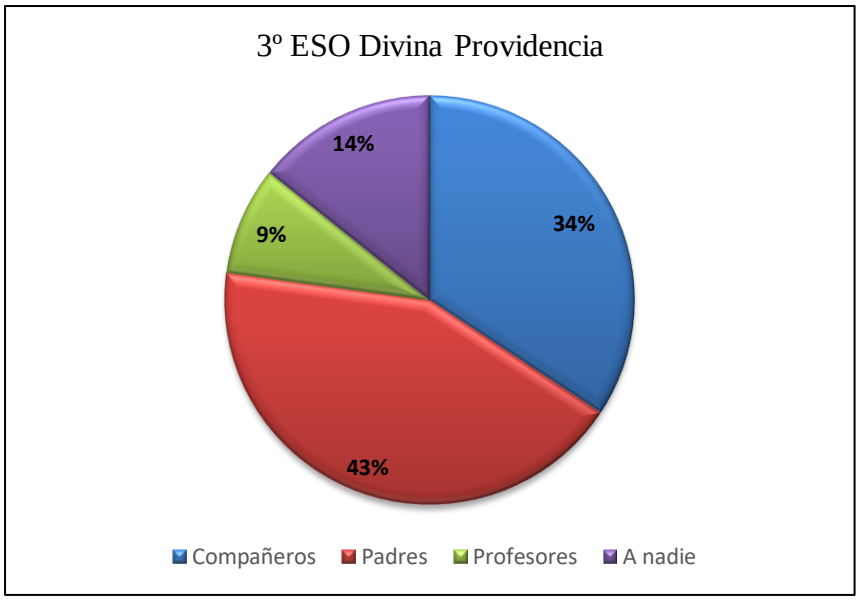

Figura 154. -3º ESO Divina Providencia: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

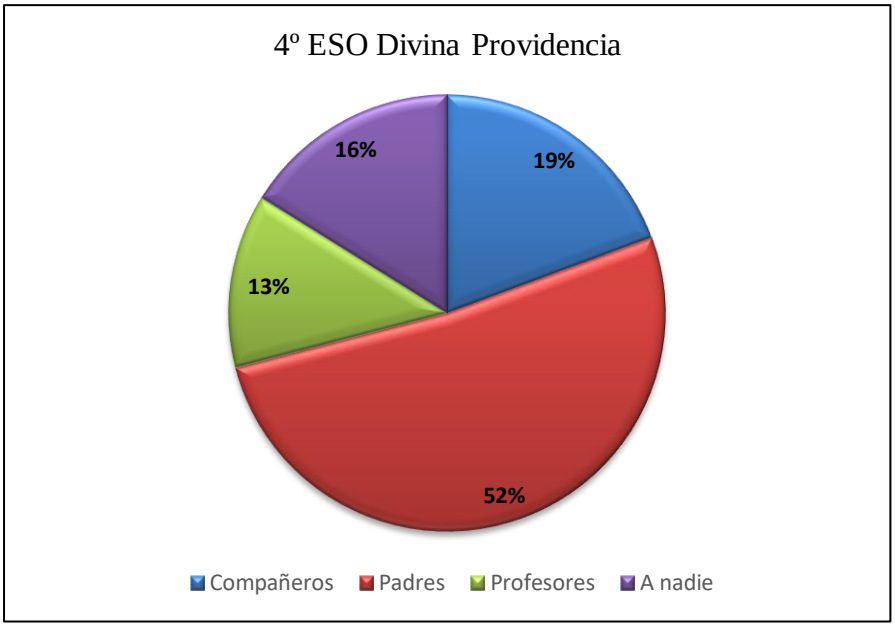

Figura 155. -4º ESO Divina Providencia: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

Por otra parte, en lo atinente a los resultados arrojados respecto a la pregunta sobre qué actividades preventivas propondrían frente a hechos o conductas de ciberacoso, y que se han plasmado en la tabla 108 y en las figuras 156 a 160, respectivamente, podemos destacar que los alumnos del Colegio Divina Providencia de la ESO, en general, optaría mayoritariamente en primer lugar por comunicar los hechos o conductas referenciados a personas adultas antes que denunciarlo a la policía.

No obstante, los alumnos de 3º de la ESO son más partidarios de pedir o solicitar ayuda preferentemente, antes que denunciar a la policía los hechos (un 26% frente a un 23%).

Curiosamente, respecto a la opción de respuesta de mediación con el ciberacosador, los resultados obtenidos oscilan del 2% al 11%, constituyendo una evidencia de que, en general, el alumnado de la ESO participante no cree en esta figura para prevenir, abordar y resolver conflictos con el ciberacosador.

Por último, podemos destacar que un porcentaje muy minoritario del alumnado participante de la ESO, concretamente, entre un 0% y un 5%, marcó como respuesta ignorar el ciberacoso, hecho que evidencia su concienciación del problema existente en nuestra sociedad con una interacción cada vez más virtual.

Tabla 108. *Resultados sobre las propuestas que hacen los menores participantes para evitar hechos o conductas de ciberacoso (Divina Providencia).*

	Colegio N. Sª de la Divina Providencia			
Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Comunicar adultos	41%	37%	30%	30%
Denunciar a la policía	35%	32%	23%	27%
Ignorar ciberacoso	2%	0%	3%	5%
Mediar con el ciberacosador	2%	5%	11%	7%
Pedir ayuda	16%	25%	26%	25%
Otras	4%	0%	8%	7%

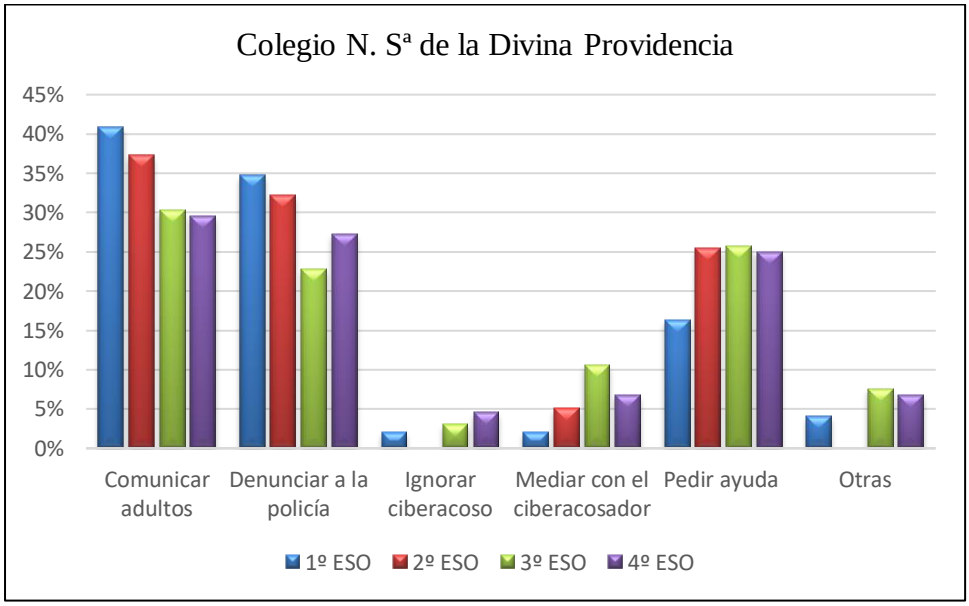

Figura 156. Comparativa de resultados 1º a 4º de la ESO Divina Providencia (tabla 108).

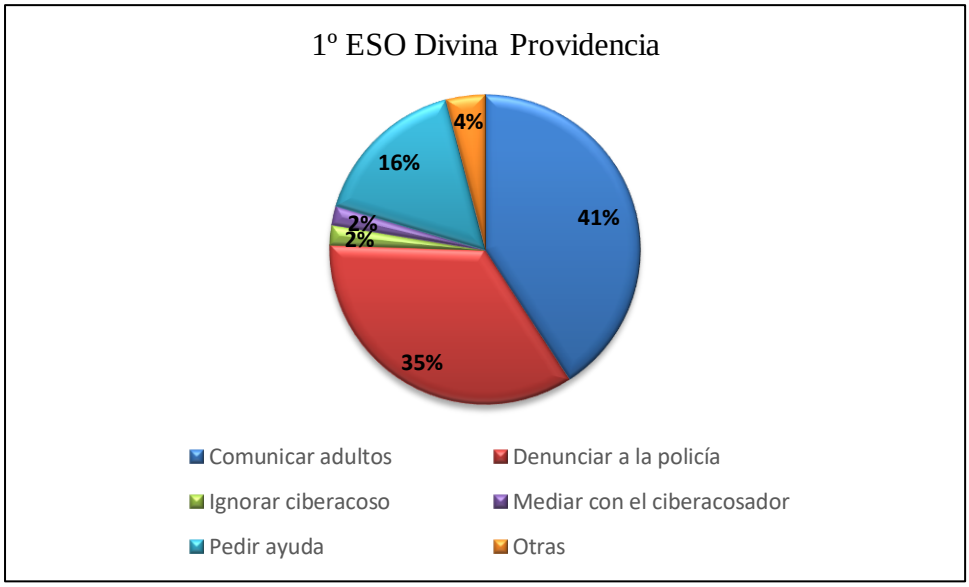

Figura 157. -1º ESO Divina Providencia: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

Figura 158. -2º ESO Divina Providencia: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

Figura 159. -3º ESO Divina Providencia: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

Figura 160. -4º ESO Divina Providencia: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

c)-IES Leopoldo Querol: de un total de 513 alumnos matriculados de la ESO, se ha tomado una muestra de este centro educativo de 109 alumnos encuestados que han participado voluntariamente, de los que un 58% son chicas y un 42% son chicos, de 12 a 16 años, correspondientes a los cursos de 1º a 4º de la ESO, tal y como podemos observar en la tabla 109 y figura 161**,** respectivamente.

Concretamente, de 1º de la ESO la media de edad es 12,38 años; de 2º de la ESO es 13,45 años; de 3º ESO es de 14,77 años y de 4º ESO es 15,42 años.

Tabla 109. *Edad y género de los menores participantes de la ESO del IES Leopoldo Querol.*

Curso académico	Edades	Chicos	Chicas	
1º ESO	12-14	13	13	26
2º ESO	13-16	14	17	31
3º ESO	14-16	8	18	26
4º ESO	15-16	11	15	26
	Totales	46	63	109

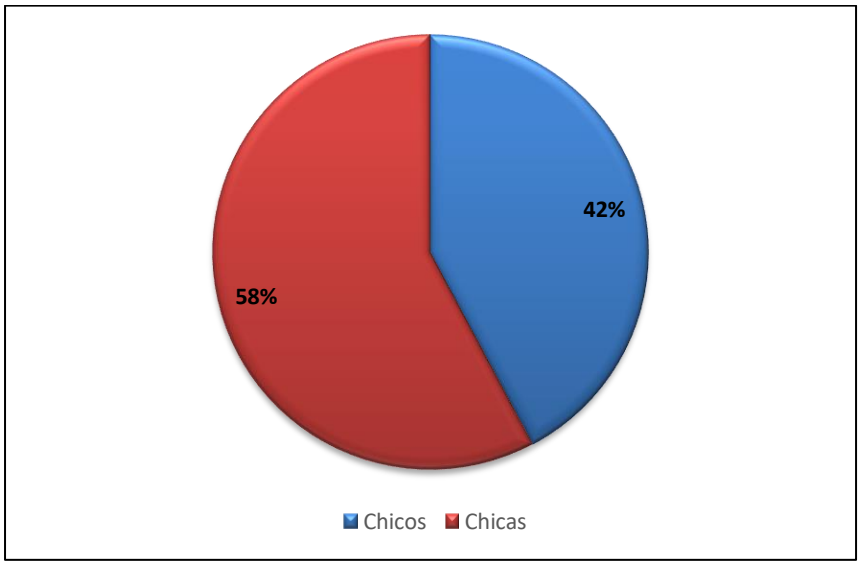

Figura 161. Porcentaje total participantes por género de la ESO del IES Leopoldo Querol.

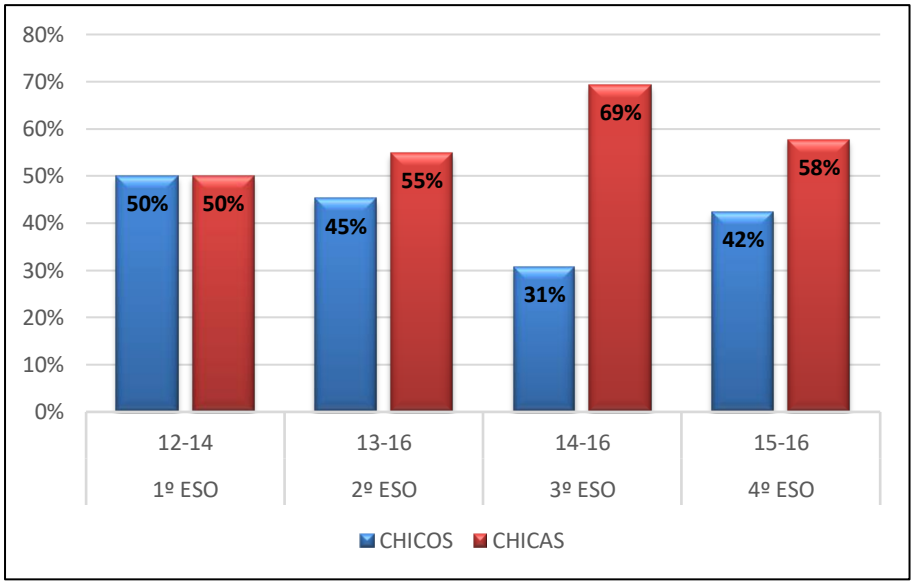

Figura 162. Menores de la ESO del IES Leopoldo Querol por curso académico y género.

En general, excepto en 1º de la ESO que se encuentran a la par, en el resto de los cursos académicos hay más chicas que chicos, destacando 3º ESO al existir una diferencia entre ambos géneros notable, es decir, un 31% chicos y un 69% chicas, tal y como podemos ver en la figura 162.

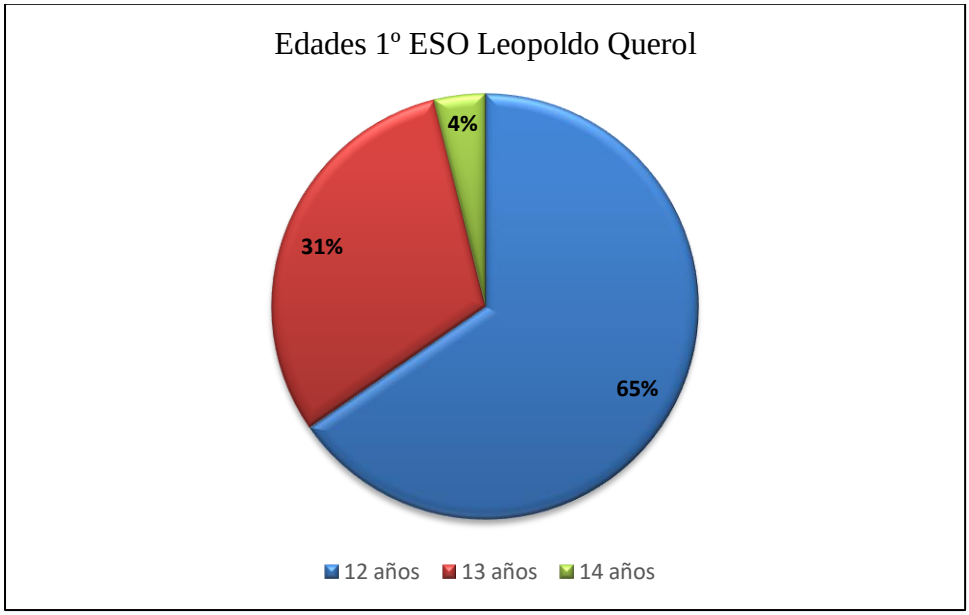

Figura 163. Edades menores de 1º ESO del IES Leopoldo Querol.

En la figura 163, podemos apreciar que dentro del rango de edad de los menores participantes en el presente estudio correspondientes al curso de 1º de la ESO del IES Leopoldo Querol, la mayoría tiene 12 años, es decir, un 65%, mientras que un 31% tiene 13 años y el 4% restante tiene 14 años.

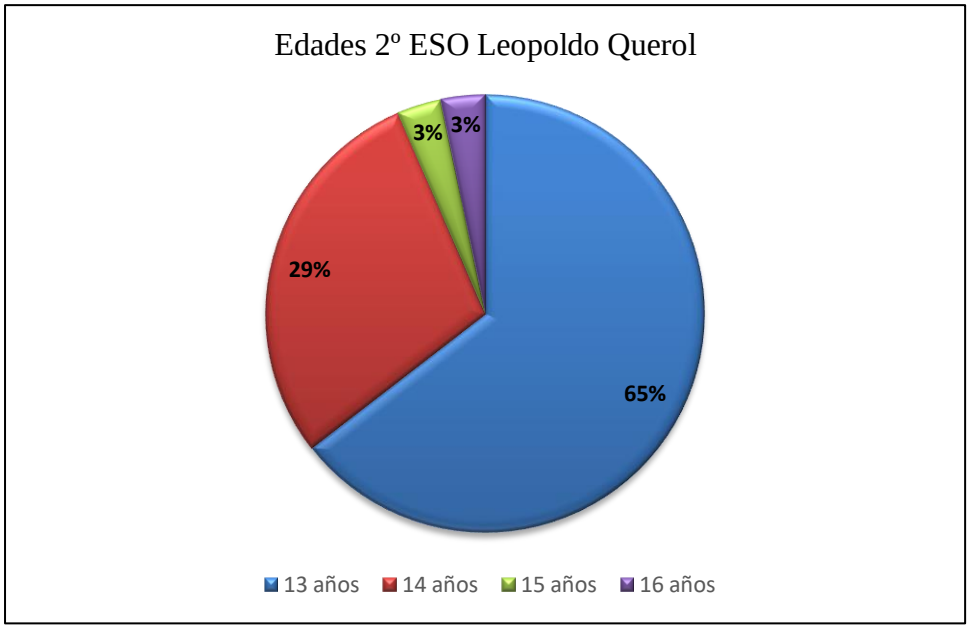

Figura 164. Edades menores de 2º ESO del IES Leopoldo Querol.

En la figura 164, podemos destacar que del curso 2º de la ESO del IES Leopoldo Querol, la mayoría de los participantes tiene 13 años, es decir, un 65%, 14 años un 29%, mientras que una minoría del 3% tiene 15 y 16 años, respectivamente.

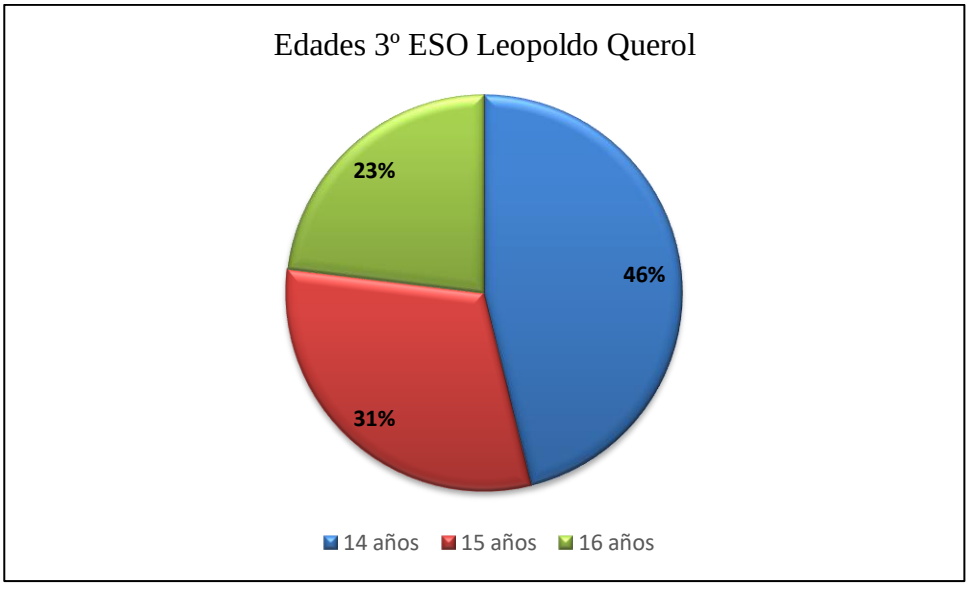

Figura 165. Edades menores de 3º ESO del IES Leopoldo Querol.

En la figura 165, podemos observar que del curso 3º de la ESO del IES Leopoldo Querol, la mayoría tiene 14 años, es decir, un 46%, 15 años tiene un 31% y el 23% restante tiene 16 años.

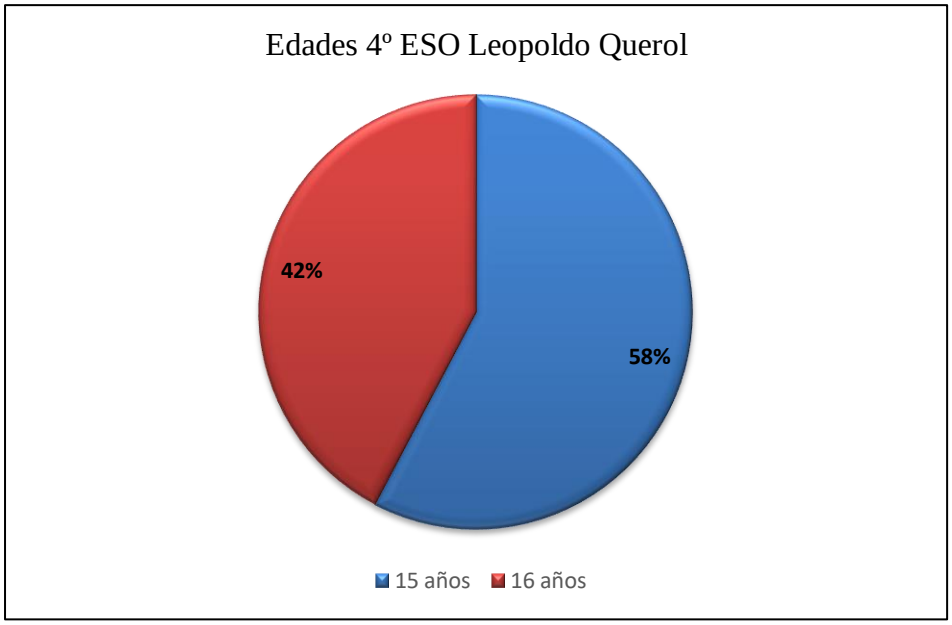

Figura 166. Edades menores de 4º ESO del IES Leopoldo Querol.

En la figura 166, podemos observar que del curso 4º de la ESO del IES Leopoldo Querol, un 58% tiene 15 años mientras que el 42% restante tiene 16 años.

Por otra parte, con relación a la interacción con las TIC de los menores que cursan la ESO en el instituto de educación secundaria Leopoldo Querol, en la encuesta de victimización social figuraban en la primera página, diez ítems con opción de respuesta "SI o "NO", así como otras preguntas con respuestas cerradas, en su caso, obteniéndose los resultados que a continuación se detallan en las tablas 110 a 113, respectivamente, así como los representados gráficamente en las figuras 167 a 206 ambas inclusive.

Tabla 110. *Resultados interacción TIC menores de 1º ESO Leopoldo Querol.*

Ítems interacciones TIC menores 1º ESO	SI	NO
Tengo ordenador en casa	21	5
Tengo webcam	10	16
Tengo teléfono móvil	26	0
Guardo información personal en el teléfono móvil	14	12
Tengo cuenta de correo electrónico	24	2
Utilizo programas de mensajería instantánea	25	1
Utilizo redes sociales	22	4
Utilizo blogs, foros en Internet	8	18

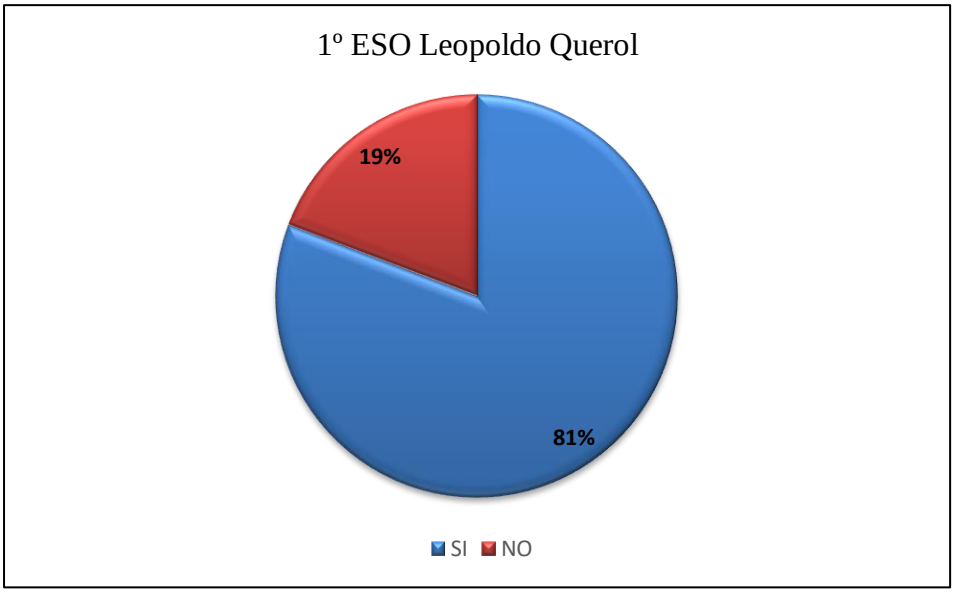

Figura 167. ¿Tienes ordenador en casa?

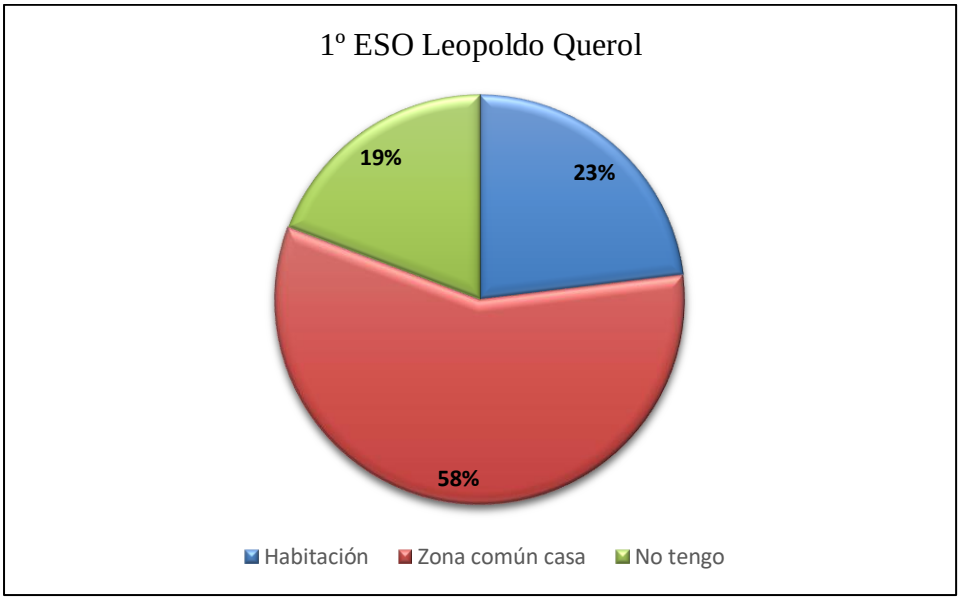

Figura 168. ¿Dónde tienes ubicado el ordenador?

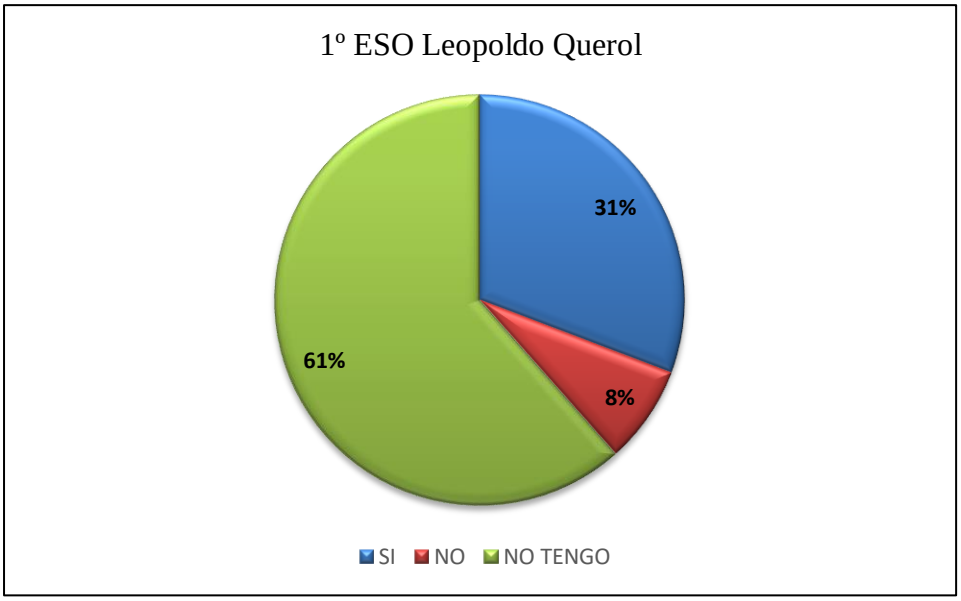

Figura 169. ¿Tapas la webcam cuando no la utilizas?

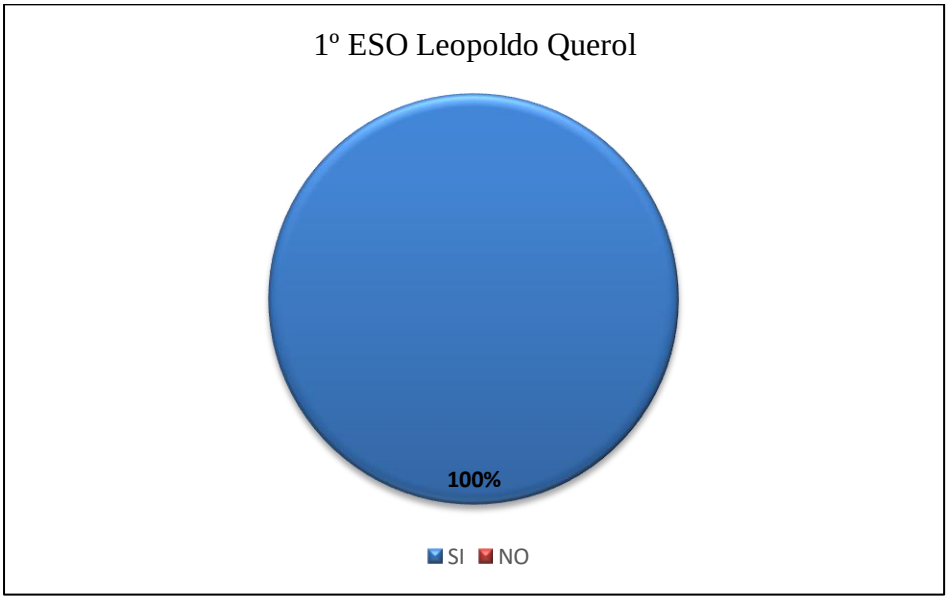

Figura 170. ¿Tienes teléfono móvil?

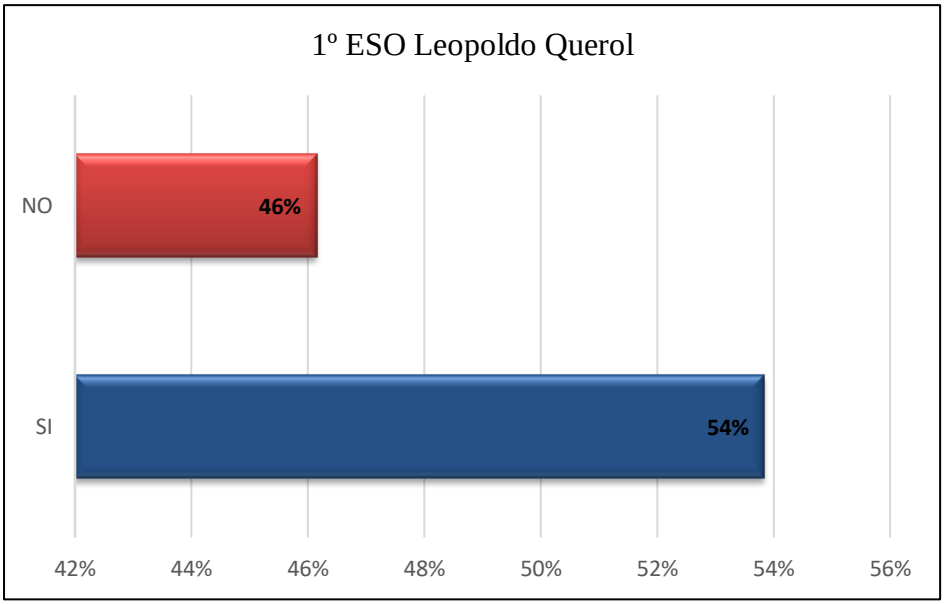

Figura 171. ¿Guardas información personal en tu teléfono móvil?

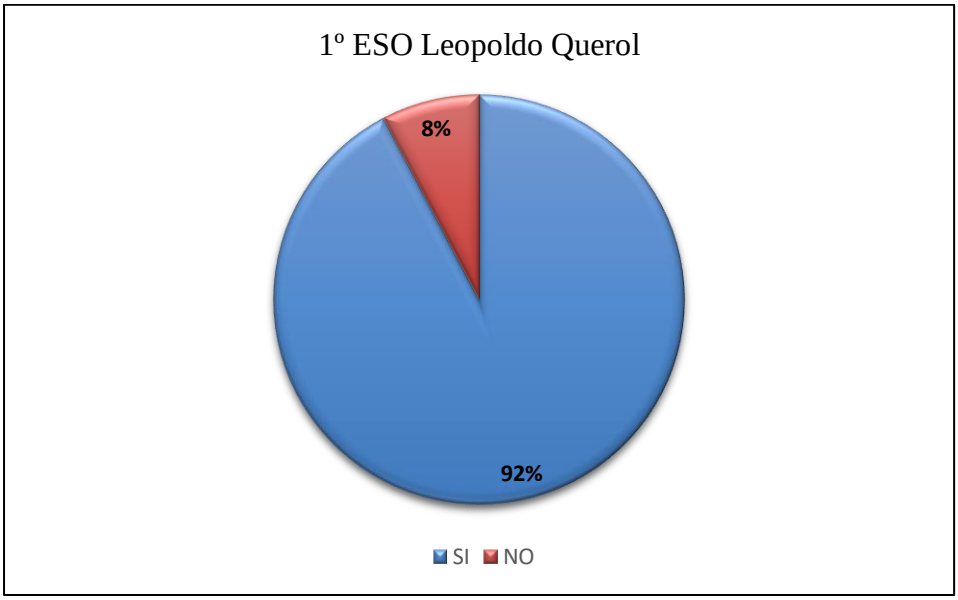

Figura 172. ¿Tienes cuenta de correo electrónico?

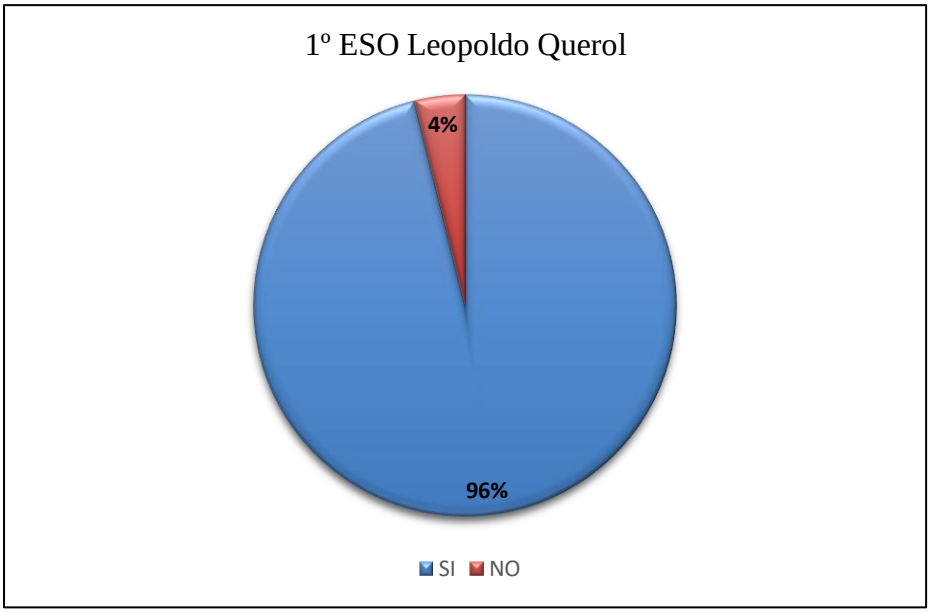

Figura 173. ¿Utilizas programas de mensajería instantánea?

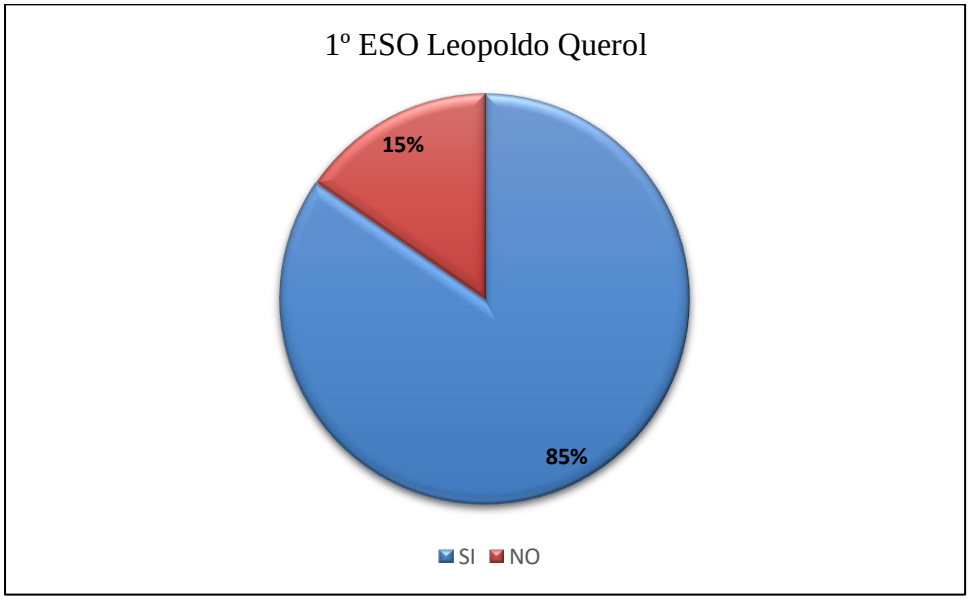

Figura 174. ¿Utilizas redes sociales?

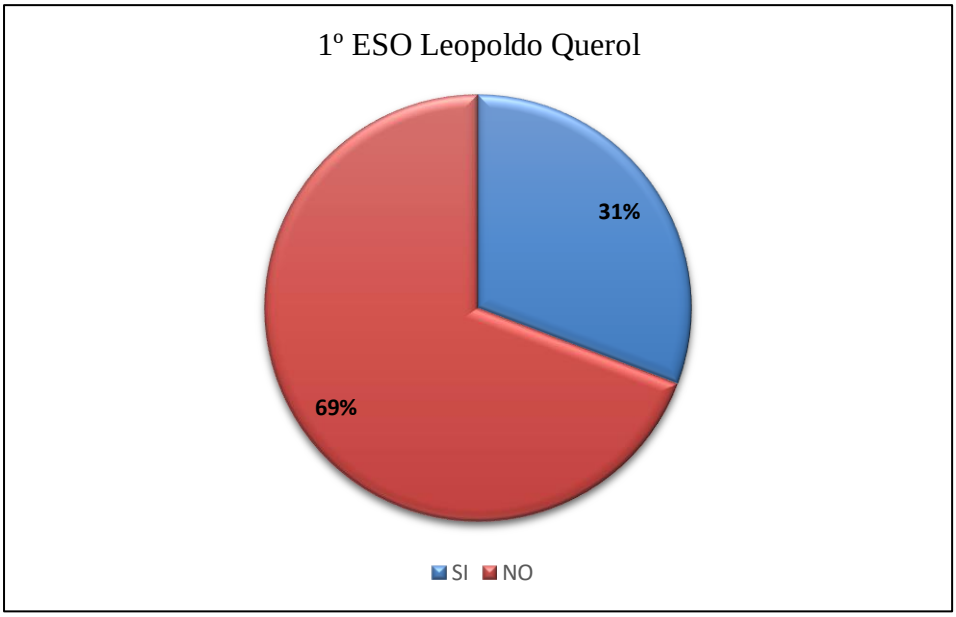

Figura 175. ¿Utilizas blogs, foros en Internet?

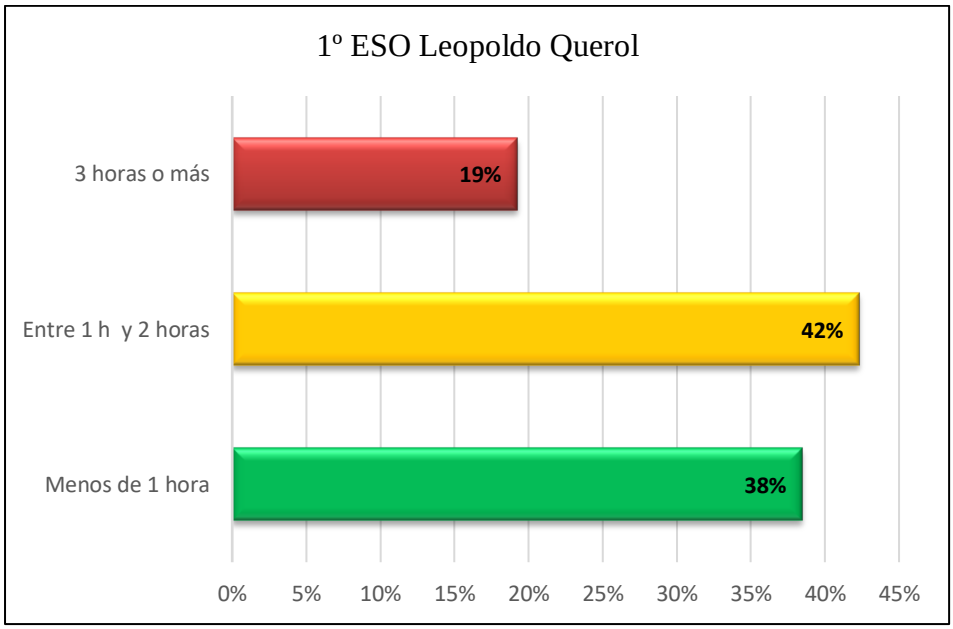

Figura 176. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Tabla 111. *Resultados interacción TIC menores de 2º ESO Leopoldo Querol.*

Ítems interacciones TIC menores 2º ESO	SI	NO
Tengo ordenador en casa	29	2
Tengo webcam	17	14
Tengo teléfono móvil	31	0
Guardo información personal en el teléfono móvil	24	7
Tengo cuenta de correo electrónico	29	2
Utilizo programas de mensajería instantánea	30	1
Utilizo redes sociales	28	3
Utilizo blogs, foros en Internet	12	19

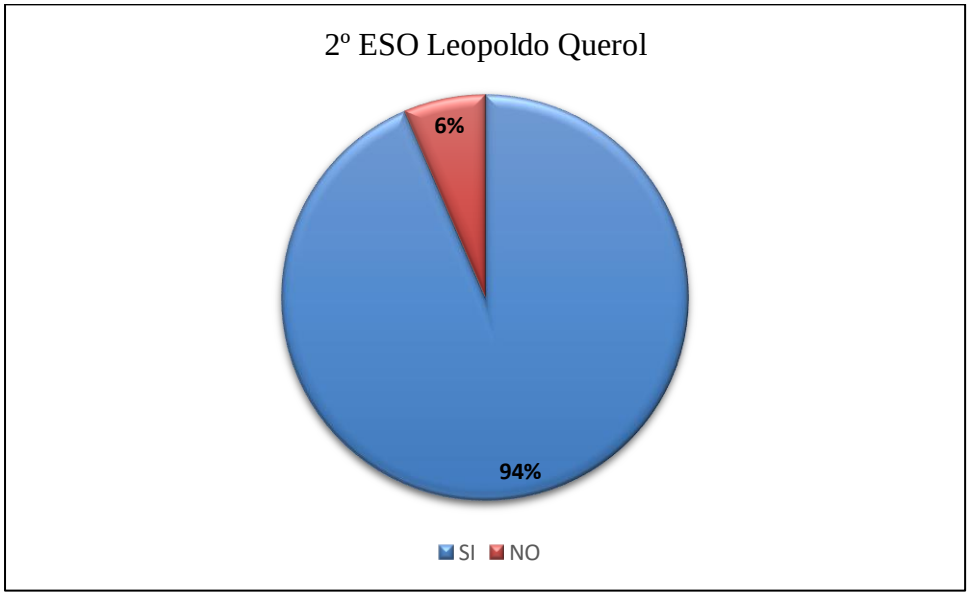

Figura 177.¿Tienes ordenador en casa?

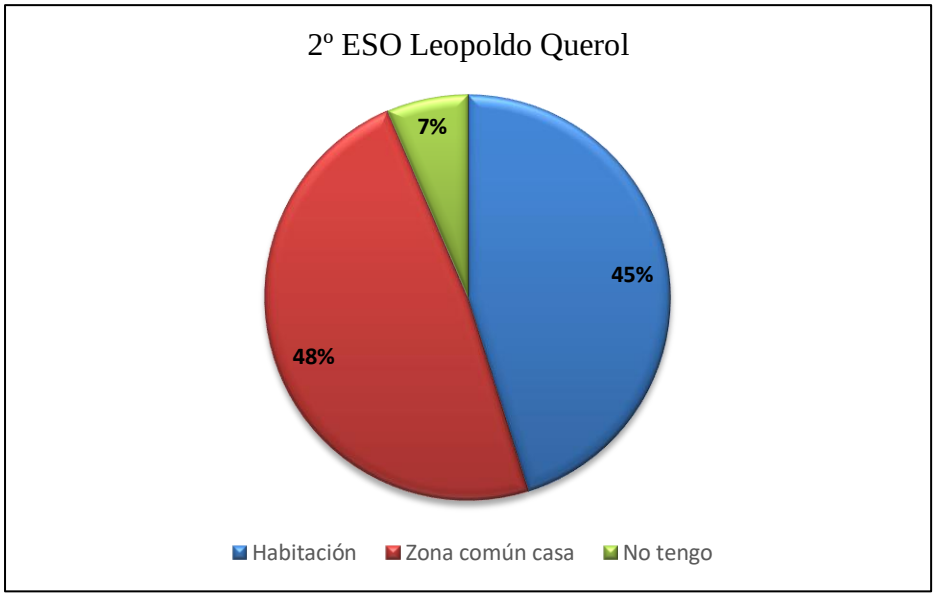

Figura 178. ¿Dónde tienes ubicado el ordenador?

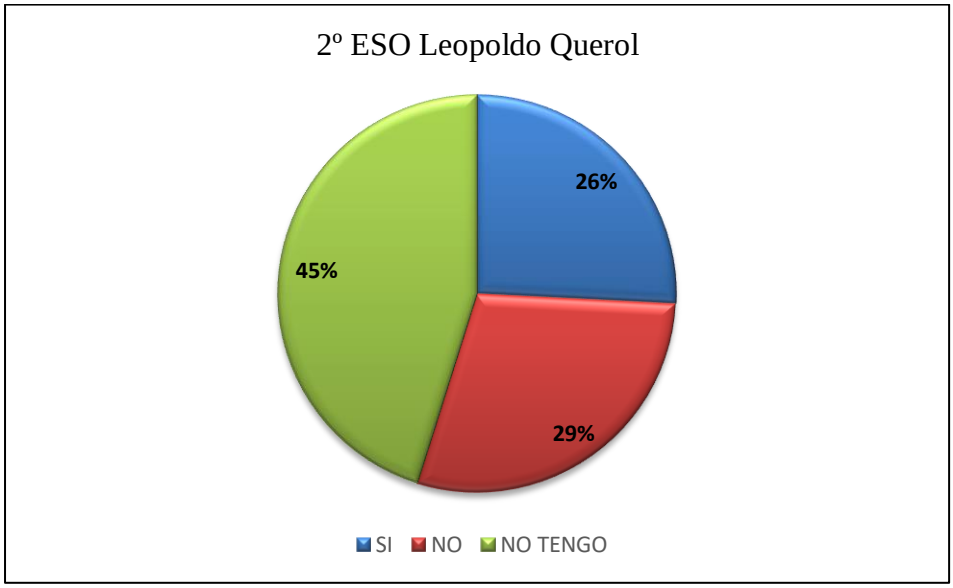

Figura 179. ¿Tapas la webcam cuando no la utilizas?

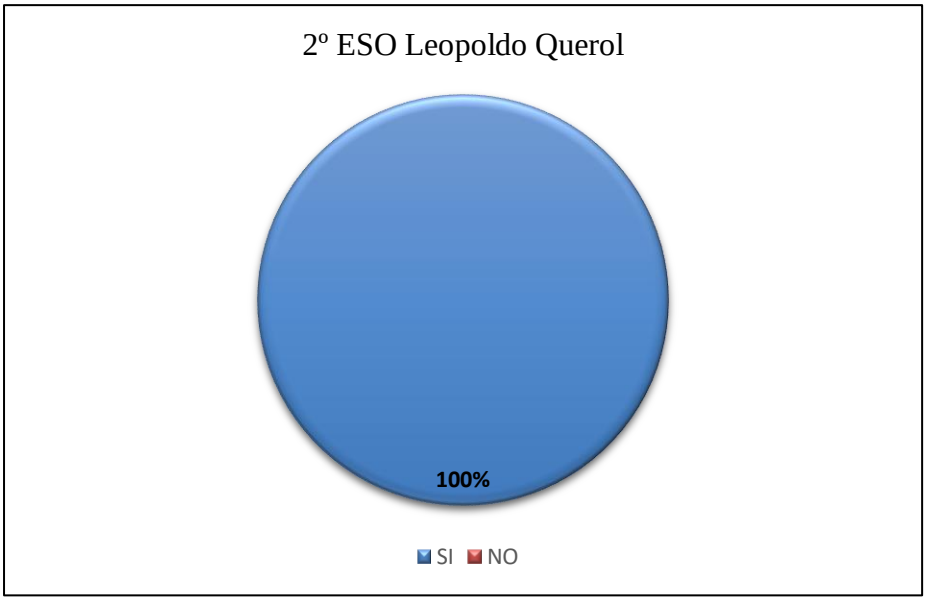

Figura 180. ¿Tienes teléfono móvil?

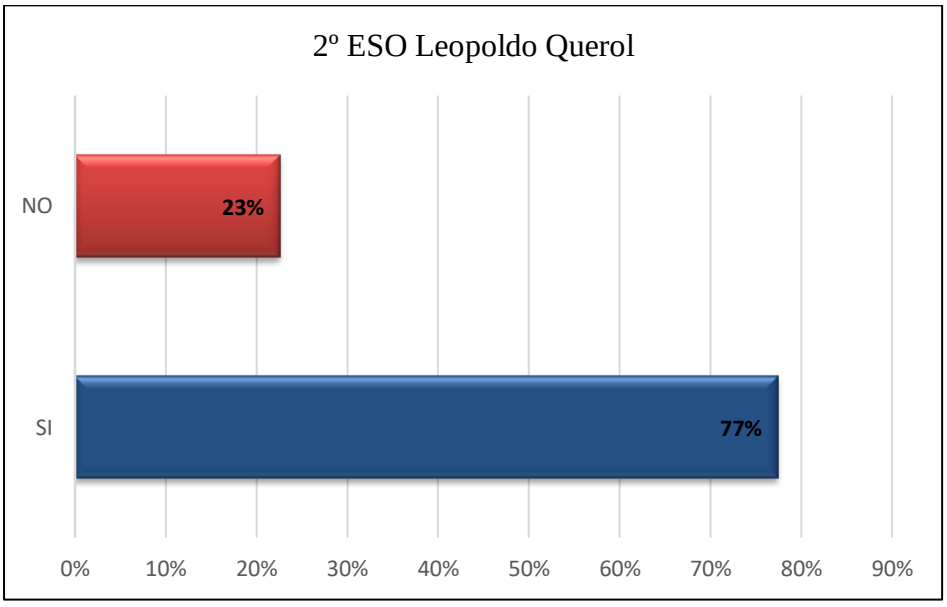

Figura 181. ¿Guardas información personal en el teléfono móvil?

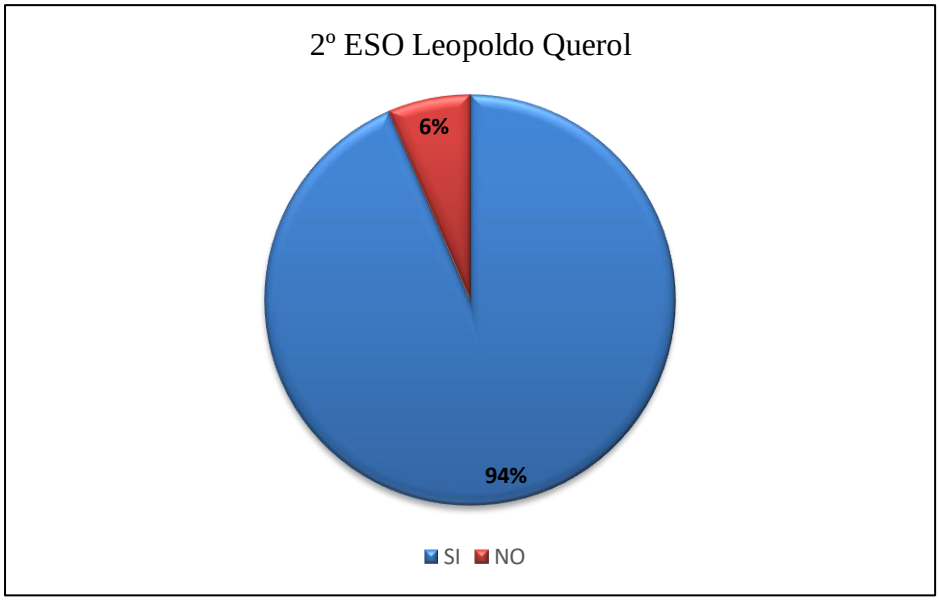

Figura 182. ¿Tienes cuenta de correo electrónico?

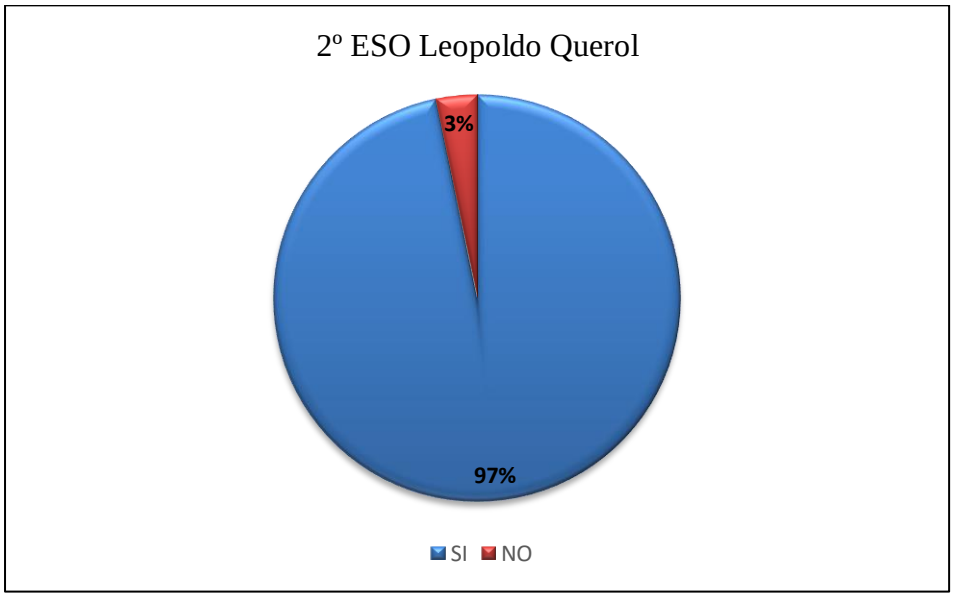

Figura 183. ¿Utilizas programas de mensajería instantánea?

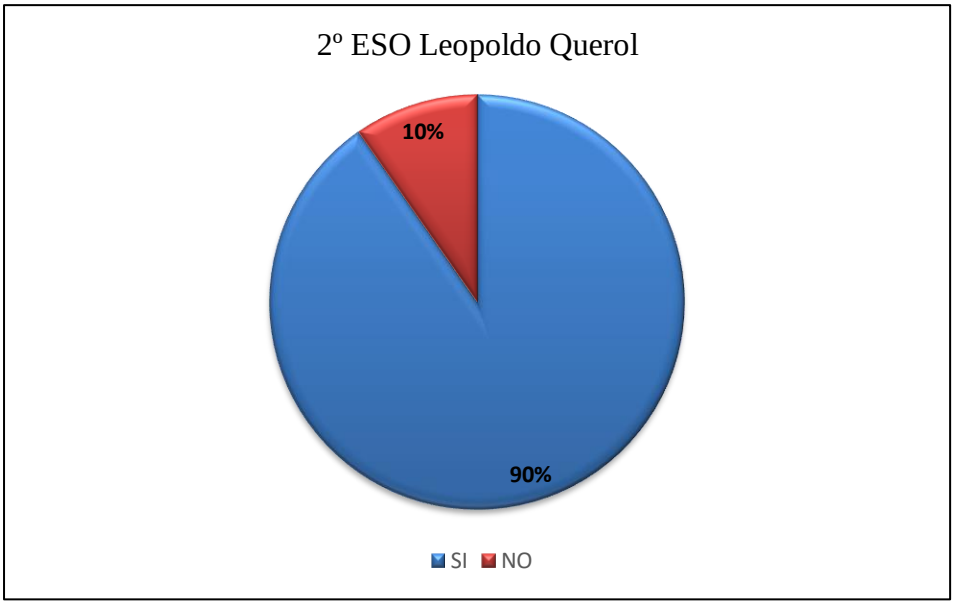

Figura 184. ¿Utilizas redes sociales?

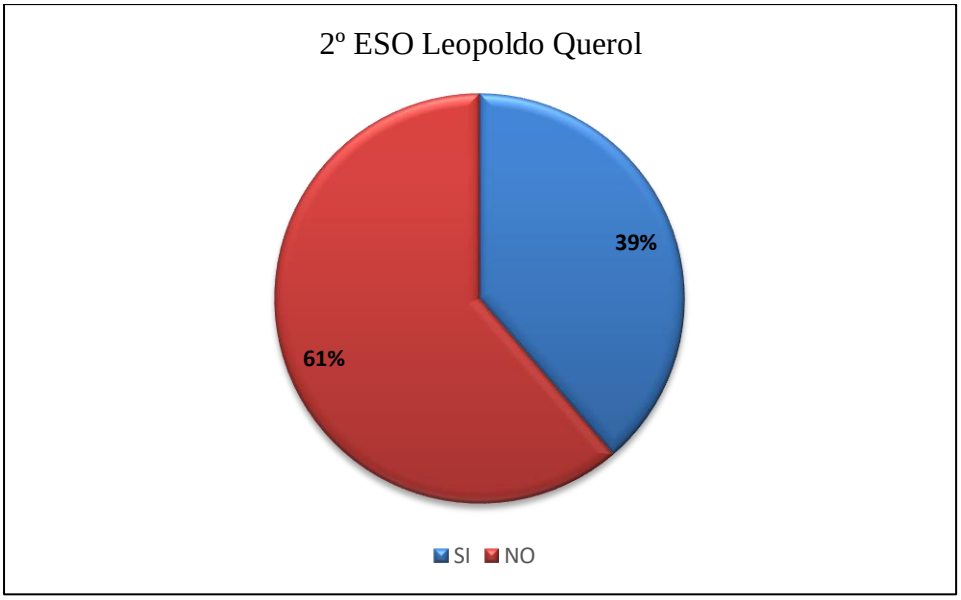

Figura 185. ¿Utilizas blogs, foros en Internet?

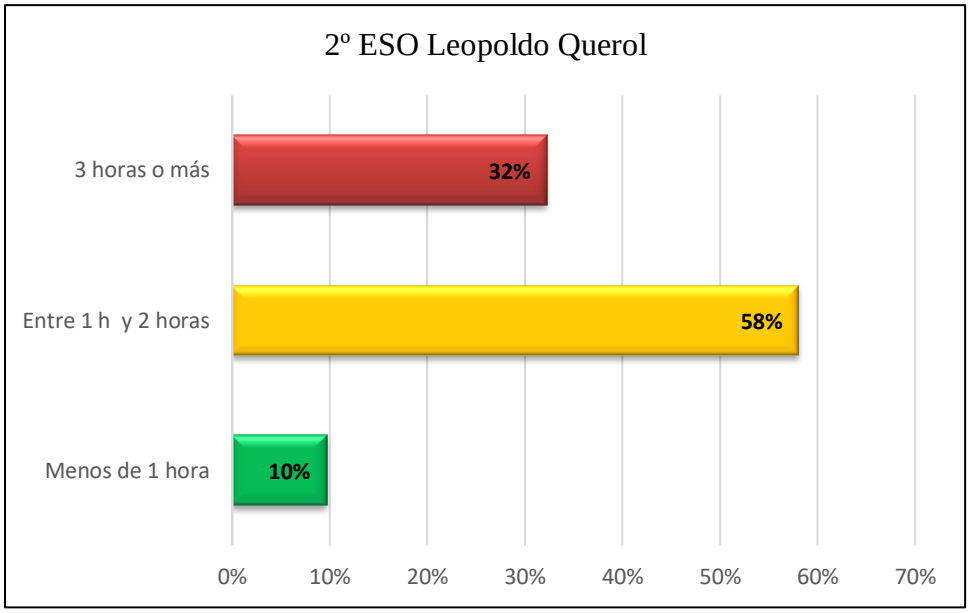

Figura 186. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Tabla 112. *Resultados interacción TIC menores de 3º ESO Leopoldo Querol.*

Ítems interacciones TIC menores 3º ESO	SI	NO
Tengo ordenador en casa	24	2
Tengo webcam	15	11
Tengo teléfono móvil	26	0
Guardo información personal en el teléfono móvil	21	5
Tengo cuenta de correo electrónico	26	0
Utilizo programas de mensajería instantánea	26	0
Utilizo redes sociales	25	1
Utilizo blogs, foros en Internet	13	13

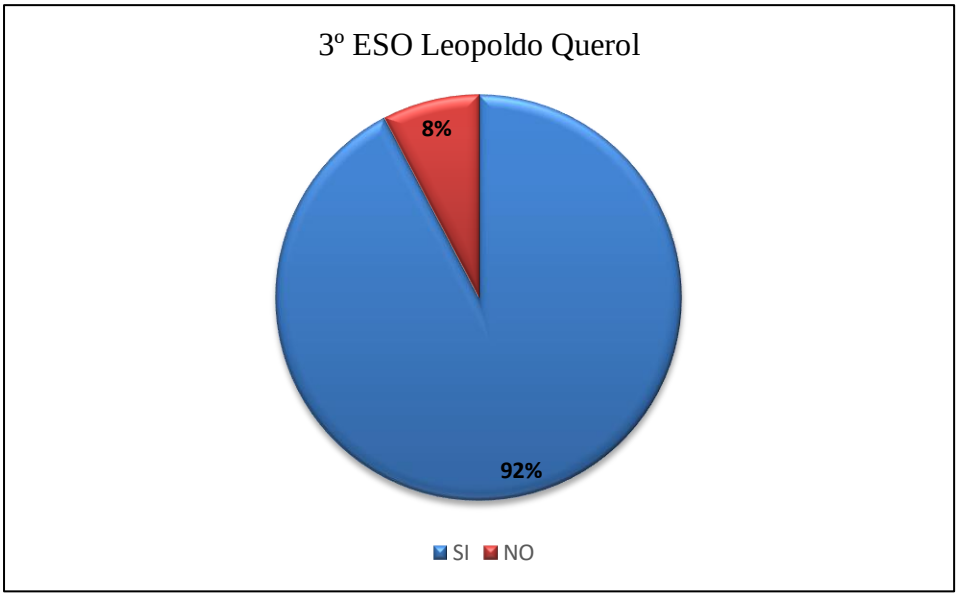

Figura 187. ¿Tienes ordenador en casa?

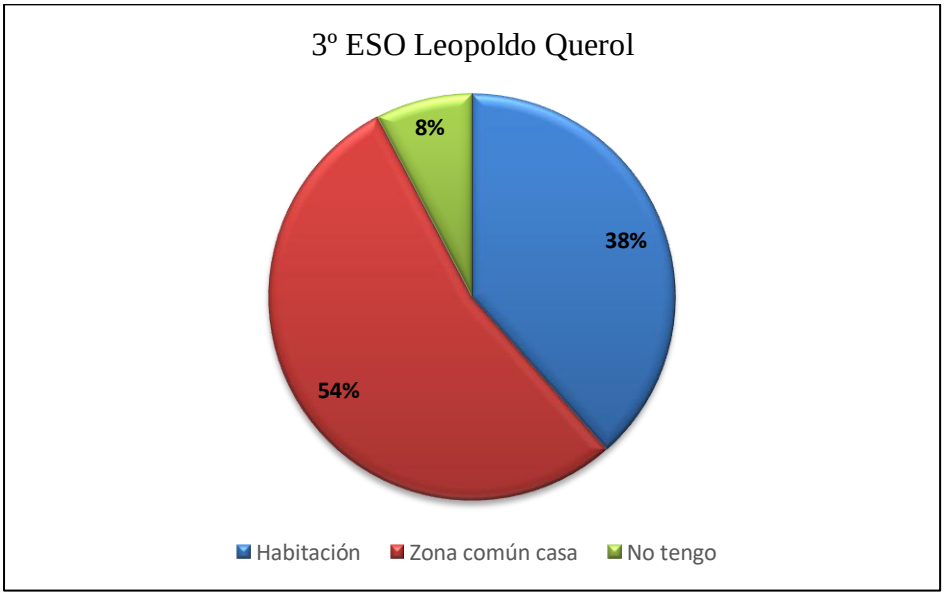

Figura 188. ¿Dónde tienes ubicado el ordenador?

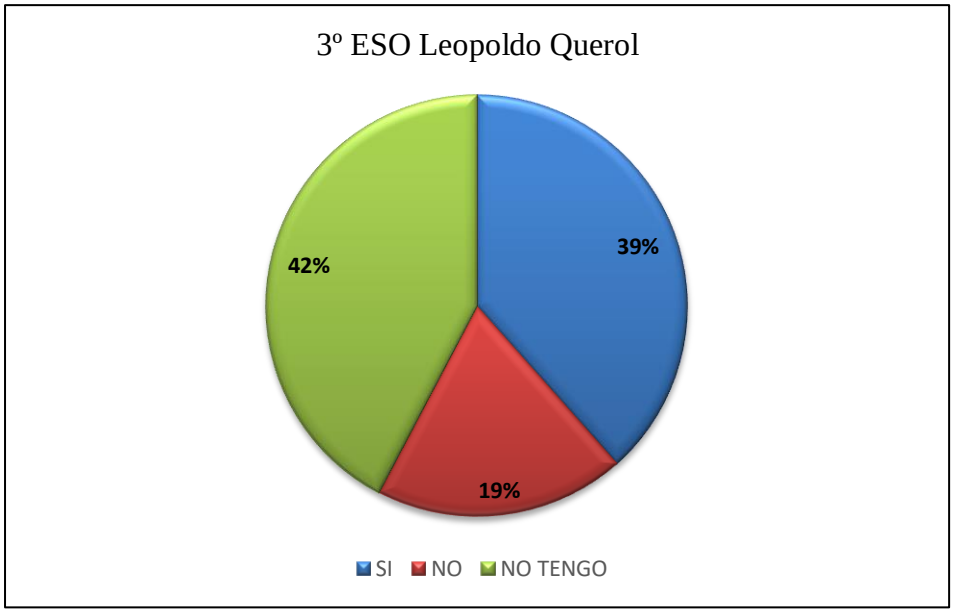

Figura 189. ¿Tapas la webcam cuando no la utilizas?

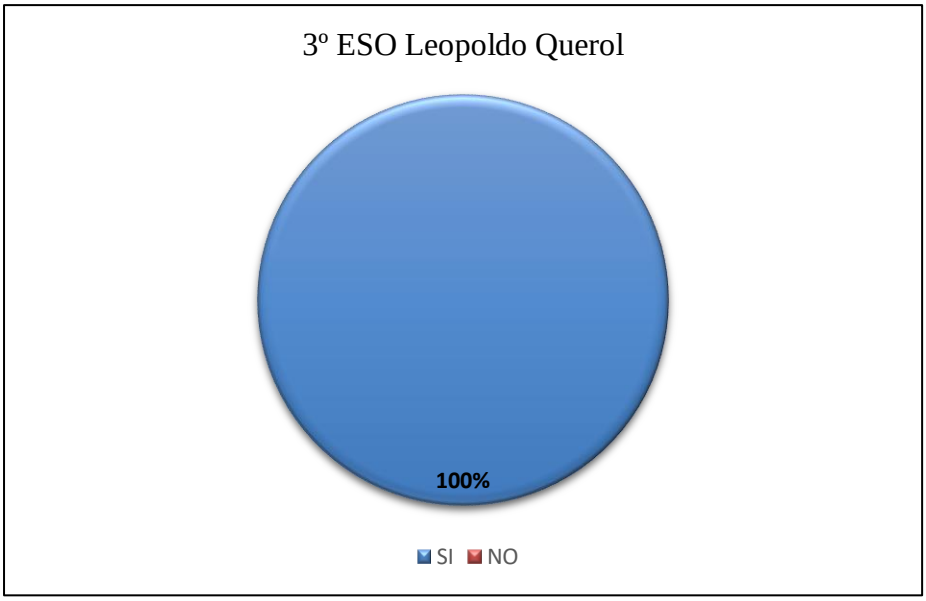

Figura 190. ¿Tienes teléfono móvil?

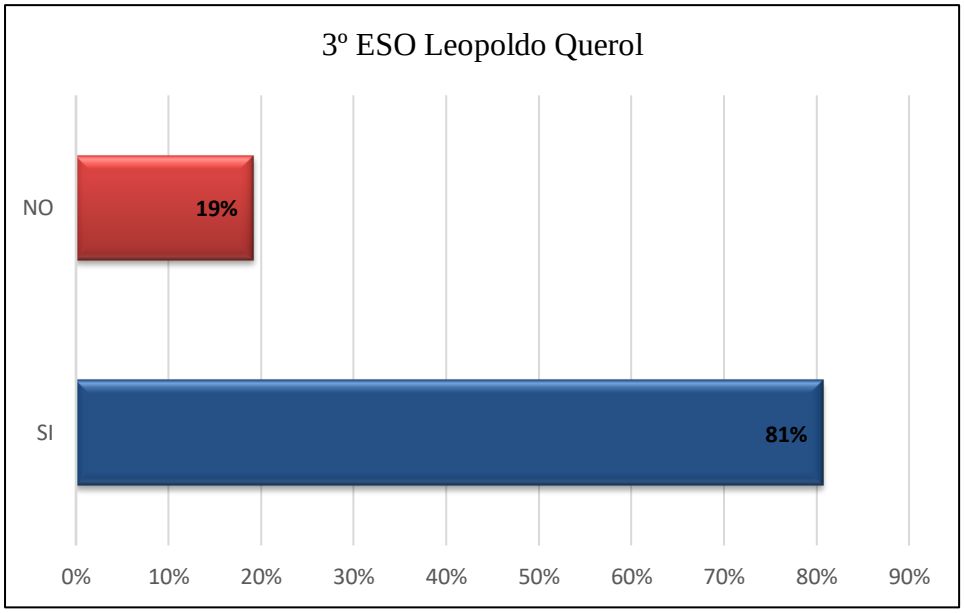

Figura 191.¿Guardas información personal en el teléfono móvil?

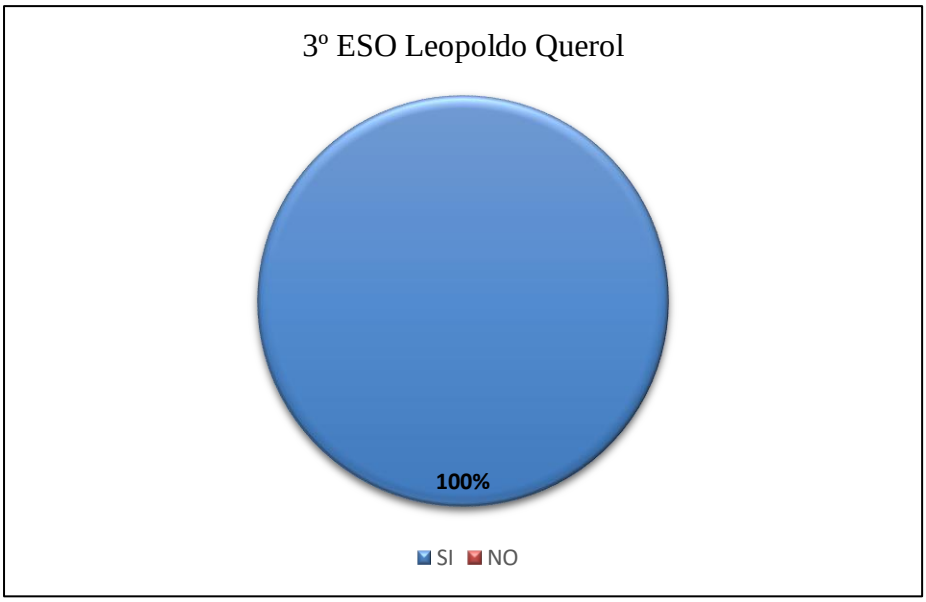

Figura 192. ¿Tienes cuenta de correo electrónico?

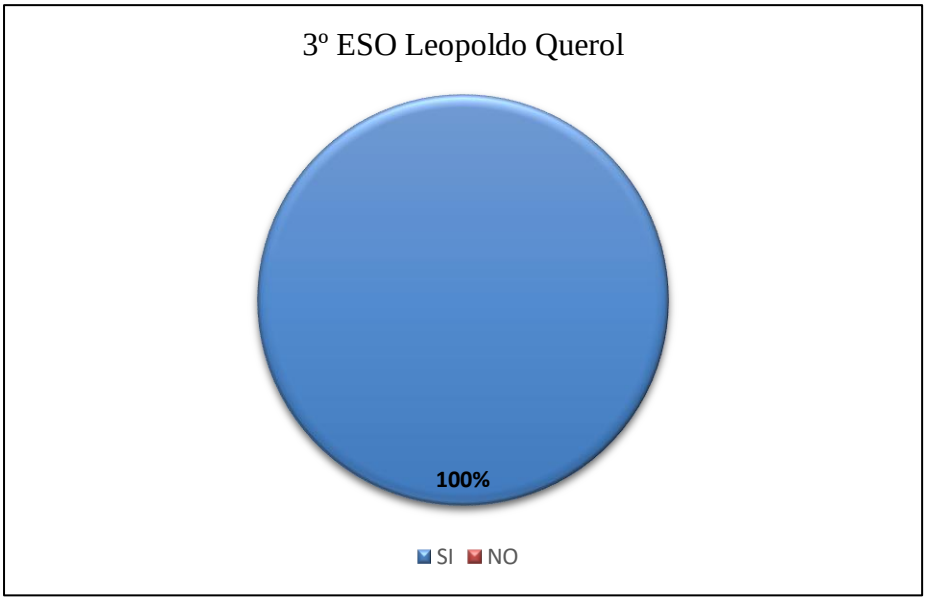

Figura 193. ¿Utilizas programas de mensajería instantánea?

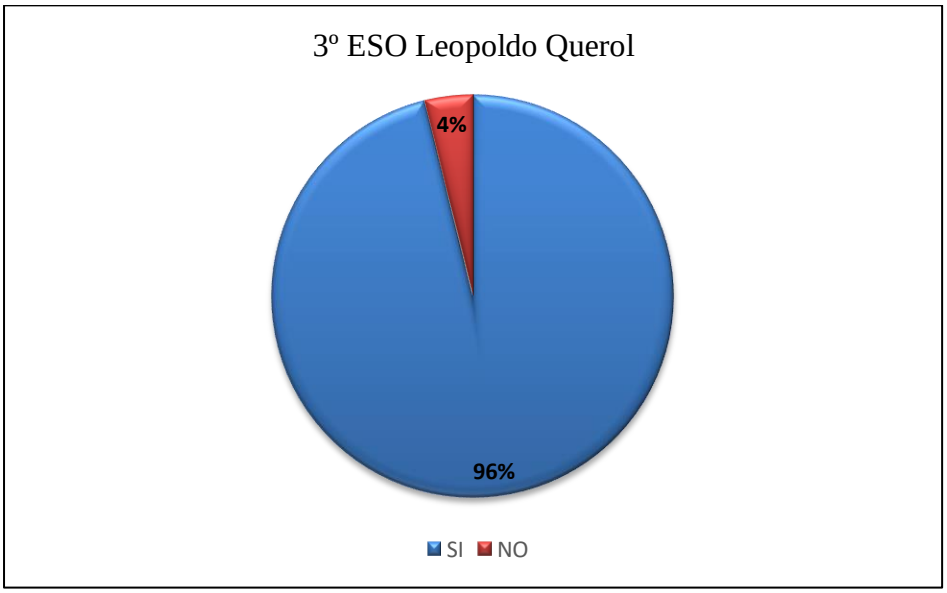

Figura 194. ¿Utilizas redes sociales?

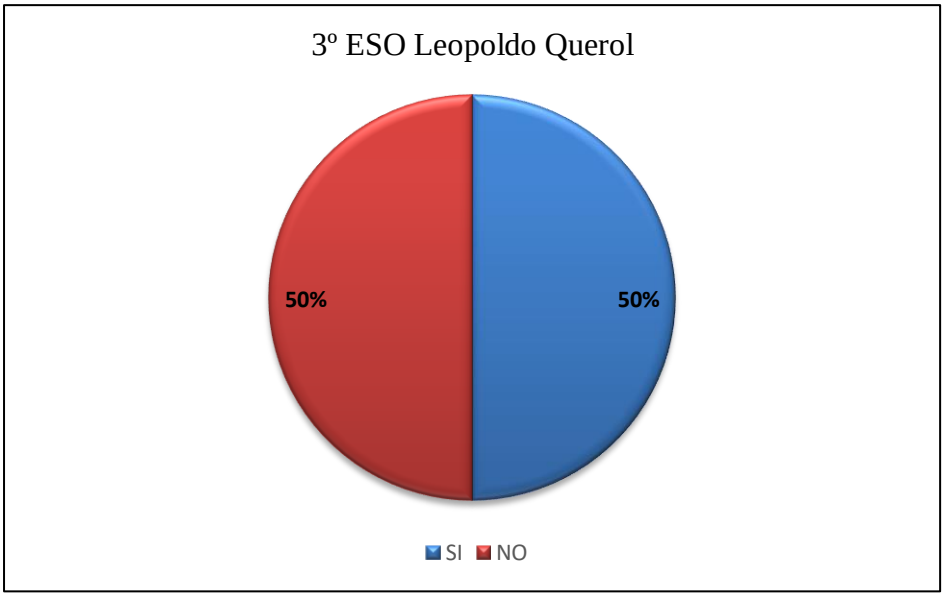

Figura 195. ¿Utilizas blogs, foros en Internet?

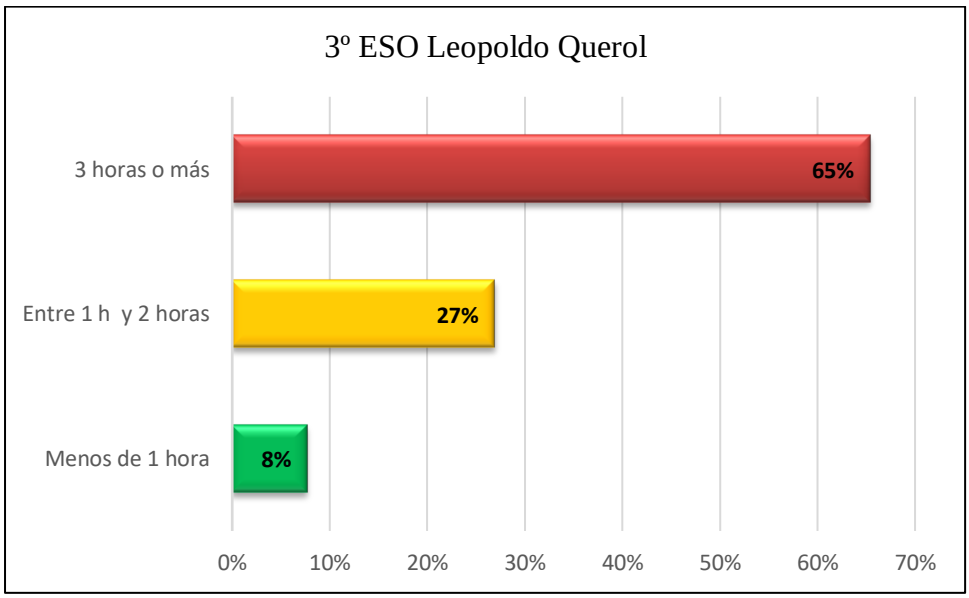

Figura 196. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Tabla 113. *Resultados interacción TIC menores de 4º ESO Leopoldo Querol.*

Ítems interacciones TIC menores 4º ESO	SI	NO
Tengo ordenador en casa	26	0
Tengo webcam	19	7
Tengo teléfono móvil	26	0
Guardo información personal en el teléfono móvil	22	4
Tengo cuenta de correo electrónico	26	0
Utilizo programas de mensajería instantánea	26	0
Utilizo redes sociales	25	1
Utilizo blogs, foros en Internet	15	11

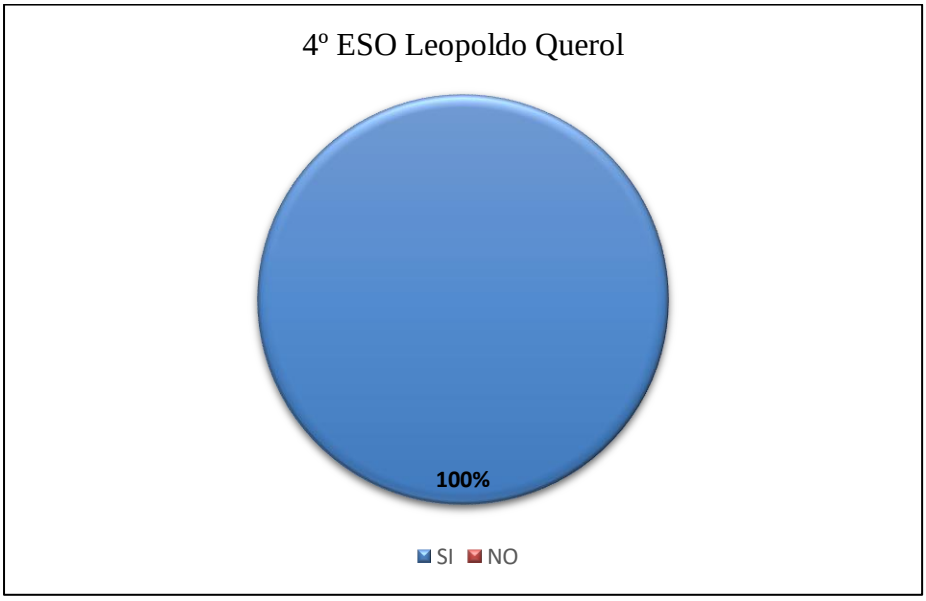

Figura 197. ¿Tienes ordenador en casa?

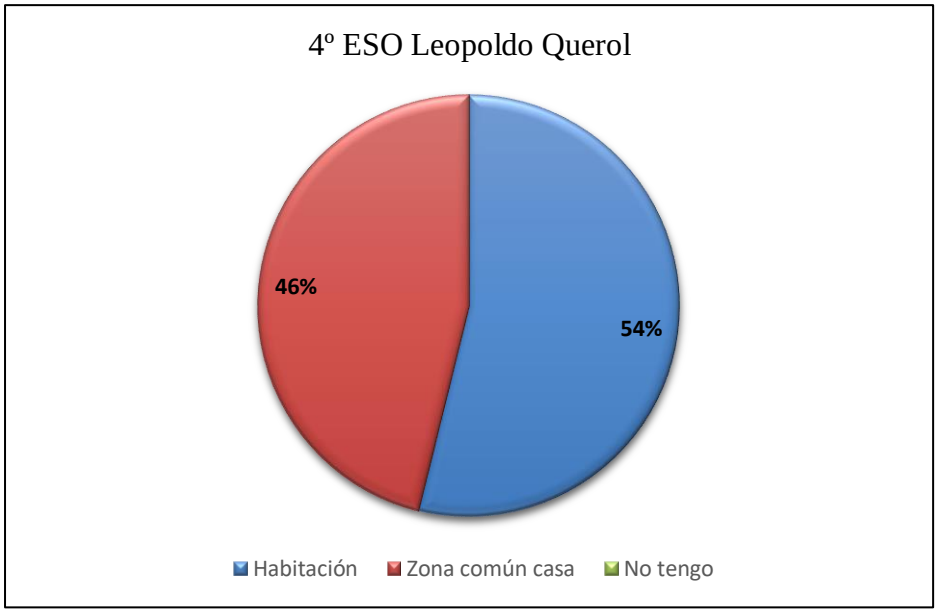

Figura 198. ¿Dónde tienes ubicado el ordenador?

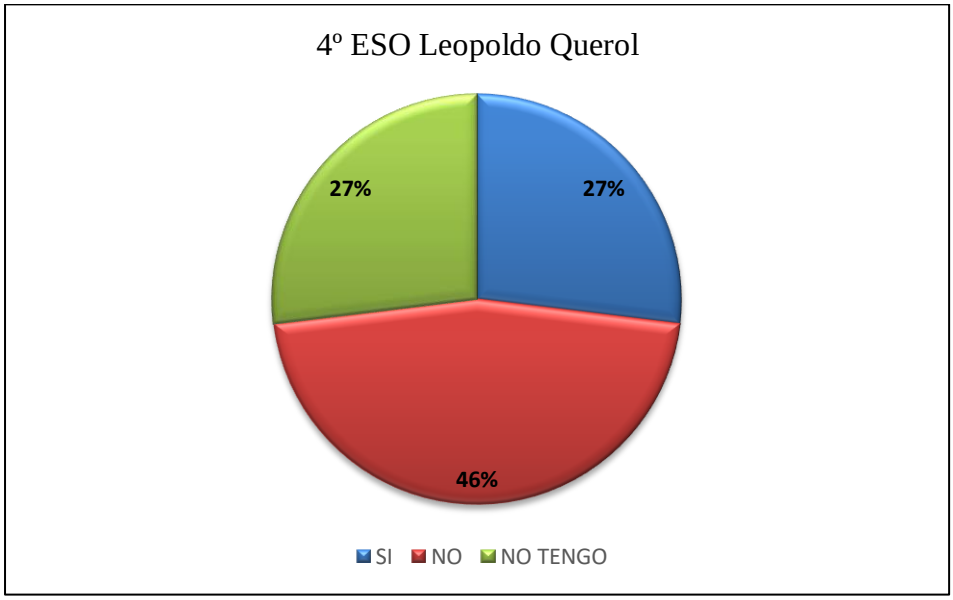

Figura 199. ¿Tapas la webcam cuando no la utilizas?

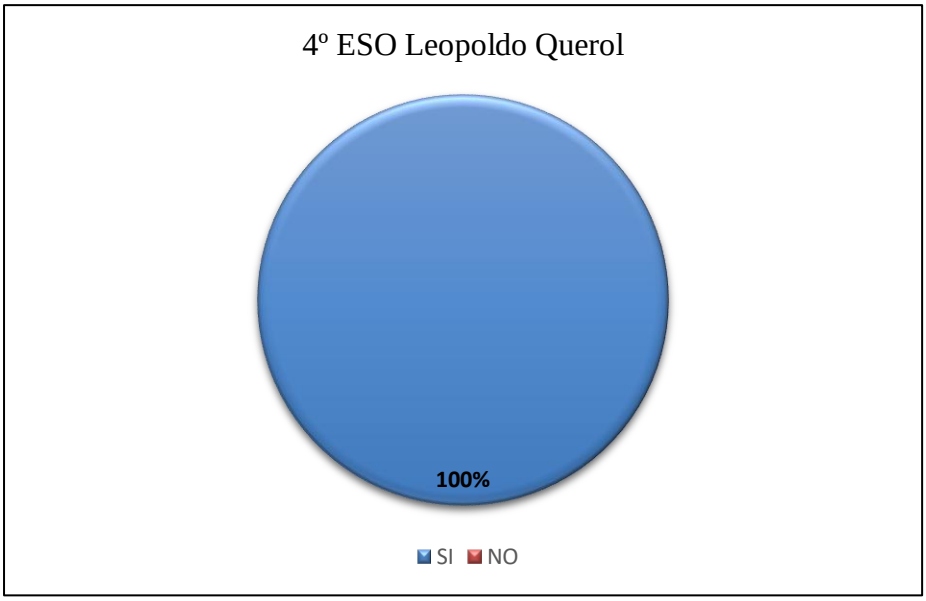

Figura 200. ¿Tienes teléfono móvil?

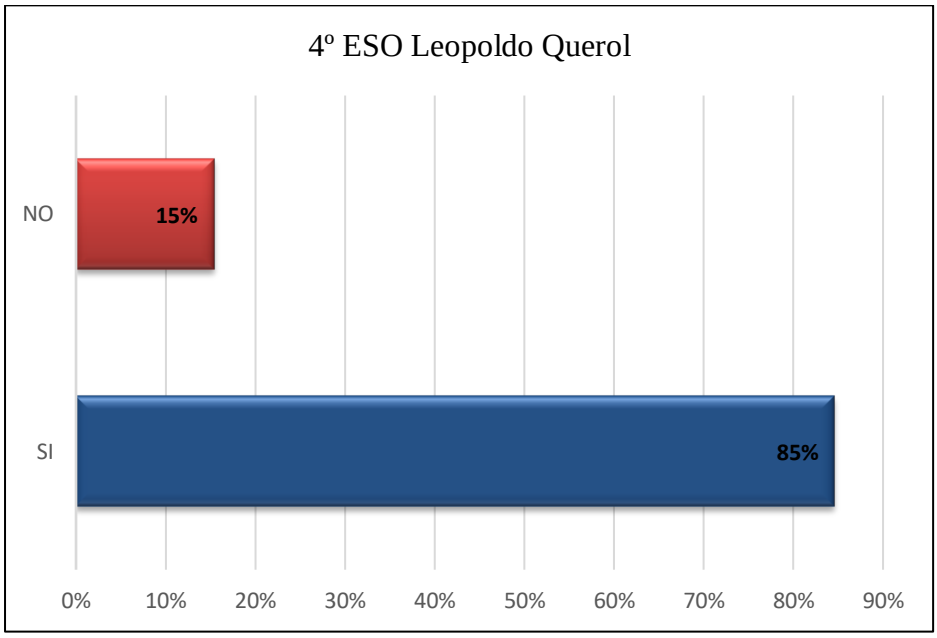

Figura 201. ¿Guardas información personal en el teléfono móvil?

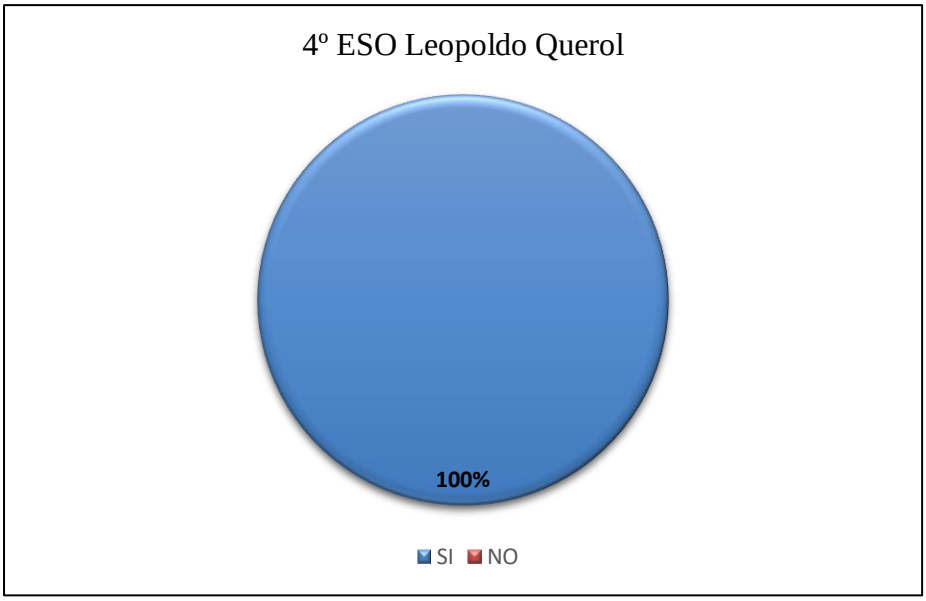

Figura 202. ¿Tienes cuenta de correo electrónico?

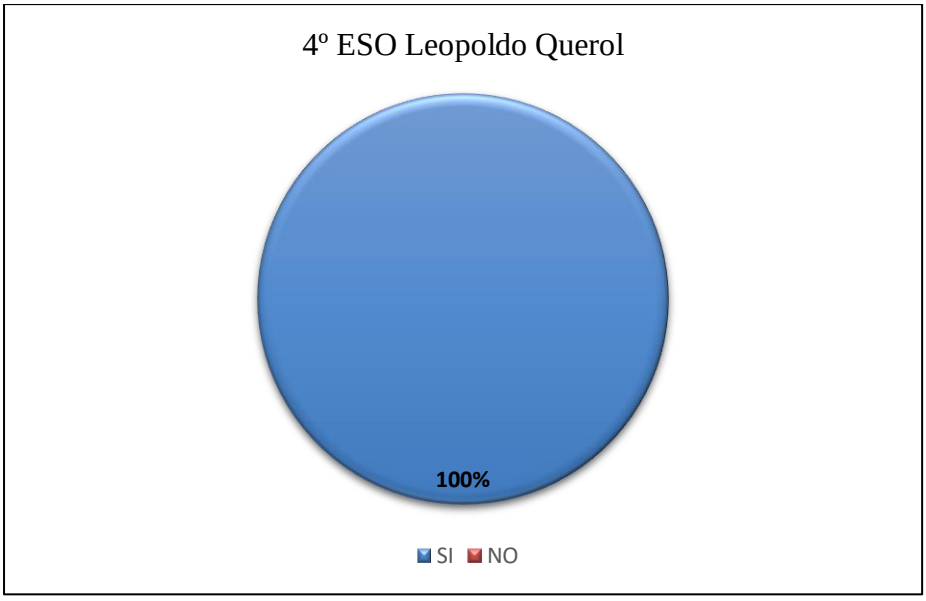

Figura 203. ¿Utilizas programas de mensajería instantánea?

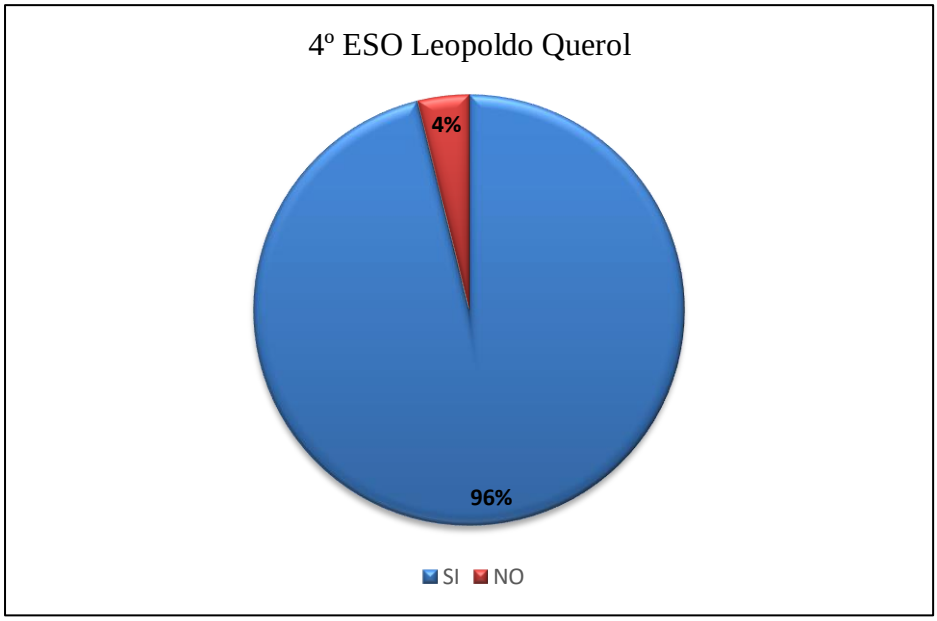

Figura 204. ¿Utilizas redes sociales?

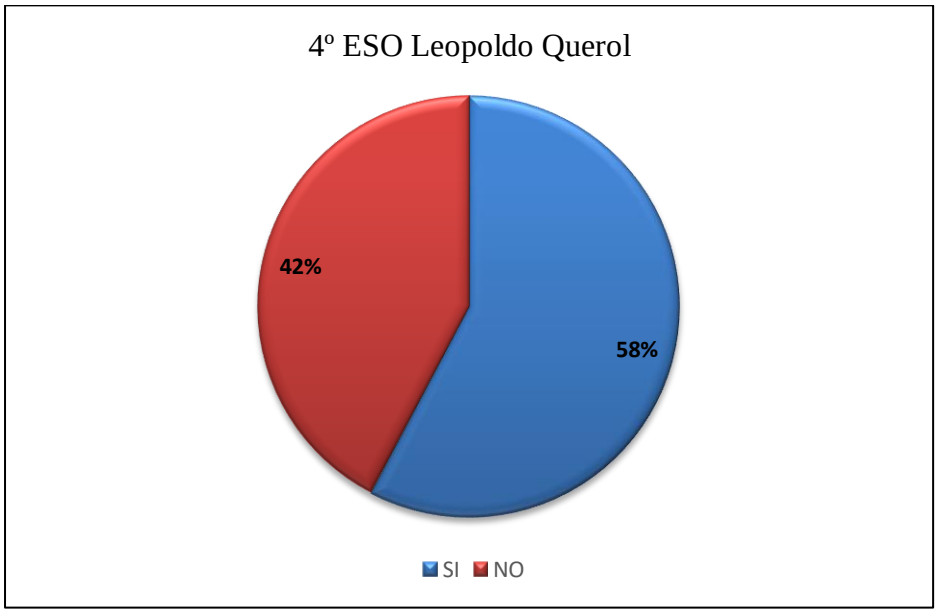

Figura 205. ¿Utilizas blogs, foros en Internet?

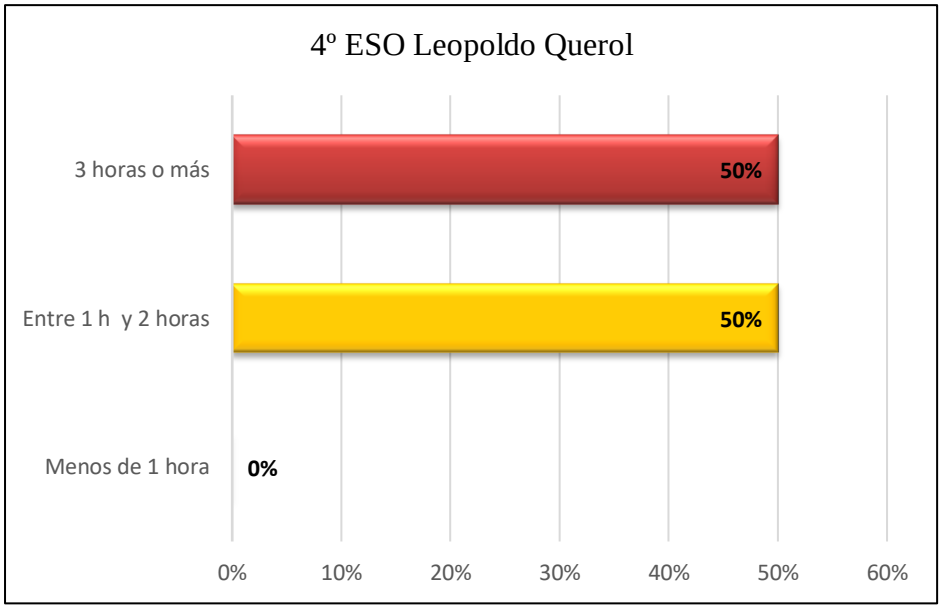

Figura 206. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

A continuación, podemos observar en las tablas 114 a 153 y figuras 207 a 226, respectivamente, los resultados obtenidos a las contestaciones de los 20 ítems, de escala frecuencia tipo Likert (de 1 a 5), relacionadas con hechos o conductas de los menores participantes de 1º a 4º de la ESO del instituto de educación secundaria Leopoldo Querol, que han servido para valorar los ciberriesgos a los que están expuestos tanto desde la perspectiva criminológica de la víctima como del victimario de ciberacoso, sexting, online grooming y violencia de género digital, en su caso.

1. ¿Has realizado mensajes y/o llamadas ofensivas a través de teléfono móvil y/o Internet?

Tabla 114. *Ítem. 1. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	69%	84%	58%	92%
2	Pocas veces	27%	16%	38%	8%
3	Algunas veces	0%	0%	4%	0%
4	Muchas veces	4%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 115. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han realizado mensajes y/o llamadas ofensivas a través de teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,38	0,697	1	4
2º ESO	1,16	0,374	1	2
3º ESO	1,46	0,582	1	3
4º ESO	1,08	0,272	1	2

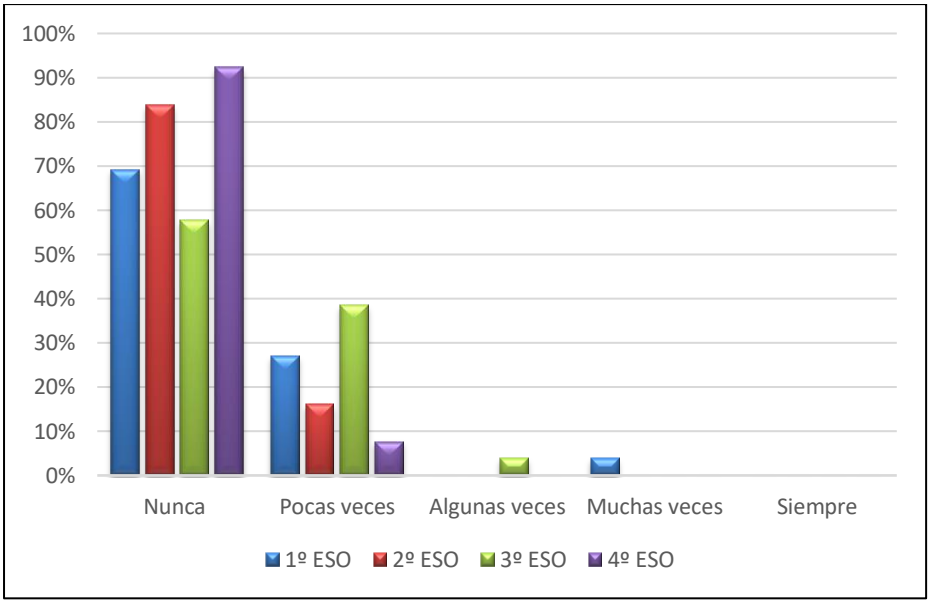

Figura 207. Ítem. 1. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

2. ¿Has colgado en Internet una pelea, agresión o burla que ha sido grabada?

Tabla 116. *Ítem. 2. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	96%	100%
2	Pocas veces	0%	0%	4%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 117. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han colgado en Internet una pelea, agresión o burla que ha sido grabada.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,04	0,196	1	2
4º ESO	1	0	1	1

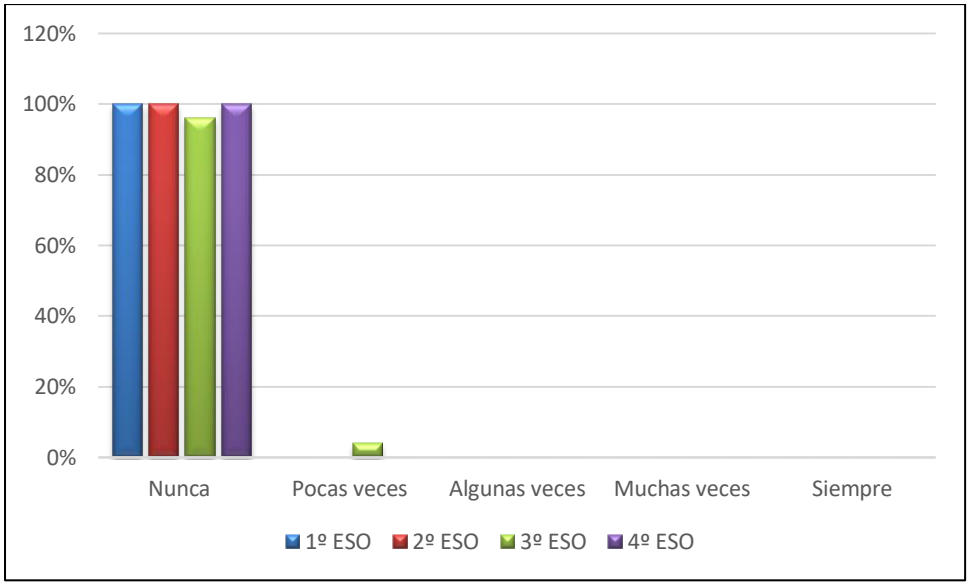

Figura 208. Ítem. 2. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

3. ¿Has realizado comportamientos de tipo sexual a través de la webcam?

Tabla 118. *Ítem. 3. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	100%	92%
2	Pocas veces	0%	0%	0%	8%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 119. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han realizado comportamientos de tipo sexual a través de la webcam.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1	0	1	1
4º ESO	1,08	0,272	1	2

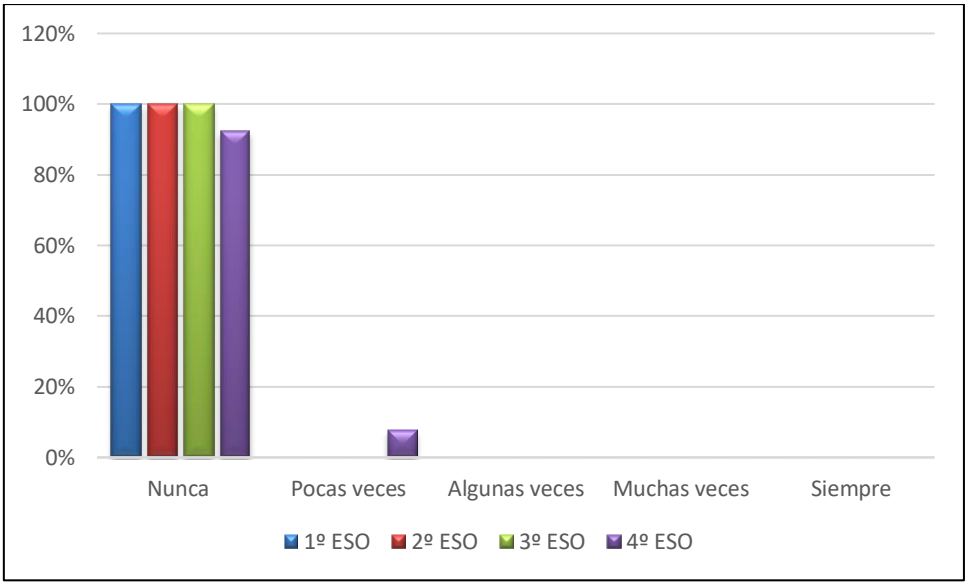

Figura 209. Ítem. 3. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

4. ¿Has difundido vídeos y/o fotos privadas o comprometidas vía teléfono móvil o Internet?

Tabla 120. *Ítem. 4. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	90%	73%	85%
2	Pocas veces	0%	10%	19%	8%
3	Algunas veces	0%	0%	8%	8%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 121. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han difundido vídeos y/o fotos privadas o comprometidas vía teléfono móvil o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,10	0,301	1	2
3º ESO	1,35	0,629	1	3
4º ESO	1,23	0,587	1	3

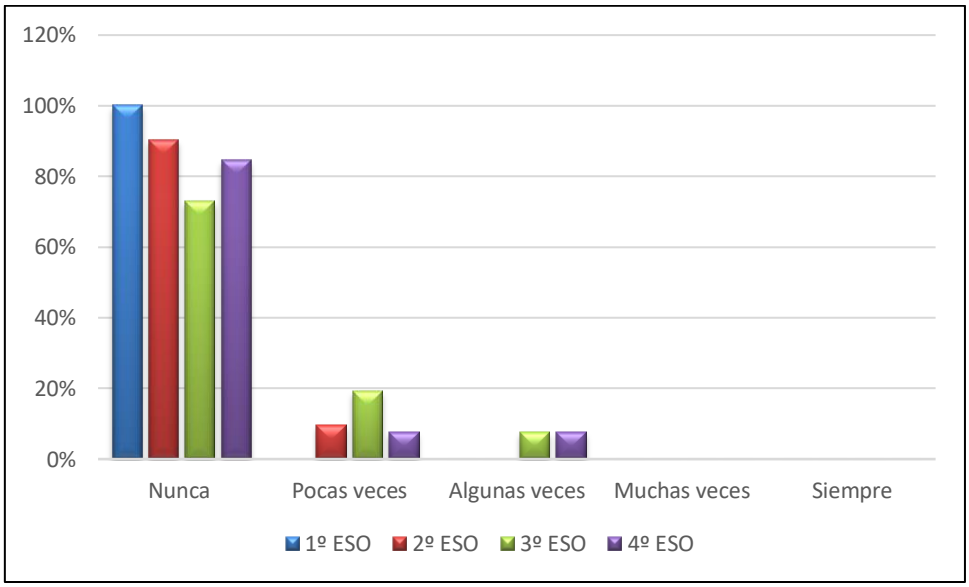

Figura 210. Ítem. 4. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

5. ¿Has colgado vídeos y/o fotos robadas en Internet o difundido a través del teléfono móvil?

Tabla 122. *Ítem. 5. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	87%	88%	92%
2	Pocas veces	0%	10%	8%	8%
3	Algunas veces	0%	3%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 123. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han colgado vídeos y/o fotos robadas en Internet o difundido a través del teléfono móvil.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,16	0,454	1	3
3º ESO	1,15	0,464	1	3
4º ESO	1,08	0,272	1	2

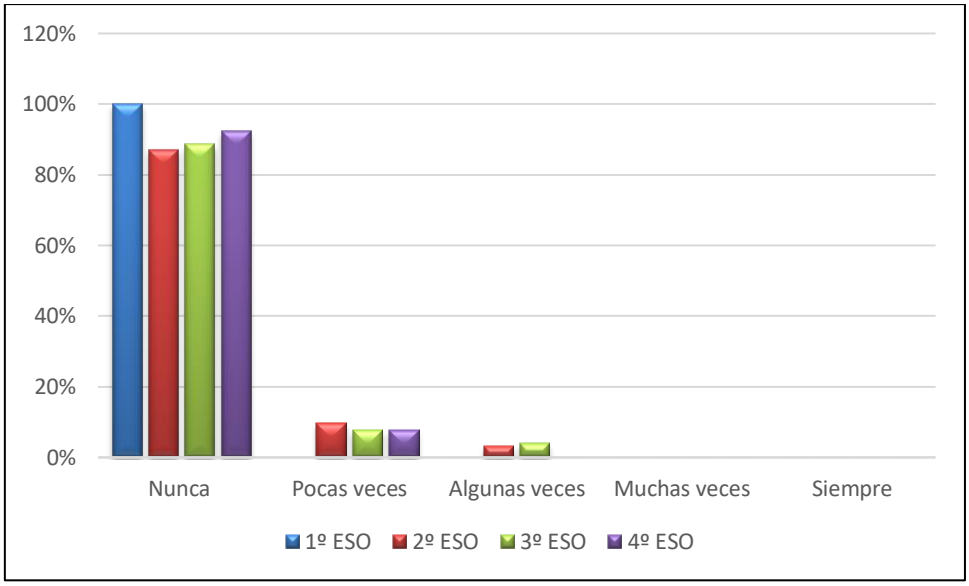

Figura 211. Ítem. 5. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

6. ¿Has realizado llamadas anónimas para asustar o intimidar?

Tabla 124. *Ítem. 6. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	73%	71%	58%	88%
2	Pocas veces	27%	19%	31%	8%
3	Algunas veces	0%	3%	0%	4%
4	Muchas veces	0%	3%	12%	0%
5	Siempre	0%	3%	0%	0%

Tabla 125. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han realizado llamadas anónimas para asustar o intimidar.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,27	0,452	1	2
2º ESO	1,48	0,962	1	5
3º ESO	1,65	0,977	1	4
4º ESO	1,15	0,464	1	3

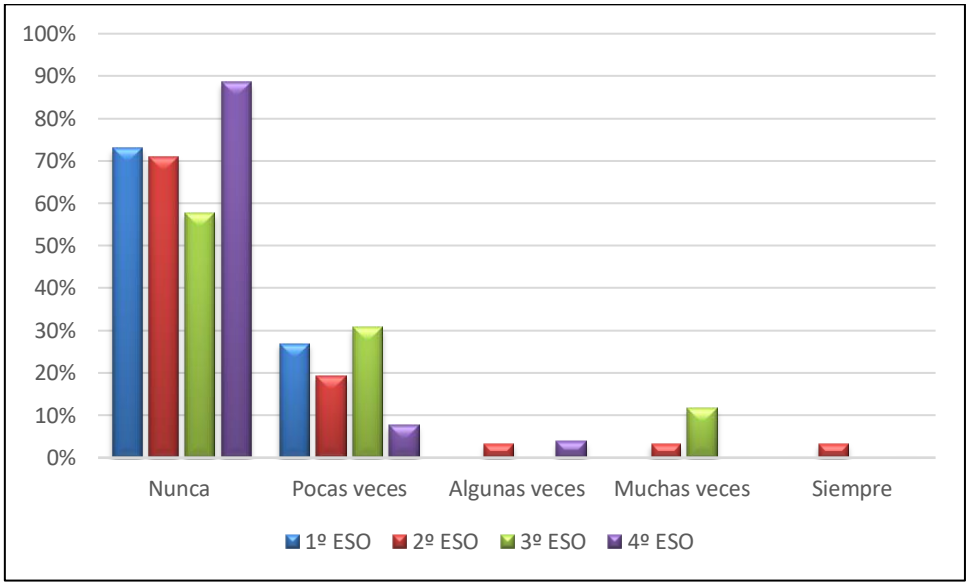

Figura 212. Ítem. 6. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

7. ¿Has realizado amenazas o chantajes a través de mensajes y/o llamadas?

Tabla 126. *Ítem. 7. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	92%	94%	88%	92%
2	Pocas veces	4%	6%	8%	8%
3	Algunas veces	0%	0%	4%	0%
4	Muchas veces	4%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 127. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han realizado amenazas o chantajes a través de mensajes y/o llamadas.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,15	0,613	1	4
2º ESO	1,06	0,250	1	2
3º ESO	1,15	0,464	1	3
4º ESO	1,08	0,272	1	2

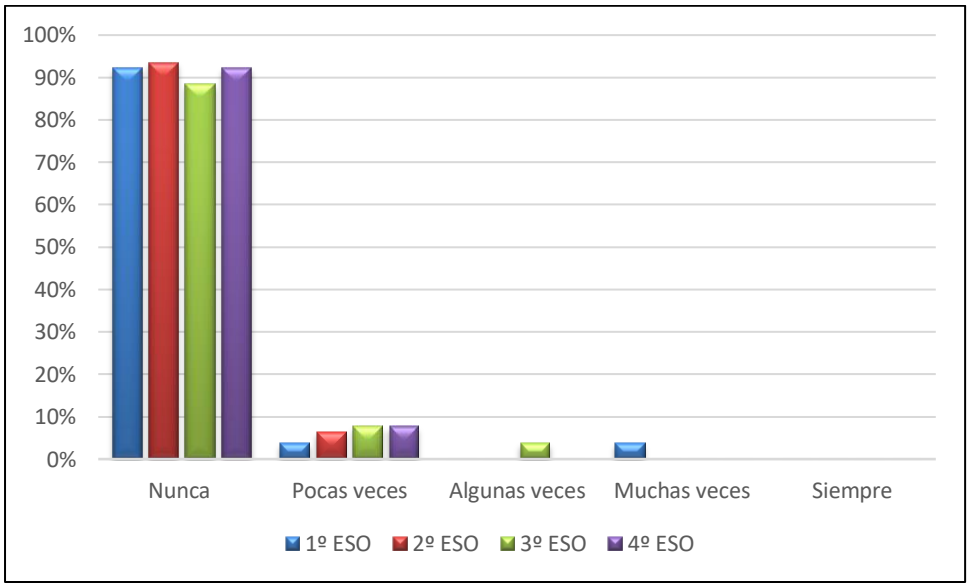

Figura 213. Ítem. 7. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

8. ¿Has acosado sexualmente a través de teléfono móvil y/o Internet?

Tabla 128. *Ítem. 8. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	96%	100%
2	Pocas veces	0%	0%	4%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 129. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han acosado sexualmente a través de teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,04	0,196	1	2
4º ESO	1	0	1	1

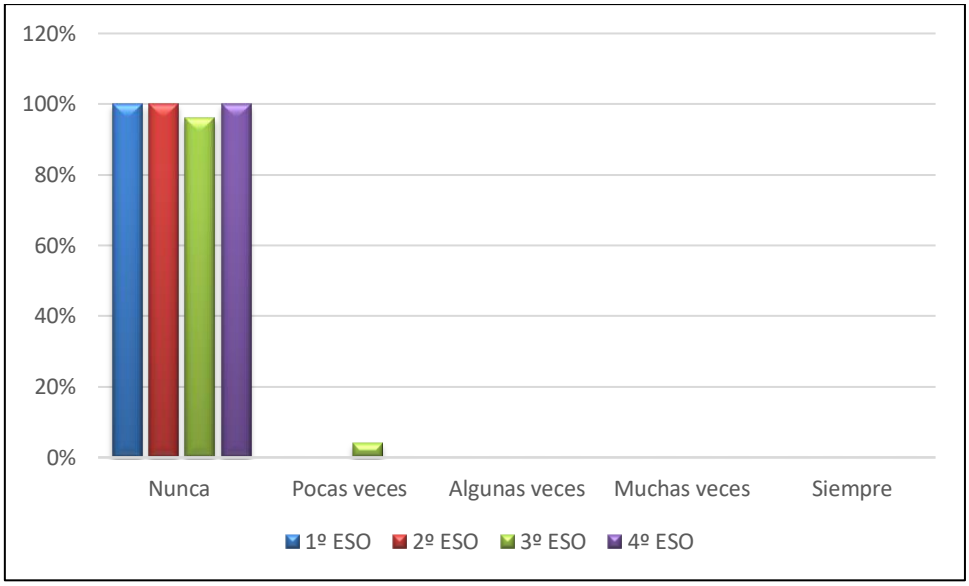

Figura 214. Ítem. 8. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

9. ¿Has suplantado a una persona para difamar, mentir o contar sus secretos?

Tabla 130. *Ítem. 9. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	96%	94%	85%	96%
2	Pocas veces	4%	3%	15%	4%
3	Algunas veces	0%	3%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 131. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han suplantado a una persona para difamar, mentir o contar sus secretos.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,04	0,196	1	2
2º ESO	1,10	0,396	1	3
3º ESO	1,15	0,368	1	2
4º ESO	1,04	0,196	1	2

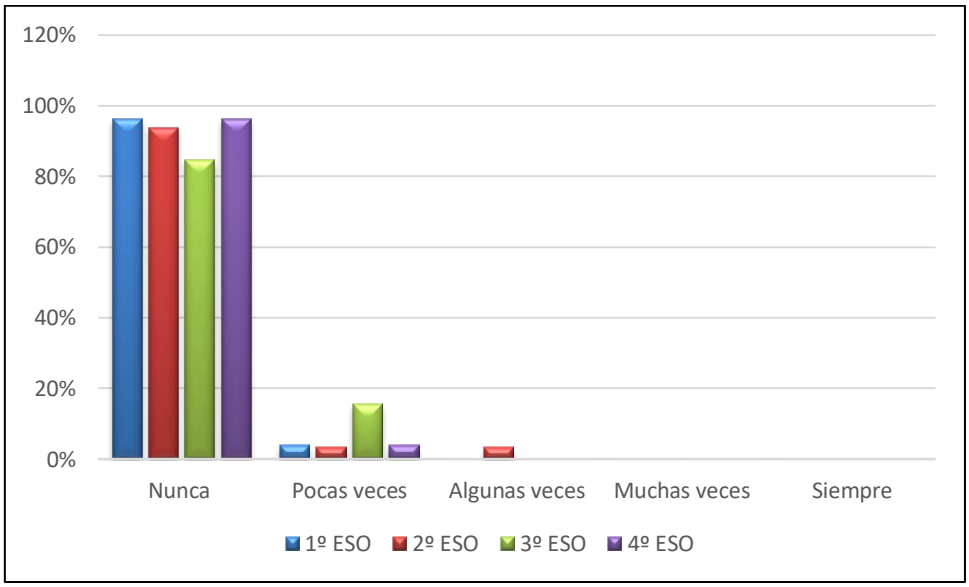

Figura 215. Ítem. 9. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

10. ¿Has robado la contraseña a una persona?

Tabla 132. *Ítem. 10. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	96%	100%	81%	92%
2	Pocas veces	4%	0%	4%	8%
3	Algunas veces	0%	0%	12%	0%
4	Muchas veces	0%	0%	4%	0%
5	Siempre	0%	0%	0%	0%

Tabla 133. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han robado la contraseña a una persona.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,04	0,196	1	2
2º ESO	1	0	1	1
3º ESO	1,38	0,852	1	4
4º ESO	1,08	0,272	1	2

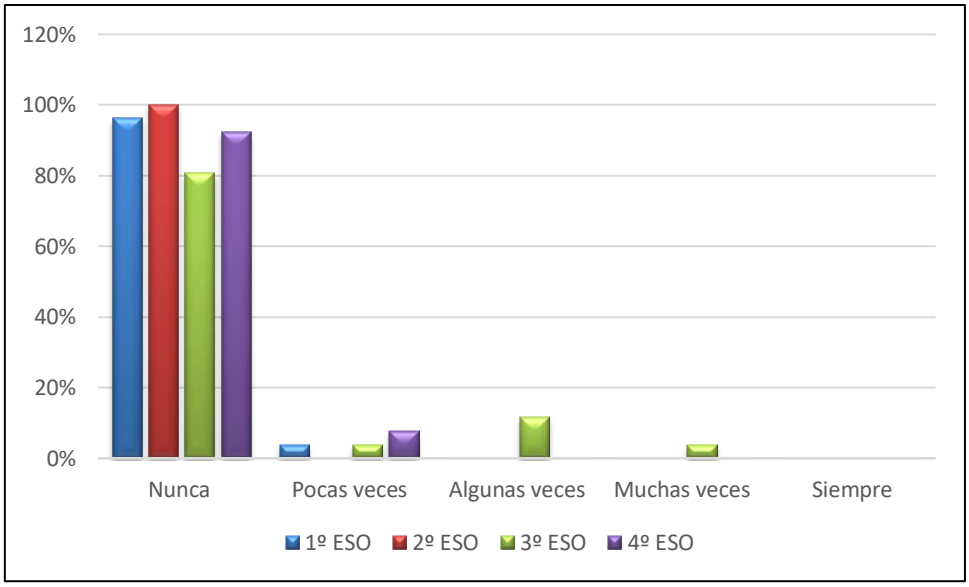

Figura 216. Ítem. 10. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

11. ¿Has trucado fotos y vídeos para difundirlos y humillar vía teléfono móvil y/o Internet?

Tabla 134. *Ítem. 11. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	96%	100%	100%	96%
2	Pocas veces	4%	0%	0%	4%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 135. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han trucado fotos y vídeos para difundirlos y humillar vía teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,04	0,196	1	2
2º ESO	1	0	1	1
3º ESO	1	0	1	1
4º ESO	1,04	0,196	1	2

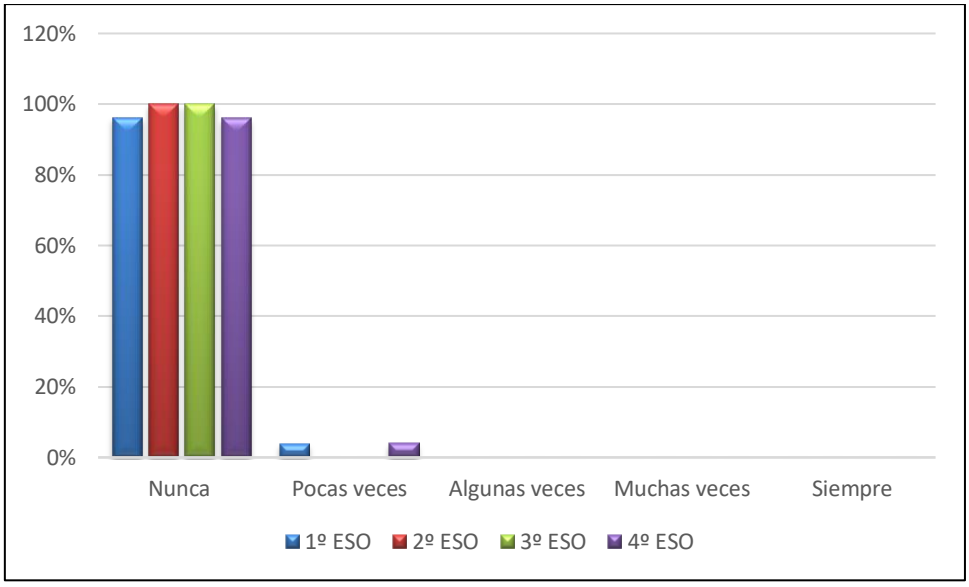

Figura 217. Ítem. 11. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

12. ¿Has acosado a alguien para aislarle de sus contactos en las redes sociales?

Tabla 136. *Ítem. 12. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	96%	100%	100%	100%
2	Pocas veces	4%	0%	0%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 137. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han acosado a alguien para aislarle de sus contactos en las redes sociales.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,04	0,196	1	2
2º ESO	1	0	1	1
3º ESO	1	0	1	1
4º ESO	1	0	1	1

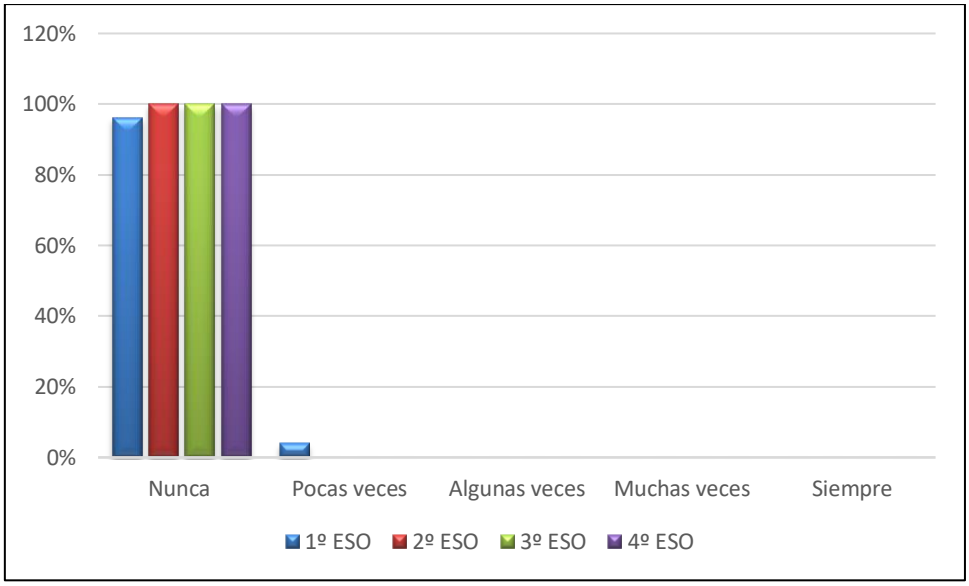

Figura 218. Ítem. 12. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

13. ¿Has chantajeado a cambio de no divulgar información íntima vía teléfono y/o internet?

Tabla 138. *Ítem. 13. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	77%	96%
2	Pocas veces	0%	0%	23%	4%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 139. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han chantajeado a cambio de no divulgar información íntima vía teléfono y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,23	0,430	1	2
4º ESO	1,04	0,196	1	2

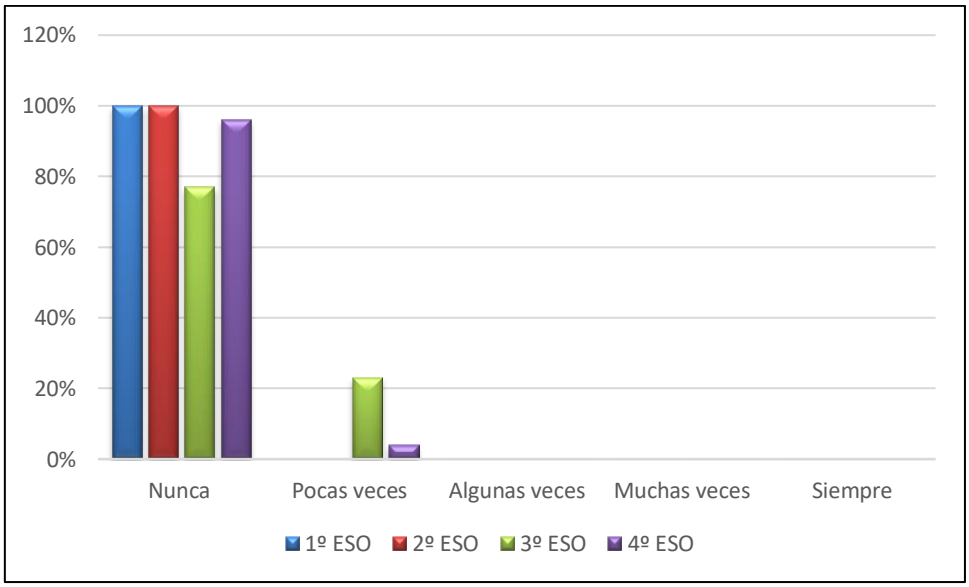

Figura 219. Ítem. 13. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

14. ¿Has amenazado de muerte a alguien a través de teléfono móvil y/o Internet?

Tabla 140. *Ítem. 14. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	88%	100%
2	Pocas veces	0%	0%	8%	0%
3	Algunas veces	0%	0%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 141. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han amenazado de muerte a alguien a través de teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,15	0,464	1	3
4º ESO	1	0	1	1

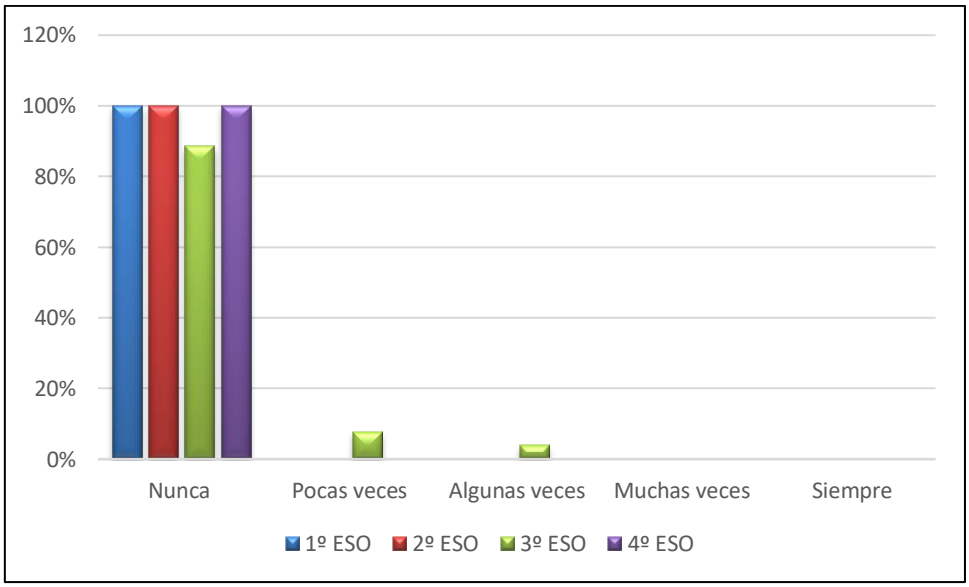

Figura 220. Ítem. 14. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

15. ¿Has difundido y/o difamado con rumores para hacer daño vía teléfono móvil y/o Internet?

Tabla 142. *Ítem. 15. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	92%	94%	92%	92%
2	Pocas veces	8%	6%	8%	8%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 143. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han difundido y/o difamado con rumores para hacer daño vía teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,08	0,272	1	2
2º ESO	1,06	0,250	1	2
3º ESO	1,08	0,272	1	2
4º ESO	1,08	0,272	1	2

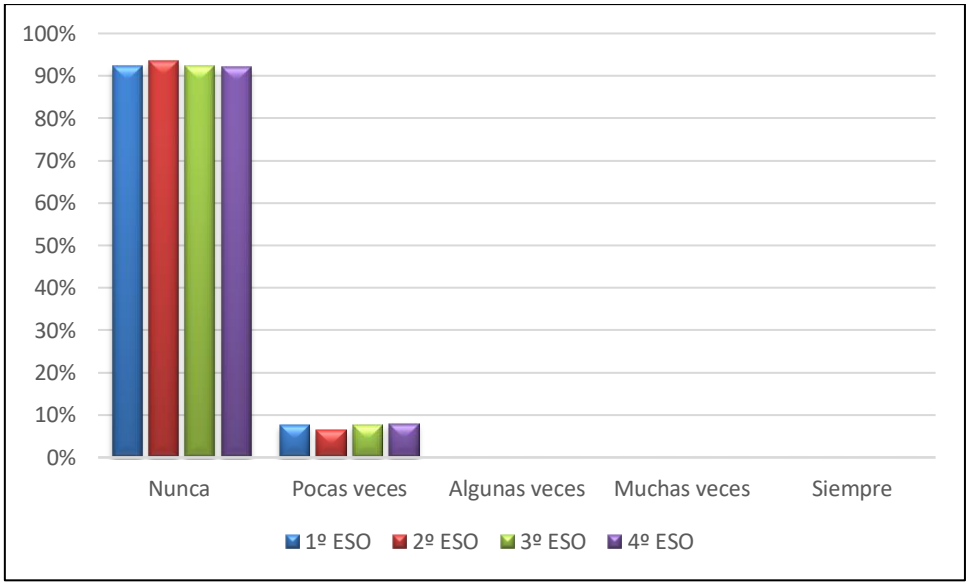

Figura 221. Ítem. 15. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

16. ¿Has contactado con un adulto que se ha ganado tu confianza en las redes sociales?

Tabla 144. *Ítem. 16. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	96%	94%	69%	88%
2	Pocas veces	4%	3%	27%	4%
3	Algunas veces	0%	3%	4%	8%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 145. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han contactado con un adulto que se ha ganado tu confianza en las redes sociales.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,04	0,196	1	2
2º ESO	1,10	0,396	1	3
3º ESO	1,35	0,562	1	3
4º ESO	1,19	0,567	1	3

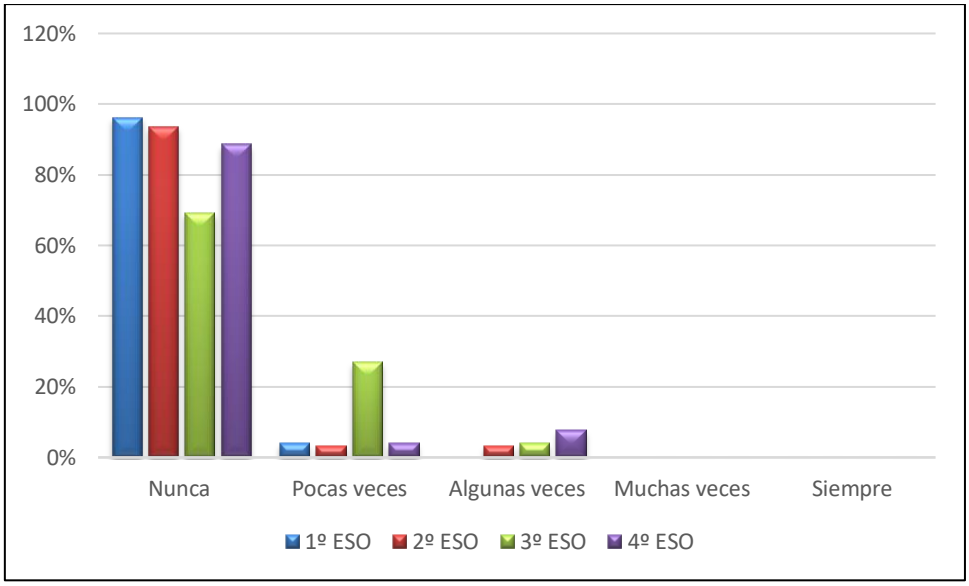

Figura 222. Ítem. 16. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

17. ¿Controlas los amigos/as en redes sociales, mensajes, WhatsApp, etc., de tu pareja?

Tabla 146. *Ítem. 17. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	96%	100%	85%	81%
2	Pocas veces	4%	0%	8%	19%
3	Algunas veces	0%	0%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	4%	0%

Tabla 147. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han controlado los amigos/as en redes sociales, mensajes, WhatsApp, etc., de su pareja.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,04	0,196	1	2
2º ESO	1	0	1	1
3º ESO	1,31	0,884	1	5
4º ESO	1,19	0,402	1	2

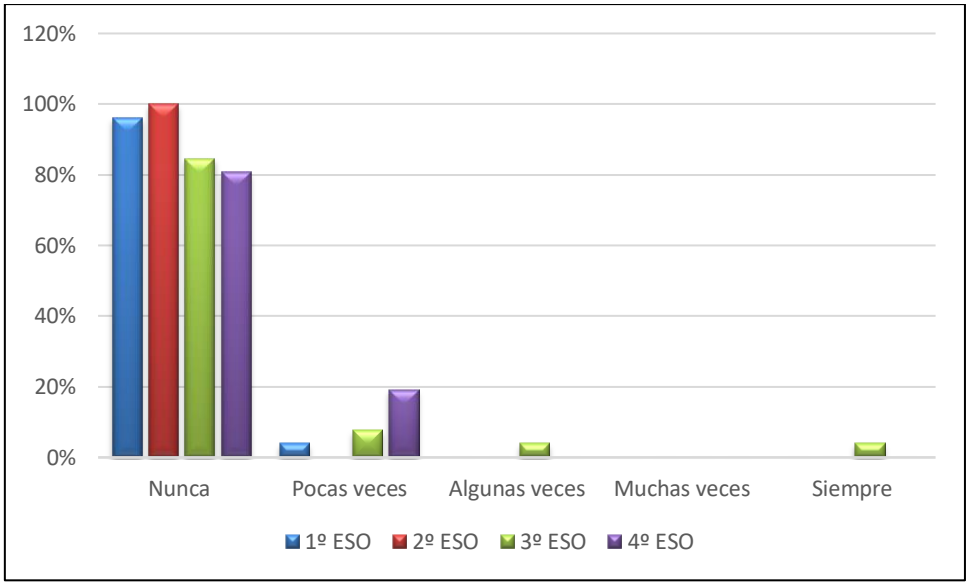

Figura 223. Ítem. 17. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

18. ¿Has pedido a tu pareja que retire fotos o comentarios de redes sociales, WhatsApp, etc.?

Tabla 148. *Ítem. 18. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	92%	97%	92%	88%
2	Pocas veces	8%	3%	4%	8%
3	Algunas veces	0%	0%	0%	4%
4	Muchas veces	0%	0%	4%	0%
5	Siempre	0%	0%	0%	0%

Tabla 149. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han pedido a su pareja que retire fotos o comentarios de redes sociales, WhatsApp, etc.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,08	0,272	1	2
2º ESO	1,03	0,180	1	2
3º ESO	1,15	0,613	1	4
4º ESO	1,15	0,464	1	3

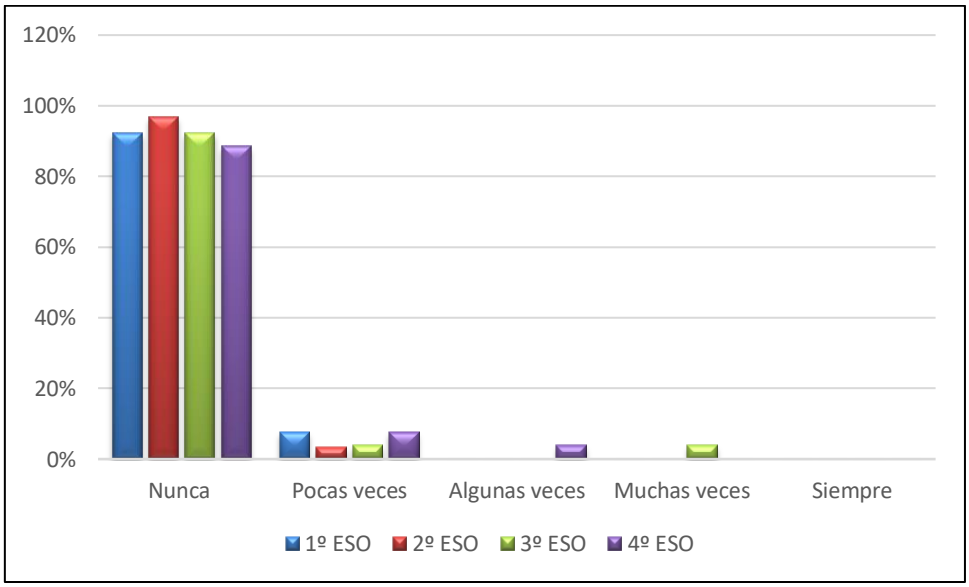

Figura 224. Ítem. 18. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

19. ¿Has pedido a tu pareja que suprima o borre a amigos/as en redes sociales, etc.?

Tabla 150. *Ítem. 19. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	96%	92%
2	Pocas veces	0%	0%	0%	8%
3	Algunas veces	0%	0%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 151. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han pedido a tu pareja que suprima o borre a amigos/as en redes sociales, etc.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1,08	0,392	1	3
4º ESO	1,08	0,272	1	2

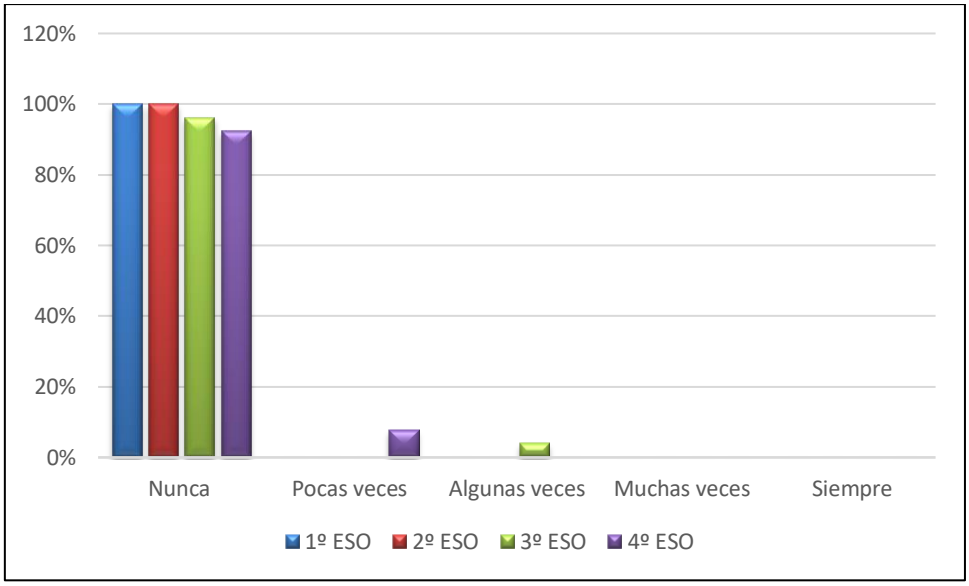

Figura 225. Ítem. 19. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

20. ¿Has obligado a tu pareja a realizar comportamientos de tipo sexual a través de la webcam?

Tabla 152. *Ítem. 20. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	100%	100%	100%
2	Pocas veces	0%	0%	0%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 153. Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Leopoldo Querol han obligado a su pareja a realizar comportamientos de tipo sexual a través de la webcam.

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1	0	1	1
3º ESO	1	0	1	1
4º ESO	1	0	1	1

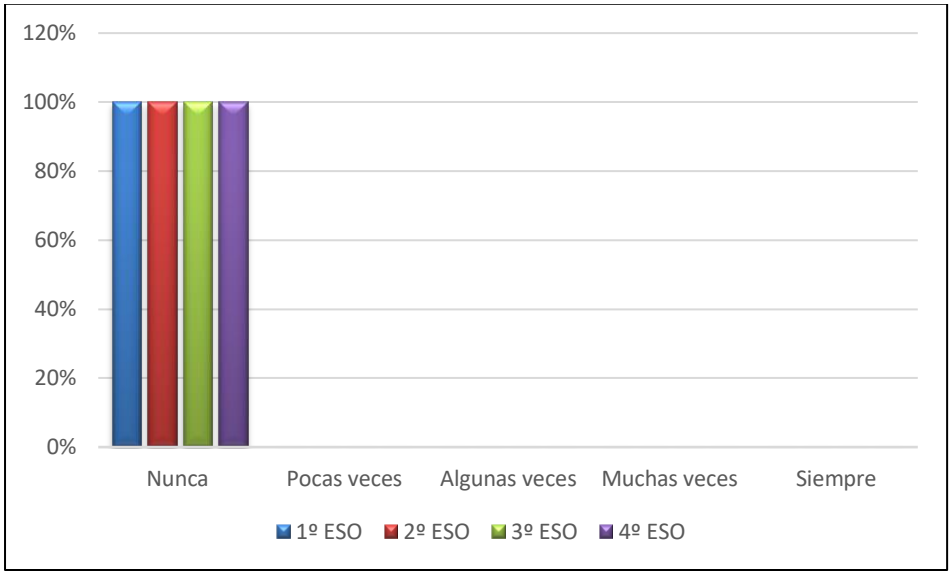

Figura 226. Ítem. 20. Contestaciones alumnos de 1º a 4º ESO del IES Leopoldo Querol.

En la tabla 154 y figura 227, podemos apreciar que, de los 109 menores participantes, 46 chicos y 63 chicas, respectivamente, de los cursos 1º a 4º de la ESO de instituto Leopoldo Querol, con relación a la pregunta de a quién comunicarían los hechos o conductas reseñados en los ítems 1 a 20, ambos inclusive, en el caso de observarlos y/o protagonizarlos, en primer lugar, la mayoría contestaron que lo participarían a sus padres, en segundo lugar, los de 3º y 4º de la ESO lo participarían a sus compañeros con diferencia, y los de 1º y 2º de la ESO los comunicarían por igual tanto a sus profesores como a sus compañeros. Por último, en tercer y cuarto lugar existen discrepancias entre los cursos.

Tabla 154. *Resultados sobre a quién comunicarían los observadores, víctimas y/o victimarios, en su caso, alguno de los hechos o conductas mencionados (Leopoldo Querol).*

	Instituto Leopoldo Querol			
Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Compañeros	13%	18%	31%	21%
Padres	63%	61%	56%	56%
Profesores	13%	18%	3%	15%
A nadie	10%	2%	9%	9%

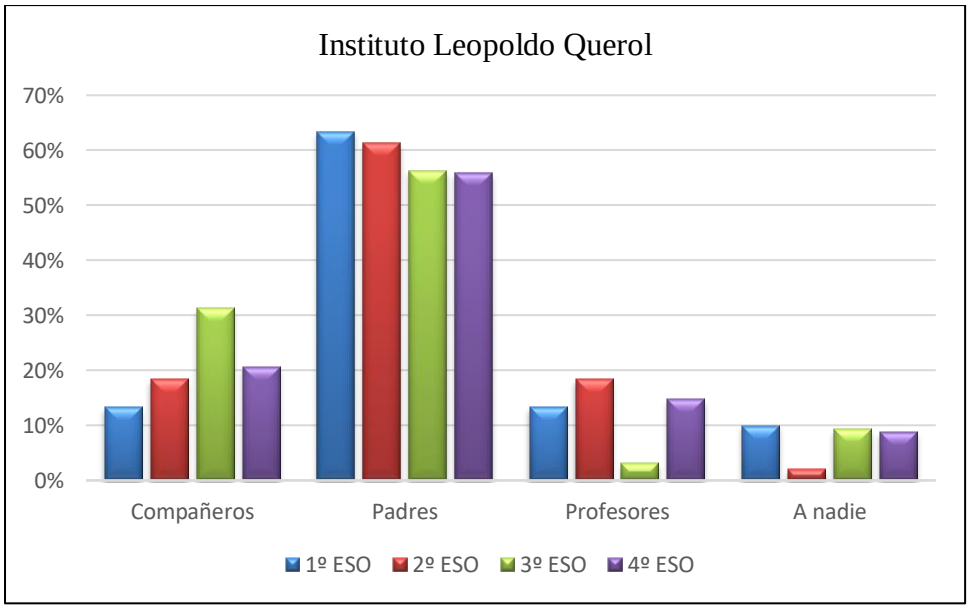

Figura 227. Comparativa de resultados de 1º a 4º de la ESO Leopoldo Querol (tabla 154).

A continuación, en las figuras 228 a 231, podemos observar por cursos de la ESO del instituto Leopoldo Querol los resultados porcentuales obtenidos en las contestaciones a la pregunta mencionada por parte de los menores que han participado en este estudio criminológico social.

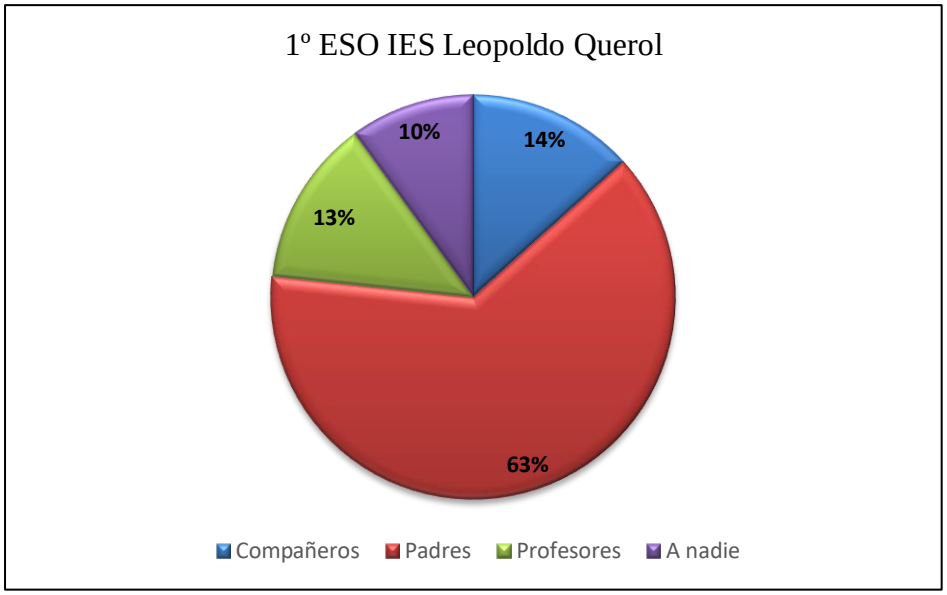

Figura 228. -1º ESO IES Leopoldo Querol: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

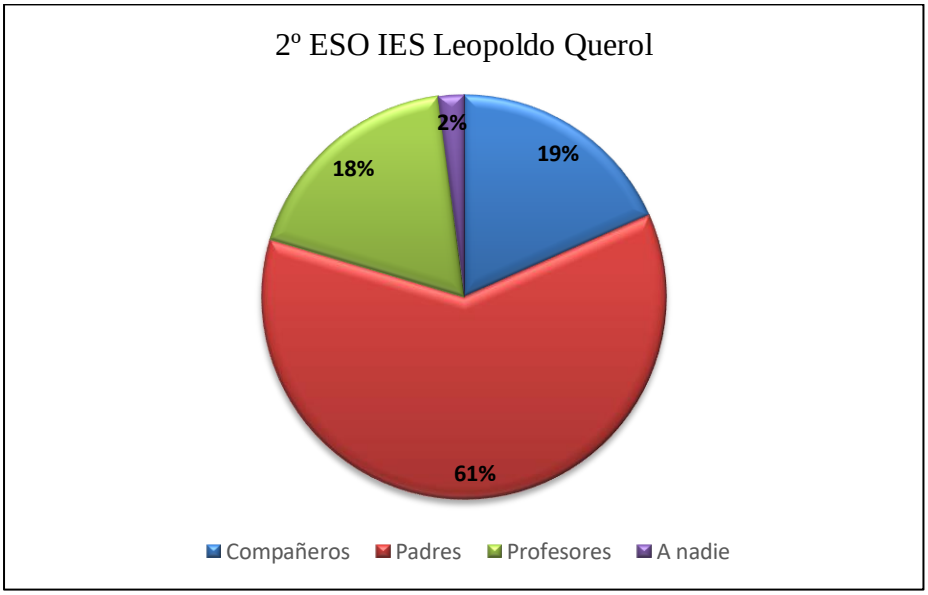

Figura 229. -2º ESO IES Leopoldo Querol: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

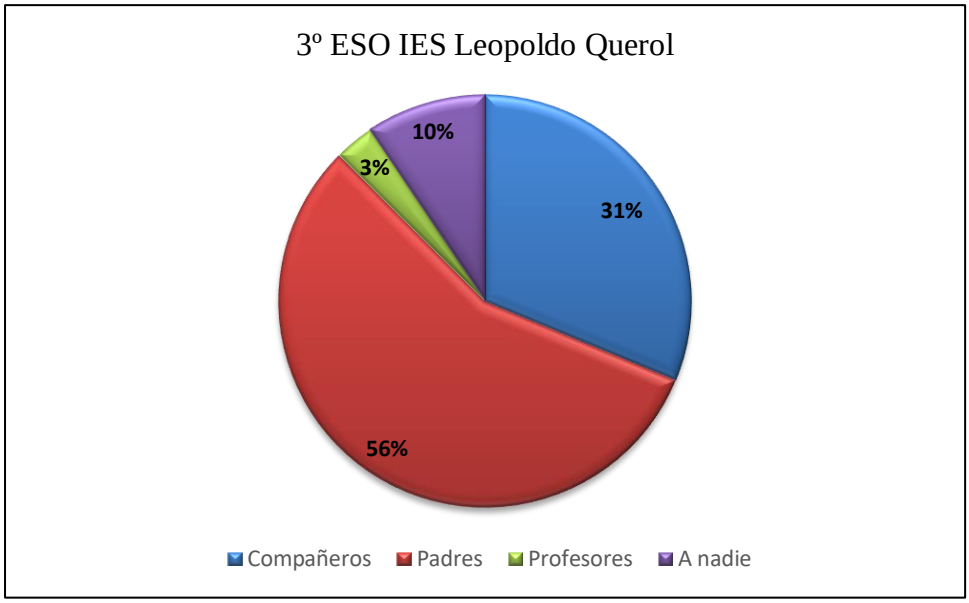

Figura 230. -3º ESO IES Leopoldo Querol: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

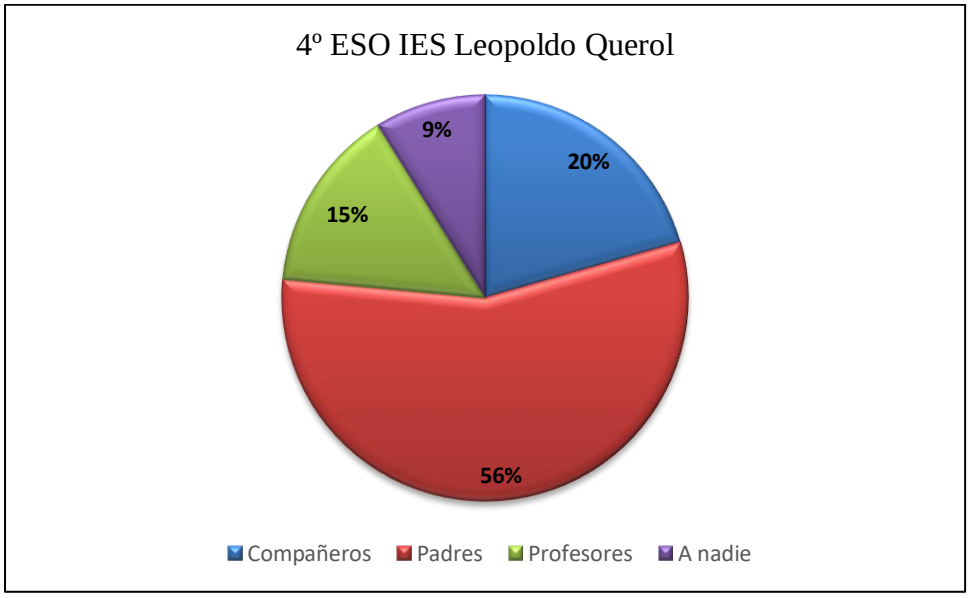

Figura 231. -4º ESO IES Leopoldo Querol: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

Por otra parte, en lo atinente a los resultados arrojados respecto a la pregunta sobre qué actividades preventivas propondrían frente a hechos o conductas de ciberacoso, y que se han plasmado en la tabla 155 y en las figuras 232 a 236, respectivamente, podemos destacar que los alumnos del IES Leopoldo Querol de la ESO, en general, optaría mayoritariamente en primer lugar por comunicar los hechos o conductas referenciados a personas adultas antes que denunciarlo a la policía.

Curiosamente, respecto a la opción de respuesta de mediación con el ciberacosador, los resultados obtenidos oscilan del 2% al 10%, constituyendo una

evidencia de que, en general, el alumnado de la ESO participante no cree en esta figura para prevenir, abordar y resolver conflictos con el ciberacosador.

Por último, podemos destacar que un porcentaje muy minoritario del alumnado participante de la ESO, concretamente, entre un 0% y un 6%, marcó como respuesta ignorar el ciberacoso, hecho que evidencia su concienciación del problema existente en nuestra sociedad con una interacción cada vez más virtual.

Tabla 155. *Resultados sobre las propuestas que hacen los menores participantes para evitar hechos o conductas de ciberacoso (Leopoldo Querol).*

	Instituto Leopoldo Querol			
Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Comunicar adultos	40%	32%	31%	40%
Denunciar a la policía	28%	31%	33%	36%
Ignorar ciberacoso	0%	3%	6%	2%
Mediar con el ciberacosador	0%	10%	4%	2%
Pedir ayuda	23%	21%	18%	17%
Otras	10%	3%	8%	2%

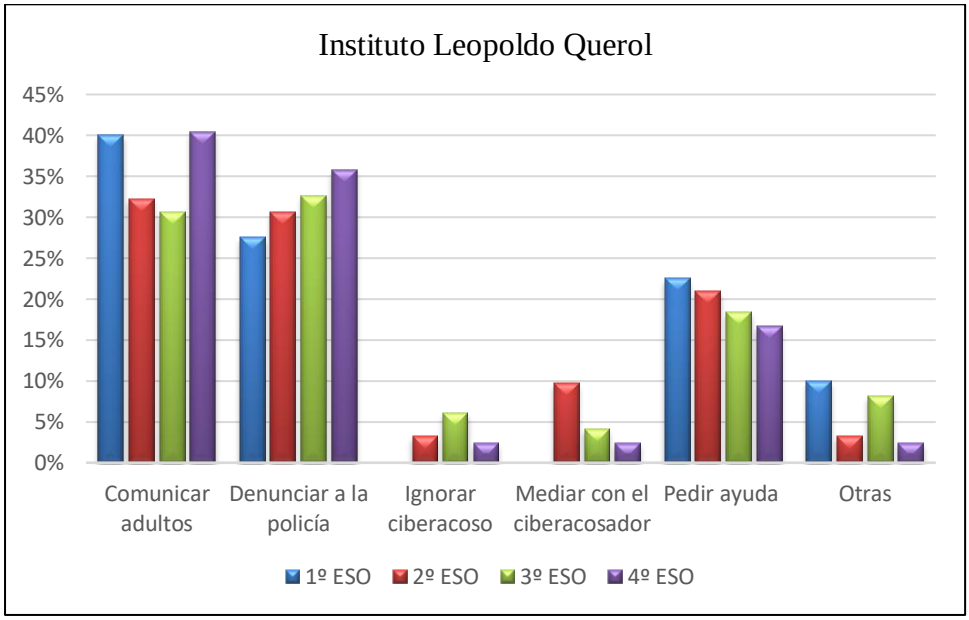

Figura 232. Comparativa de resultados 1º a 4º de la ESO Instituto Leopoldo Querol (tabla 155).

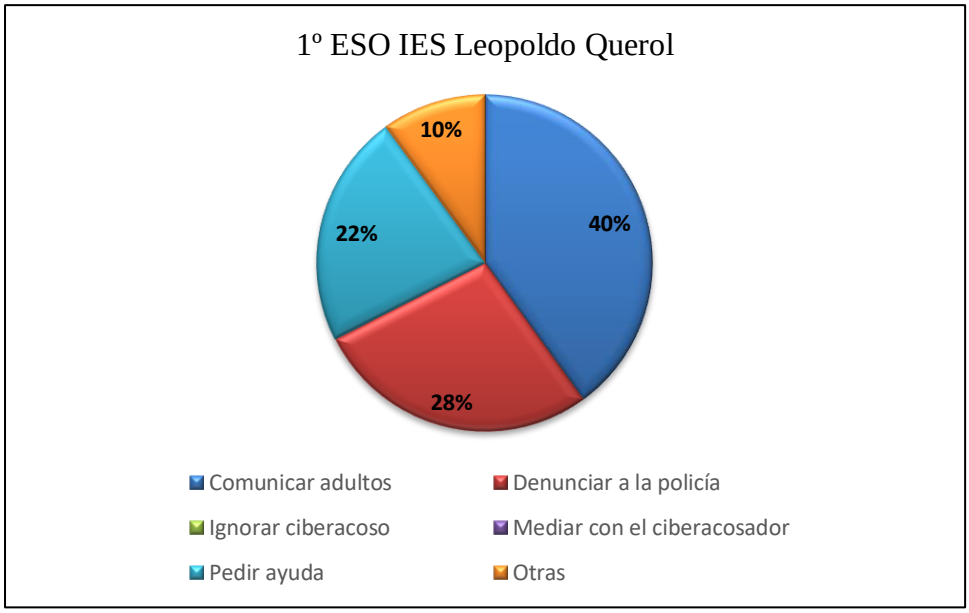

Figura 233. -1º ESO Leopoldo Querol: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

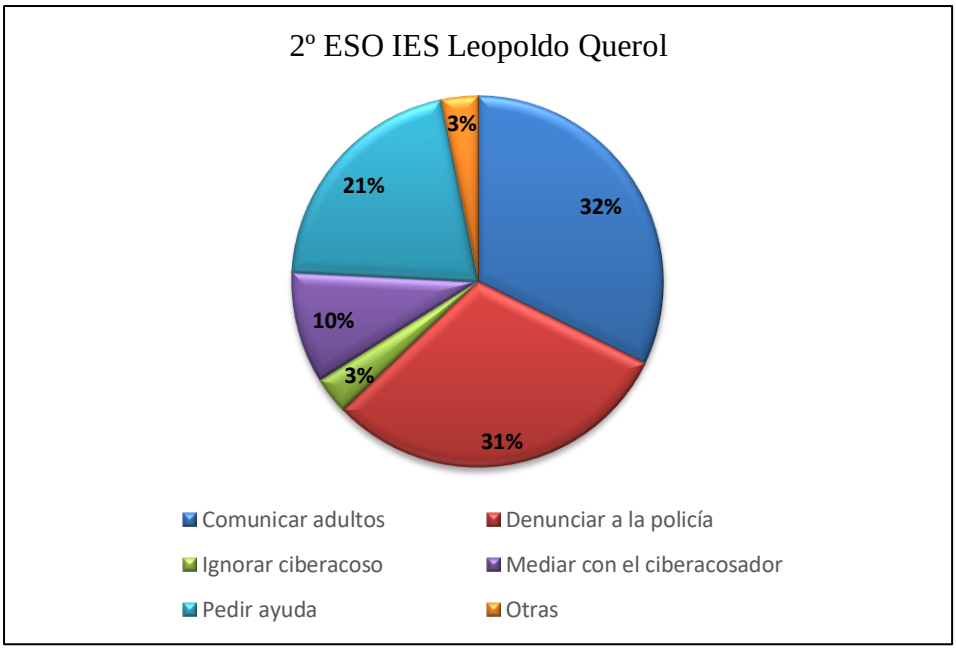

Figura 234. -2º ESO Leopoldo Querol: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

Figura 235. -3º ESO Leopoldo Querol: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

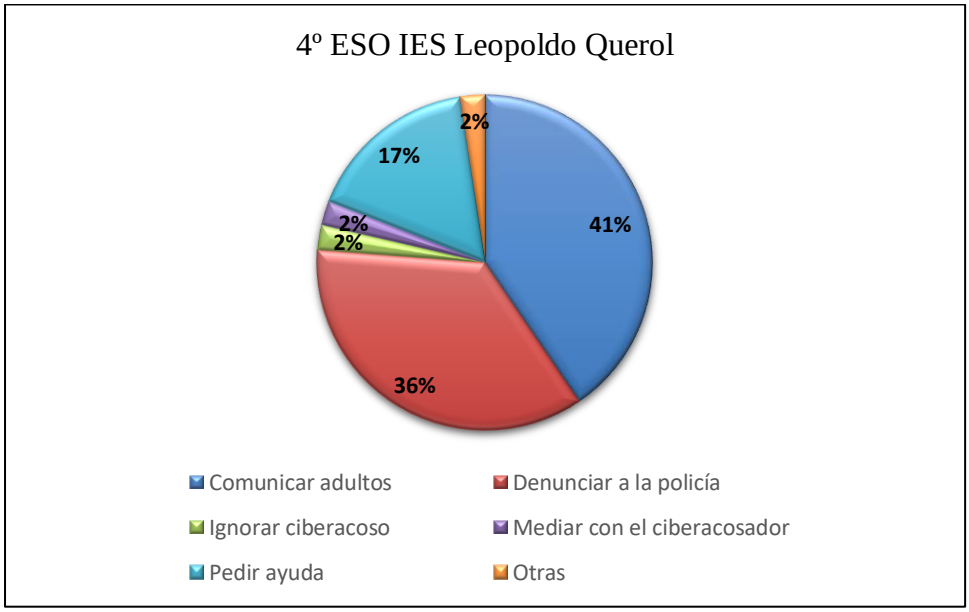

Figura 236. -4º ESO Leopoldo Querol: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

d)-IES Sanchis y Vilaplana: de un total de 479 alumnos matriculados de la ESO, se ha tomado una muestra de este centro educativo de 109 alumnos encuestados que han participado voluntariamente, de los que un 57% son chicas y un 43% son chicos, de 11 a 16 años, correspondientes a los cursos de 1º a 4º de la ESO, tal y como podemos observar en la tabla 156 y figura 237**,** respectivamente.

Concretamente, de 1º de la ESO la media de edad es 12,67 años; de 2º de la ESO es 13,88 años; de 3º ESO es de 14,67 años y de 4º ESO es 15,97 años.

Tabla 156. *Edad y género de los menores participantes de la ESO del IES Sanchis y Vilaplana.*

Curso académico	Edades	Chicos	Chicas	
1º ESO	12-15	16	11	27
2º ESO	13-15	13	13	26
3º ESO	14-17	12	15	27
4º ESO	15-17	6	23	29
	Totales	46	63	109

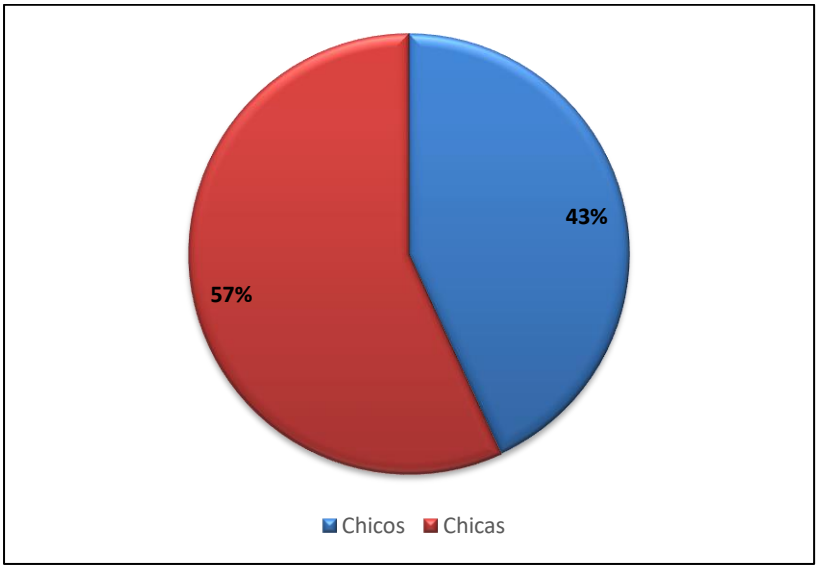

Figura 237. Porcentaje total participantes por género de la ESO IES Sanchis y Vilaplana.

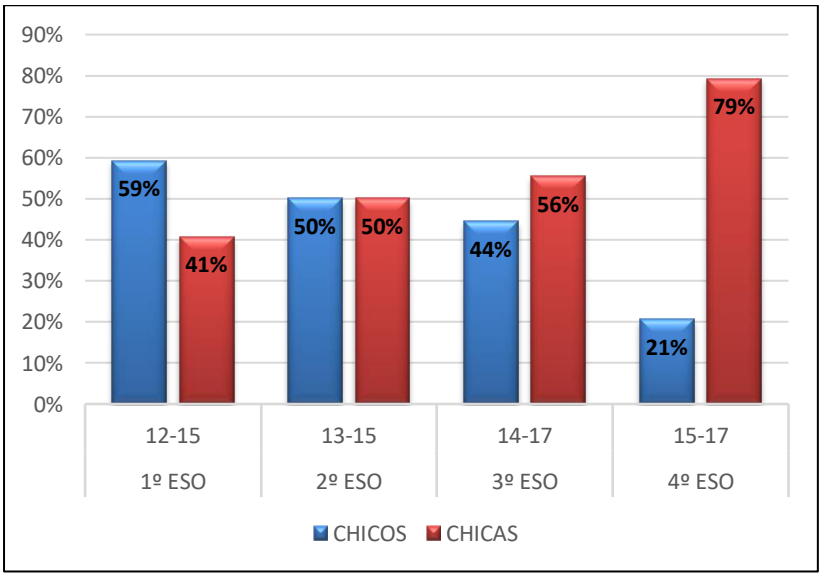

Figura 238. Menores de la ESO IES Sanchis y Vilaplana por curso académico y género.

En general, existe una paridad aproximada entre chicas y chicos de los cursos académicos de la ESO, excepto en 4º al existir una diferencia entre ambos géneros considerable, es decir, un 21% chicos y un 79% chicas, tal y como podemos apreciar en la figura 238.

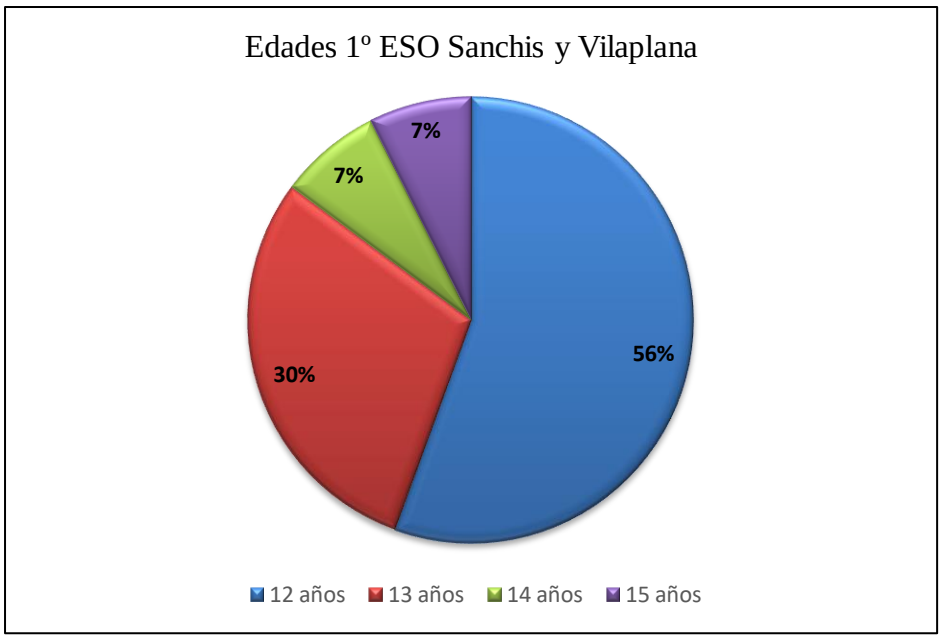

Figura 239. Edades menores de 1º ESO del IES Sanchis y Vilaplana.

En la figura 239, podemos apreciar que dentro del rango de edad de los menores participantes en el presente estudio correspondientes al curso de 1º de la ESO del IES Sanchis y Vilaplana, la mayoría tiene 12 años, es decir, un 56%, mientras que un 30% tiene 13 años y los restantes tienen 14 (7%) y 15 años (7%), respectivamente.

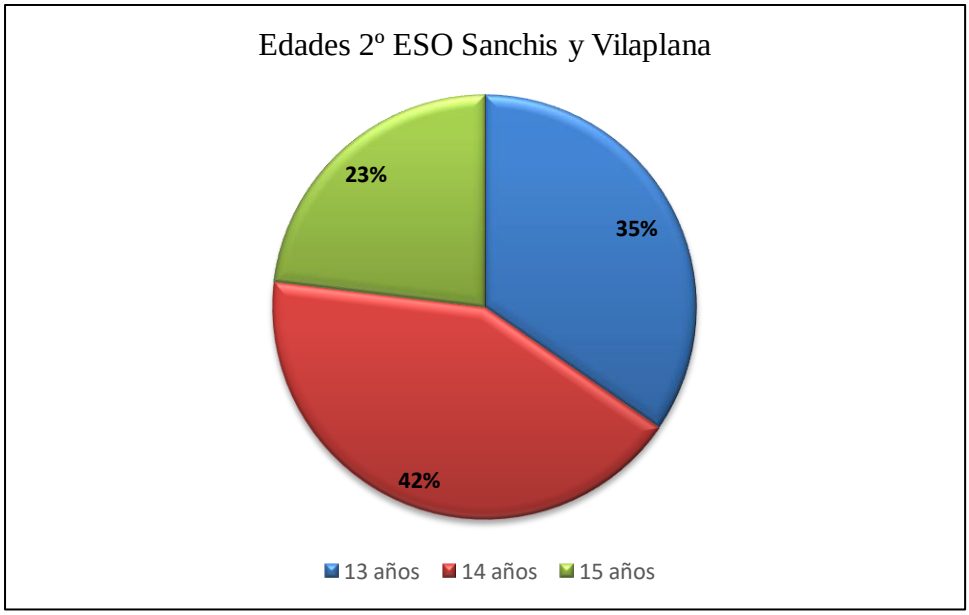

Figura 240. Edades menores de 2º ESO del IES Sanchis y Vilaplana.

En la figura 240, podemos destacar que del curso 2º de la ESO del IES Sanchis y Vilaplana, el 42% de los participantes tiene 14 años, un 35% tiene 13 años, y el resto tiene 15 años, es decir, un 23%.

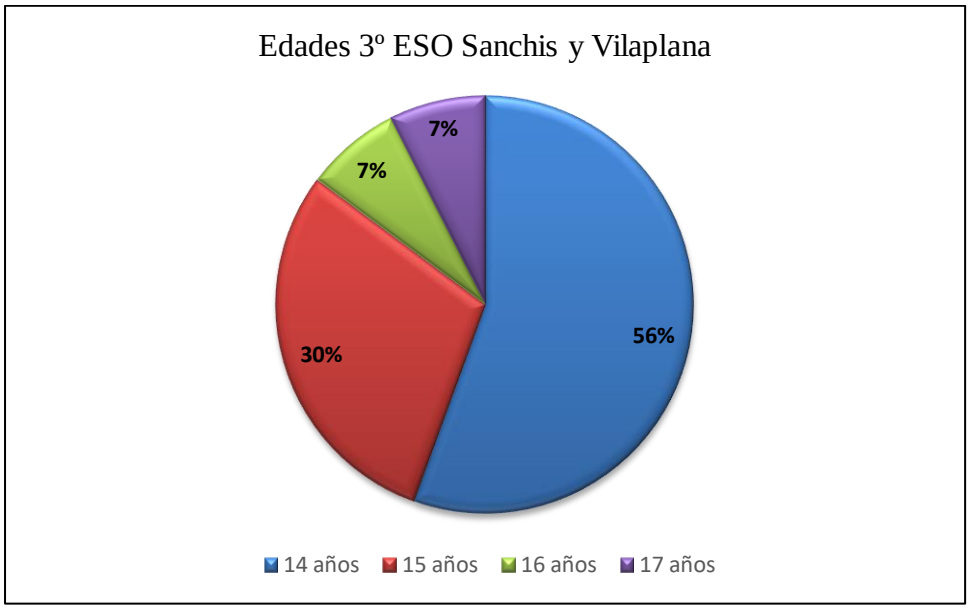

Figura 241. Edades menores de 3º ESO del IES Sanchis y Vilaplana.

En la figura 241, podemos observar que del curso 3º de la ESO del IES Sanchis y Vilaplana, la mayoría tiene 14 años, es decir, un 56%, 15 años tiene un 30% y el resto tiene 16 (7%) y 17 años (7%), respectivamente.

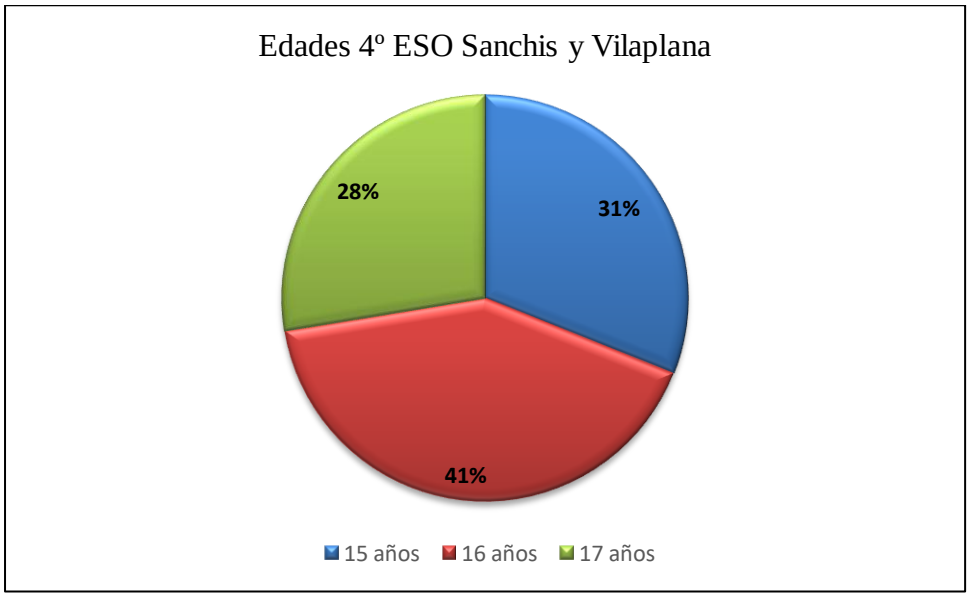

Figura 242. Edades menores de 4º ESO del IES Sanchis y Vilaplana.

En la figura 242, podemos observar que del curso 4º de la ESO del IES Sanchis y Vilaplana, un 41% tiene 16 años, un 31% tiene 15 años y el 28% restante tiene 17 años.

Por otra parte, con relación a la interacción con las TIC de los menores que cursan la ESO en el instituto de educación secundaria Sanchis y Vilaplana, en la encuesta de victimización social figuraban en la primera página, diez ítems con opción de respuesta "SI o "NO", así como otras preguntas con respuestas cerradas, en su caso, obteniéndose los resultados que a continuación se detallan en las tablas 157 a 160, respectivamente, así como los representados gráficamente en las figuras 243 a 282 ambas inclusive.

Tabla 157. *Resultados interacción TIC menores de 1º ESO Sanchis y Vilaplana*.

Ítems interacciones TIC menores 1º ESO	SI	NO
Tengo ordenador en casa	24	3
Tengo webcam	8	19
Tengo teléfono móvil	27	0
Guardo información personal en el teléfono móvil	21	6
Tengo cuenta de correo electrónico	27	0
Utilizo programas de mensajería instantánea	26	1
Utilizo redes sociales	24	3
Utilizo blogs, foros en Internet	3	24

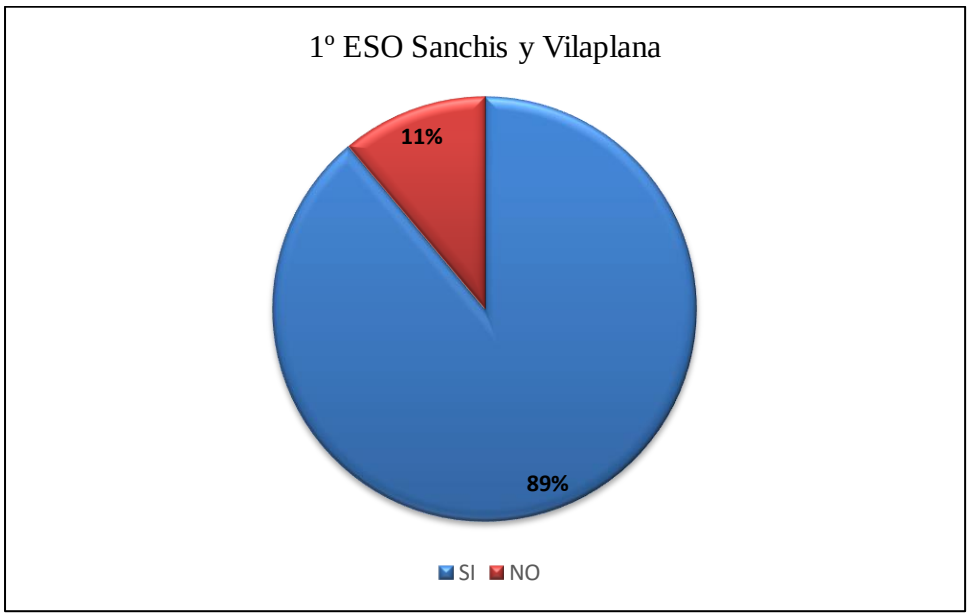

Figura 243. ¿Tienes ordenador en casa?

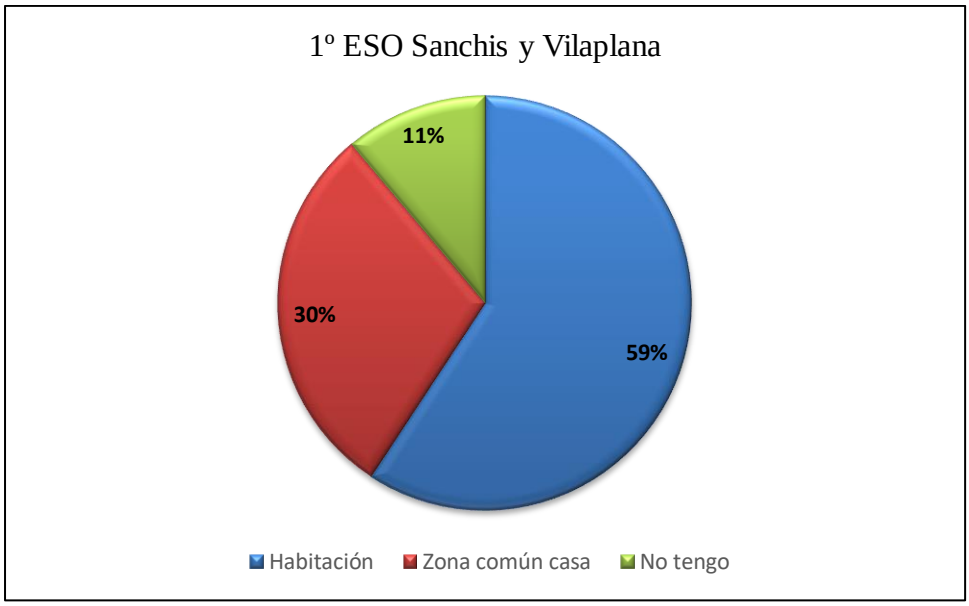

Figura 244. ¿Dónde tienes ubicado el ordenador?

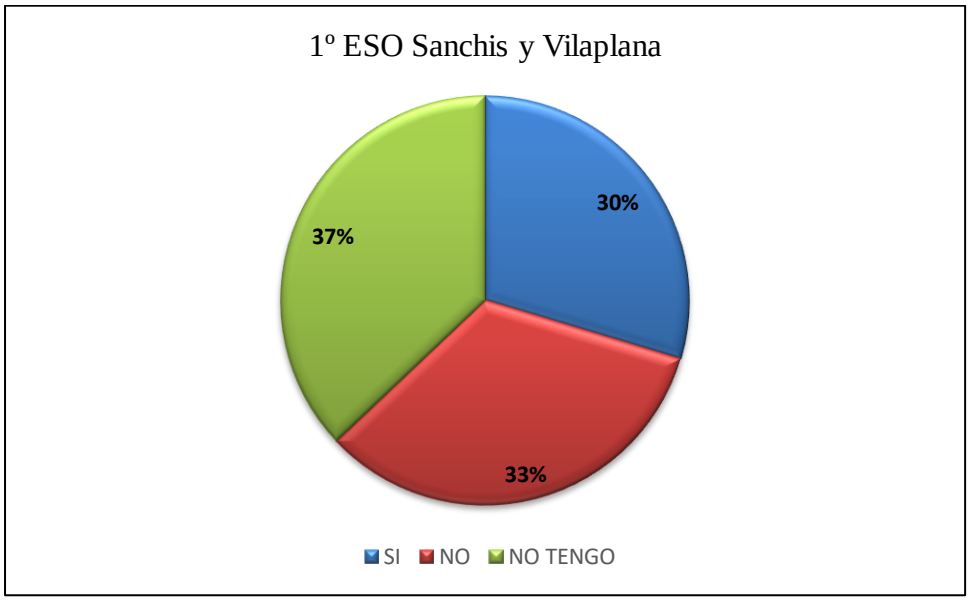

Figura 245. ¿Tapas la webcam cuando no la utilizas?

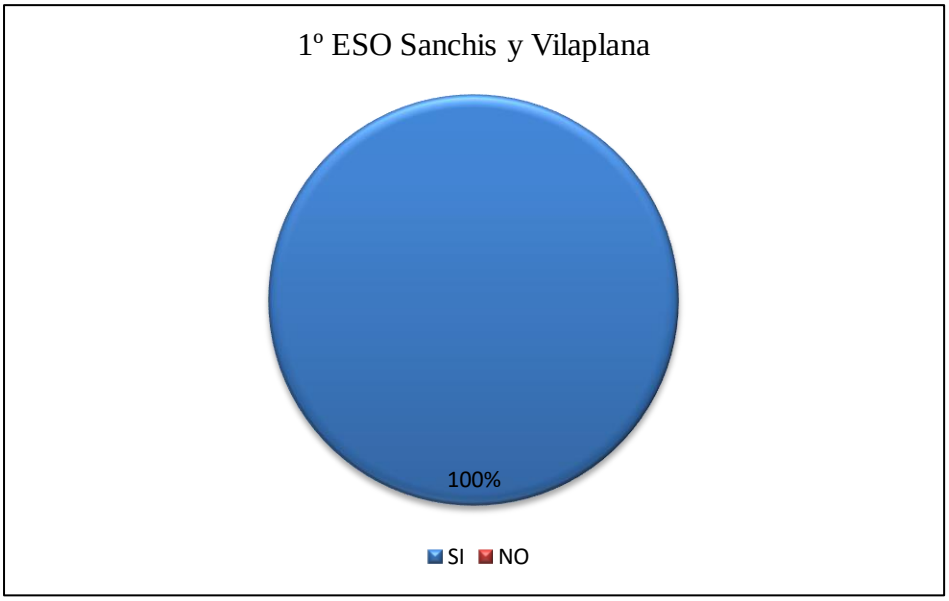

Figura 246. ¿Tienes teléfono móvil?

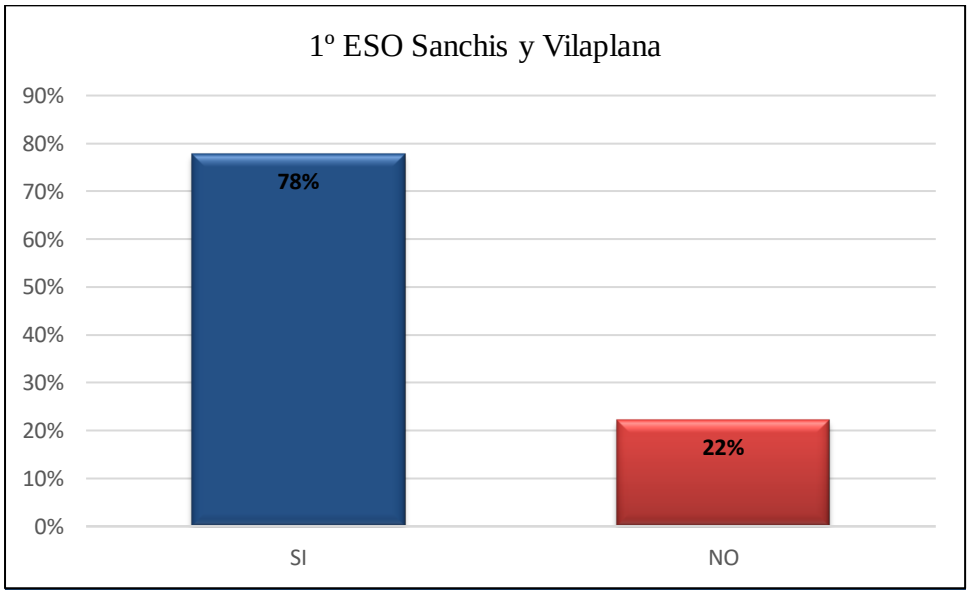

Figura 247. ¿Guardas información personal en el teléfono móvil?

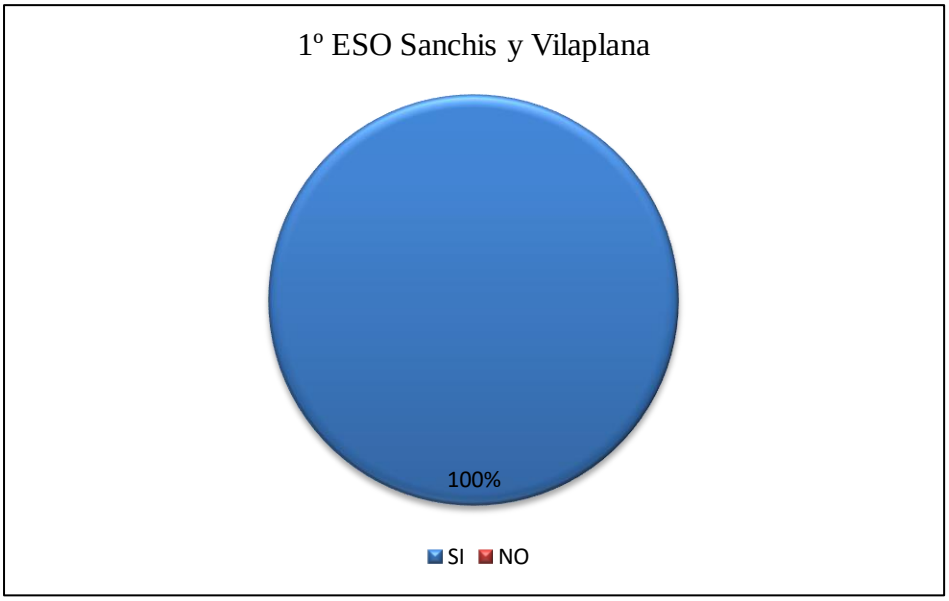

Figura 248. ¿Tienes cuenta de correo electrónico?

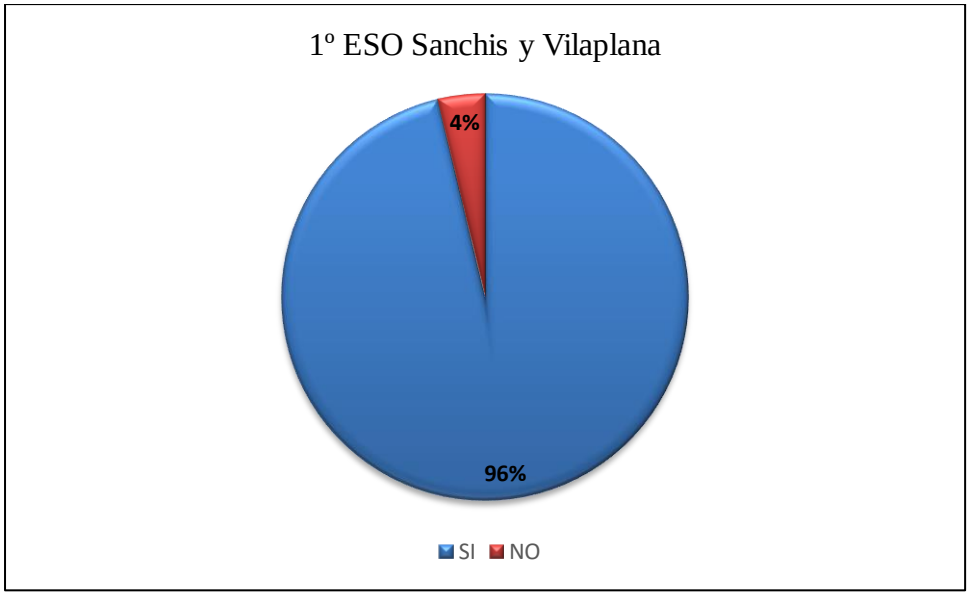

Figura 249. ¿Utilizas programas de mensajería instantánea?

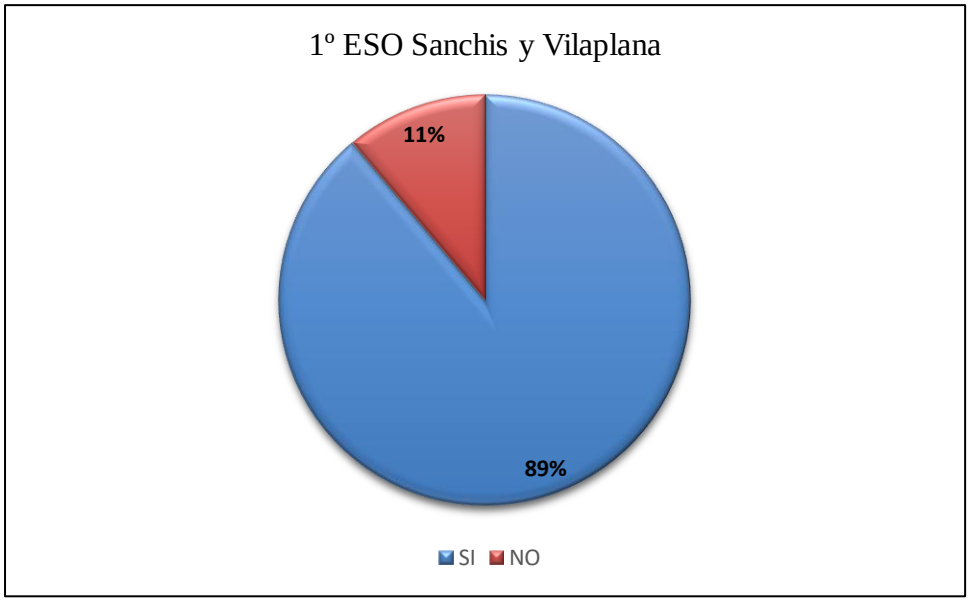

Figura 250. ¿Utilizas redes sociales?

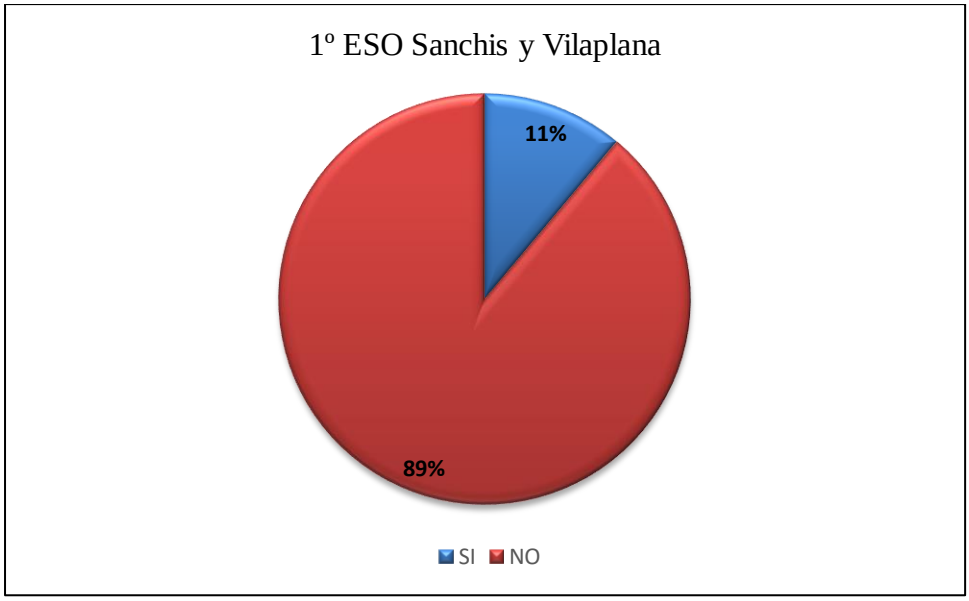

Figura 251. ¿Utilizas blogs, foros en Internet?

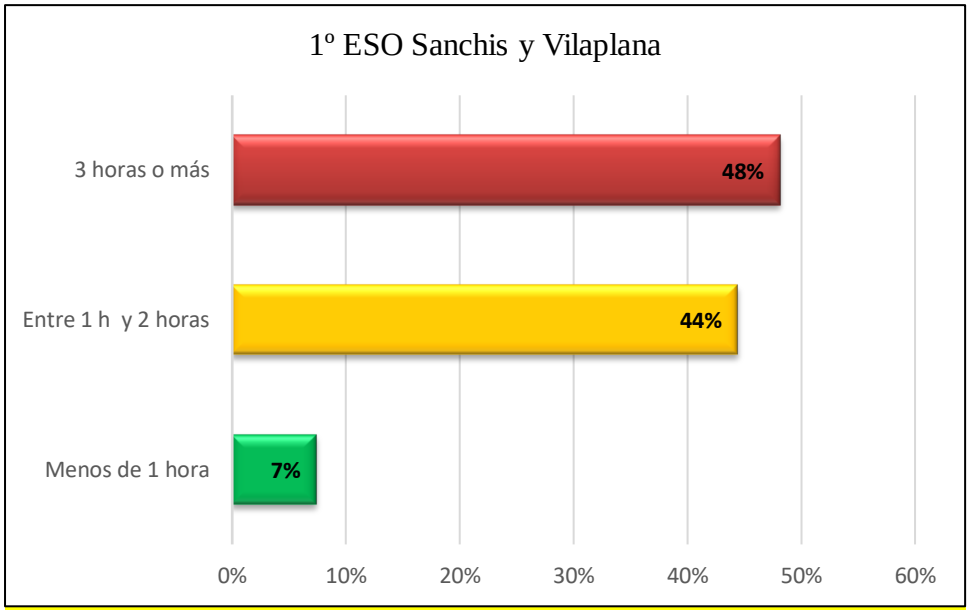

Figura 252. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Tabla 158. *Resultados interacción TIC menores de 2º ESO Sanchis y Vilaplana.*

Ítems interacciones TIC menores 2º ESO	SI	NO
Tengo ordenador en casa	23	3
Tengo webcam	5	21
Tengo teléfono móvil	25	1
Guardo información personal en el teléfono móvil	17	9
Tengo cuenta de correo electrónico	24	2
Utilizo programas de mensajería instantánea	25	1
Utilizo redes sociales	20	6
Utilizo blogs, foros en Internet	6	20

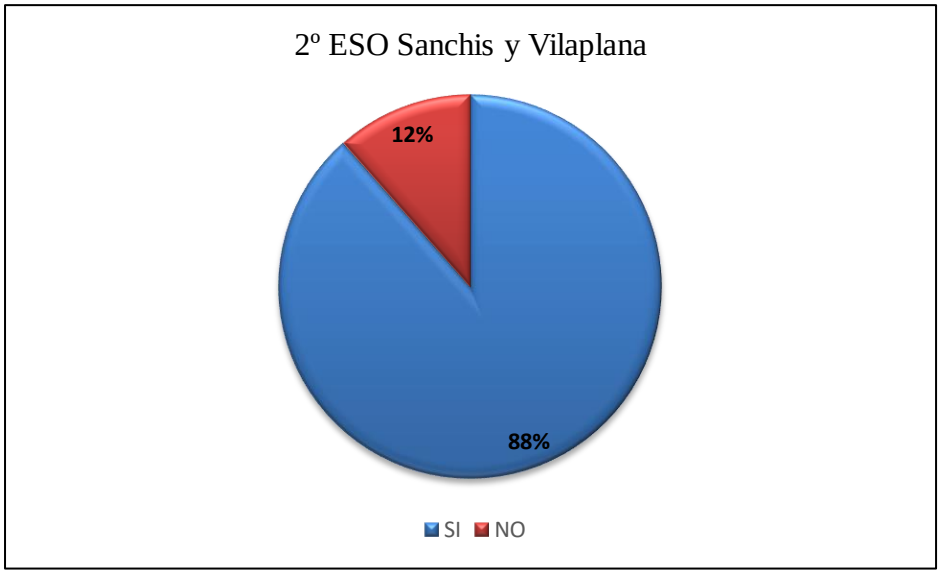

Figura 253. ¿Tienes ordenador en casa?

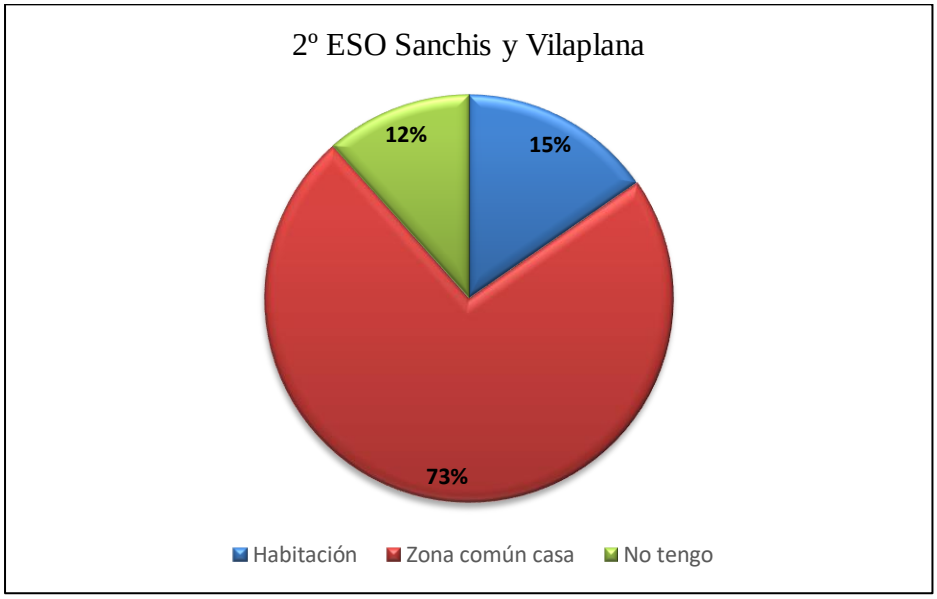

Figura 254. ¿Dónde tienes ubicado el ordenador?

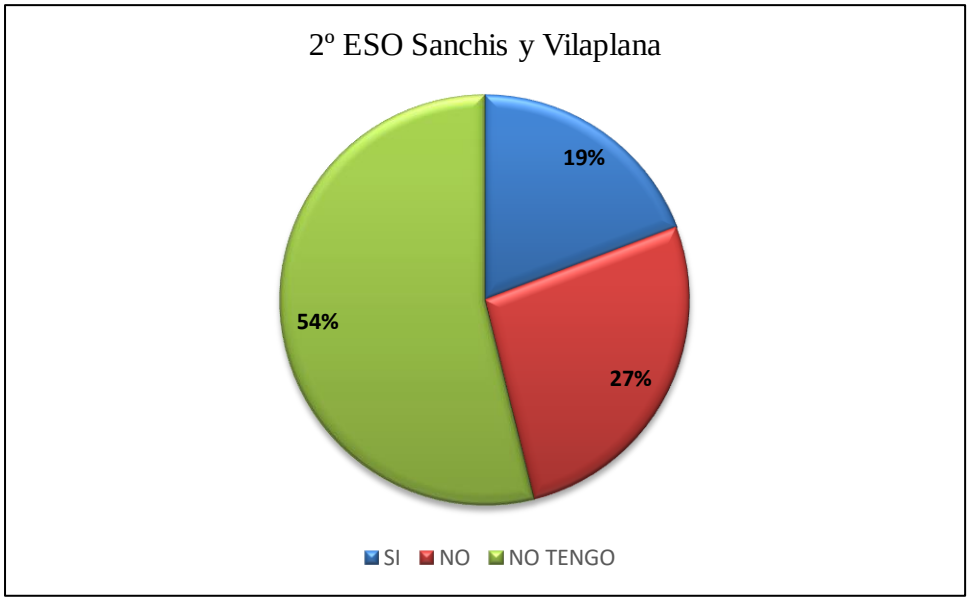

Figura 255. ¿Tapas la webcam cuando no la utilizas?

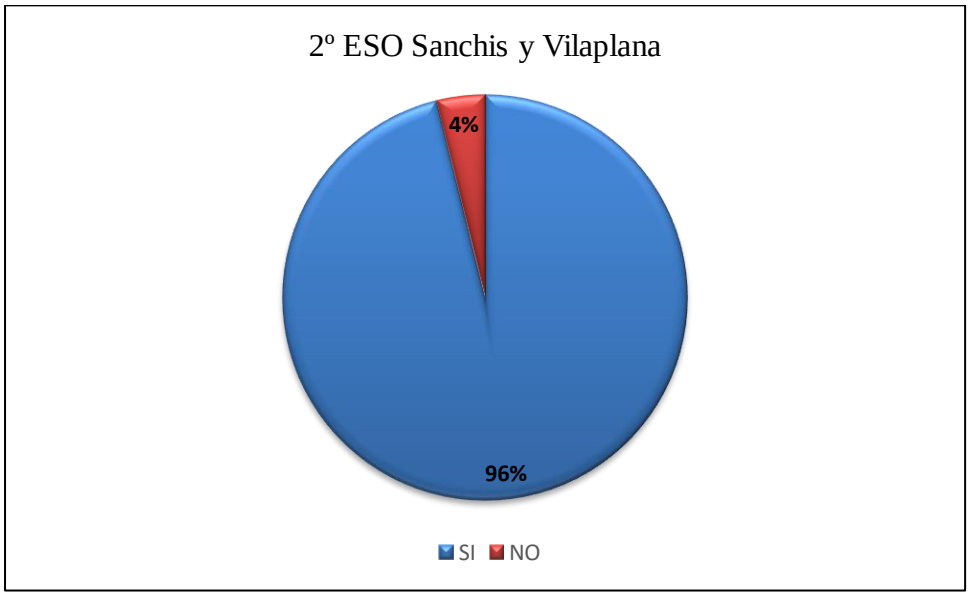

Figura 256. ¿Tienes teléfono móvil?

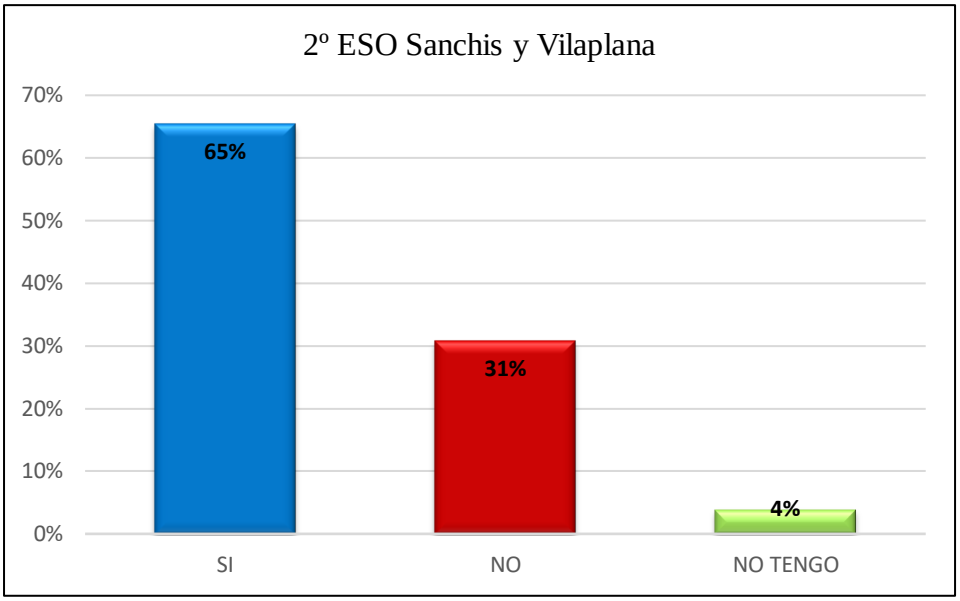

Figura 257. ¿Guardas información personal en el teléfono móvil?

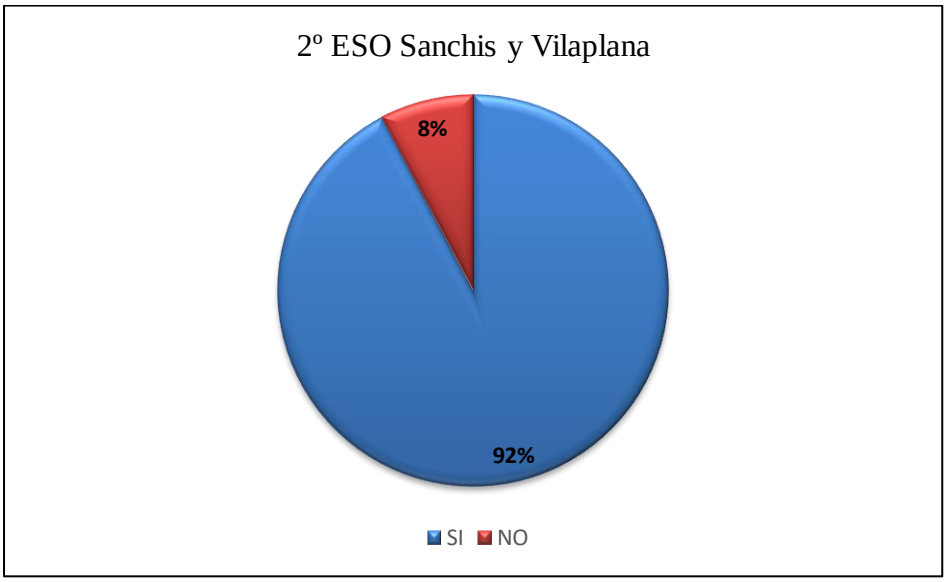

Figura 258. ¿Tienes cuenta de correo electrónico?

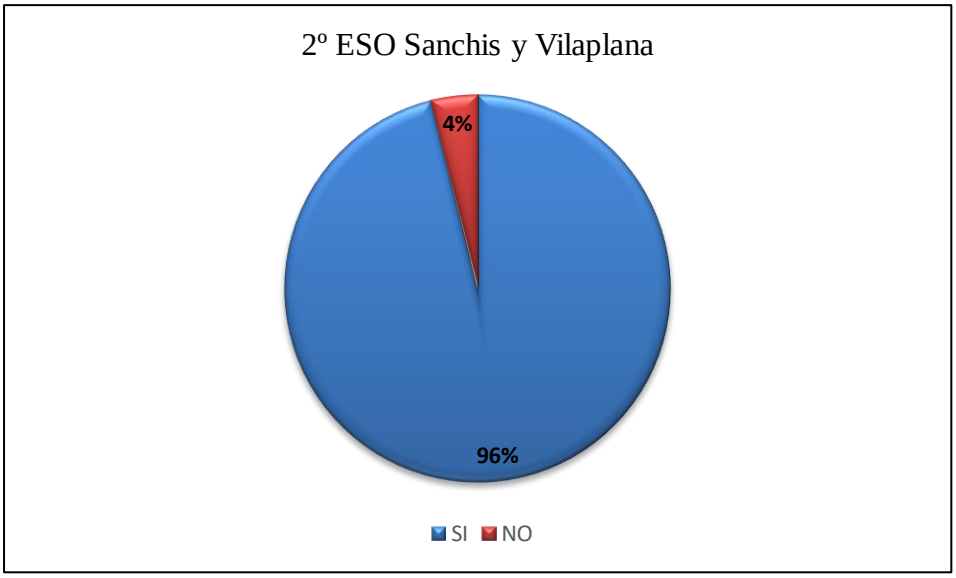

Figura 259. ¿Utilizas programas de mensajería instantánea?

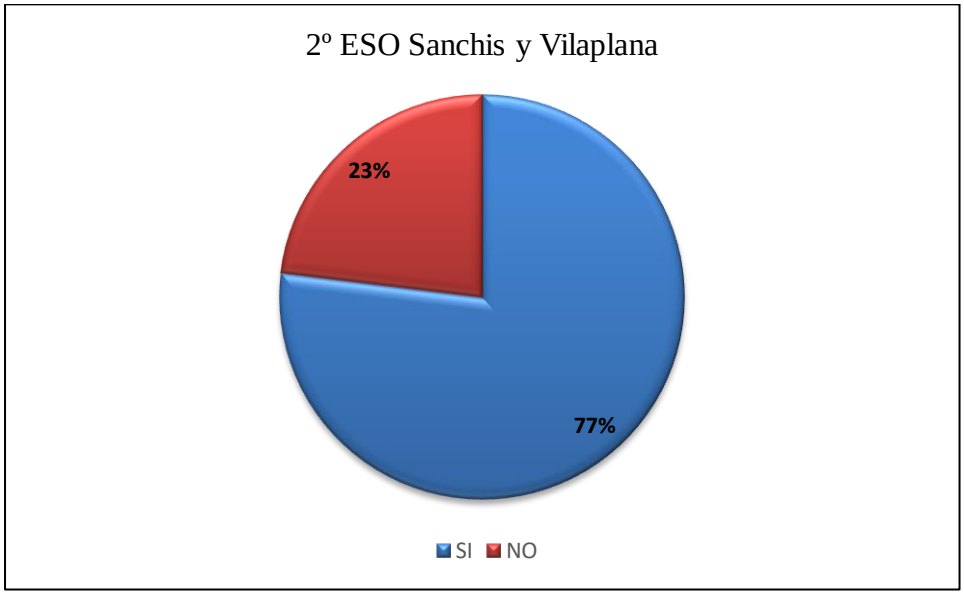

Figura 260. ¿Utilizas redes sociales?

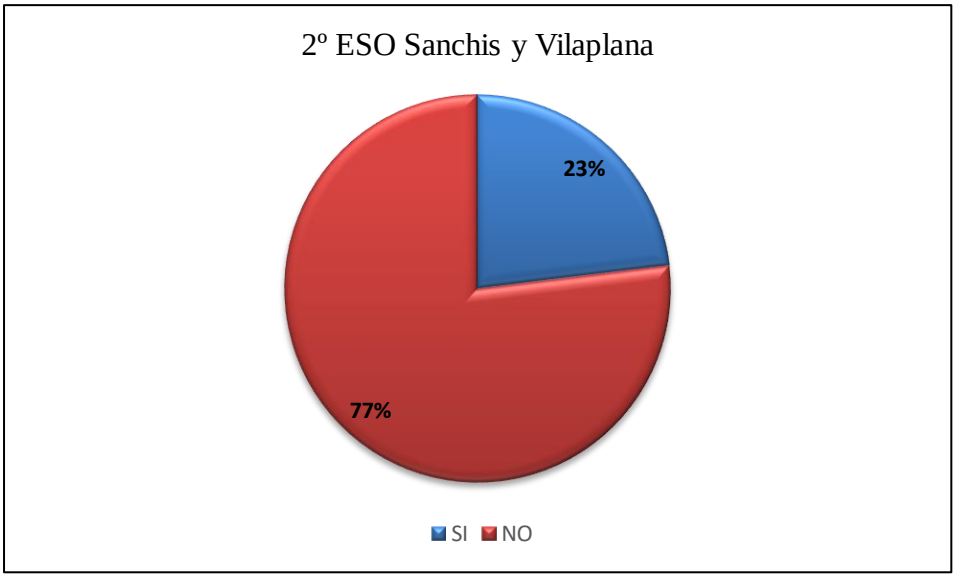

Figura 261. ¿Utilizas blogs, foros en Internet?

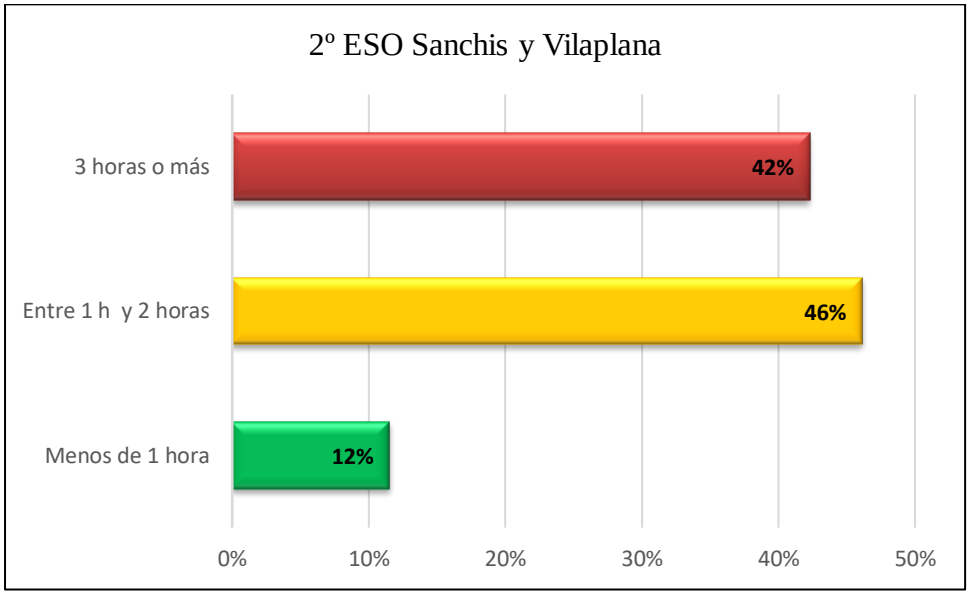

Figura 262. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Tabla 159. *Resultados interacción TIC menores de 3º ESO Sanchis y Vilaplana.*

Ítems interacciones TIC menores 3º ESO	SI	NO
Tengo ordenador en casa	26	1
Tengo webcam	9	18
Tengo teléfono móvil	26	1
Guardo información personal en el teléfono móvil	25	2
Tengo cuenta de correo electrónico	27	0
Utilizo programas de mensajería instantánea	26	1
Utilizo redes sociales	26	1
Utilizo blogs, foros en Internet	13	14

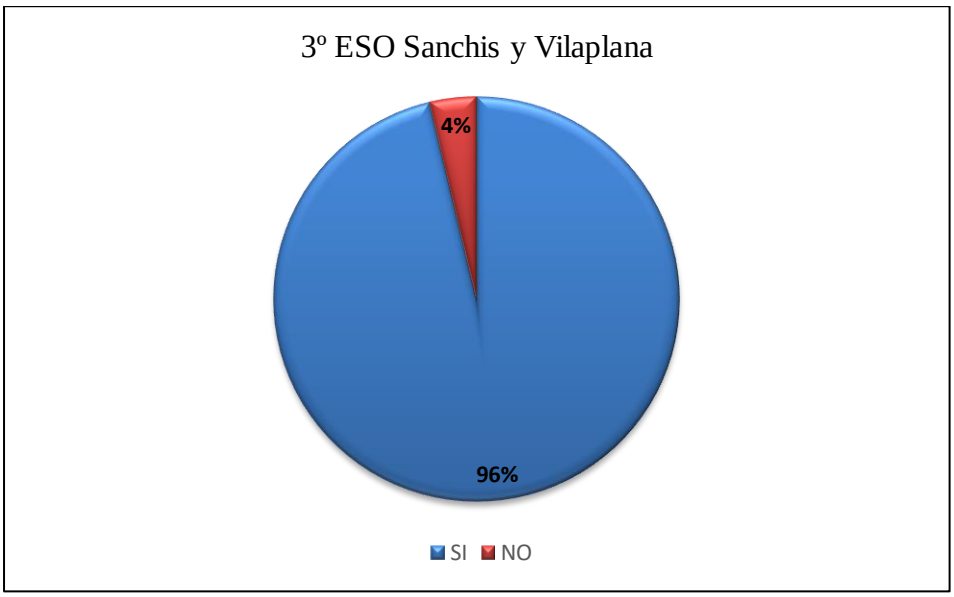

Figura 263. ¿Tienes ordenador en casa?

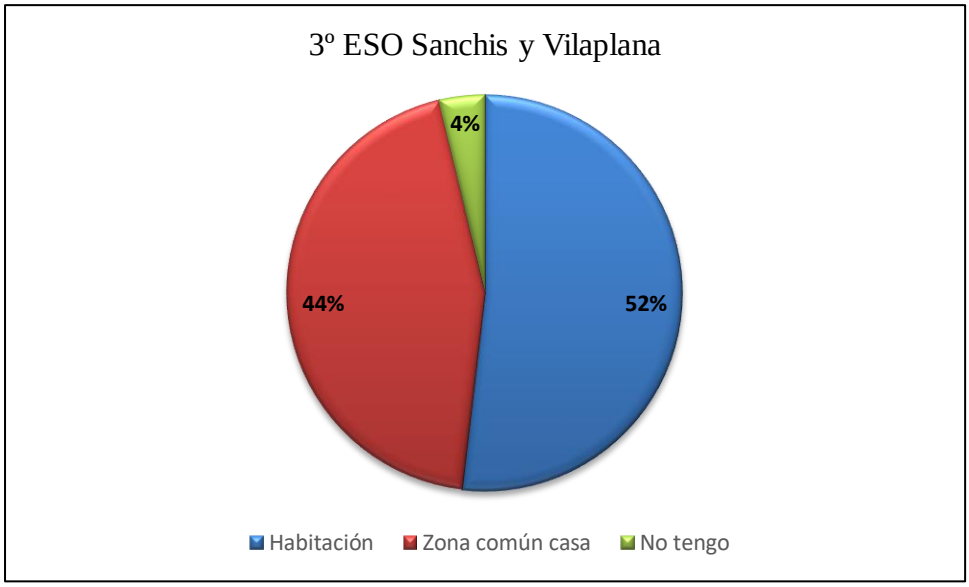

Figura 264. ¿Dónde tienes ubicado el ordenador?

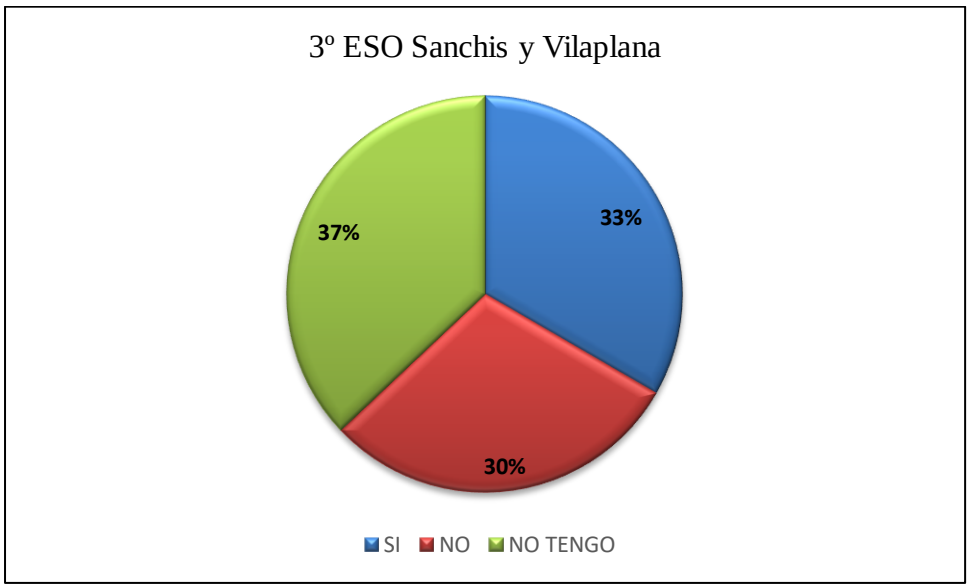

Figura 265. ¿Tapas la webcam cuando no la utilizas?

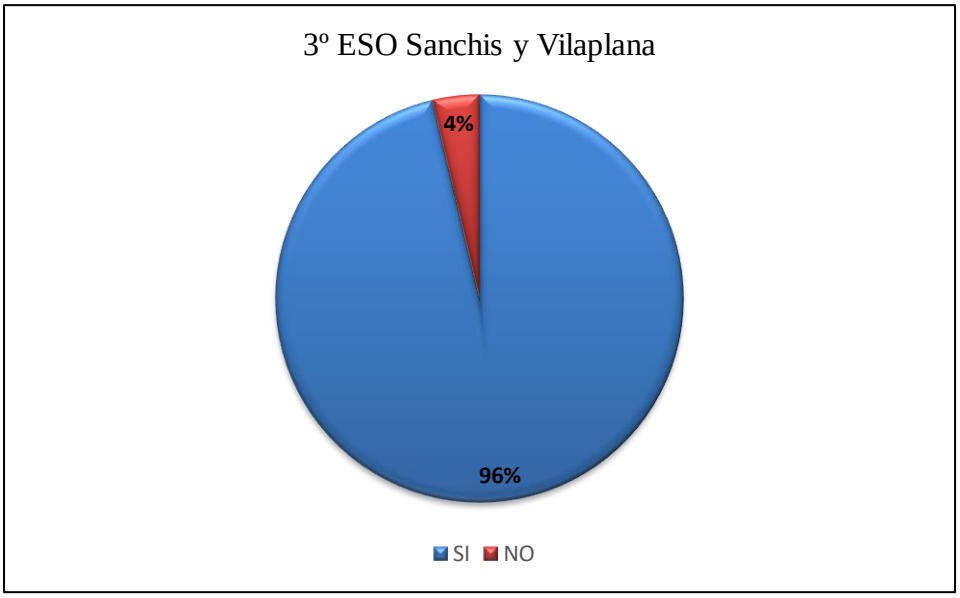

Figura 266. ¿Tienes teléfono móvil?

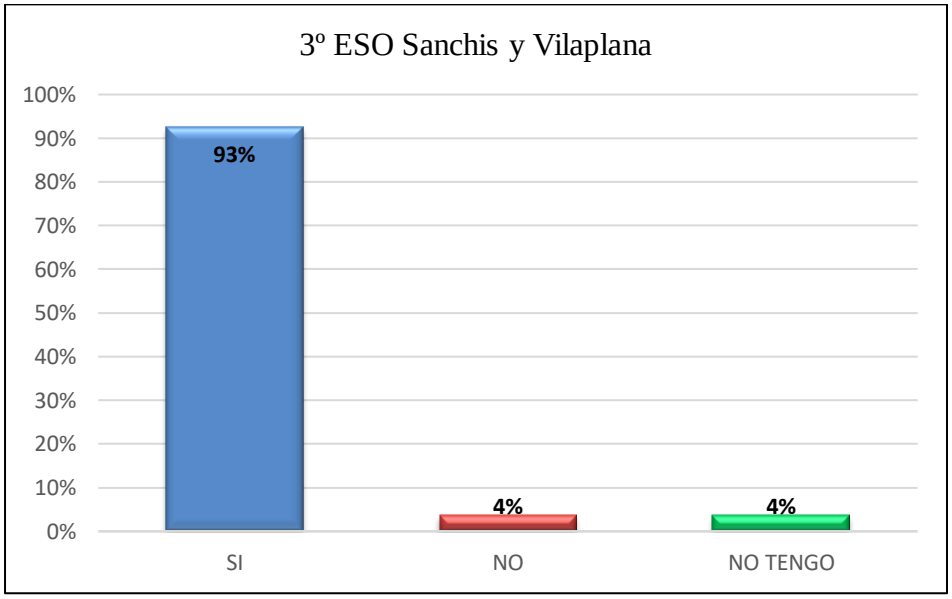

Figura 267. ¿Guardas información personal en el teléfono móvil?

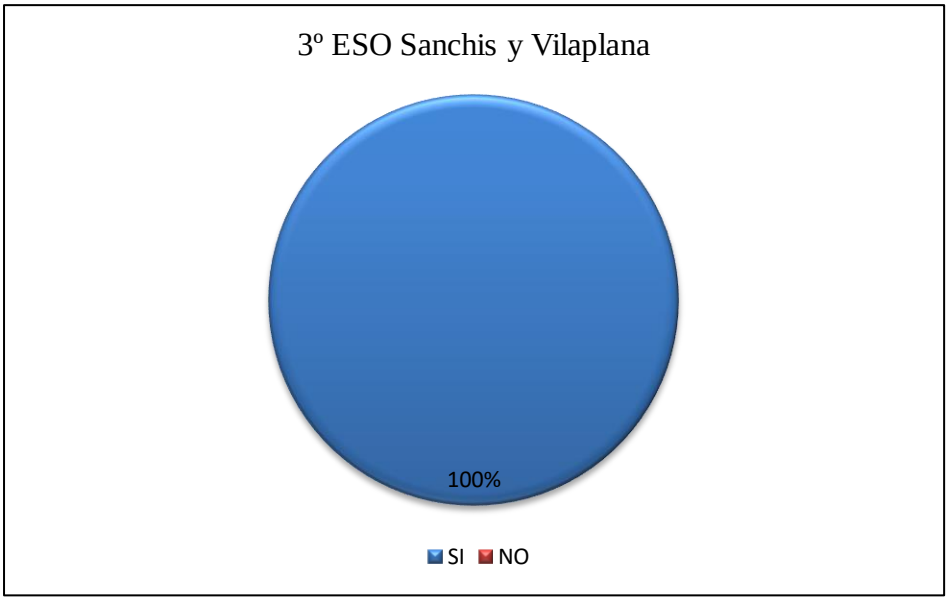

Figura 268. ¿Tienes cuenta de correo electrónico?

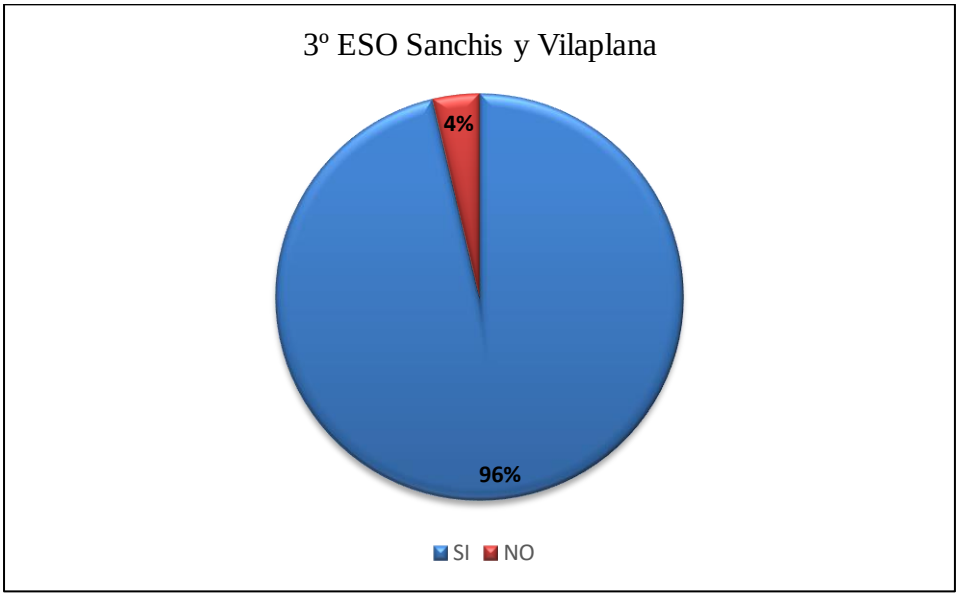

Figura 269. ¿Utilizas programas de mensajería instantánea?

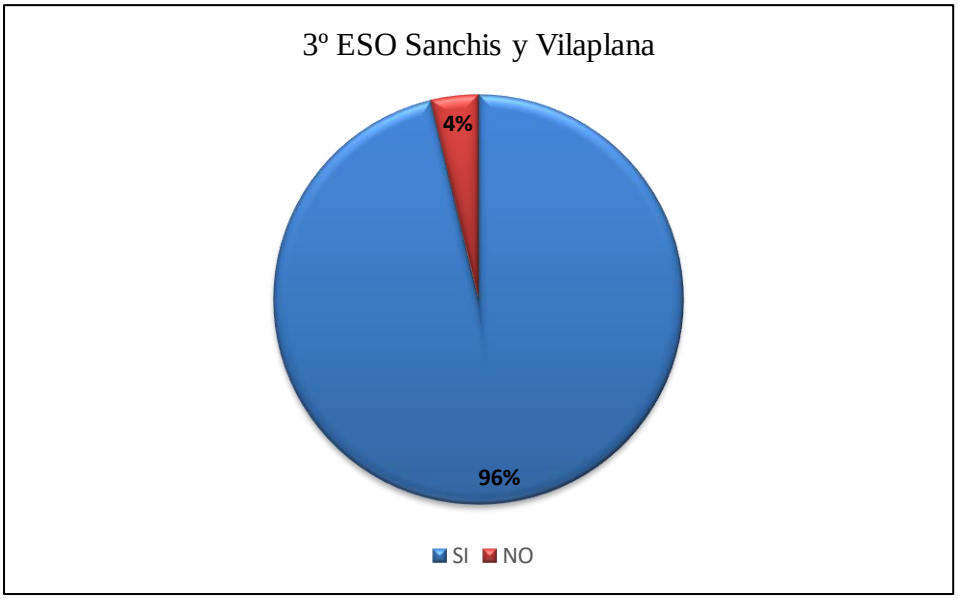

Figura 270. ¿Utilizas redes sociales?

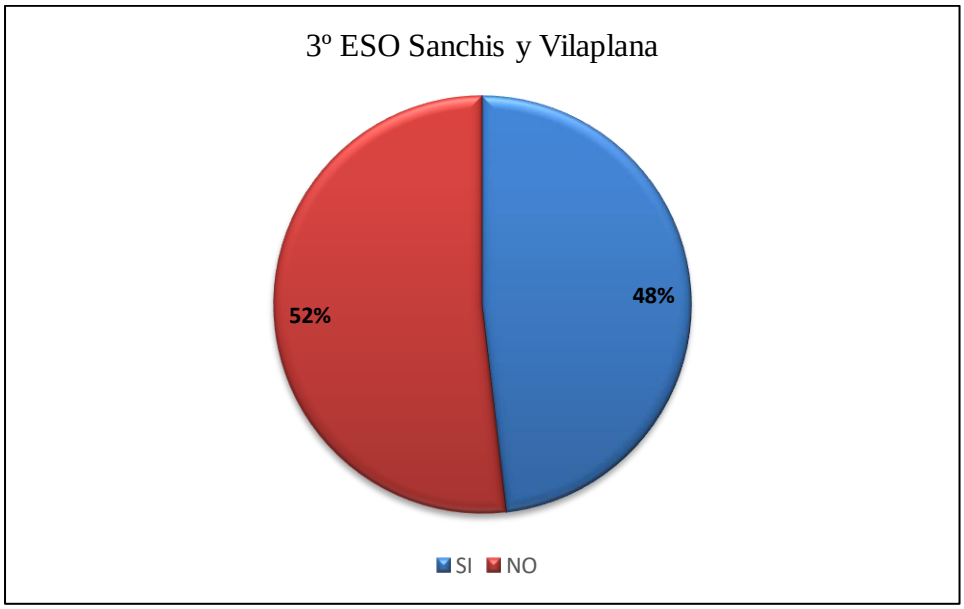

Figura 271. ¿Utilizas blogs, foros en Internet?

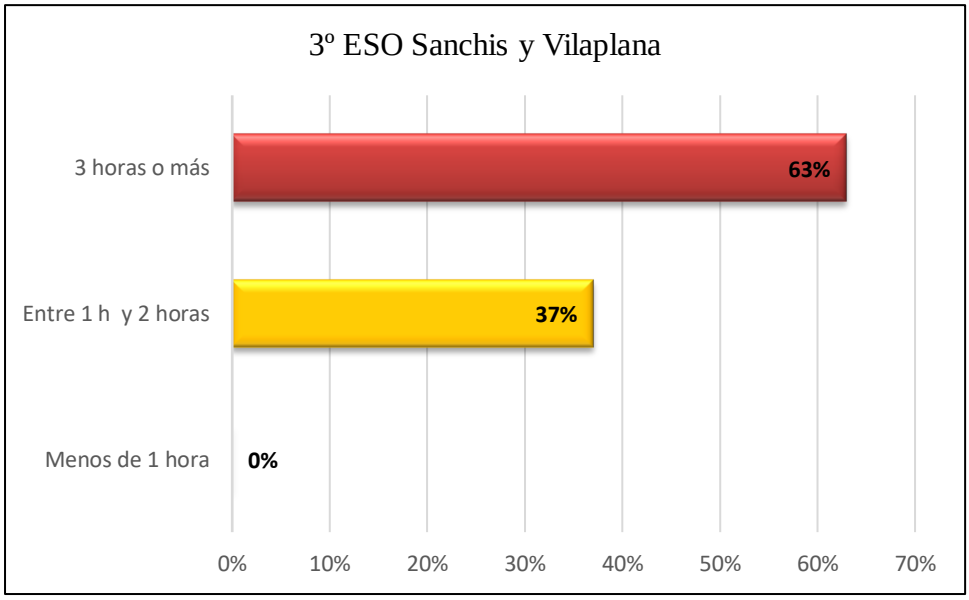

Figura 272. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Tabla 160. *Resultados interacción TIC menores de 4º ESO Sanchis y Vilaplana.*

Ítems interacciones TIC menores 4º ESO	SI	NO
Tengo ordenador en casa	27	2
Tengo webcam	11	18
Tengo teléfono móvil	29	0
Guardo información personal en el teléfono móvil	21	8
Tengo cuenta de correo electrónico	29	0
Utilizo programas de mensajería instantánea	28	1
Utilizo redes sociales	28	1
Utilizo blogs, foros en Internet	11	18

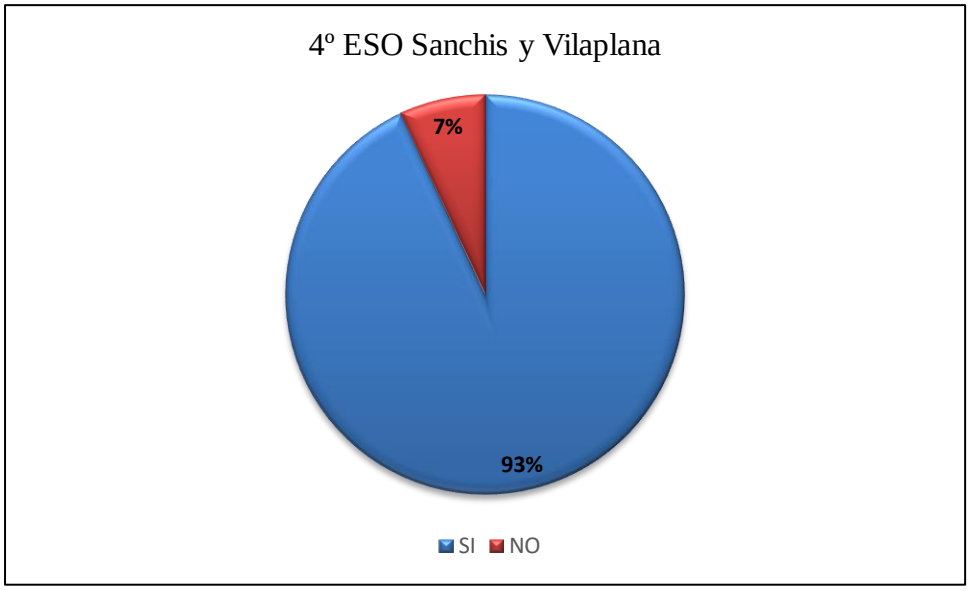

Figura 273. ¿Tienes ordenador en casa?

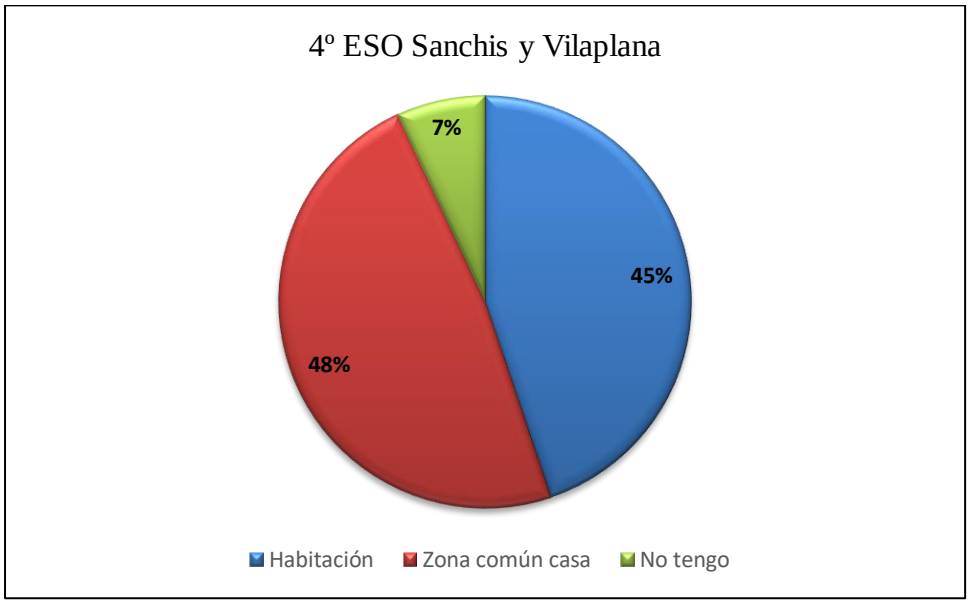

Figura 274. ¿Dónde tienes ubicado el ordenador?

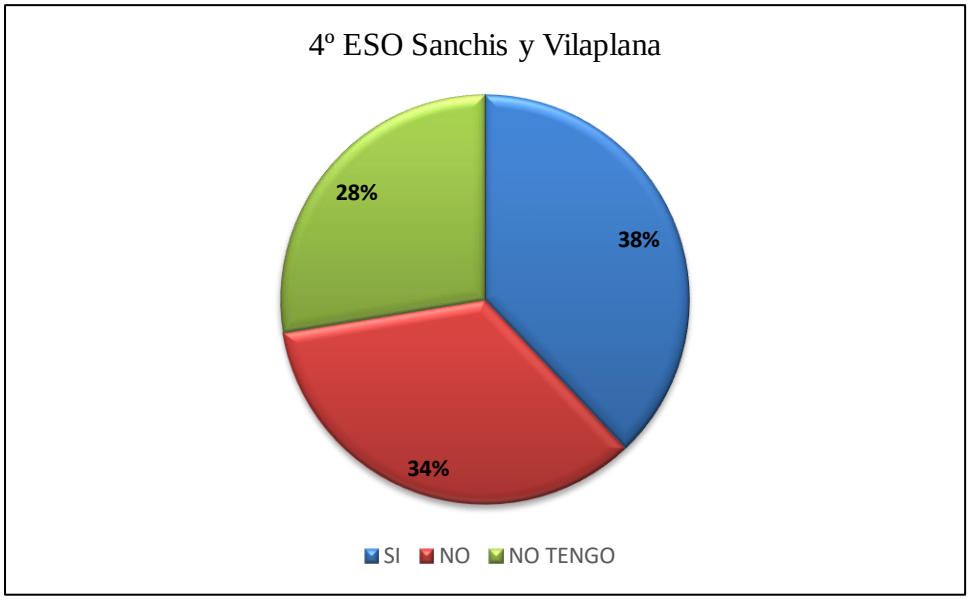

Figura 275. ¿Tapas la webcam cuando no la utilizas?

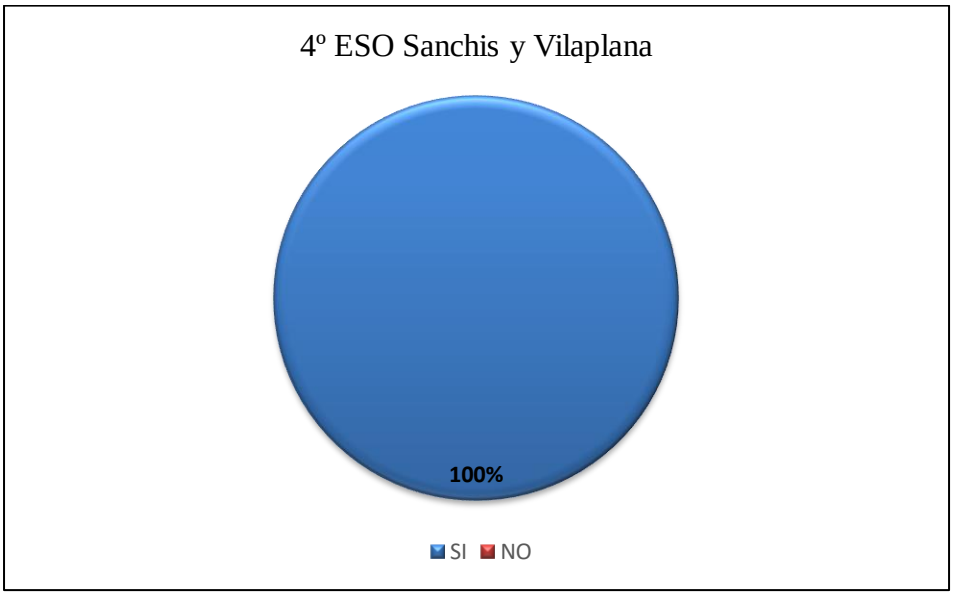

Figura 276. ¿Tienes teléfono móvil?

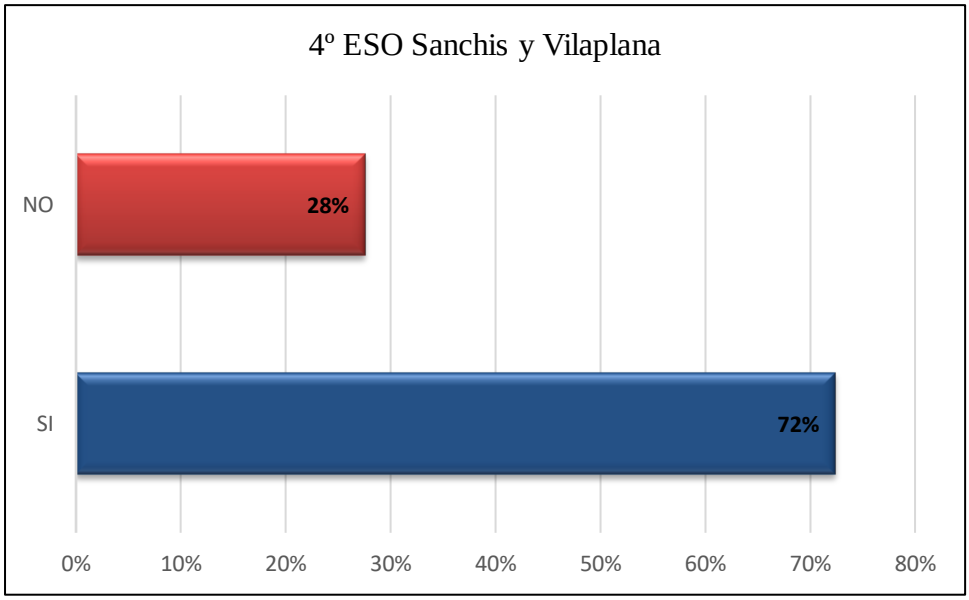

Figura 277. ¿Guardas información personal en el teléfono móvil?

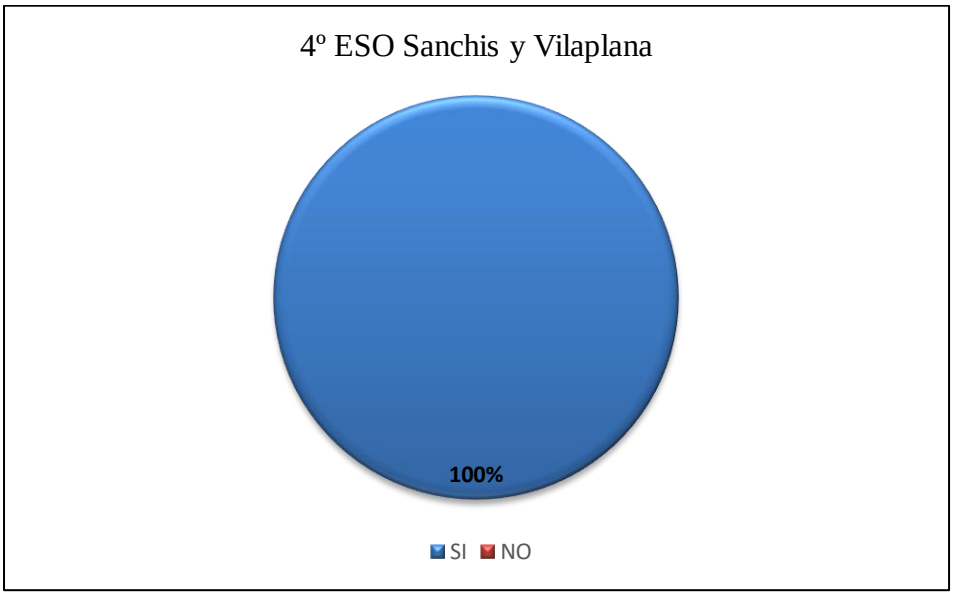

Figura 278. ¿Tienes cuenta de correo electrónico?

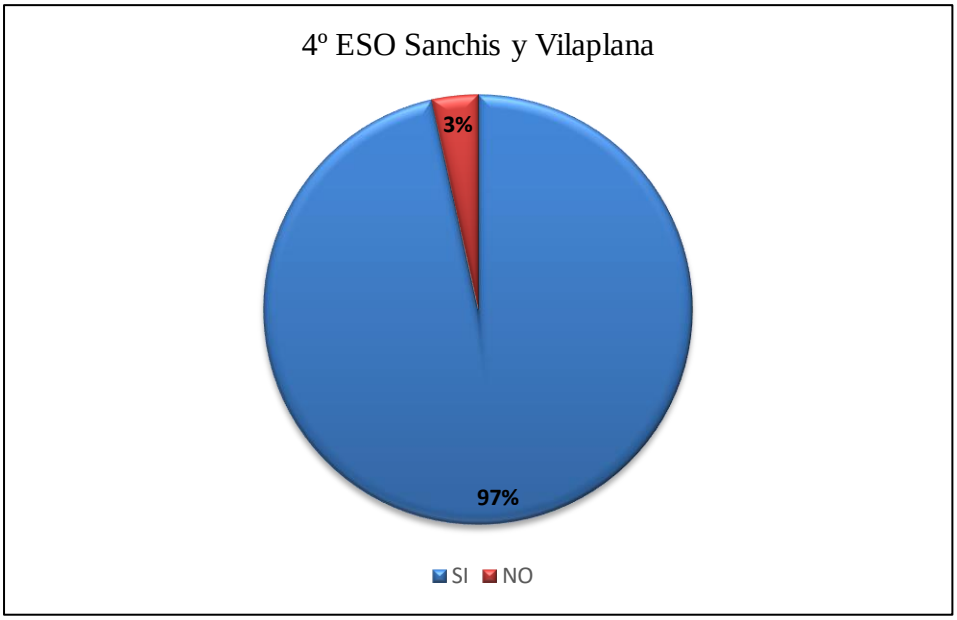

Figura 279. ¿Utilizas programas de mensajería instantánea?

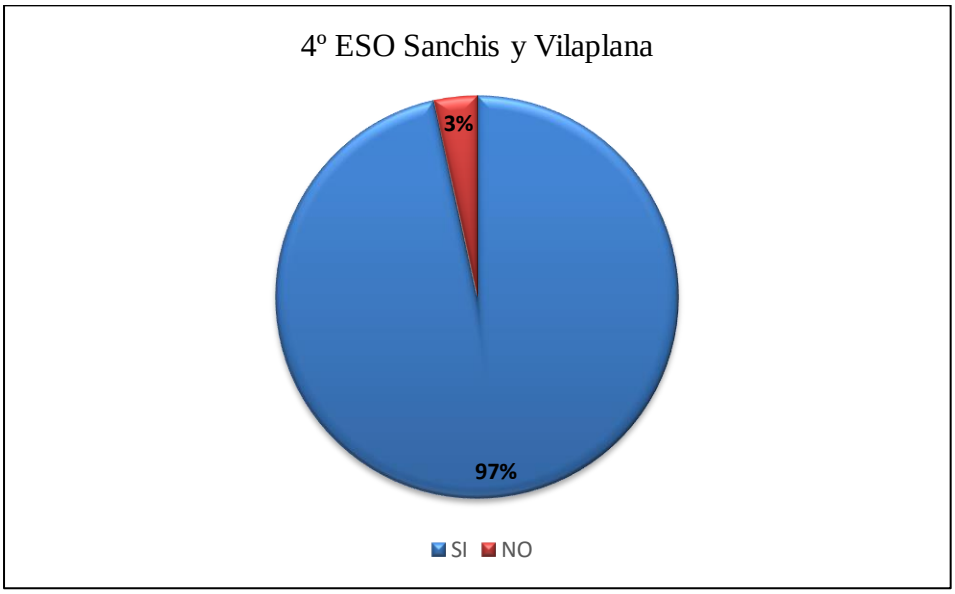

Figura 280. ¿Utilizas redes sociales?

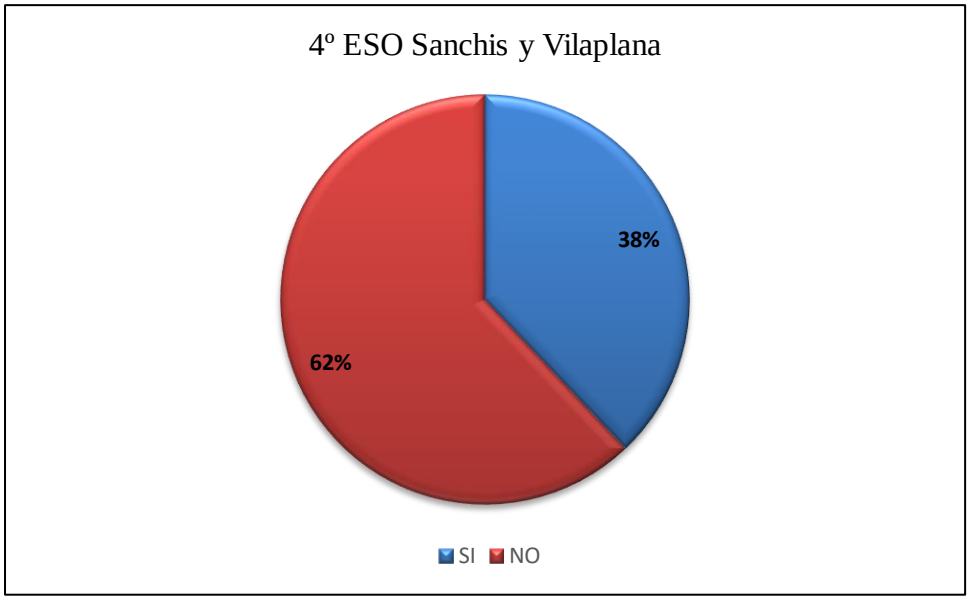

Figura 281. ¿Utilizas blogs, foros en Internet?

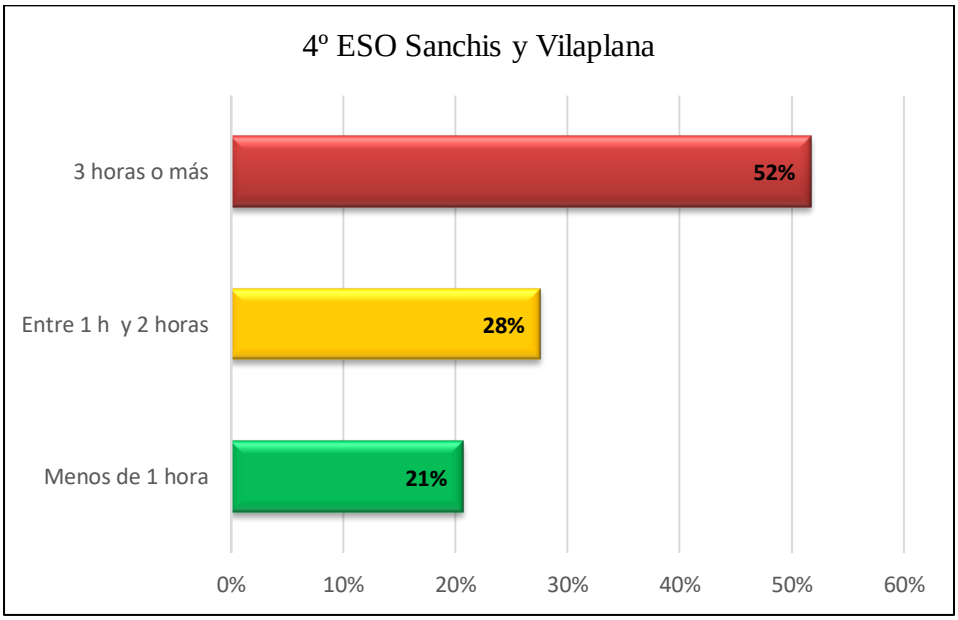

Figura 282. ¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

A continuación, podemos observar en las tablas 161 a 200 y figuras 283 a 302, respectivamente, los resultados obtenidos a las contestaciones de los 20 ítems, de escala frecuencia tipo Likert (de 1 a 5), relacionadas con hechos o conductas de los menores participantes de 1º a 4º de la ESO del instituto de educación secundaria Sanchis y Vilaplana, que han servido para valorar los ciberriesgos a los que están expuestos tanto desde la perspectiva criminológica de la víctima como del victimario de ciberacoso, sexting, online grooming y violencia de género digital, en su caso.

1. ¿Has realizado mensajes y/o llamadas ofensivas a través de teléfono móvil y/o Internet?

Tabla 161. *Ítem. 1. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	67%	77%	59%	86%
2	Pocas veces	22%	19%	26%	3%
3	Algunas veces	7%	0%	7%	3%
4	Muchas veces	4%	4%	7%	3%
5	Siempre	0%	0%	0%	3%

Tabla 162. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han realizado mensajes y/o llamadas ofensivas a través de teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,48	0,802	1	4
2º ESO	1,88	1,657	1	4
3º ESO	1,63	0,926	1	4
4º ESO	1,34	0,974	1	5

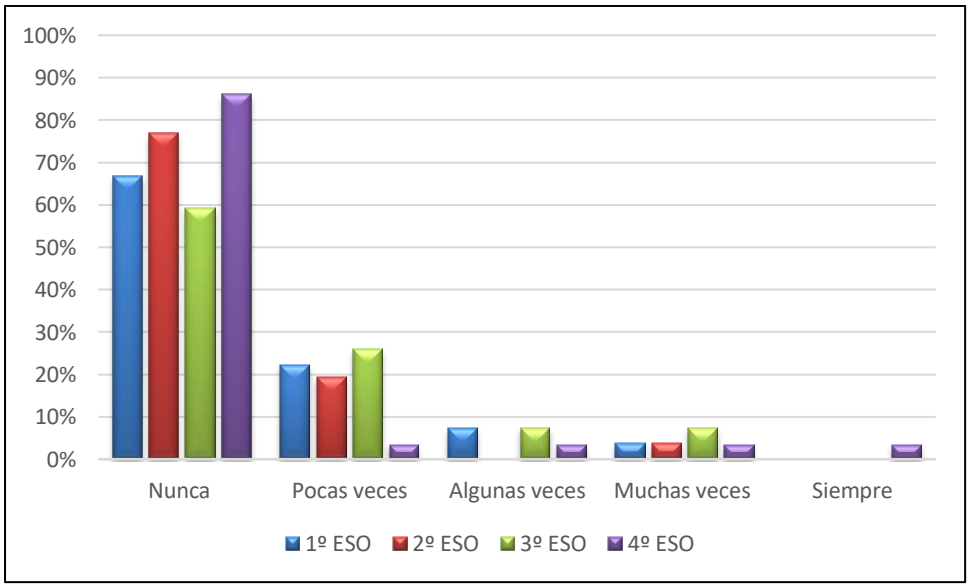

Figura 283. Ítem. 1. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

2. ¿Has colgado en Internet una pelea, agresión o burla que ha sido grabada?

Tabla 163. *Ítem. 2. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	92%	93%	97%
2	Pocas veces	0%	4%	0%	3%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	7%	0%
5	Siempre	0%	4%	0%	0%

Tabla 164. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han colgado en Internet una pelea, agresión o burla que ha sido grabada.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,19	0,801	1	5
3º ESO	1,22	0,801	1	4
4º ESO	1,03	0,186	1	2

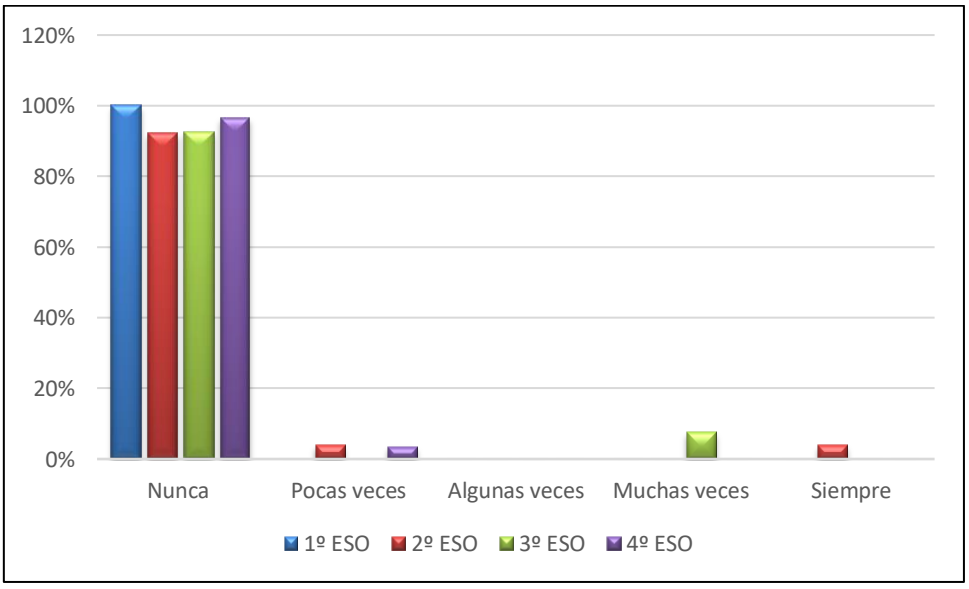

Figura 284. Ítem. 2. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

3. ¿Has realizado comportamientos de tipo sexual a través de la webcam?

Tabla 165. *Ítem. 3. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	88%	96%	93%
2	Pocas veces	0%	0%	0%	0%
3	Algunas veces	0%	4%	0%	3%
4	Muchas veces	0%	4%	4%	0%
5	Siempre	0%	4%	0%	3%

Tabla 166. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han realizado comportamientos de tipo sexual a través de la webcam.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,35	1,018	1	5
3º ESO	1,11	0,577	1	4
4º ESO	1,21	0,819	1	5

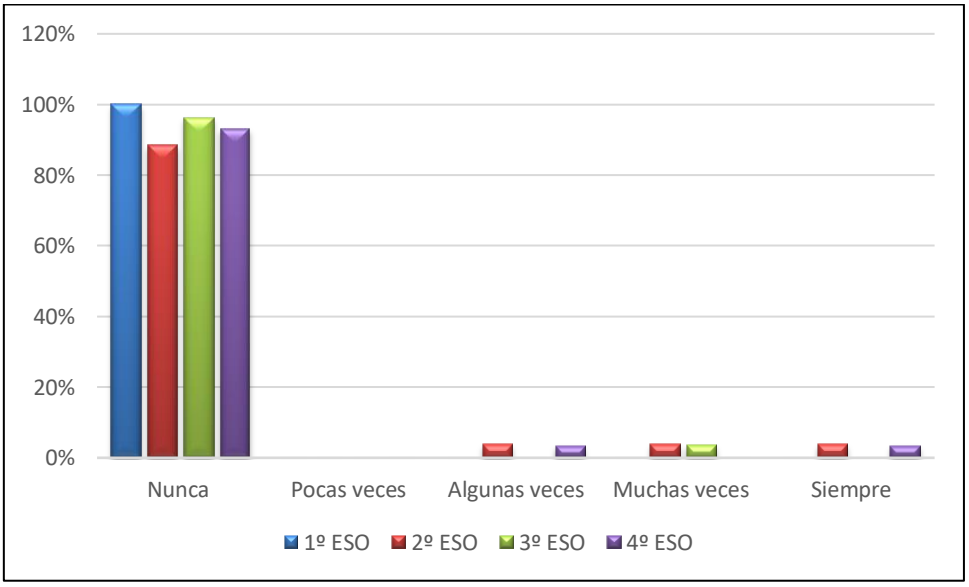

Figura 285. Ítem. 3. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

4. ¿Has difundido vídeos y/o fotos privadas o comprometidas vía teléfono móvil o Internet?

Tabla 167. *Ítem. 4. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	85%	81%	93%	79%
2	Pocas veces	15%	15%	7%	17%
3	Algunas veces	0%	0%	0%	3%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	4%	0%	0%

Tabla 168. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han difundido vídeos y/o fotos privadas o comprometidas vía teléfono móvil o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,15	0,362	1	2
2º ESO	1,31	0,838	1	5
3º ESO	1,07	0,267	1	2
4º ESO	1,24	0,511	1	3

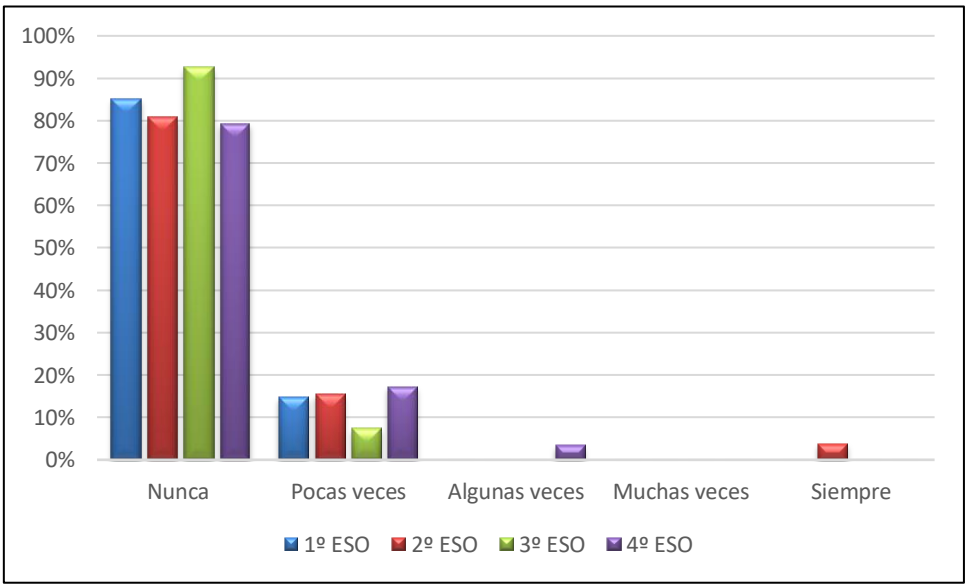

Figura 286. Ítem. 4. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

5. ¿Has colgado vídeos y/o fotos robadas en internet o difundirlos a través del teléfono móvil?

Tabla 169. *Ítem. 5. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	85%	96%	86%
2	Pocas veces	0%	4%	0%	14%
3	Algunas veces	0%	8%	4%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	4%	0%	0%

Tabla 170. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han colgado vídeos y/o fotos robadas en Internet o difundirlos a través del teléfono móvil.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,35	0,936	1	5
3º ESO	1,07	0,385	1	3
4º ESO	1,14	0,351	1	2

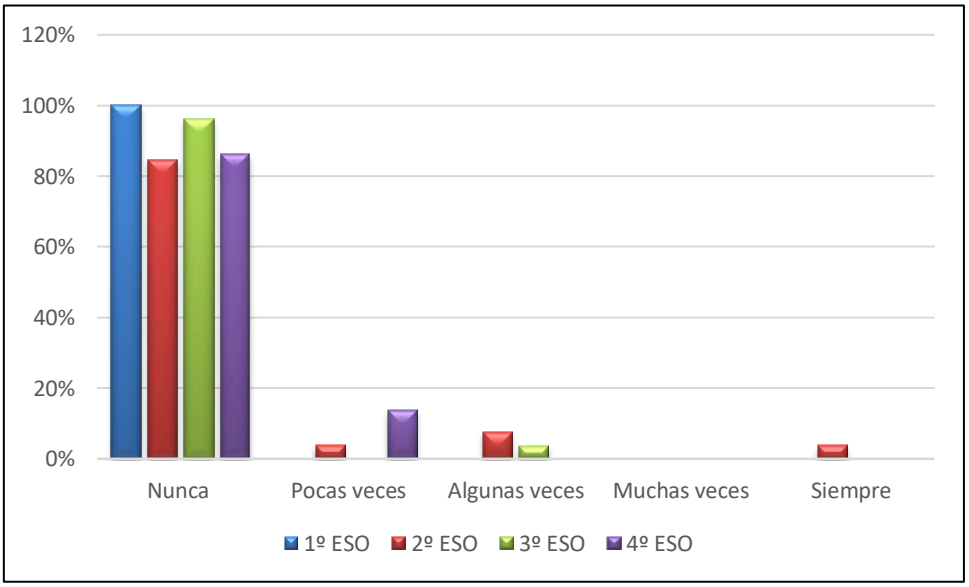

Figura 287. Ítem. 5. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

6. ¿Has realizado llamadas anónimas para asustar o intimidar?

Tabla 171. *Ítem. 6. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	74%	73%	56%	79%
2	Pocas veces	22%	19%	22%	17%
3	Algunas veces	0%	0%	11%	0%
4	Muchas veces	4%	4%	11%	3%
5	Siempre	0%	4%	0%	0%

Tabla 172. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han realizado llamadas anónimas para asustar o intimidar.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,33	0,679	1	4
2º ESO	1,46	0,989	1	5
3º ESO	1,78	1,050	1	4
4º ESO	1,28	0,649	1	4

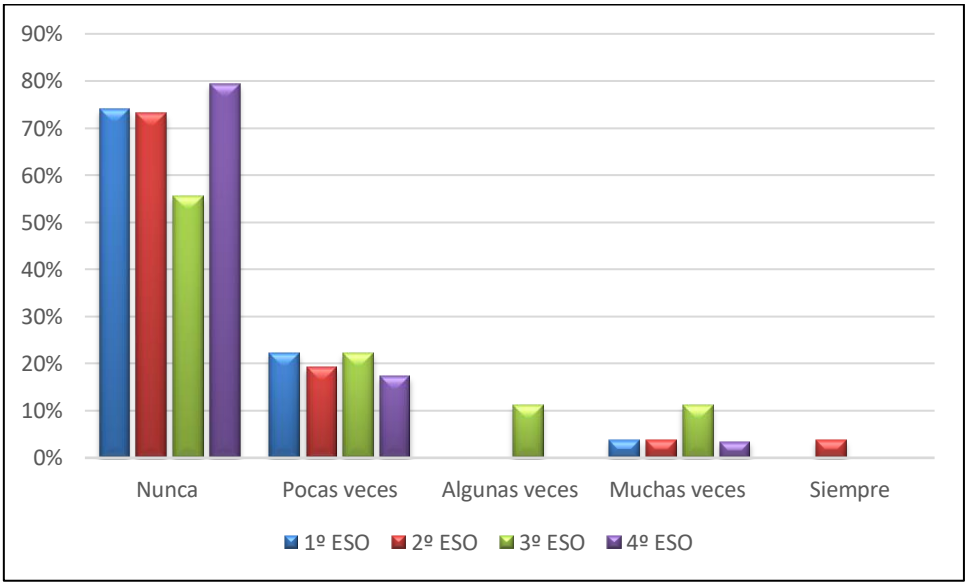

Figura 288. Ítem. 6. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

7. ¿Has realizado amenazas o chantajes a través de mensajes y/o llamadas?

Tabla 173. *Ítem. 7. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	85%	88%	89%	93%
2	Pocas veces	11%	8%	11%	3%
3	Algunas veces	4%	4%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	3%

Tabla 174. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han realizado amenazas o chantajes a través de mensajes y/o llamadas.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,19	0,483	1	3
2º ESO	1,15	0,464	1	3
3º ESO	1,11	0,320	1	2
4º ESO	1,17	0,759	1	5

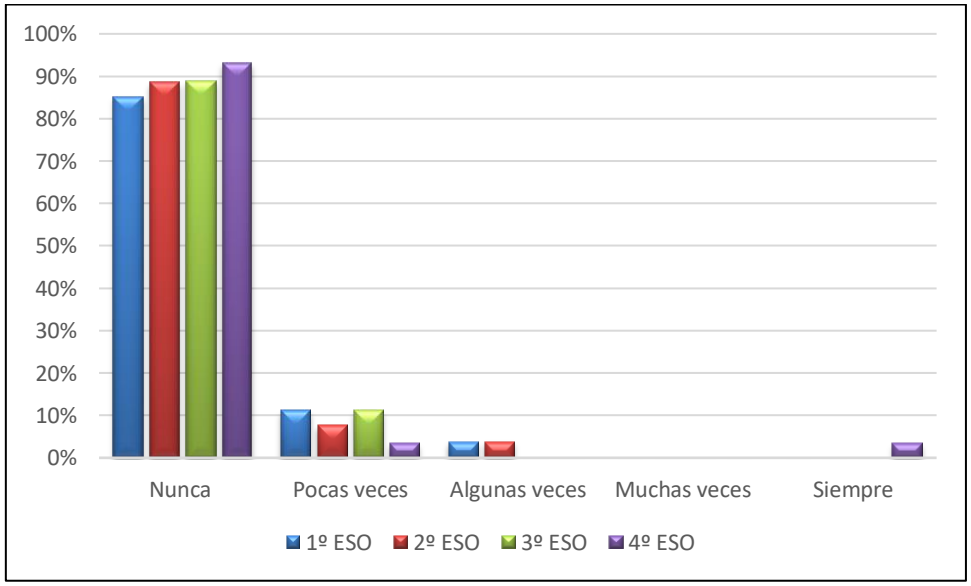

Figura 289. Ítem. 7. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

8. ¿Has acosado sexualmente a través de teléfono móvil y/o Internet?

Tabla 175. *Ítem. 8. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	96%	96%	100%
2	Pocas veces	0%	0%	0%	0%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	4%	0%
5	Siempre	0%	4%	0%	0%

Tabla 176. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han acosado sexualmente a través de teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,15	0,784	1	5
3º ESO	1,11	0,577	1	4
4º ESO	1	0	1	1

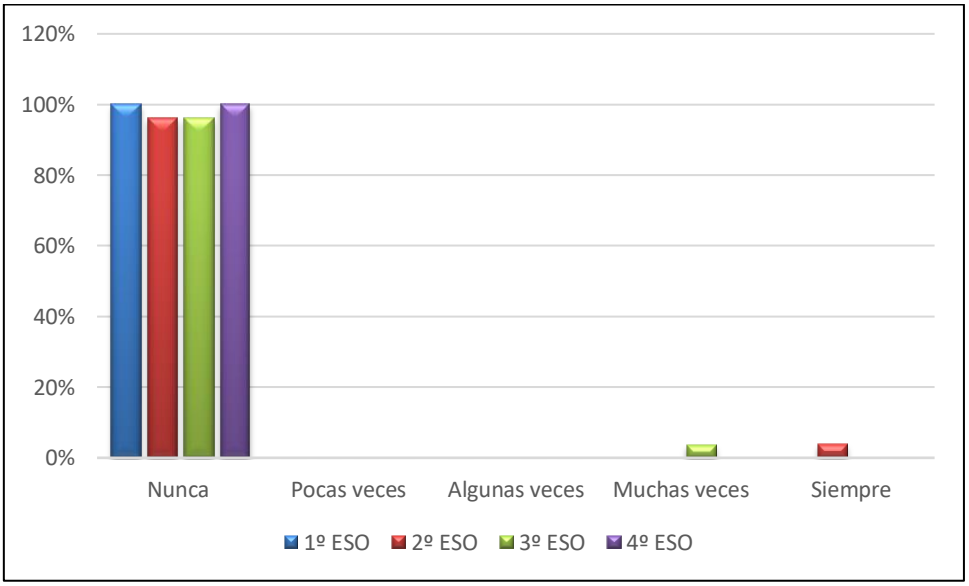

Figura 290. Ítem. 8. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

9. ¿Has suplantado a una persona para difamar, mentir o contar sus secretos?

Tabla 177. *Ítem. 9. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	85%	88%	96%	93%
2	Pocas veces	15%	4%	4%	3%
3	Algunas veces	0%	8%	0%	0%
4	Muchas veces	0%	0%	0%	3%
5	Siempre	0%	0%	0%	0%

Tabla 178. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han suplantado a una persona para difamar, mentir o contar sus secretos.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,15	0,362	1	2
2º ESO	1,19	0,567	1	3
3º ESO	1,04	0,192	1	2
4º ESO	1,14	0,581	1	4

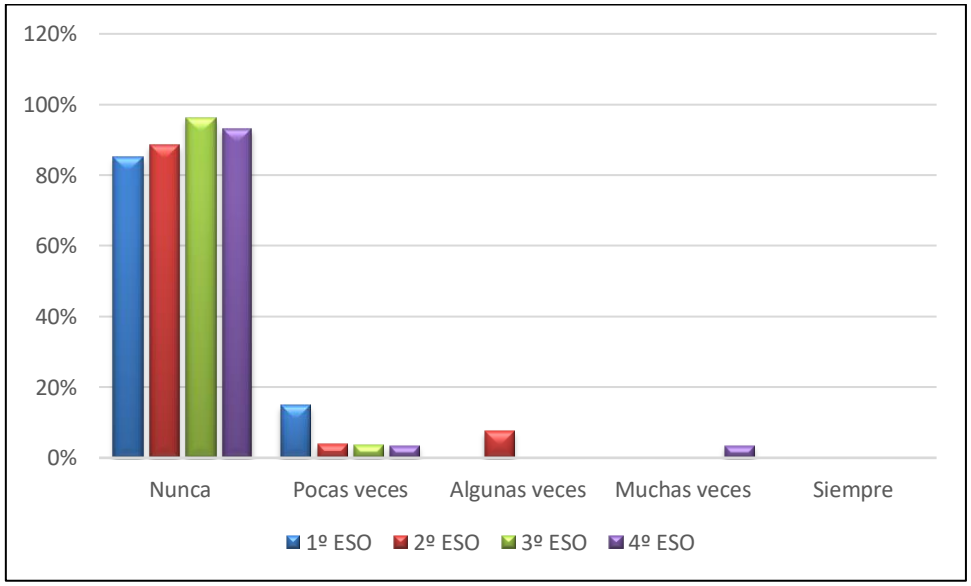

Figura 291. Ítem. 9. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

10. ¿Has robado la contraseña a una persona?

Tabla 179. *Ítem. 10. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	85%	85%	85%	90%
2	Pocas veces	11%	8%	7%	10%
3	Algunas veces	0%	4%	4%	0%
4	Muchas veces	4%	0%	0%	0%
5	Siempre	0%	4%	4%	0%

Tabla 180. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han robado la contraseña a una persona.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,22	0,641	1	4
2º ESO	1,31	0,884	1	5
3º ESO	1,30	0,869	1	5
4º ESO	1,10	0,310	1	2

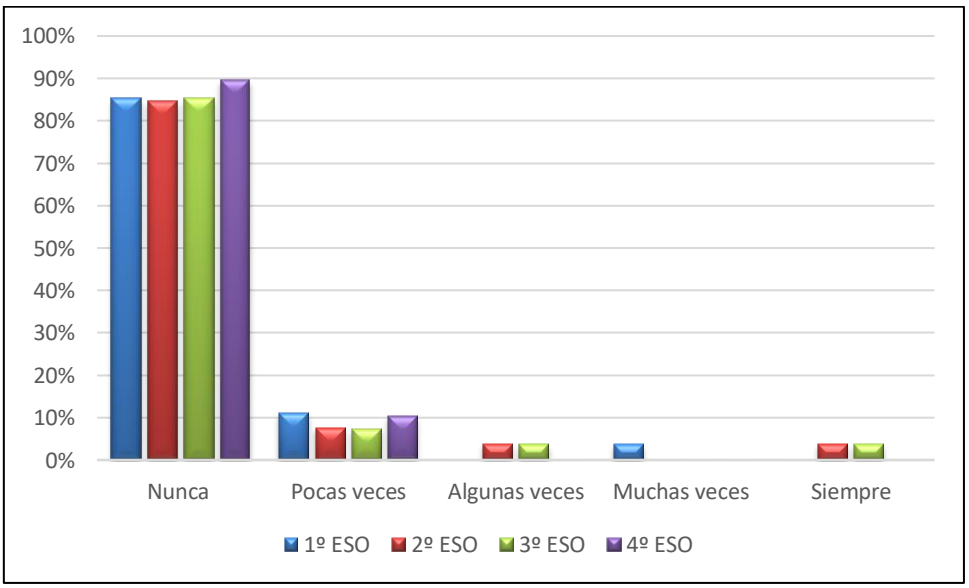

*Figura 292.*Ítem. 10. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

11. ¿Has trucado fotos y vídeos para difundirlos y humillar vía teléfono móvil y/o Internet?

Tabla 181. *Ítem. 11. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	88%	93%	90%
2	Pocas veces	0%	4%	7%	7%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	8%	0%	3%

Tabla 182. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han trucado fotos y vídeos para difundirlos y humillar vía teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,35	1,093	1	5
3º ESO	1,07	0,267	1	2
4º ESO	1,21	0,774	1	5

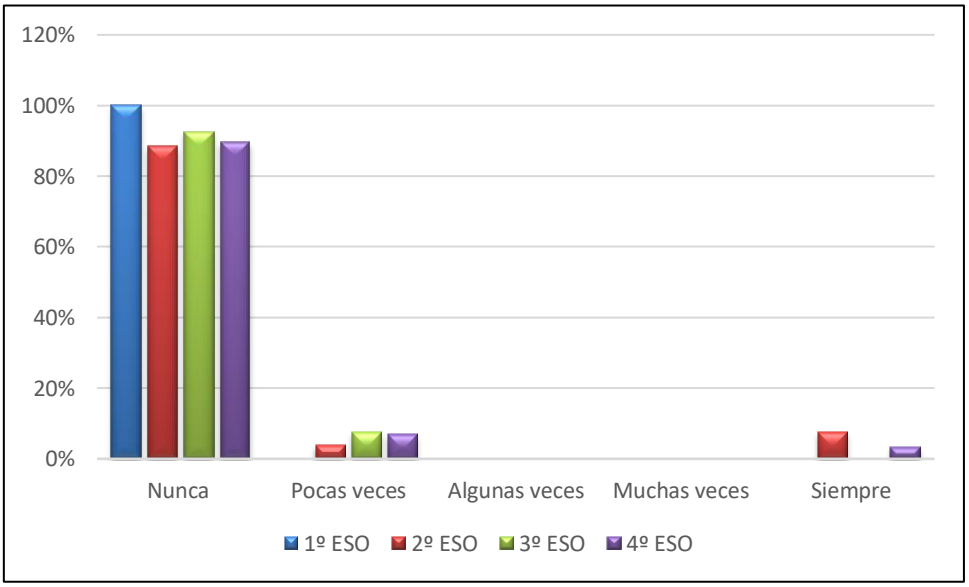

*Figura 293.*Ítem. 11. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

12. ¿Has acosado a alguien para aislarle de sus contactos en las redes sociales?

Tabla 183. *Ítem. 12. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	96%	100%	93%
2	Pocas veces	0%	4%	0%	7%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	0%	0%	0%

Tabla 184. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han acosado a alguien para aislarle de sus contactos en las redes sociales.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,04	0,196	1	2
3º ESO	1	0	1	1
4º ESO	1,07	0,258	1	2

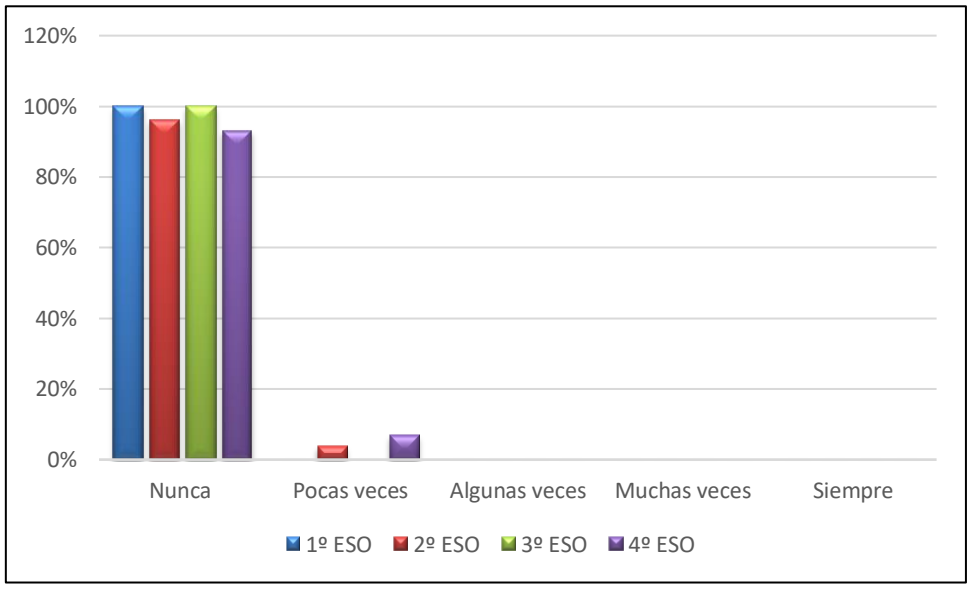

*Figura 294.*Ítem. 12. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

13. ¿Has chantajeado a cambio de no divulgar información íntima vía teléfono y/o Internet?

Tabla 185. *Ítem. 13. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	96%	85%	93%	97%
2	Pocas veces	4%	12%	7%	3%
3	Algunas veces	0%	0%	0%	0%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	4%	0%	0%

Tabla 186. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han chantajeado a cambio de no divulgar información íntima vía teléfono y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,04	0,192	1	2
2º ESO	1,27	0,827	1	5
3º ESO	1,07	0,267	1	2
4º ESO	1,03	0,186	1	2

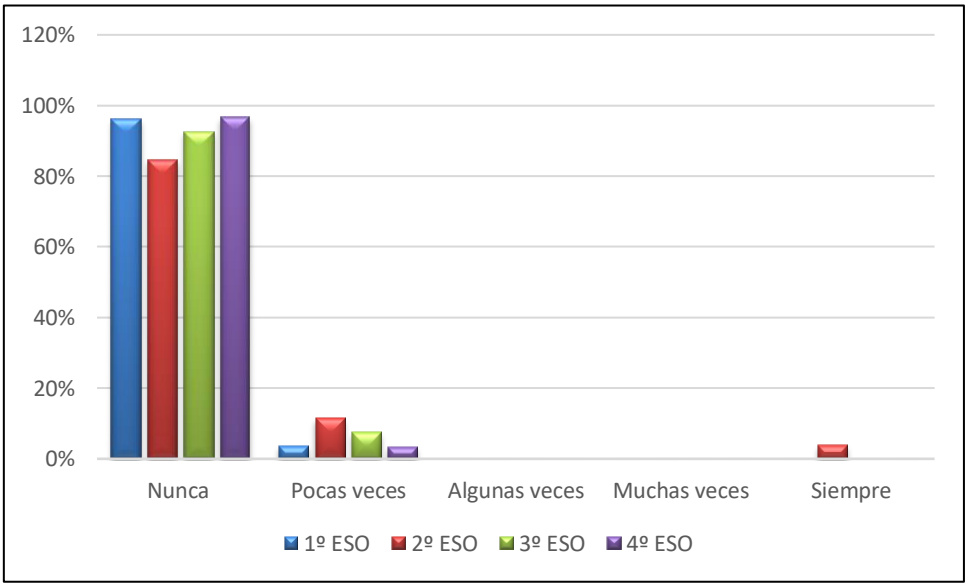

*Figura 295.*Ítem. 13. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

14. ¿Has amenazado de muerte a alguien a través de teléfono móvil y/o Internet?

Tabla 187. *Ítem. 14. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	96%	92%	100%	93%
2	Pocas veces	4%	4%	0%	3%
3	Algunas veces	0%	0%	0%	3%
4	Muchas veces	0%	0%	0%	0%
5	Siempre	0%	4%	0%	0%

Tabla 188. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han amenazado de muerte a alguien a través de teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,04	0,192	1	2
2º ESO	1,19	0,801	1	5
3º ESO	1	0	1	1
4º ESO	1,10	0,409	1	3

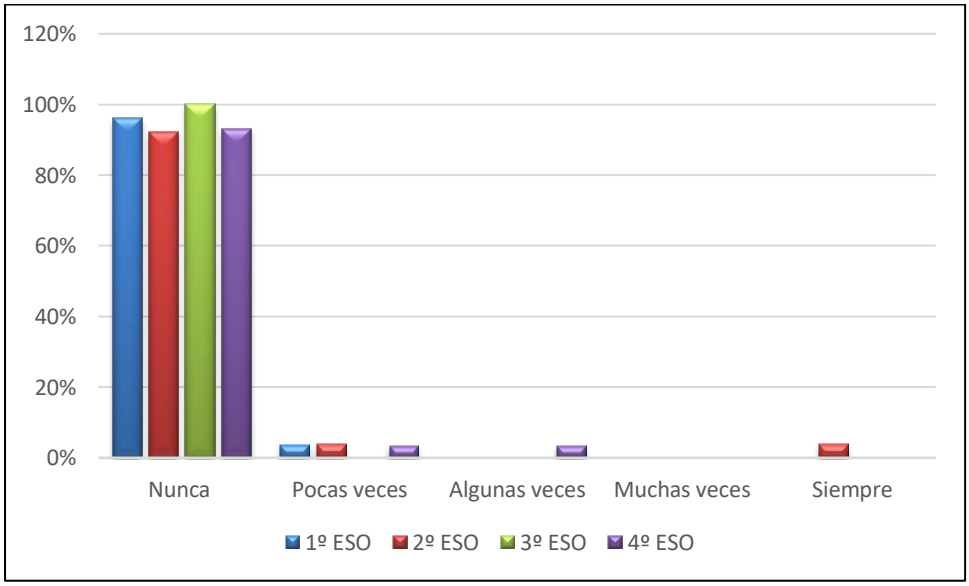

*Figura 296.*Ítem. 14. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

15. ¿Has difundido y/o difamado con rumores para hacer daño vía teléfono móvil y/o Internet?

Tabla 189. *Ítem. 15. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	78%	85%	93%	93%
2	Pocas veces	19%	8%	4%	7%
3	Algunas veces	4%	4%	0%	0%
4	Muchas veces	0%	0%	4%	0%
5	Siempre	0%	4%	0%	0%

Tabla 190. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han difundido y/o difamado con rumores para hacer daño vía teléfono móvil y/o Internet.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,26	0,526	1	3
2º ESO	1,31	0,884	1	5
3º ESO	1,15	0,602	1	4
4º ESO	1,07	0,258	1	2

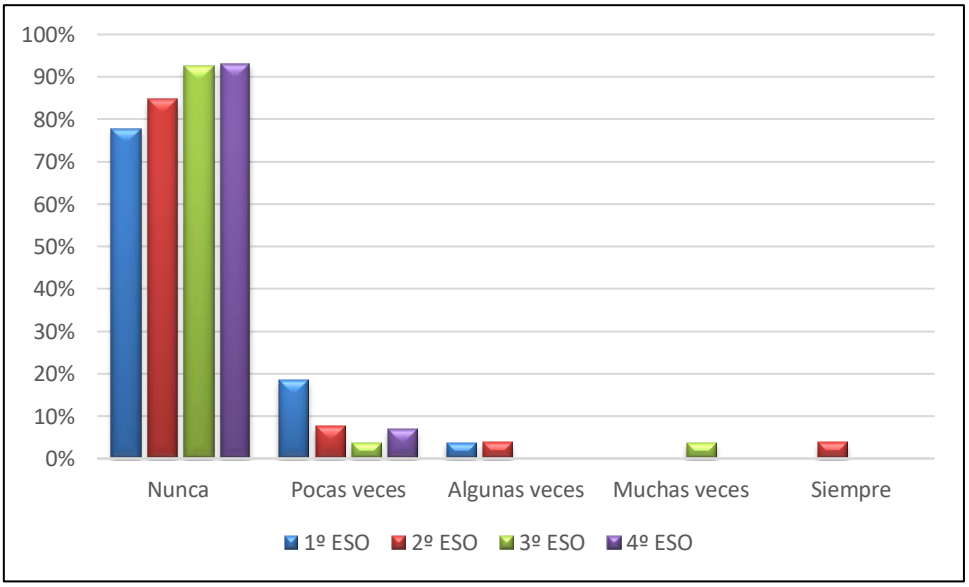

*Figura 297.*Ítem. 15. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

16. ¿Has contactado con un adulto que se ha ganado tu confianza en las redes sociales?

Tabla 191. *Ítem. 16. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	96%	77%	93%	97%
2	Pocas veces	4%	4%	0%	3%
3	Algunas veces	0%	8%	4%	0%
4	Muchas veces	0%	4%	0%	0%
5	Siempre	0%	8%	4%	0%

Tabla 192. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han contactado con un adulto que se ha ganado tu confianza en las redes sociales.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,04	0,192	1	2
2º ESO	1,62	1,267	1	5
3º ESO	1,22	0,847	1	5
4º ESO	1,03	0,186	1	2

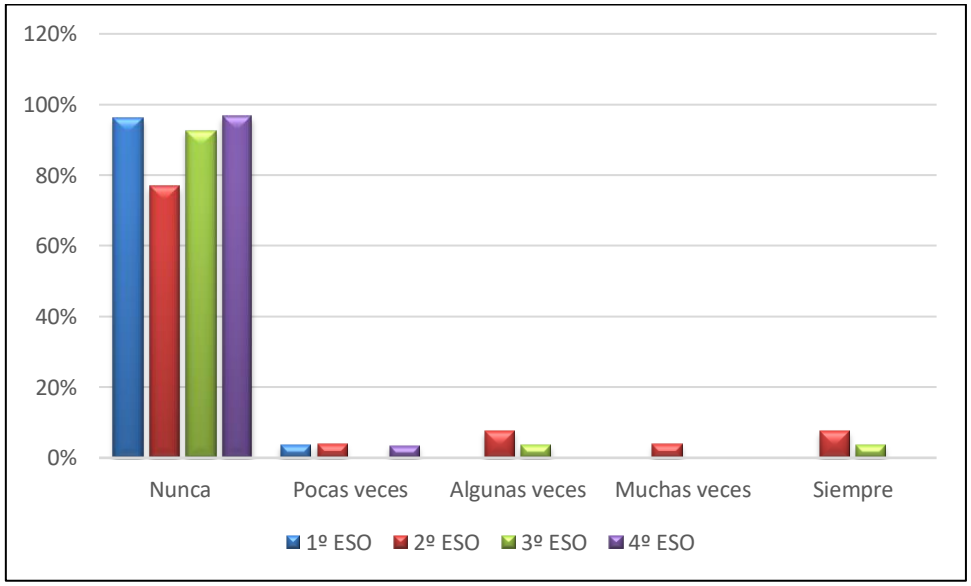

*Figura 298.*Ítem. 16. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

17. ¿Controlas los amigos/as en redes sociales, mensajes, WhatsApp, etc., de tu pareja?

Tabla 193. *Ítem. 17. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	85%	73%	67%	79%
2	Pocas veces	15%	15%	19%	7%
3	Algunas veces	0%	12%	4%	10%
4	Muchas veces	0%	0%	7%	0%
5	Siempre	0%	0%	4%	3%

Tabla 194. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han controlado los amigos/as en redes sociales, mensajes, WhatsApp, etc., de su pareja.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,15	0,362	1	2
2º ESO	1,38	0,697	1	3
3º ESO	1,63	1,115	1	5
4º ESO	1,41	0,946	1	5

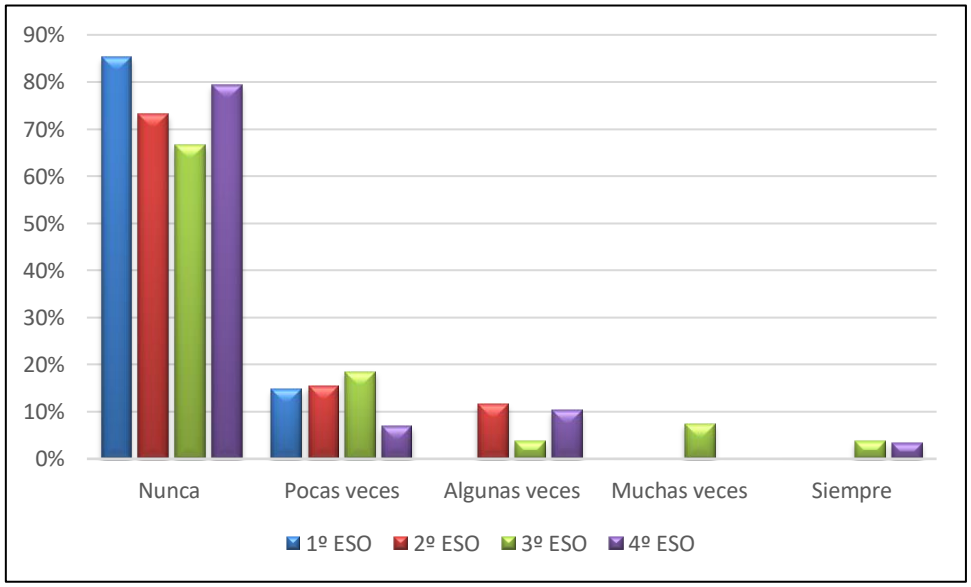

Figura 299. Ítem. 17. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

18. ¿Has pedido a tu pareja que retire fotos o comentarios de redes sociales, WhatsApp, etc.?

Tabla 195. *Ítem. 18. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	81%	73%	93%	90%
2	Pocas veces	15%	8%	4%	7%
3	Algunas veces	4%	12%	0%	3%
4	Muchas veces	0%	8%	0%	0%
5	Siempre	0%	0%	4%	0%

Tabla 196. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han pedido a su pareja que retire fotos o comentarios de redes sociales, WhatsApp, etc.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,22	0,506	1	3
2º ESO	1,54	0,989	1	4
3º ESO	1,19	0,786	1	5
4º ESO	1,14	0,441	1	3

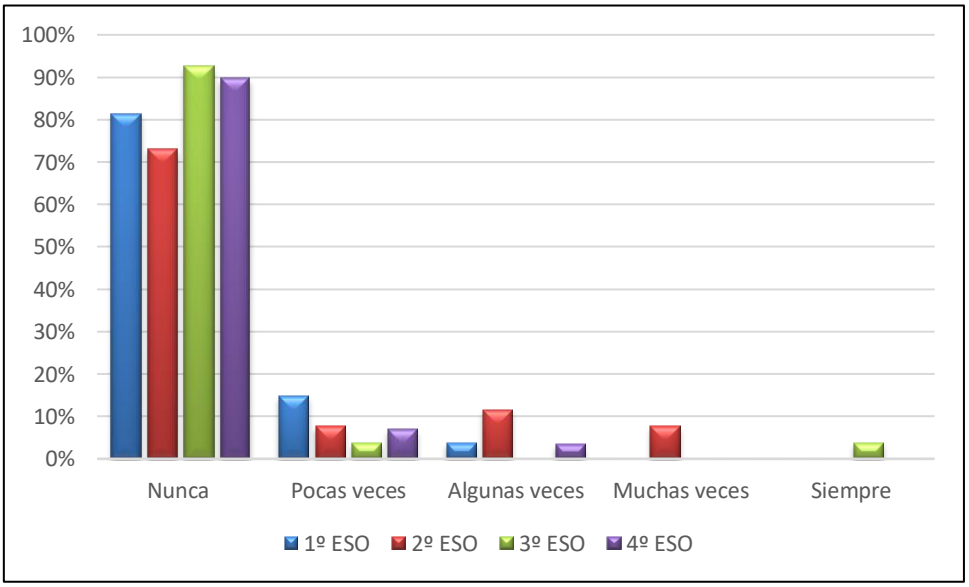

*Figura 300.*Ítem. 18. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

19. ¿Has pedido a tu pareja que suprima o borre a amigos/as en redes sociales, etc.?

Tabla 197. *Ítem. 19. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	93%	81%	85%	100%
2	Pocas veces	7%	8%	7%	0%
3	Algunas veces	0%	8%	4%	0%
4	Muchas veces	0%	0%	4%	0%
5	Siempre	0%	4%	0%	0%

Tabla 198. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han pedido a su pareja que suprima o borre a amigos/as en redes sociales, etc.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1,07	0,267	1	2
2º ESO	1,38	0,941	1	5
3º ESO	1,26	0,712	1	4
4º ESO	1	0	1	1

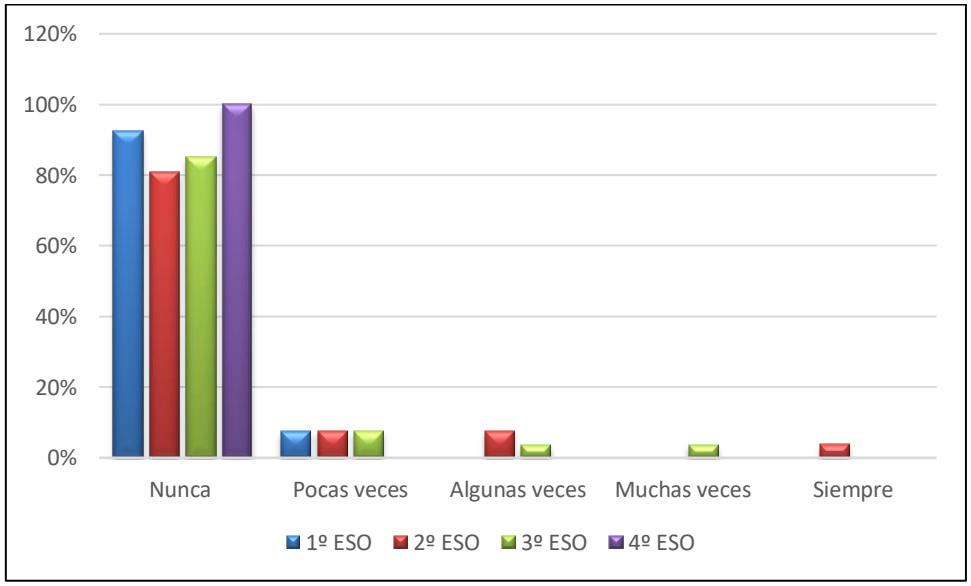

*Figura 301.*Ítem. 19. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

20. ¿Has obligado a tu pareja a realizar comportamientos de tipo sexual a través de la webcam?

Tabla 199. *Ítem. 20. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.*

Nº	Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
1	Nunca	100%	88%	100%	97%
2	Pocas veces	0%	0%	0%	0%
3	Algunas veces	0%	4%	0%	0%
4	Muchas veces	0%	4%	0%	0%
5	Siempre	0%	4%	0%	3%

Tabla 200. *Descriptivos de la frecuencia con la que los menores participantes de 1º a 4º de la ESO del instituto Sanchis y Vilaplana han obligado a tu pareja a realizar comportamientos de tipo sexual a través de la webcam.*

Escala Frecuencia tipo Likert (de 1 a 5)	M	DT	Min	Max
1º ESO	1	0	1	1
2º ESO	1,35	1,018	1	5
3º ESO	1	0	1	1
4º ESO	1,14	0,743	1	5

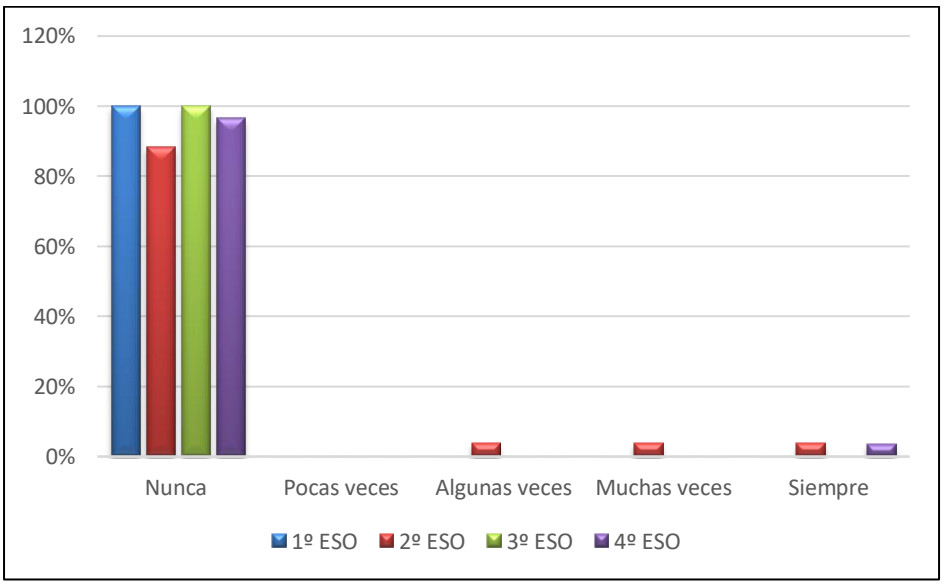

*Figura 302.*Ítem. 20. Contestaciones alumnos de 1º a 4º ESO del IES Sanchis y Vilaplana.

En la tabla 201 y figura 303, podemos apreciar que, de los 109 menores participantes, 47 chicos y 62 chicas, respectivamente, de los cursos 1º a 4º de la ESO de instituto Sanchis y Vilaplana, con relación a la pregunta de a quién comunicarían los hechos o conductas reseñados en los ítems 1 a 20, ambos inclusive, en el caso de observarlos y/o protagonizarlos, en primer lugar, la mayoría contestaron que lo participarían a sus padres, en segundo lugar, lo pondrían en conocimiento de sus compañeros a excepción de los de 1º de la ESO.

En este orden de cosas, en tercer lugar, la mayoría de los participantes de los cursos de la ESO lo comunicarían a sus profesores y por último lugar a nadie.

Tabla 201. *Resultados sobre a quién comunicarían los observadores, víctimas y/o victimarios, en su caso, alguno de los hechos o conductas mencionados (Sanchis y Vilaplana).*

	Instituto Sanchis y Vilaplana			
Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Compañeros	14%	23%	31%	24%
Padres	59%	54%	51%	55%
Profesores	17%	17%	14%	16%
A nadie	10%	6%	3%	5%

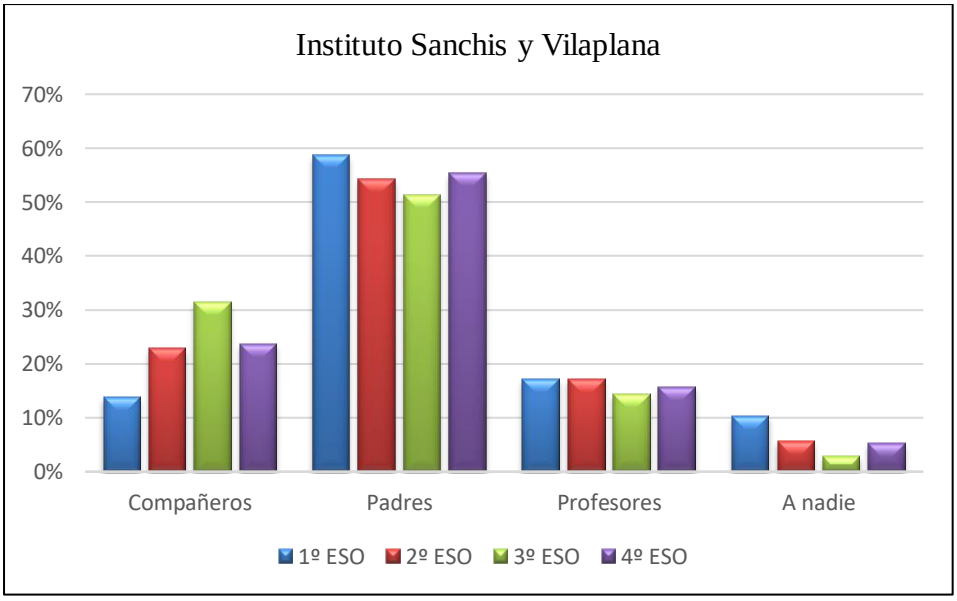

Figura 303. Comparativa de resultados de 1º a 4º de la ESO Sanchis y Vilaplana (tabla 201).

A continuación, en las figuras 304 a 307, podemos observar por cursos de la ESO del instituto Sanchis y Vilaplana los resultados porcentuales obtenidos en las contestaciones a la pregunta mencionada por parte de los menores que han participado en este estudio criminológico social.

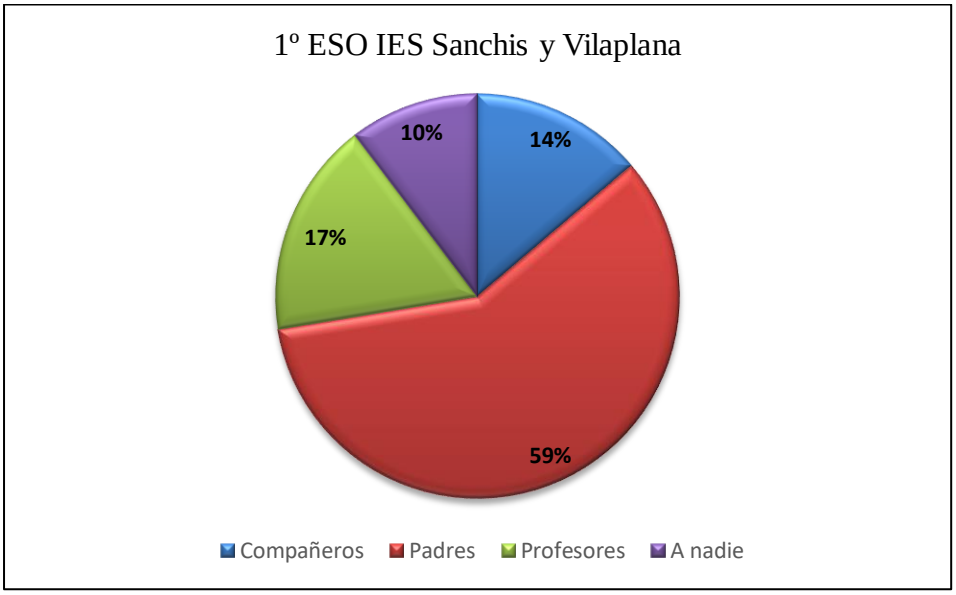

Figura 304. 1º ESO IES Sanchis y Vilaplana: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

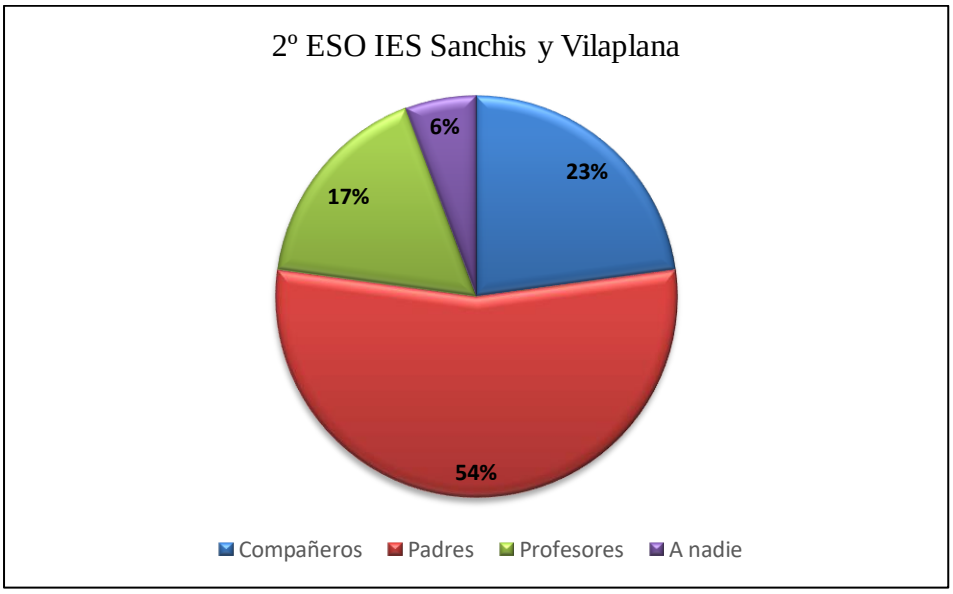

Figura 305. 2º ESO IES Sanchis y Vilaplana: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

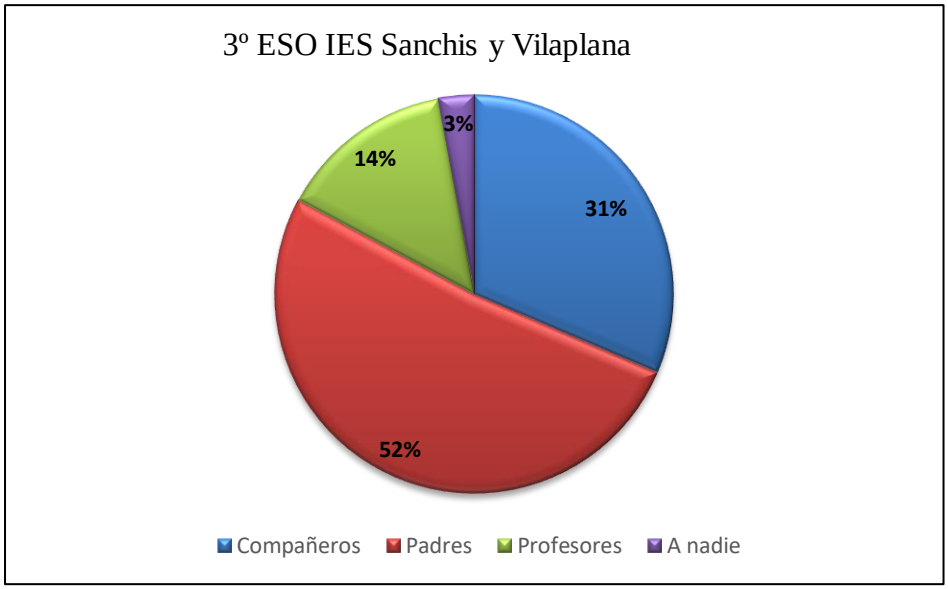

Figura 306. 3º ESO IES Sanchis y Vilaplana: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

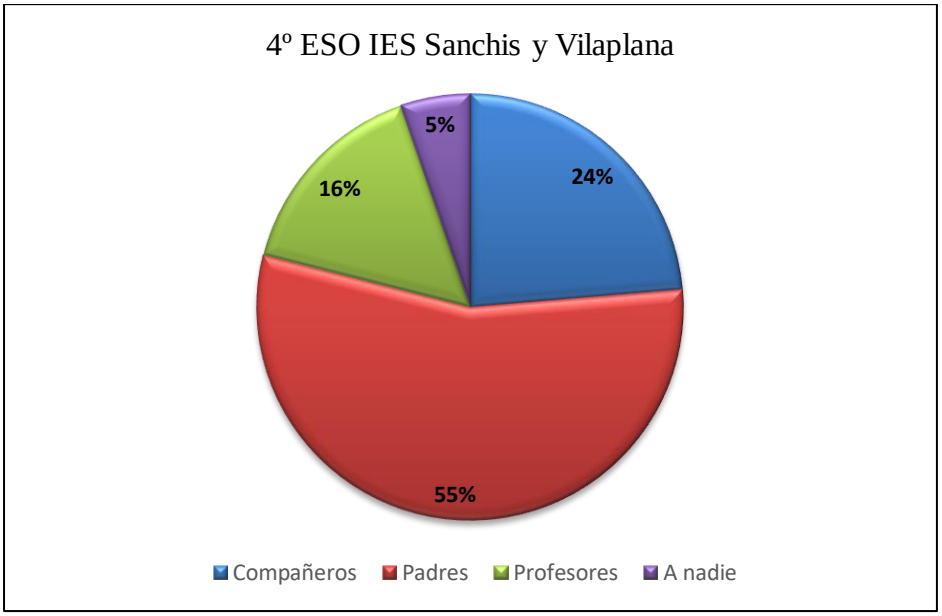

Figura 307. 4º ESO IES Sanchis y Vilaplana: En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿a quién lo comunicarías?

Por otra parte, en lo atinente a los resultados arrojados respecto a la pregunta sobre qué actividades preventivas propondrían los participantes frente a hechos o conductas de ciberacoso, y que se han plasmado en la tabla 202 y en las figuras 308 a 312, respectivamente, podemos destacar que los alumnos del IES Sanchis y Vilaplana de la ESO, en general, optaría mayoritariamente en primer lugar por denunciarlo a la policía antes que comunicar los hechos o conductas referenciados a personas adultas, salvo los

alumnos de 2º de la ESO.

Seguidamente, podemos observar que, en tercer lugar, la totalidad de los participantes de la ESO han seleccionado la opción de pedir ayuda (17-25%).

Por último, tenemos que destacar que, respecto a la opción de respuesta de mediación con el ciberacosador, los resultados obtenidos oscilan del 2% al 9%, constituyendo una evidencia de que, en general, el alumnado de la ESO participante no cree en esta figura para prevenir, abordar y resolver conflictos con el ciberacosador, dando más preferencia los alumnos de 1º y 3º de la ESO a ignorar el ciberacoso que a mediar en el conflicto con el ciberacosador.

Tabla 202. *Resultados sobre las propuestas que hacen los menores participantes para evitar hechos o conductas de ciberacoso (Sanchis y Vilaplana).*

	Instituto Sanchis y Vilaplana			
Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Comunicar adultos	33%	33%	26%	27%
Denunciar a la policía	35%	22%	35%	31%
Ignorar ciberacoso	8%	5%	6%	2%
Mediar con el ciberacosador	2%	9%	2%	4%
Pedir ayuda	17%	24%	24%	25%
Otras	4%	7%	7%	12%

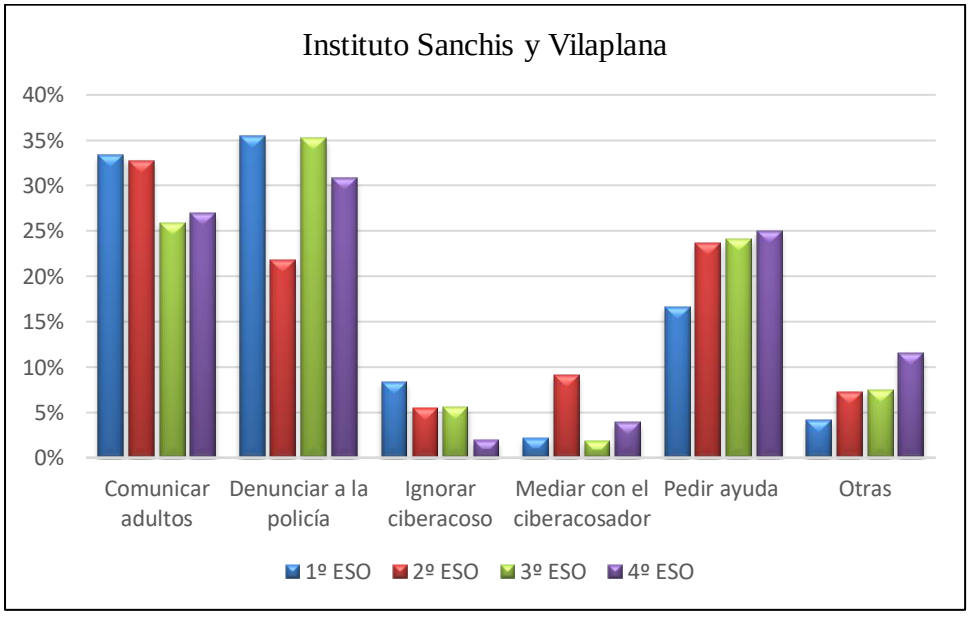

Figura 308. Comparativa de resultados 1º a 4º de la ESO Instituto Sanchis y Vilaplana (tabla 202).

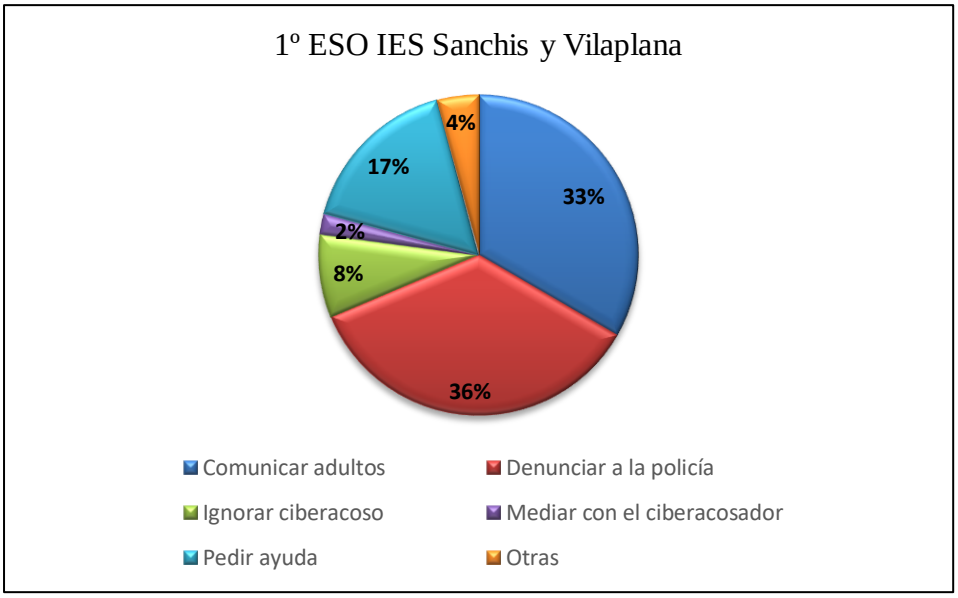

Figura 309. -1º ESO Sanchis y Vilaplana: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

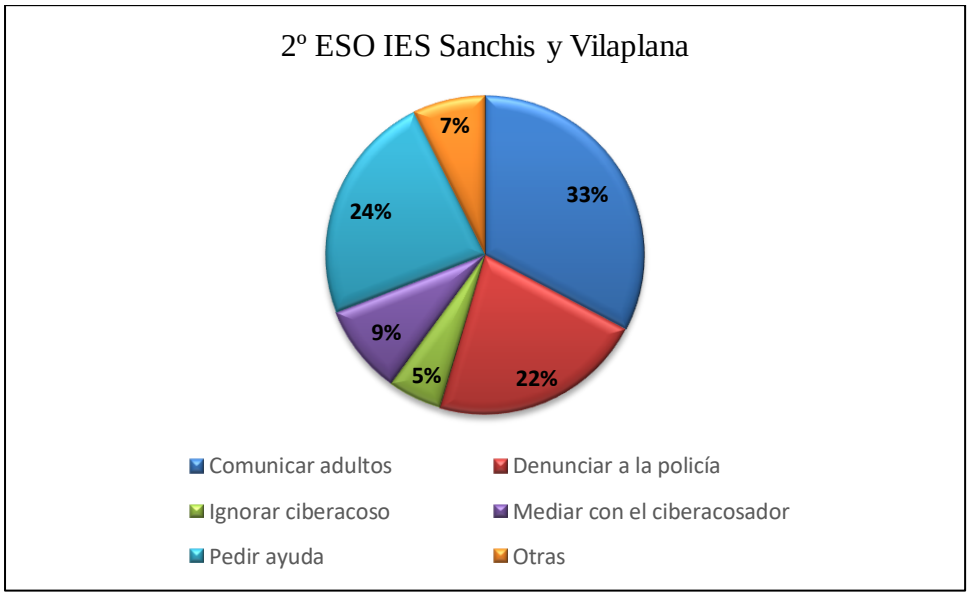

Figura 310. -2º ESO Sanchis y Vilaplana: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

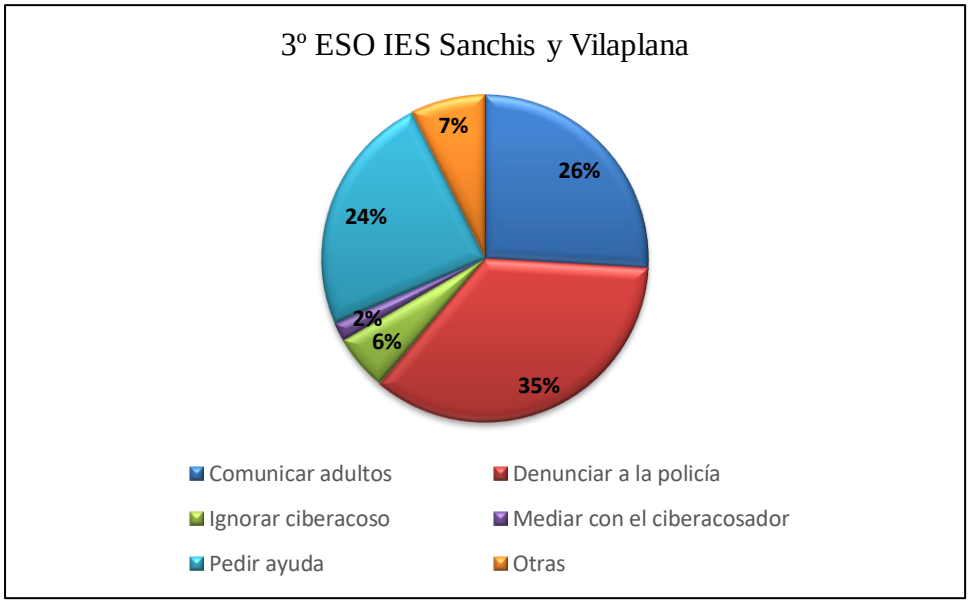

Figura 311. -3º ESO Sanchis y Vilaplana: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

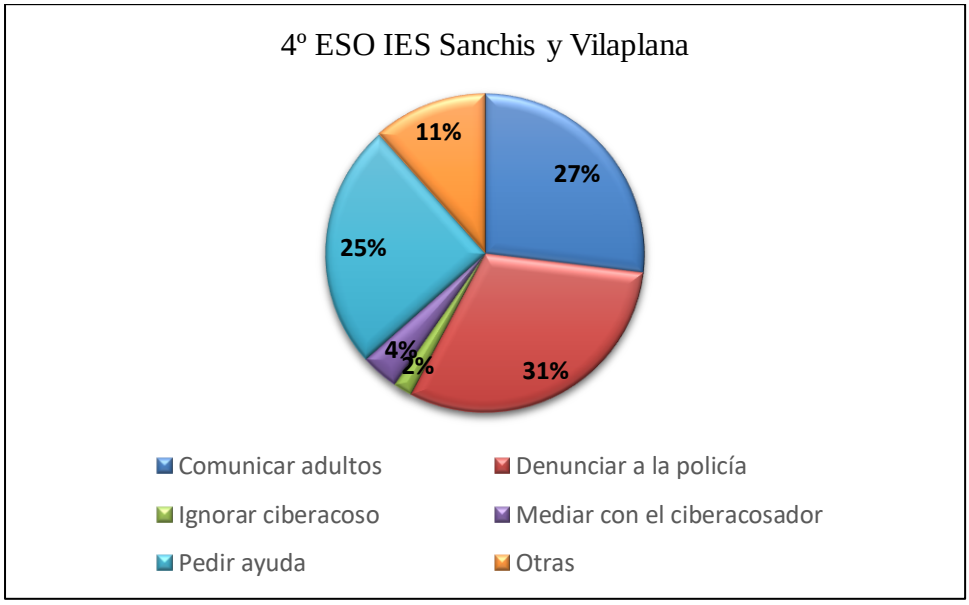

Figura 312. -4º ESO Sanchis y Vilaplana: ¿qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

IV.1.1. Resultados ponderados Colegio N. Sª Consolación.

A continuación, en las tablas 203 a 206, así como en la figura 313, respectivamente se exponen las puntuaciones totales obtenidas en los hechos o conductas reseñados de los ítems número 1 al 20, respectivamente, de los cursos 1º a 4º de la ESO del Colegio Nuestra Señora de la Consolación y a las que se les ha aplicado un valor o factor de ponderación multiplicador que va desde el número 1 hasta el número 5, en función del riesgo de

estimado.

Tabla 203. *Resultados ponderados (ítems 1-20) 1º ESO Colegio N. Sª de la Consolación.*

Puntuaciones totales ítems (1-20)	526	11	3	0	0	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	526	22	9	0	0	
Total ponderado						**557**

Tabla 204. *Resultados ponderados (ítems 1-20) 2º ESO Colegio N. Sª de la Consolación.*

Puntuaciones totales ítems (1-20)	509	23	6	2	0	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	509	46	18	8	0	
Total ponderado						**581**

Tabla 205. *Resultados ponderados (ítems 1-20) 3º ESO Colegio N. Sª de la Consolación.*

Puntuaciones totales ítems (1-20)	508	37	13	1	1	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	508	74	39	4	5	
Total ponderado						**630**

Tabla 206. *Resultados ponderados (ítems 1-20) 4º ESO Colegio N. Sª de la Consolación.*

Puntuaciones totales ítems (1-20)	494	30	14	1	1	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	494	60	42	4	5	
Total ponderado						**605**

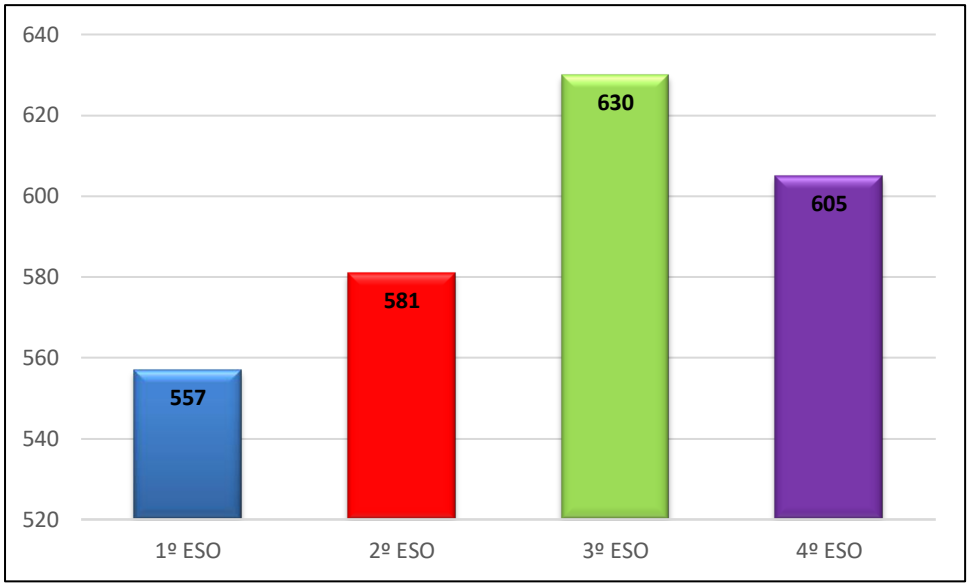

Figura 313. Resultados ponderados (ítems 1-20) 1º a 4º ESO Colegio N. Sª Consolación.

Posteriormente, procedemos a la suma del resultado total ponderado que hemos obtenido de las tablas 203 a 206, respectivamente, arrojando un resultado total de 2373 puntos.

A continuación, comprobamos que el resultado obtenido, se encuentra en el rango de puntuación de nivel de riesgo (2000-2400) de la tabla 13 que contempla el baremo de niveles de riesgo generalizado o global para los cursos de 1º a 4º de la ESO de ser víctima o victimario, en su caso, de la cibercriminalidad social.

Según el rango de clasificación referenciado, la valoración policial de riesgo (VPR, en adelante) es no apreciada y la probabilidad generalizada de ser víctima o victimario, en su caso, es muy baja siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

Por otra parte, si observamos los resultados obtenidos individualmente para los cursos de 1º a 4º de la ESO, podemos comprobar en la tabla 12 que se encuentran en los siguientes rangos de puntuación de nivel de riesgo:

-1º de la ESO con un resultado de 557, se encuentra en el rango de puntuación de nivel de riesgo (400-600) cuya VPR es baja y la probabilidad individualizada de ser víctima o victimario, en su caso, es baja también, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-2º de la ESO con un resultado de 581, se encuentra en el rango de puntuación de nivel de riesgo (400-600) cuya VPR es baja y la probabilidad individualizada de ser víctima o victimario, en su caso, es baja también, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-3º de la ESO con un resultado de 630, se encuentra en el rango de puntuación de nivel de riesgo (600-800) cuya VPR es media y la probabilidad individualizada de ser víctima o victimario, en su caso, es media también, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-4º de la ESO con un resultado de 605, se encuentra en el rango de puntuación de nivel de riesgo (600-800) cuya VPR es media y la probabilidad individualizada de ser víctima o victimario, en su caso, es media también, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

IV.1.2. Resultados ponderados Colegio N. Sª Divina Providencia.

En primer lugar, en las tablas 207 a 210, así como en la figura 314, respectivamente se exponen las puntuaciones totales obtenidas en los hechos o conductas reseñados de los ítems número 1 al 20, respectivamente, de los cursos 1º a 4º de la ESO del Colegio Nuestra Señora de la Divina Providencia y a las que se les ha aplicado un valor o factor de ponderación multiplicador que va desde el número 1 hasta el número 5, en función del riesgo de estimado.

Tabla 207. *Resultados ponderados (ítems 1-20) 1º ESO Colegio N. Sª de la Divina Providencia.*

Puntuaciones totales						
ítems (1-20)	598	16	4	1	1	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	598	32	12	4	5	
Total ponderado						**651**

Tabla 208. *Resultados ponderados (ítems 1-20) 2º ESO Colegio N. Sª de la Divina Providencia.*

Puntuaciones totales						
ítems (1-20)	510	17	9	1	3	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	510	34	27	4	15	
Total ponderado						**590**

Tabla 209. *Resultados ponderados (ítems 1-20) 3º ESO Colegio N. Sª de la Divina Providencia.*

Puntuaciones totales						
ítems (1-20)	456	39	15	10	0	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	456	78	45	40	0	
Total ponderado						**619**

Tabla 210. *Resultados ponderados (ítems 1-20) 4º ESO Colegio N. Sª de la Divina Providencia.*

Puntuaciones totales						
ítems (1-20)	440	38	17	0	5	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	440	76	51	0	25	
Total ponderado						**592**

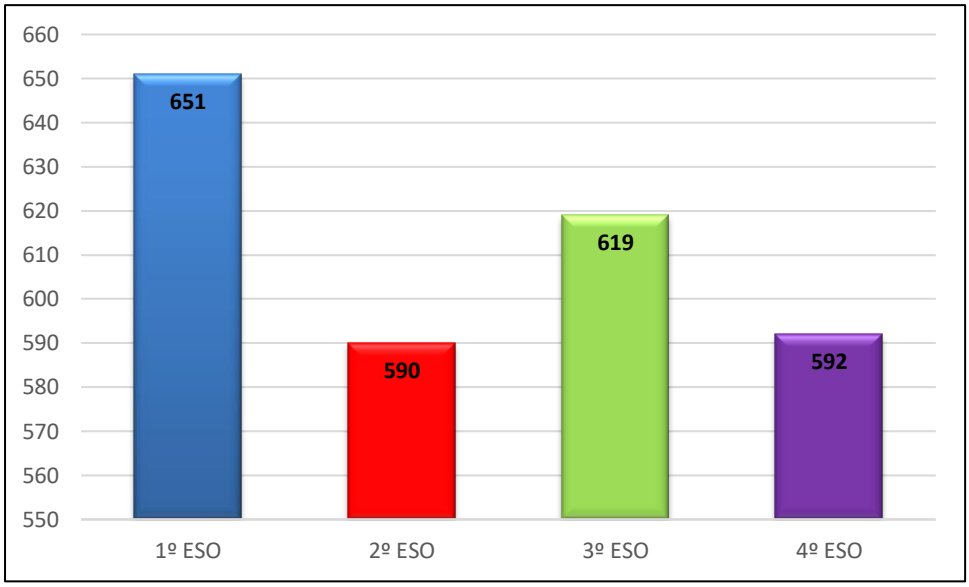

Figura 314. Resultados ponderados (ítems 1-20) 1º a 4º ESO Colegio N. Sª Divina Providencia.

En segundo lugar, procedemos a la suma del resultado total ponderado que hemos obtenido de las tablas 207 a 210, respectivamente, arrojando un resultado total de 2452 puntos.

Seguidamente, comprobamos que el resultado obtenido, se encuentra en el rango de puntuación de nivel de riesgo (2400-2800) de la tabla 13 que contempla el baremo de niveles de riesgo generalizado o global para los cursos de 1º a 4º de la ESO de ser víctima o victimario, en su caso, de la cibercriminalidad social.

Según el rango de clasificación referenciado, la valoración policial de riesgo (VPR, en adelante) y la probabilidad generalizada de ser víctima o victimario, en su caso, es baja siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

Por otra parte, si observamos los resultados obtenidos individualmente para los cursos de 1º a 4º de la ESO, podemos comprobar en la tabla 12 que se encuentran en los siguientes rangos de puntuación de nivel de riesgo:

-1º de la ESO con un resultado de 651, se encuentra en el rango de puntuación de nivel de riesgo (600-800) cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es media, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-2º de la ESO con un resultado de 590, se encuentra en el rango de puntuación de nivel de riesgo (400-600) cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es baja también, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-3º de la ESO con un resultado de 619, se encuentra en el rango de puntuación de nivel de riesgo (600-800) cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es media, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-4º de la ESO con un resultado de 592, se encuentra en el rango de puntuación de nivel de riesgo (400-600) cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es baja, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

IV.1.3. Resultados ponderados IES Leopoldo Querol.

A continuación, en las tablas 211 a 214, así como en la figura 315, respectivamente se exponen las puntuaciones totales obtenidas en los hechos o conductas reseñados de los ítems número 1 al 20, respectivamente, de los cursos 1º a 4º de la ESO del IES Leopoldo Querol y a las que se les ha aplicado un valor o factor de ponderación multiplicador que va desde el número 1 hasta el número 5, en función del riesgo de estimado.

Tabla 211. *Resultados ponderados (ítems 1-20) 1º ESO IES Leopoldo Querol.*

Puntuaciones totales ítems (1-20)	456	24	0	0	0	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	456	48	0	0	0	
Total ponderado						**504**

Tabla 212. *Resultados ponderados (ítems 1-20) 2º ESO IES Leopoldo Querol.*

Puntuaciones totales						
ítems (1-20)	590	24	4	1	1	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	590	48	12	4	5	
Total ponderado						**659**

Tabla 213. *Resultados ponderados (ítems 1-20) 3º ESO IES Leopoldo Querol.*

Puntuaciones totales						
ítems (1-20)	448	54	12	5	1	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	448	108	36	20	5	
Total ponderado						**617**

Tabla 214. *Resultados ponderados (ítems 1-20) 4º ESO IES Leopoldo Querol.*

Puntuaciones totales						
ítems (1-20)	485	29	6	0	0	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	485	58	18	0	0	
Total ponderado						**561**

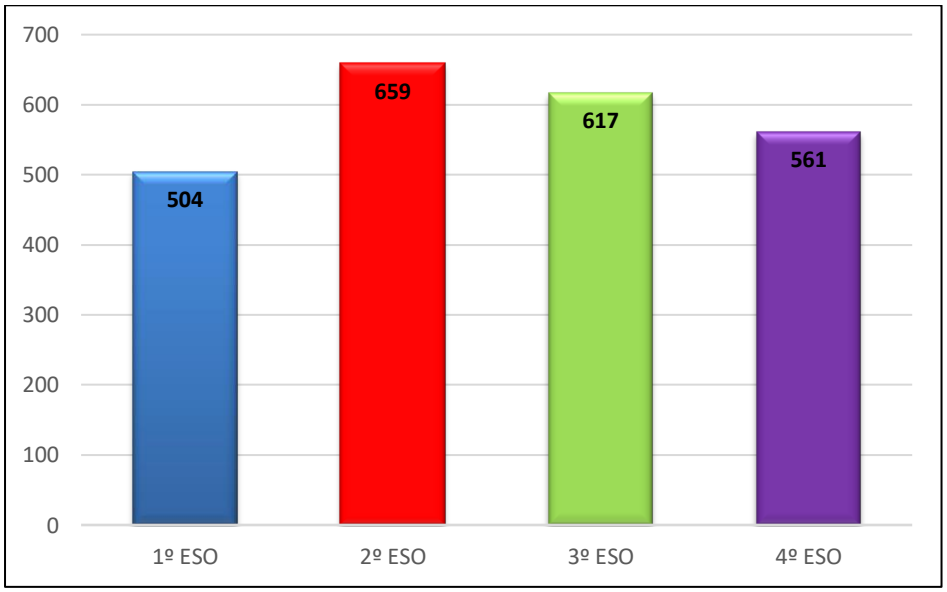

Figura 315. Resultados ponderados (ítems 1-20) 1º a 4º ESO IES Leopoldo Querol.

En segundo lugar, procedemos a la suma del resultado total ponderado que hemos obtenido de las tablas 211 a 214, respectivamente, arrojando un resultado total de 2341 puntos.

Seguidamente, comprobamos que el resultado obtenido, se encuentra en el rango de puntuación de nivel de riesgo (2000-2400) de la tabla 13 que contempla el baremo de niveles de riesgo generalizado o global para los cursos de 1º a 4º de la ESO de ser víctima o victimario, en su caso, de la cibercriminalidad social.

Según el rango de clasificación referenciado, la VPR es no apreciada y la probabilidad generalizada de ser víctima o victimario, en su caso, es muy baja siendo recomendable, igualmente, como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

Por otra parte, si observamos los resultados obtenidos individualmente para los cursos de 1º a 4º de la ESO, podemos comprobar en la tabla 12 que se encuentran en los siguientes rangos de puntuación de nivel de riesgo:

-1º de la ESO con un resultado de 504, se encuentra en el rango de puntuación de nivel de riesgo (400-600) cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es baja, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-2º de la ESO con un resultado de 659, se encuentra en el rango de puntuación de nivel de riesgo (600-800) cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es media, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-3º de la ESO con un resultado de 617, se encuentra en el rango de puntuación de nivel de riesgo (600-800) cuya VPR y probabilidad individualizada de ser víctima o

victimario, en su caso, es media, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-4º de la ESO con un resultado de 561, se encuentra en el rango de puntuación de nivel de riesgo (400-600) cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es baja, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

IV.1.4. Resultados ponderados IES Sanchis y Vilaplana.

Primeramente, en las tablas 215 a 218, así como en la figura 316, respectivamente se exponen las puntuaciones totales obtenidas en los hechos o conductas reseñados de los ítems número 1 al 20, respectivamente, de los cursos 1º a 4º de la ESO del IES Sanchis y Vilaplana y a las que se les ha aplicado un valor o factor de ponderación multiplicador que va desde el número 1 hasta el número 5, en función del riesgo de estimado.

Tabla 215. *Resultados ponderados (ítems 1-20) 1º ESO IES Sanchis y Vilaplana.*

Puntuaciones totales ítems (1-20)	488	44	5	3	0	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	488	88	15	12	0	
Total ponderado						**603**

Tabla 216. *Resultados ponderados (ítems 1-20) 2º ESO IES Sanchis y Vilaplana.*

Puntuaciones totales ítems (1-20)	440	38	19	7	16	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	440	76	57	28	80	
Total ponderado						**681**

Tabla 217. *Resultados ponderados (ítems 1-20) 3º ESO IES Sanchis y Vilaplana.*

Puntuaciones totales ítems (1-20)	479	34	10	13	4	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	479	68	30	52	20	
Total ponderado						**649**

Tabla 218. *Resultados ponderados (ítems 1-20) 4º ESO IES Sanchis y Vilaplana.*

Puntuaciones totales ítems (1-20)	529	34	8	3	6	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	529	68	24	12	30	
Total ponderado						**663**

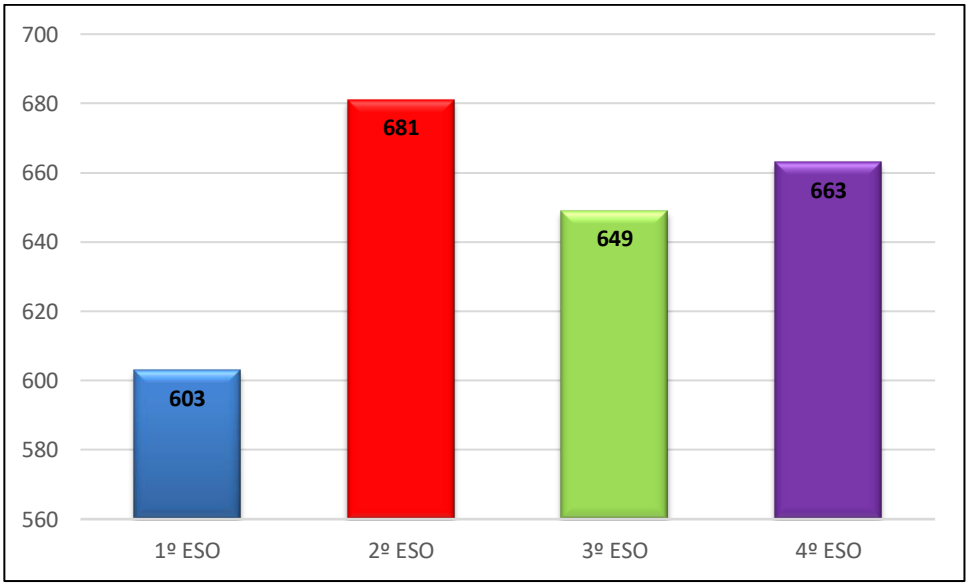

Figura 316. Resultados ponderados (ítems 1-20) 1º a 4º ESO IES Sanchis y Vilaplana.

En segundo lugar, procedemos a la suma del resultado total ponderado que hemos obtenido de las tablas 215 a 218, respectivamente, arrojando un resultado total de 2596 puntos.

Seguidamente, comprobamos que el resultado obtenido, se encuentra en el rango de puntuación de nivel de riesgo (2400-2800) de la tabla 13 que contempla el baremo de

niveles de riesgo generalizado o global para los cursos de 1º a 4º de la ESO de ser víctima o victimario, en su caso, de la cibercriminalidad social.

Según el rango de clasificación referenciado, la VPR y la probabilidad generalizada de ser víctima o victimario, en su caso, es baja siendo recomendable, igualmente, como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

Por otra parte, si observamos los resultados obtenidos individualmente para los cursos de 1º a 4º de la ESO, podemos comprobar en la tabla 12 que se encuentran en los siguientes rangos de puntuación de nivel de riesgo:

-1º de la ESO con un resultado de 603, se encuentra en el rango de puntuación de nivel de riesgo (600-800) cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es media, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-2º de la ESO con un resultado de 681, se encuentra en el rango de puntuación de nivel de riesgo (600-800) cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es media, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-3º de la ESO con un resultado de 649, se encuentra en el rango de puntuación de nivel de riesgo (600-800) cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es media, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-4º de la ESO con un resultado de 663, se encuentra en el rango de puntuación de nivel de riesgo (400-600) cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es media, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

IV.2. Resultados estudio de cibercriminalidad económica.

Casualmente, de la muestra de los cien participantes encuestados, podemos apreciar en la tabla 219 y figura 317, respectivamente, que el 50% son hombres y el 50% son mujeres, y que el rango de edad que más hombres hay es el de 50-55 años, y mujeres en el rango de 45-50 años.

Por el contrario, el rango en el que menos hombres hay es en el de 20-25 años, es decir 0, y mujeres en el rango de 20-25 años y en el de 60-65 años, respectivamente, concretamente, 1.

La media de edad es de 44,31 años. Si la especificamos por género, la media de edad de los participantes que son hombres es de 45,44 años, y la media de edad de las participantes que son mujeres es de 43,18 años.

Tabla 219. *Rango de edades y género de los participantes en el estudio*

Edades	Hombres	Mujeres	Totales
20-25	0	1	1
25-30	4	3	7
30-35	9	7	16
35-40	7	9	16
40-45	3	8	11
45-50	7	10	17
50-55	10	6	16
55-60	6	5	11
60-65	4	1	5
Total	50	50	100

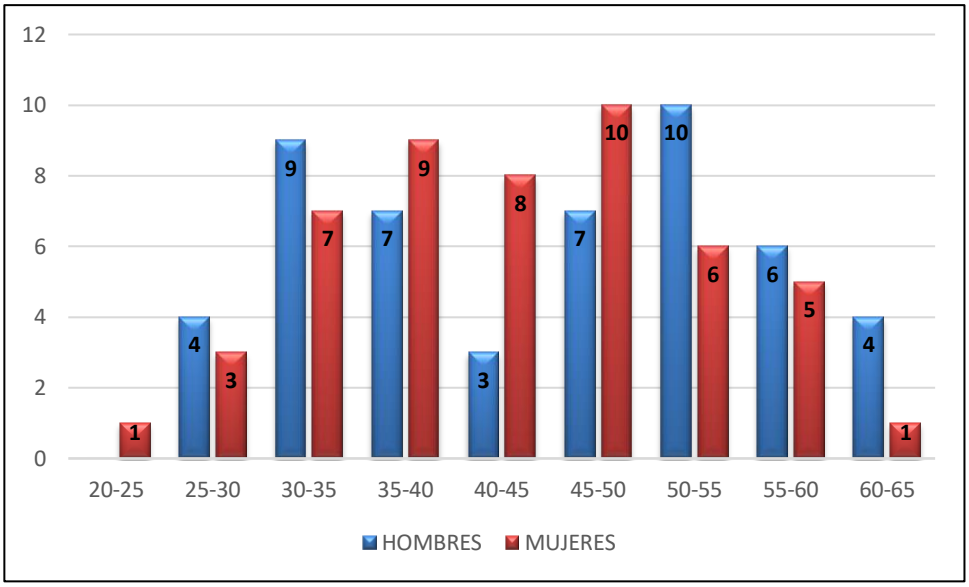

Figura 317. Edad y género de los regentes de establecimientos participantes.

Respecto a la interacción con las TIC de los regentes de los comercios, establecimientos públicos y/o microempresas, en su caso, en la encuesta de victimización económica figuraban en primera instancia, nueve ítems con posibilidad de respuesta "SI o "NO", obteniéndose los resultados que figuran en la tabla 220.

Tabla 220. *Resultados interacción TIC regentes establecimientos y comercios Vinaròs*

Interacción TIC regentes establecimientos y comercios	SI	NO
Tengo ordenador en casa	84	16
Tengo ordenador en negocio o empresa	92	8
Tengo teléfono móvil	100	0
Guardo información personal y/o confidencial del negocio en el teléfono móvil	52	48
Tengo cuenta de correo electrónico con fines comerciales	74	26
Tengo una página web de mi negocio o empresa	54	46
Utilizo programas de mensajería instantánea como Whatsapp	67	33
Utilizo redes sociales con fines comerciales	77	23
Utilizo blogs, foros en internet con fines comerciales	25	75

De los cien regentes encuestados, podemos observar en las figuras 318 hasta la 326, la representación porcentual de los resultados obtenidos, ítem por ítem.

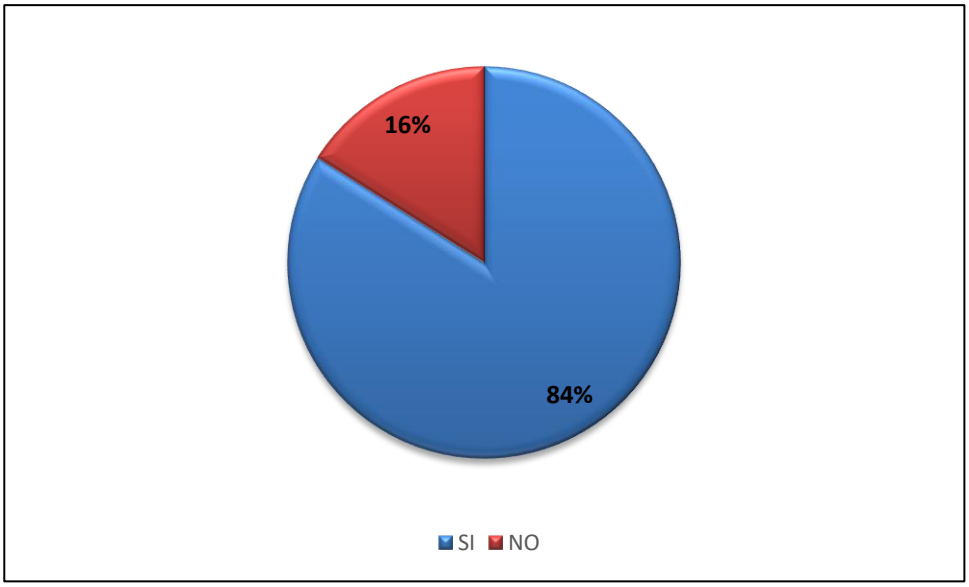

Figura 318. ¿Tiene ordenador en casa?

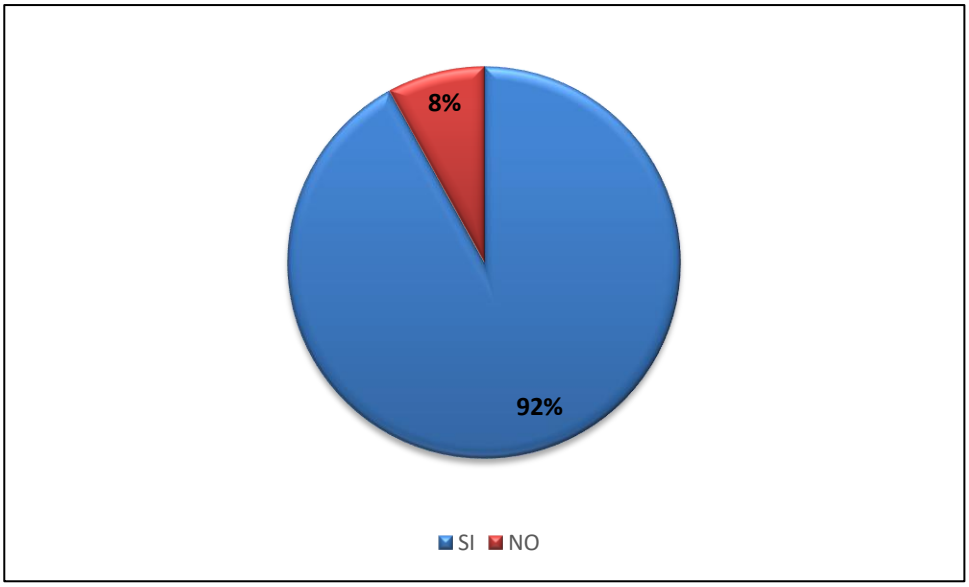

Figura 319.¿Tiene ordenador en su negocio o empresa?

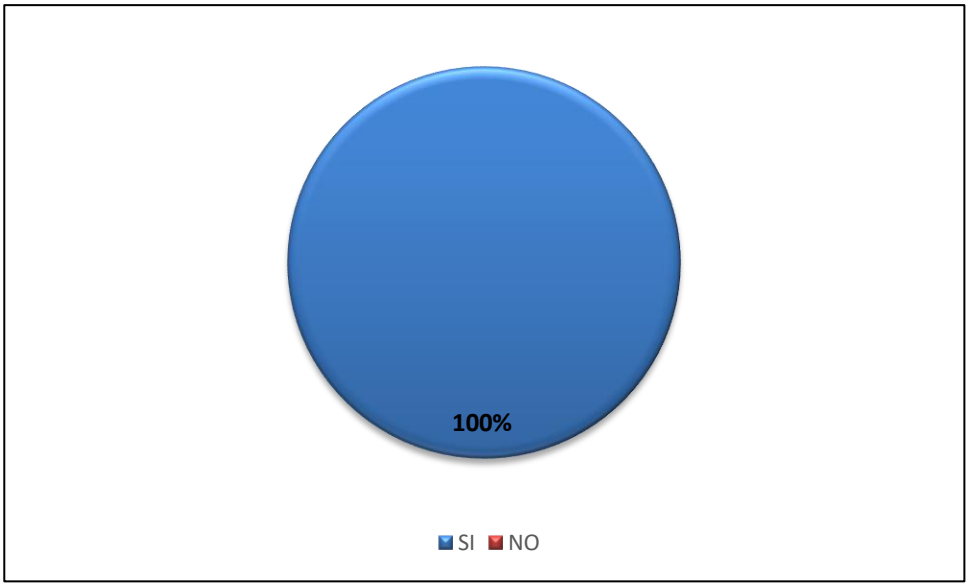

Figura 320. ¿Tiene teléfono móvil?

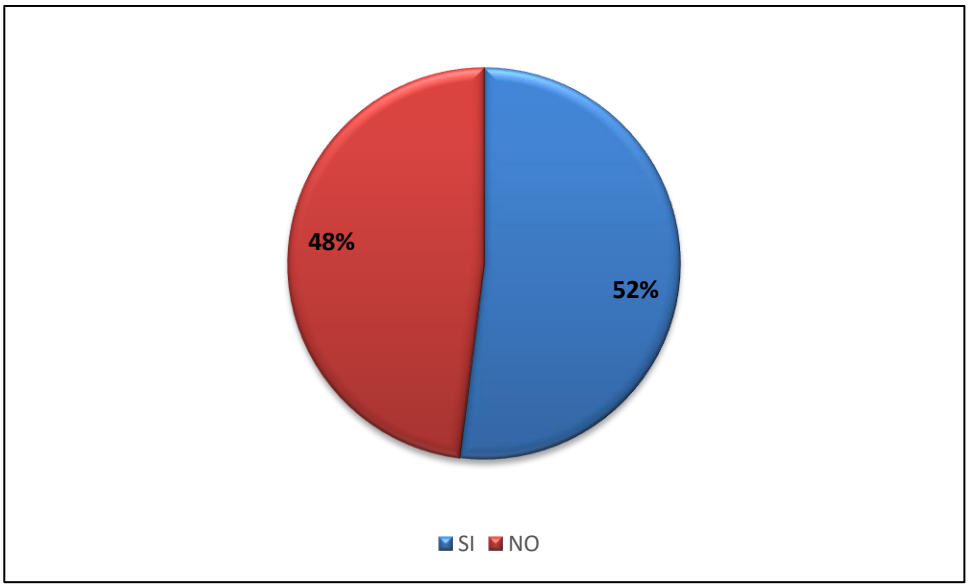

Figura 321. ¿Guarda información personal y/o confidencial de su negocio u empresa en el teléfono móvil?

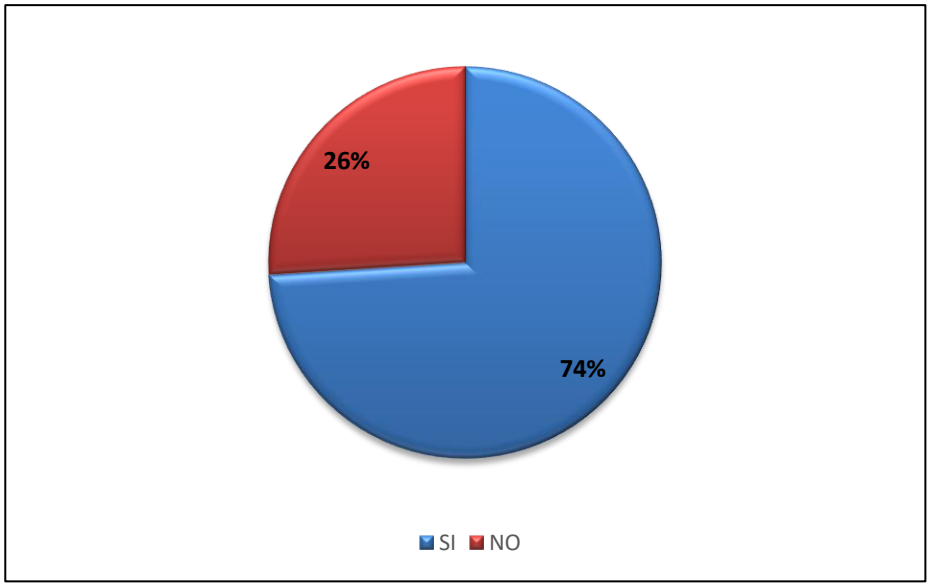

Figura 322. ¿Tiene una cuenta de correo electrónico con fines comerciales?

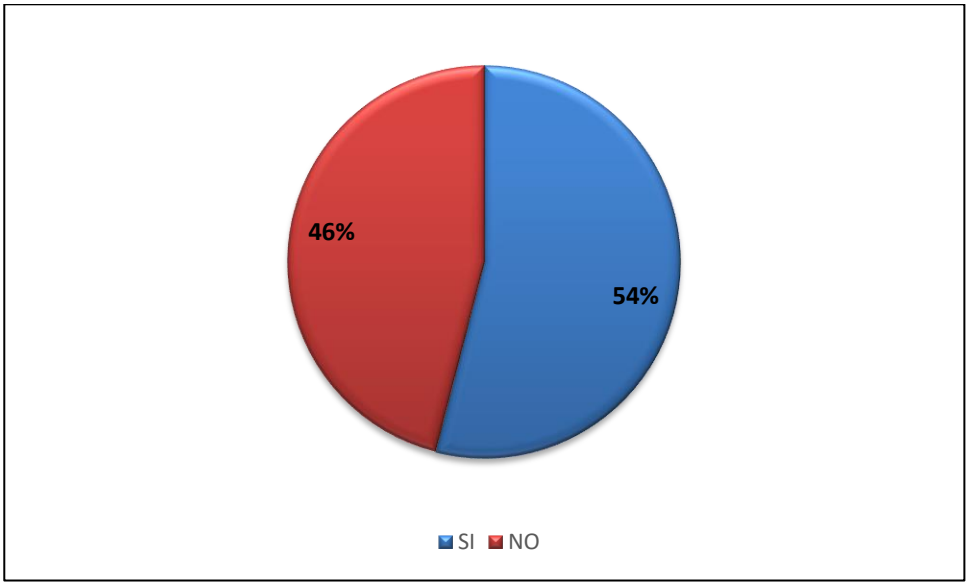

Figura 323.¿Tiene una página web de su negocio o empresa?

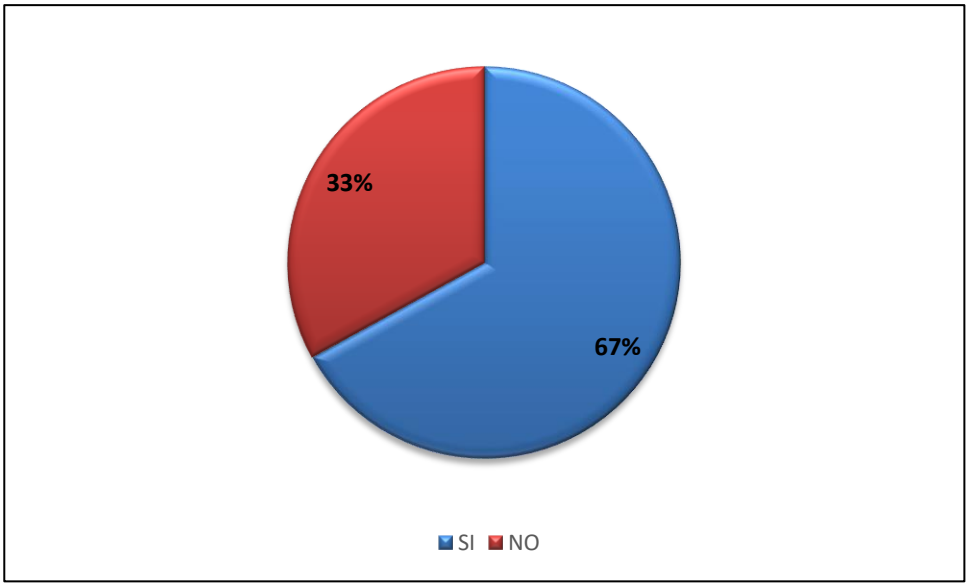

Figura 324. ¿Utiliza programas de mensajería instantánea como WhatsApp, Telegram, etc., con fines comerciales?

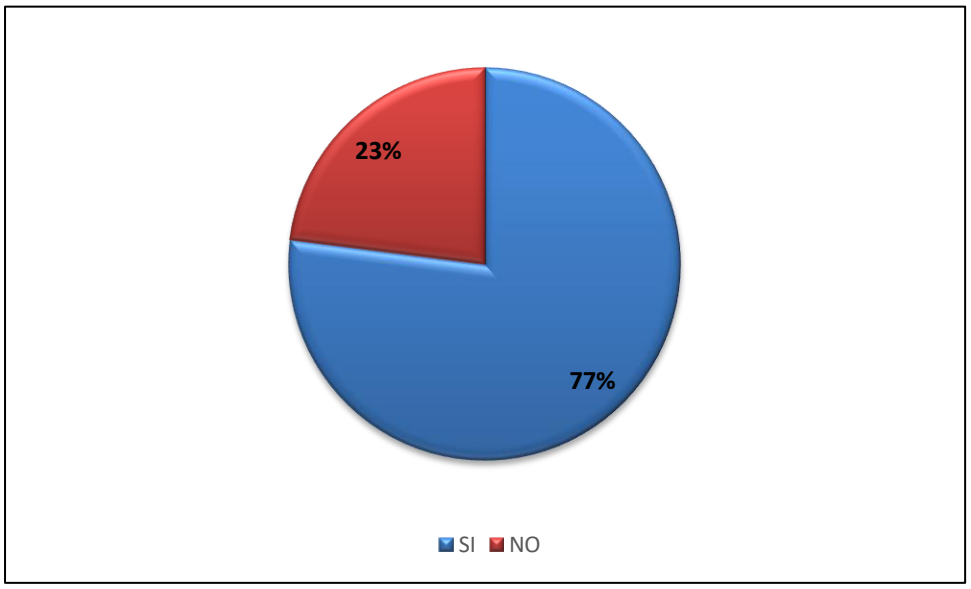

Figura 325. ¿Utiliza redes sociales tales como Facebook, Twitter, etc., con fines comerciales?

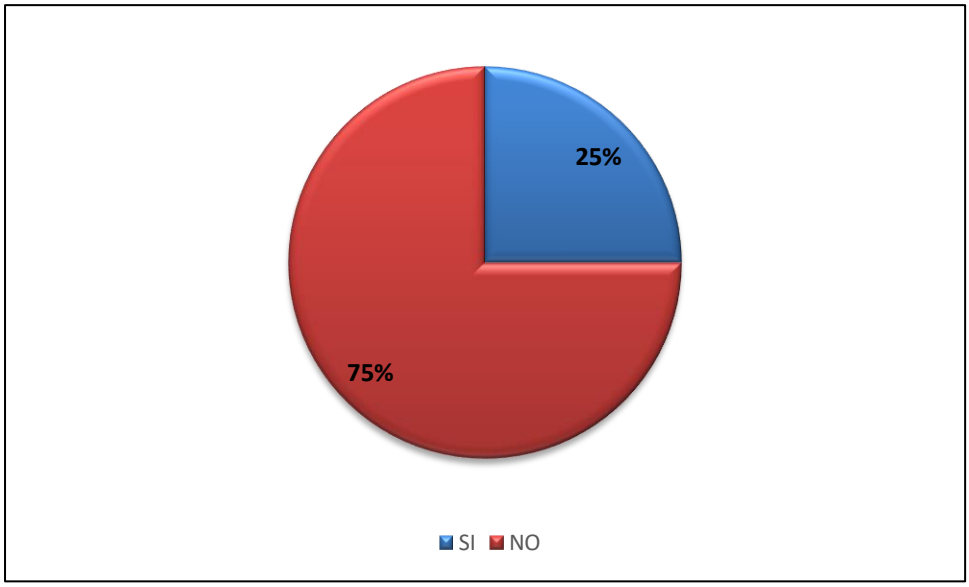

Figura 326. ¿Utiliza blogs, foros en internet con fines comerciales?

Actualmente, existen diversas tecnologías biométricas aplicadas a la ciberseguridad con el fin de proteger la información confidencial de teléfonos móviles, ordenadores, tabletas, etc. A continuación, en la tabla 221 y figuras 327 y 328, respectivamente, se exponen los resultados obtenidos en la encuesta de cibercriminalidad económica con relación al ítem sobre el conocimiento de los regentes de los establecimientos públicos y comercios de la existencia de una serie determinada de tecnologías biométricas, destacando como la que más conocen, con un 84% la huella dactilar, y la que menos con un 6%, la de reconocimiento vascular.

No obstante, podemos observar que hay más participantes que no conocen, en general, las tecnologías biométricas (497 contestaciones negativas) frente a los que sí las conocen (403 contestaciones positivas).

Tabla 221. *Conocimiento de los participantes sobre tecnologías biométricas*

Tipología Tecnologías Biométricas	SI	NO
Huella dactilar	84	16
Reconocimiento facial	68	32
Reconocimiento del iris	58	42
Reconocimiento de la geometría de la mano	25	75
Reconocimiento de la firma	53	47
Reconocimiento de la voz	68	32
Reconocimiento vascular	6	94

Reconocimiento de la escritura	32	68
Otras formas de biometría	9	91
Totales	403	497

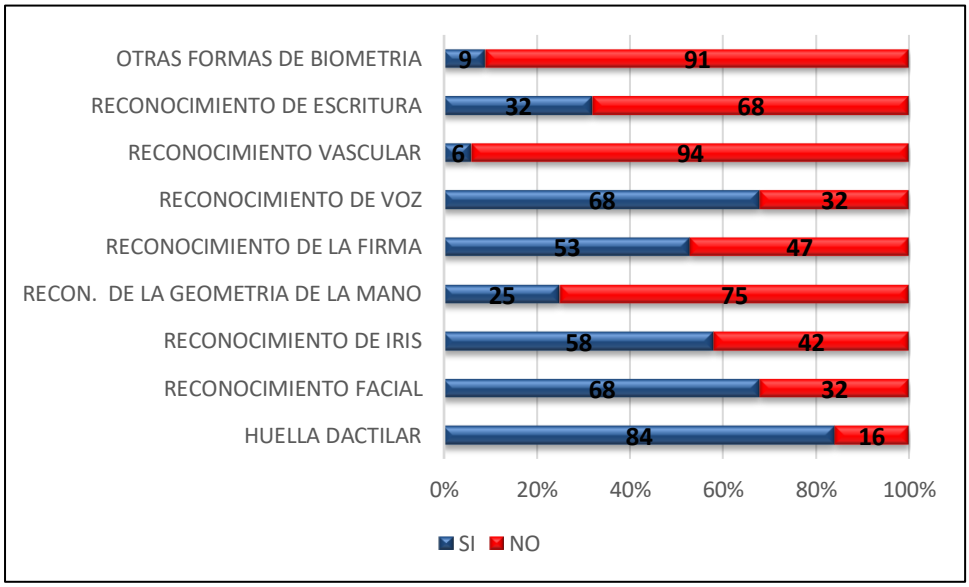

Figura 327. Resultados porcentuales sobre el conocimiento de los participantes de los diversos tipos de tecnologías biométricas.

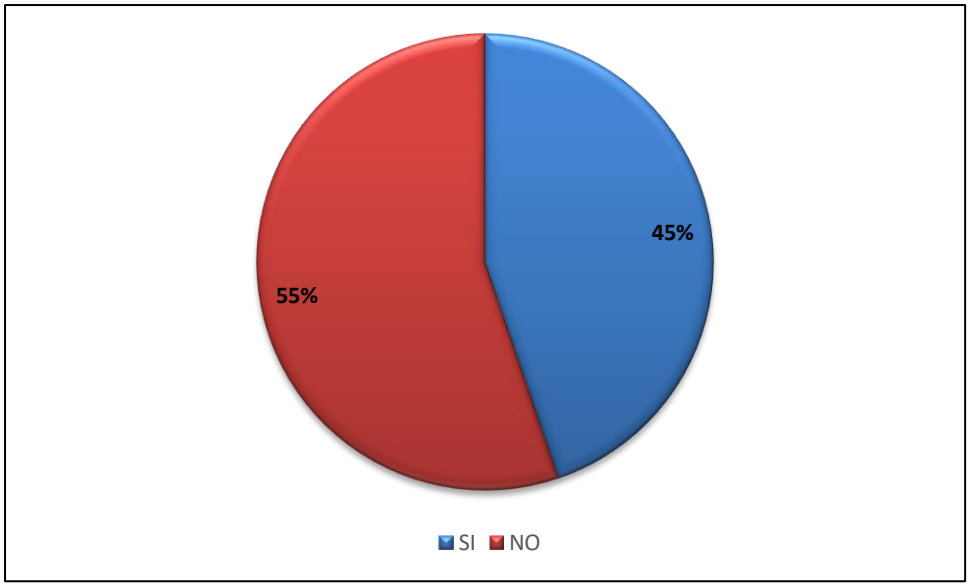

Figura 328. Resultados porcentuales sobre el conocimiento general de los participantes sobre tecnologías biométricas.

Los resultados de la evaluación de ciberriesgos o riesgos de cibervictimización de los regentes de los comercios, establecimientos públicos y microempresas o micropymes, en su caso, con relación a los ítems 1 a 20, respectivamente, han sido los siguientes:

1. ¿Ha perdido alguna vez el teléfono móvil, tableta, ordenador portátil, etc.?

Tabla 222. *Ítem 1. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	65	65%
2	Pocas veces	29	29%
3	Algunas veces	6	6%
4	Muchas veces	0	0%
5	Siempre	0	0%
	TOTALES	100	100%

Tabla 223. *Ítem 1. Descriptivos de la frecuencia con la que los participantes han perdido alguna vez el teléfono, tableta, ordenador portátil, etc*.

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	1,41	0,605	1	3

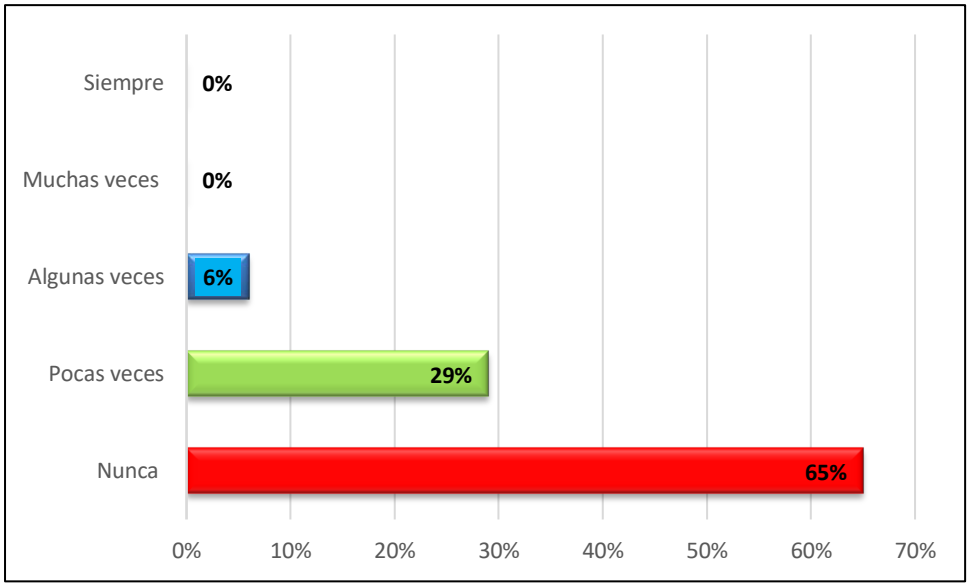

*Figura 329.*Porcentaje de respuestas ítem 1 encuesta VCE[27]

2. ¿Le han sustraído alguna vez el teléfono móvil, tableta, ordenador portátil, etc.?

Tabla 224. *Ítem 2. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	74	74%
2	Pocas veces	22	22%
3	Algunas veces	4	4%
4	Muchas veces	0	0%
5	Siempre	0	0%
	TOTALES	100	100%

Tabla 225.*Ítem 2. Descriptivos de la frecuencia con la que los participantes les han sustraído alguna vez el teléfono móvil, tableta, ordenador portátil, etc.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	1,30	0,541	1	3

[27] VCE: Victimización cibercriminalidad económica.

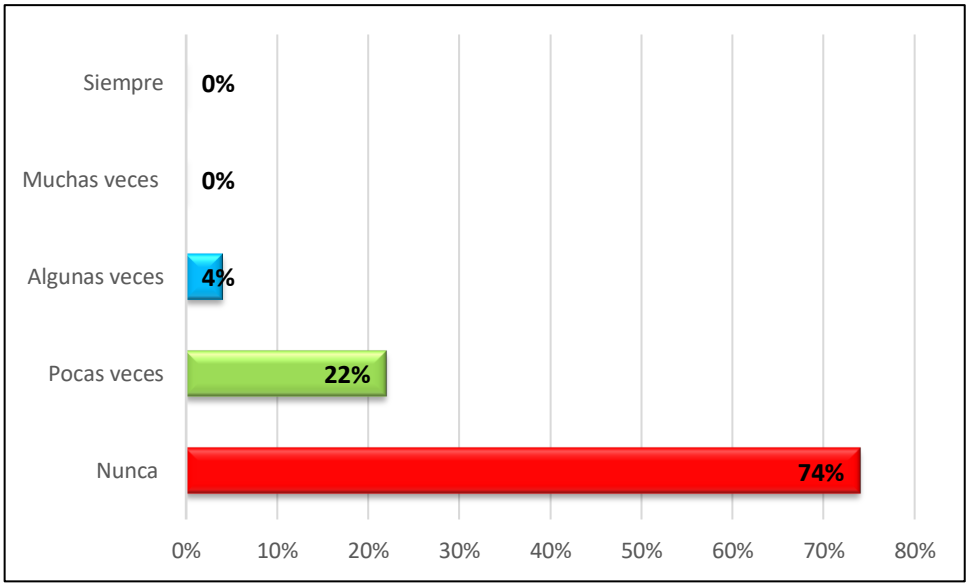

Figura 330. Porcentaje de respuestas ítem 2 encuesta VCE

3. ¿Ha perdido alguna vez un pendrive con información confidencial de su negocio y/o particular de usted?

Tabla 226. *Ítem 3. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	92	92%
2	Pocas veces	5	5%
3	Algunas veces	3	3%
4	Muchas veces	0	0%
5	Siempre	0	0%
	TOTALES	100	100%

Tabla 227. *Ítem 3. Descriptivos de la frecuencia con la que los participantes han perdido alguna vez un pendrive con información confidencial de su negocio y/o particular de éstos.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	1,11	0,399	1	3

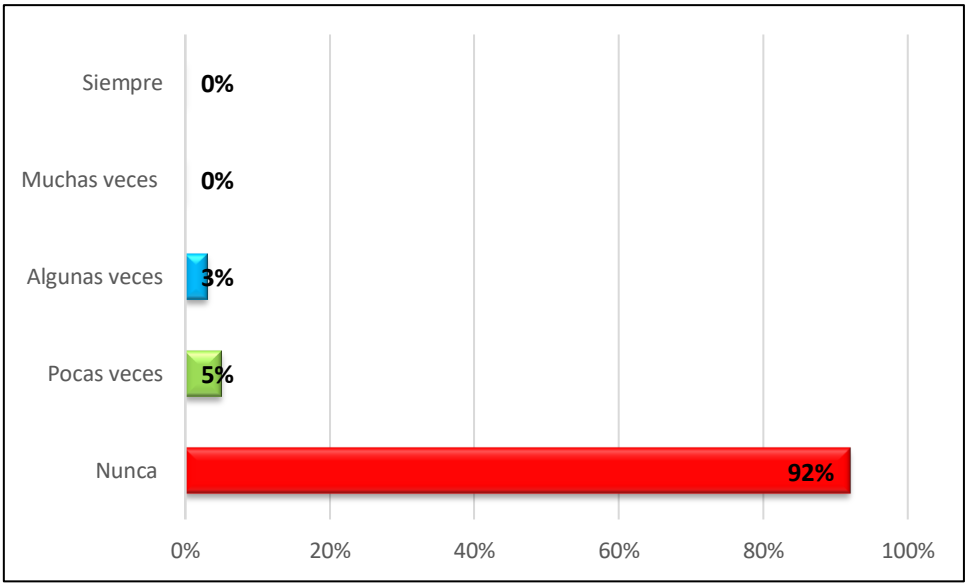

Figura 331. Porcentaje de respuestas ítem 3 encuesta VCE

4. ¿Se le ha infectado alguna vez su ordenador, teléfono móvil, tableta, etc., con algún virus o malware?

Tabla 228. *Ítem 4. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	24	24%
2	Pocas veces	43	43%
3	Algunas veces	26	26%
4	Muchas veces	7	7%
5	Siempre	0	0%
	TOTALES	100	100%

Tabla 229. *Ítem 4. Descriptivos de la frecuencia con la que a los participantes se les ha infectado alguna vez su ordenador, teléfono móvil, tableta, etc., con algún virus o programa maligno.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	2,16	0,873	1	4

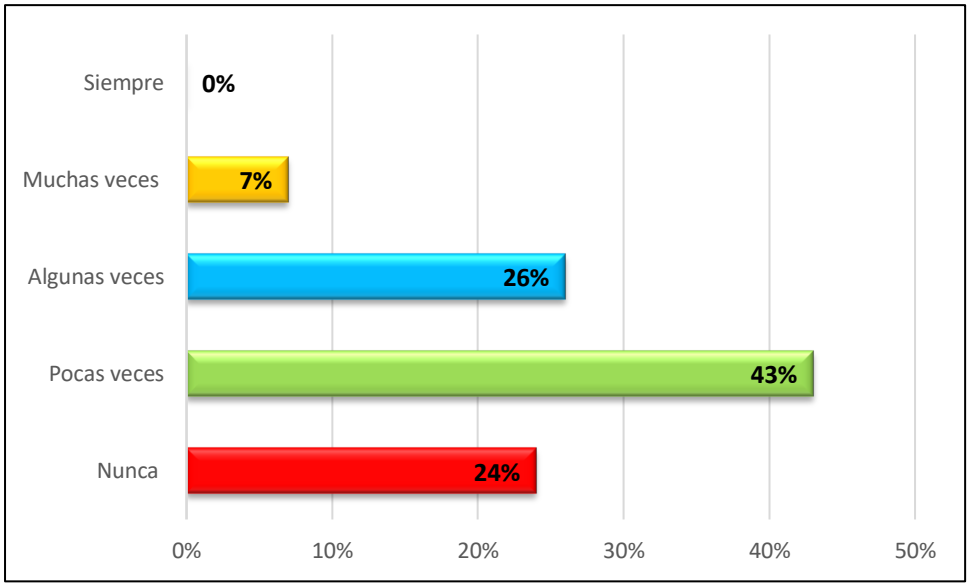

Figura 332. Porcentaje de respuestas ítem 4 encuesta VCE

5. ¿Alguna vez ha perdido archivos de su negocio por infección de malware?

Tabla 230. *Ítem 5. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	74	74%
2	Pocas veces	18	18%
3	Algunas veces	8	8%
4	Muchas veces	0	0%
5	Siempre	0	0%
	TOTALES	100	100%

Tabla 231. *Ítem 5. Descriptivos de la frecuencia con la que los participantes han perdido archivos de su negocio por infección de programas malignos.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	1,34	0,623	1	3

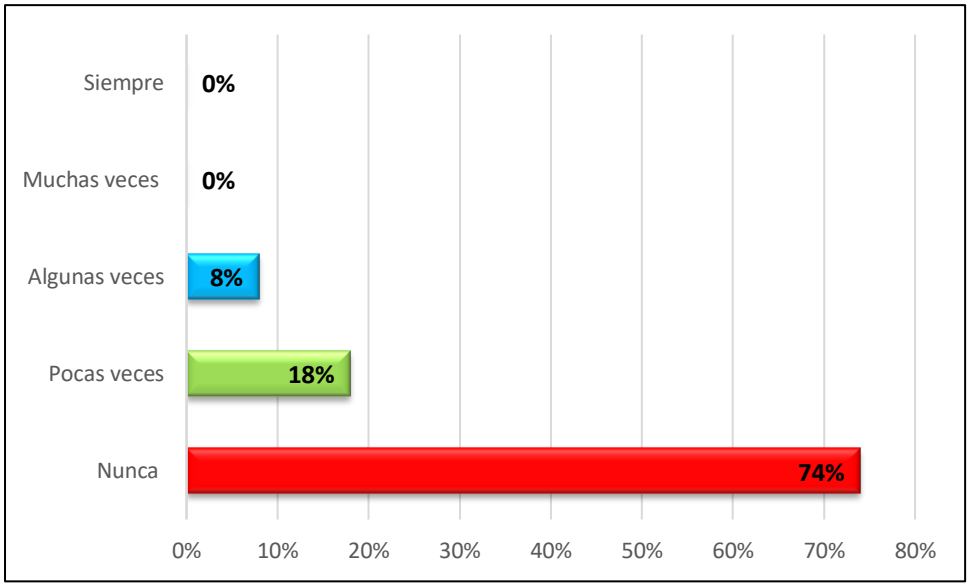

Figura 333. Porcentaje de respuestas ítem 5 encuesta VCE

6. ¿Ha recibido alguna vez mensajes por WhatsApp, correo electrónico, redes sociales, etc., en la que se prometen grandes cantidades de dinero a cambio de pequeñas transferencias relacionadas con la lotería, trabajo, etc.(scam)?

Tabla 232. *Ítem 6. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	39	39%
2	Pocas veces	26	26%
3	Algunas veces	21	21%
4	Muchas veces	13	13%
5	Siempre	1	1%
	TOTALES	100	100%

Tabla 233. *Ítem 6. Descriptivos de la frecuencia con la que los participantes han recibido alguna vez mensajes por WhatsApp, correo electrónico, redes sociales, etc., en la que se prometen grandes cantidades de dinero a cambio de pequeñas transferencias.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	2,11	1,100	1	5

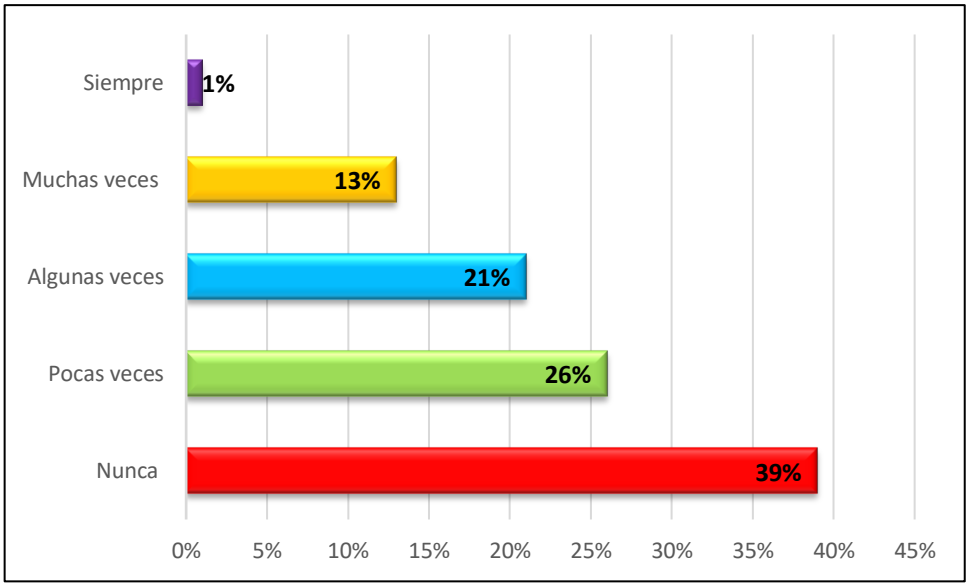

Figura 334. Porcentaje de respuestas ítem 6 encuesta VCE

7. ¿Ha recibido alguna vez masivamente correos electrónicos no deseados de publicidad (spam)?

Tabla 234. *Ítem 7. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	8	8%
2	Pocas veces	17	17%
3	Algunas veces	29	29%
4	Muchas veces	38	38%
5	Siempre	8	8%
	TOTALES	100	100%

Tabla 235. *Ítem 7. Descriptivos de la frecuencia con la que los participantes han recibido alguna vez masivamente correos electrónicos no deseados de publicidad (spam)*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	3,21	1,076	1	5

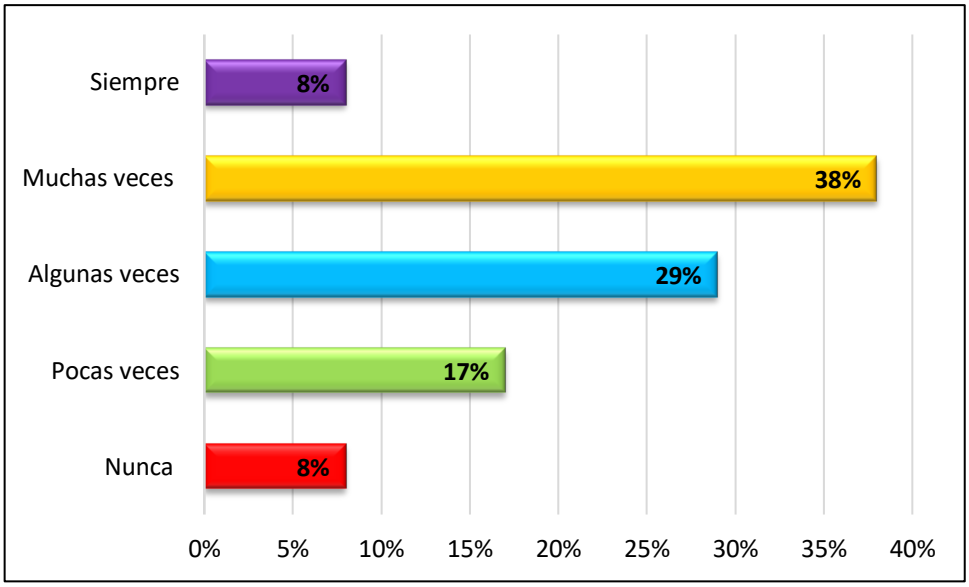

Figura 335. Porcentaje de respuestas ítem 7 encuesta VCE

8. ¿Alguna vez han suplantado la página web, Facebook, etc., de su negocio?

Tabla 236. *Ítem 8. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	95	95%
2	Pocas veces	4	4%
3	Algunas veces	1	1%
4	Muchas veces	0	0%
5	Siempre	0	0%
	TOTALES	100	100%

Tabla 237. *Ítem 8. Descriptivos de la frecuencia con la que a los participantes les han suplantado la página web, Facebook, etc., de su negocio.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	1,06	0,278	1	3

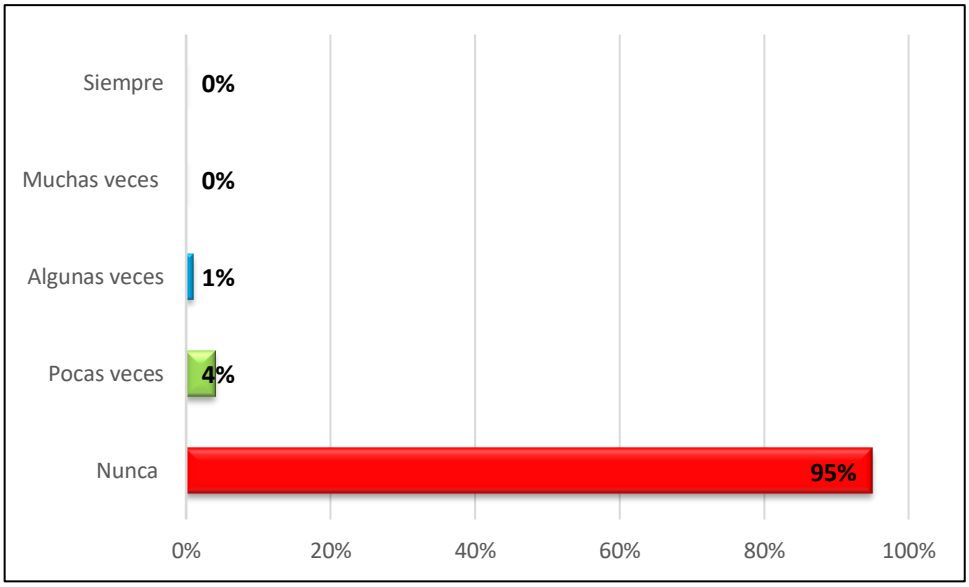

Figura 336. Porcentaje de respuestas ítem 8 encuesta VCE

9. Al contactar telemáticamente con proveedores o clientes, en su caso, ¿le han sustraído contraseñas, datos personales de la tarjeta de crédito y/o cuenta bancaria mediante diferentes técnicas tales como correos electrónicos que llevan a páginas falsas en las que se solicita la introducción de estos datos, o mediante infección por virus?

Tabla 238. *Ítem 9. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	91	91%
2	Pocas veces	7	7%
3	Algunas veces	2	2%
4	Muchas veces	0	0%
5	Siempre	0	0%
	TOTALES	100	100%

Tabla 239. *Ítem. 9. Descriptivos de la frecuencia con la que los participantes al contactar telemáticamente con proveedores o clientes, en su caso, les han sustraído contraseñas, datos personales de la tarjeta de crédito, etc.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	1,11	0,373	1	3

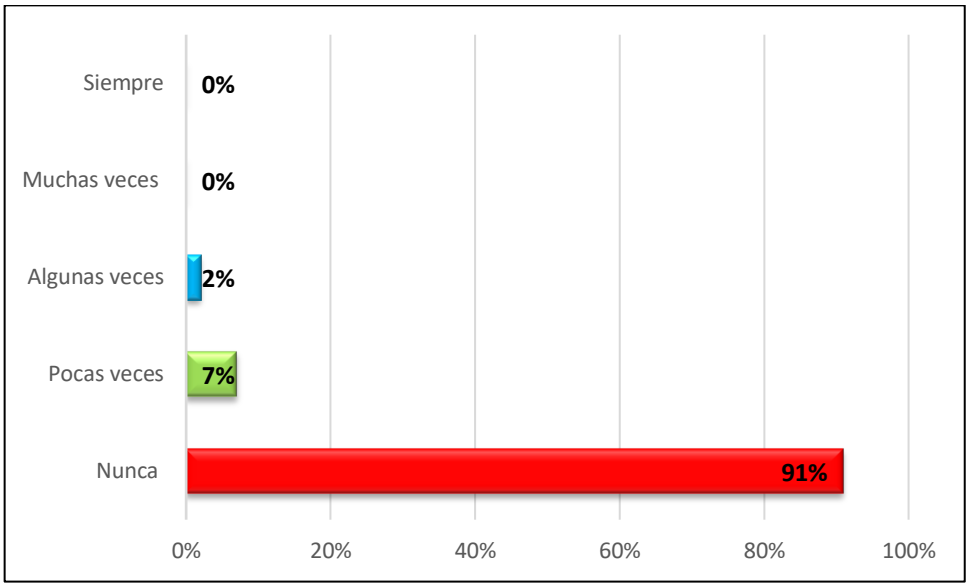

Figura 337. Porcentaje de respuestas ítem 9 encuesta VCE

10. Al efectuar una compraventa en su negocio, ¿alguna vez un cliente ha utilizado una tarjeta de crédito sustraída?

Tabla 240. *Ítem 10. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	81	81%
2	Pocas veces	13	13%
3	Algunas veces	6	6%
4	Muchas veces	0	0%
5	Siempre	0	0%
	TOTALES	100	100%

Tabla 241. *Ítem 10. Descriptivos de la frecuencia con la que los participantes al efectuar una compraventa en su negocio un cliente ha utilizado una tarjeta de crédito sustraída.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	1,25	0,557	1	3

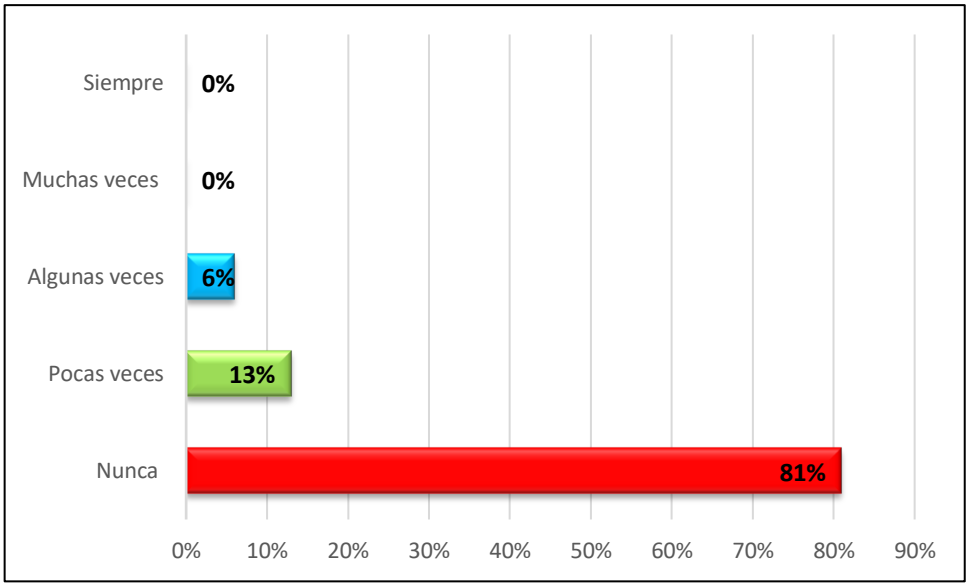

Figura 338. Porcentaje de respuestas ítem 10 encuesta VCE

11. ¿Ha sido víctima de algún tipo de fraude online, extorsión, etc.?

Tabla 242. *Ítem 11. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	81	81%
2	Pocas veces	14	14%
3	Algunas veces	4	4%
4	Muchas veces	1	1%
5	Siempre	0	0%
	TOTALES	100	100%

Tabla 243. *Ítem 11. Descriptivos de la frecuencia con la que los participantes han sido víctimas de algún tipo de fraude online, extorsión, etc.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	1,25	0,575	1	4

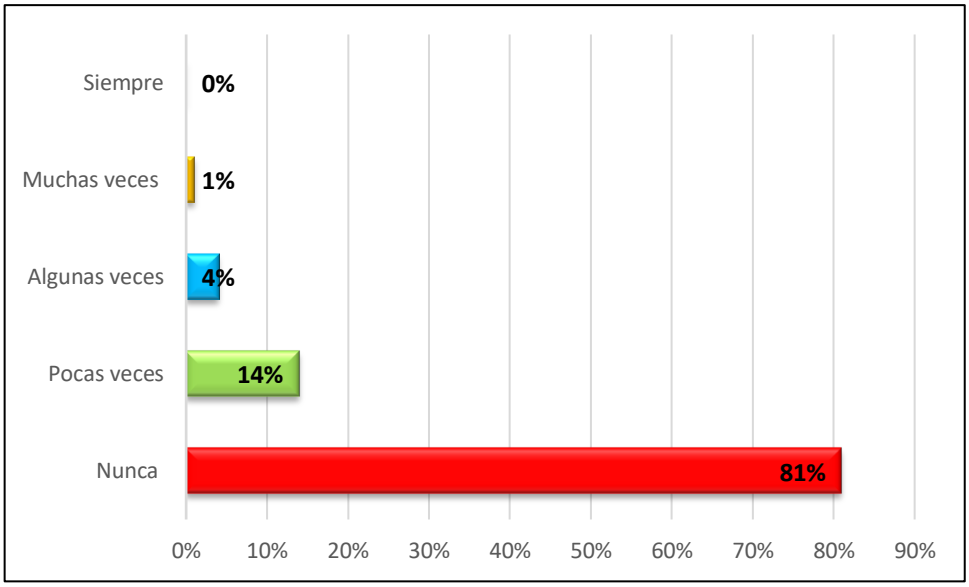

Figura 339. Porcentaje de respuestas ítem 11 encuesta VCE

12. ¿Emite opiniones personales de carácter político, religioso o ideológico en redes sociales abiertas, profesionales o mixtas?

Tabla 244. *Ítem 12. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	87	87%
2	Pocas veces	11	11%
3	Algunas veces	1	1%
4	Muchas veces	0	0%
5	Siempre	1	1%
	TOTALES	100	100%

Tabla 245. *Ítem 12. Descriptivos de la frecuencia con la que los participantes emiten opiniones de carácter político, religioso o ideológico en redes sociales abiertas, profesionales o mixtas.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	1,17	0,533	1	5

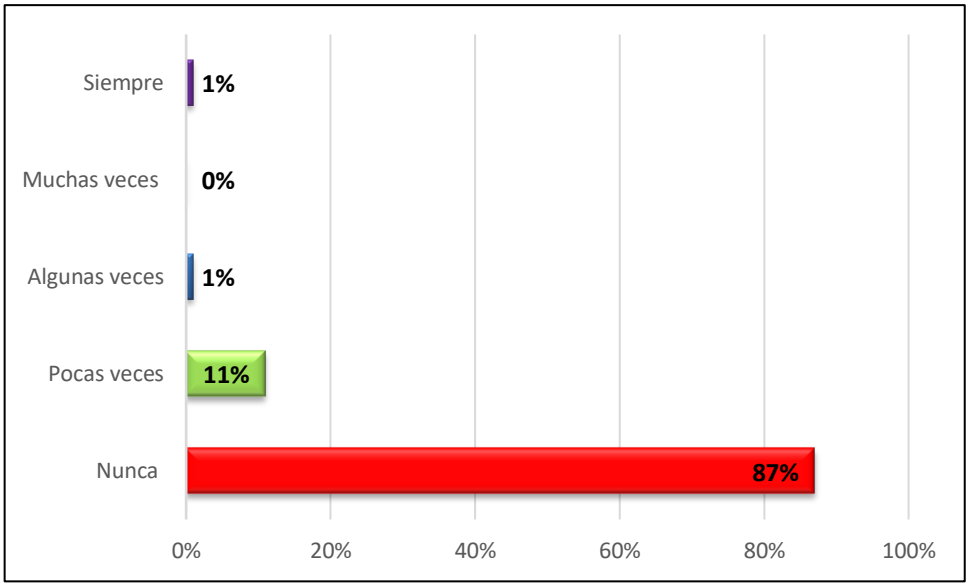

Figura 340. Porcentaje de respuestas ítem 12 encuesta VCE

13. ¿Critica de manera irresponsable y sin argumentos productos o proyectos de la competencia?

Tabla 246. *Ítem 13. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	95	95%
2	Pocas veces	3	3%
3	Algunas veces	0	0%
4	Muchas veces	0	0%
5	Siempre	2	2%
	TOTALES	100	100%

Tabla 247. *Ítem 13. Descriptivos de la frecuencia con la que los participantes critican de manera irresponsable y sin argumentos productos o proyectos de la competencia.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	1,11	0,584	1	5

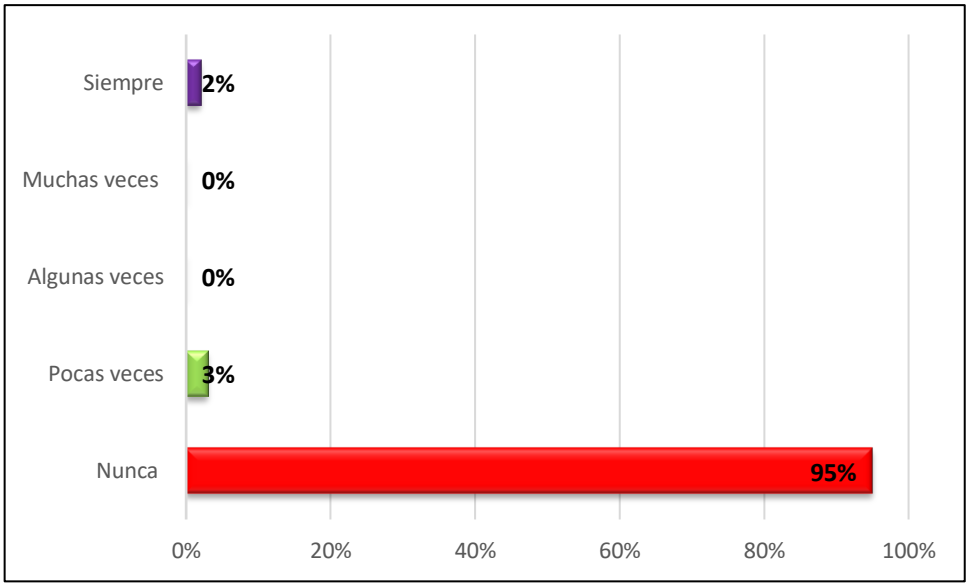

Figura 341. Porcentaje de respuestas ítem 13 encuesta VCE

14. ¿Evita entrar en debates y discusiones con clientes o potenciales clientes a través de las redes sociales?

Tabla 248. *Ítem 14. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	25	25%
2	Pocas veces	4	4%
3	Algunas veces	4	4%
4	Muchas veces	1	1%
5	Siempre	66	66%
	TOTALES	100	100%

Tabla 249. *Ítem 14. Descriptivos de la frecuencia con la que los participantes evitan entrar en debates y discusiones con clientes o potenciales clientes a través de las redes sociales.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	3,79	1,760	1	5

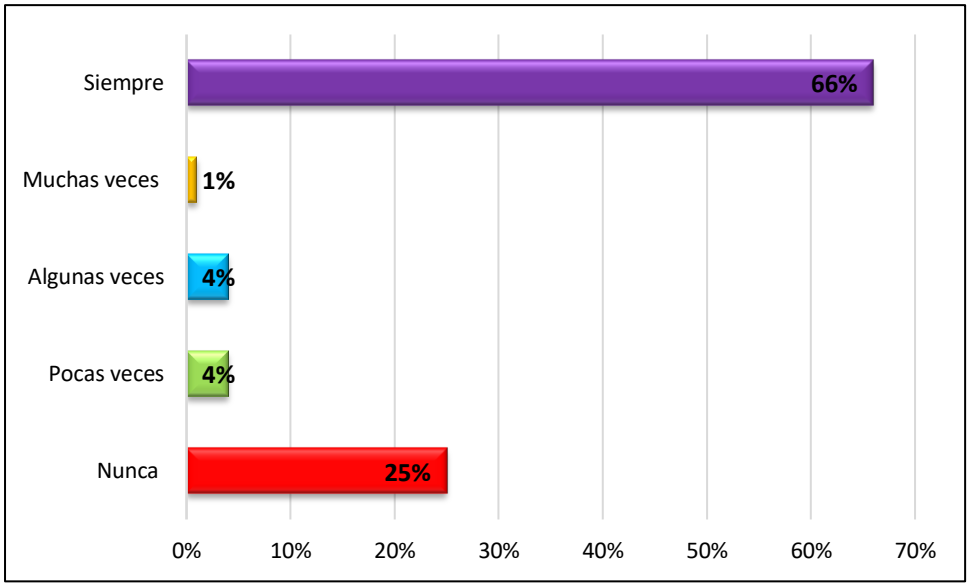

Figura 342. Porcentaje de respuestas ítem 14 encuesta VCE

15. ¿Evita dar información confidencial sobre su negocio que pueda usar la competencia?

Tabla 250. *Ítem 15. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	14	14%
2	Pocas veces	7	7%
3	Algunas veces	10	10%
4	Muchas veces	5	5%
5	Siempre	64	64%
	TOTALES	100	100%

Tabla 251. *Ítem 15. Descriptivos de la frecuencia con la que los participantes evitan dar información confidencial sobre su negocio que pueda usar la competencia.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	3,98	1,517	1	5

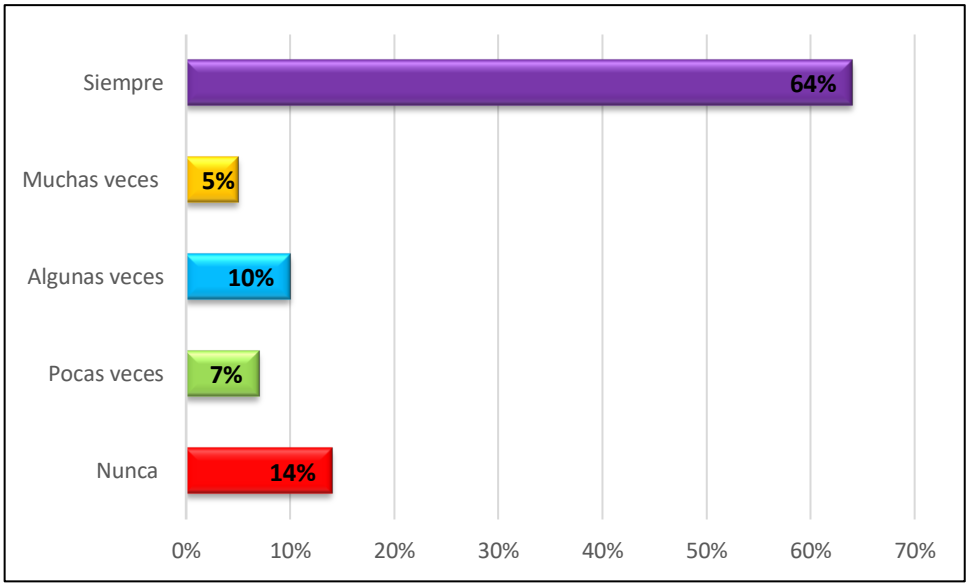

Figura 343. Porcentaje de respuestas ítem 15 encuesta VCE

16. ¿Elimina de forma segura la información confidencial archivada que no necesita?

Tabla 252. *Ítem 16. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	12	12%
2	Pocas veces	12	12%
3	Algunas veces	11	11%
4	Muchas veces	9	9%
5	Siempre	56	56%
	TOTALES	100	100%

Tabla 253. *Ítem 16. Descriptivos de la frecuencia con la que los participantes eliminan de forma segura la información confidencial archivada que no necesita.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	3,85	1,493	1	5

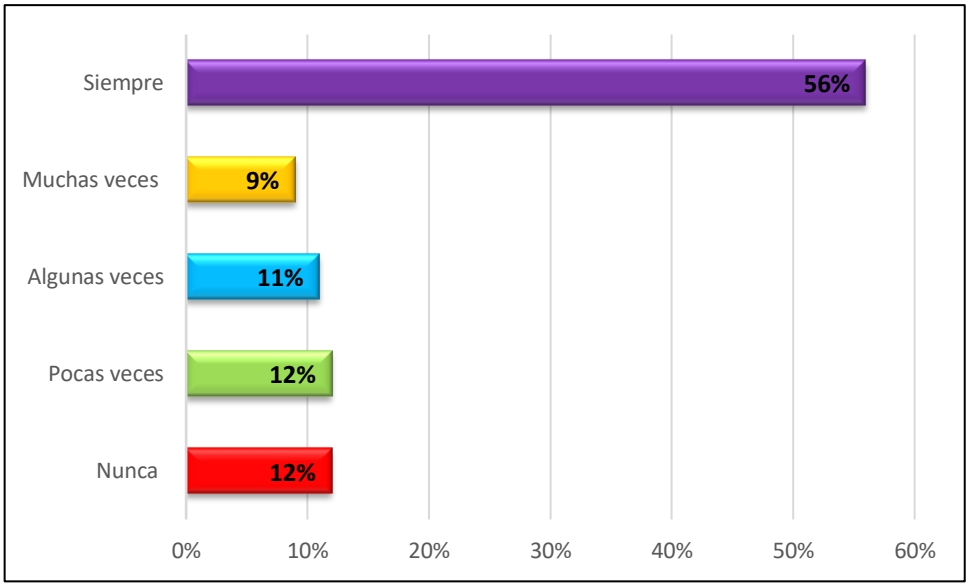

Figura 344. Porcentaje de respuestas ítem 16 encuesta VCE

17. ¿Cifra la información confidencial?

Tabla 254. *Ítem 17. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	44	44%
2	Pocas veces	12	12%
3	Algunas veces	5	5%
4	Muchas veces	7	7%
5	Siempre	32	32%
	TOTALES	100	100%

Tabla 255. *Ítem 17. Descriptivos de la frecuencia con la que los participantes cifran la información confidencial.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	2,71	1,783	1	5

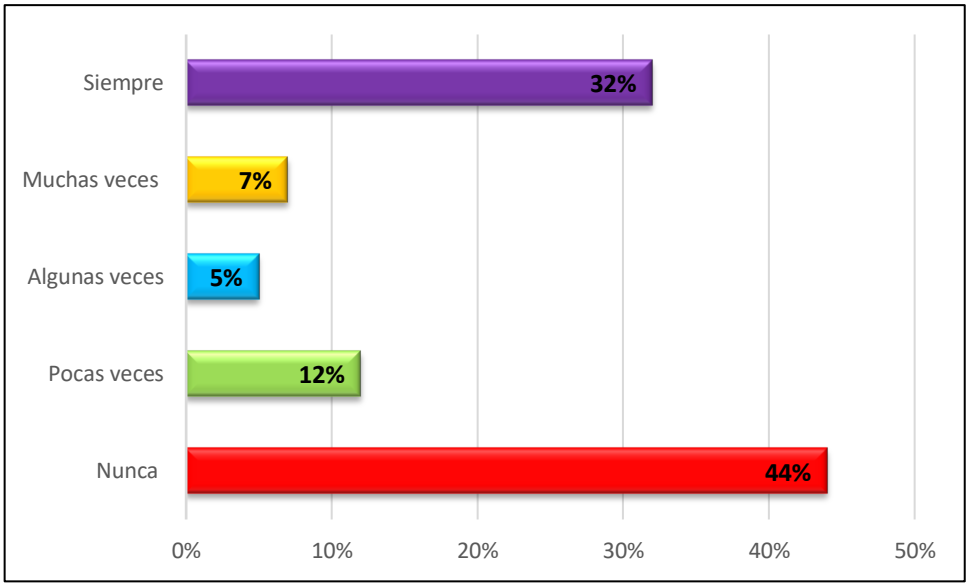

Figura 345. Porcentaje de respuestas ítem 17 encuesta VCE

18. ¿Utiliza los servicios de almacenamiento en la nube?

Tabla 256. *Ítem 18. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	38	38%
2	Pocas veces	14	14%
3	Algunas veces	20	20%
4	Muchas veces	11	11%
5	Siempre	17	17%
	TOTALES	100	100%

Tabla 257. *Ítem 18. Descriptivos de la frecuencia con la que los participantes utilizan los servicios de almacenamiento en la nube.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	2,55	1,507	1	5

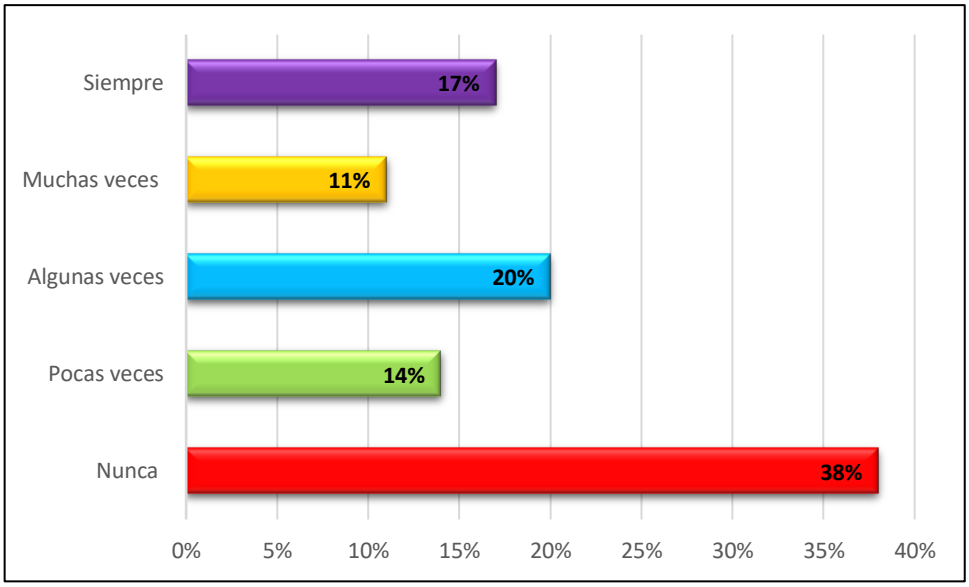

Figura 346. Porcentaje de respuestas ítem 18 encuesta VCE

19. ¿Realiza copias de seguridad en otro soporte de la información almacenada en el teléfono móvil, ordenador, tableta, etc.?

Tabla 258. *Ítem 19. Encuesta victimización cibercriminalidad económica.*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	16	16%
2	Pocas veces	14	14%
3	Algunas veces	14	14%
4	Muchas veces	11	11%
5	Siempre	45	45%
	TOTALES	100	100%

Tabla 259. *Ítem 19. Descriptivos de la frecuencia con la que los participantes realizan copias de seguridad en otro soporte de la información almacenada en el teléfono móvil, ordenador, tableta, etc.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	3,55	1,553	1	5

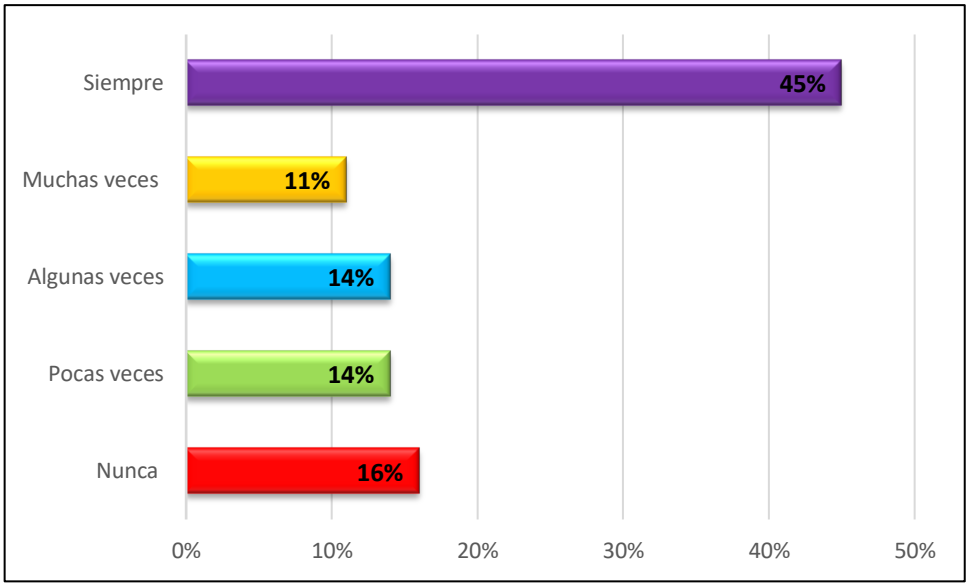

Figura 347. Porcentaje respuestas ítem 19 encuesta VCE

20. ¿Utiliza códigos de desbloqueo de pantalla (código numérico o patrón) en su teléfono móvil, tableta, ordenador, etc.?

Tabla 260. *Ítem 20. Encuesta victimización cibercriminalidad económica*

Nº	RESPUESTAS	Frecuencia (n)	Porcentaje (%)
1	Nunca	12	12%
2	Pocas veces	7	7%
3	Algunas veces	6	6%
4	Muchas veces	7	7%
5	Siempre	68	68%
	TOTALES	100	100%

Tabla 261. *Ítem 20. Descriptivos de la frecuencia con la que los participantes utilizan códigos de desbloqueo de pantalla (código numérico o patrón) en su teléfono móvil, tableta, ordenador, etc.*

Escala Frecuencia tipo Likert	M	DT	Min	Max
De 1 a 5	4,12	1,451	1	5

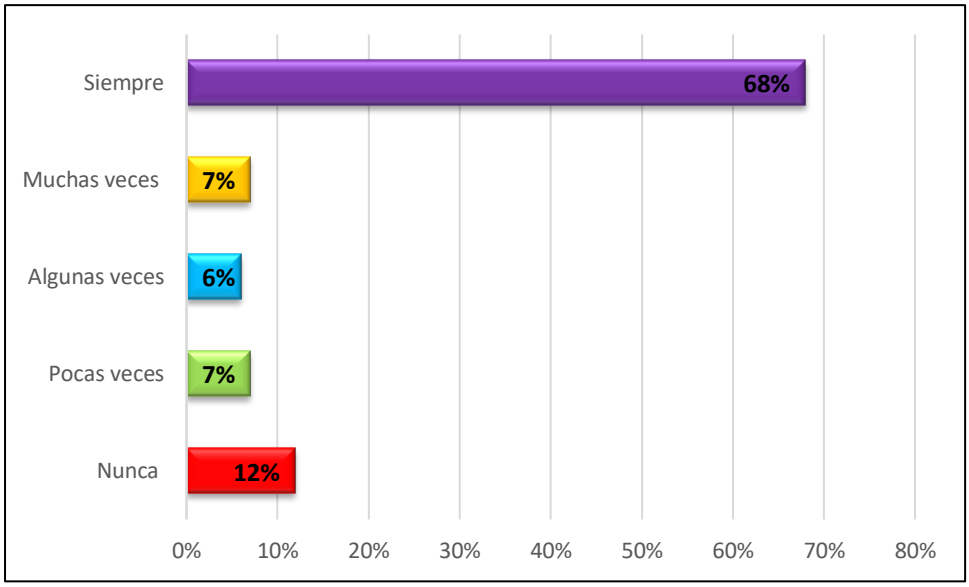

Figura 348. Porcentaje de respuestas ítem 20 encuesta VCE

Los resultados de las puntuaciones totales obtenidas en los hechos o conductas reseñados de los ítems número 1 al 13, respectivamente, son las que figuran en la tabla 262, en las que los participantes tenían como opción cinco posibles respuestas:

1=NUNCA: Cero veces.

2=POCAS VECES: Una o dos ocasiones o veces en un año.

3=ALGUNAS VECES: Tres o cuatro ocasiones o veces en un año.

4=MUCHAS VECES: Desde cinco hasta diez ocasiones o veces en un año.

5=SIEMPRE: Habitualmente o con mucha frecuencia (diez o más veces) en un año.

Tabla 262. *Ítems para evaluación de ciberriesgos con valores de ponderación (1-5)*

Hechos o conductas	Escala de frecuencia conductual				
	1	**2**	**3**	**4**	**5**
1. ¿Ha perdido alguna vez el teléfono móvil, tableta, ordenador portátil, etc.?	65	29	6	0	0
2. ¿Le han sustraído alguna vez el teléfono móvil, tableta, ordenador portátil, etc.?	74	22	4	0	0

3. ¿Ha perdido alguna vez un pendrive con información confidencial de su negocio y/o particular de usted?	92	5	3	0	0
4. ¿Se le ha infectado alguna vez su ordenador, teléfono móvil, tableta, etc., con algún virus o malware?	24	43	26	7	0
5. ¿Alguna vez ha perdido archivos de su negocio por infección de malware?	74	18	8	0	0
6. ¿Ha recibido alguna vez mensajes por WhatsApp, correo electrónico, redes sociales, etc., en la que se prometen grandes cantidades de dinero a cambio de pequeñas transferencias relacionadas con la lotería, trabajo, etc. (scam)?	39	26	21	13	1
7. ¿Ha recibido alguna vez masivamente correos electrónicos no deseados de publicidad (spam)?	8	17	29	38	8
8. ¿Alguna vez han suplantado la página web, Facebook, etc., de su negocio?	95	4	1	0	0
9. Al contactar telemáticamente con proveedores o clientes, en su caso, ¿le han sustraído contraseñas, datos personales de la tarjeta de crédito y/o cuenta bancaria mediante diferentes técnicas tales como correos electrónicos que llevan a páginas falsas en las que se solicita la introducción de estos datos, o mediante infección por virus?	91	7	2		0

10. Al efectuar una compraventa en su negocio, ¿alguna vez un cliente ha utilizado una tarjeta de crédito sustraída?	81	13	6	0	0
11. ¿Ha sido víctima de algún tipo de fraude online, extorsión, etc.?	81	14	4	1	0
12. ¿Emite opiniones personales de carácter político, religioso o ideológico en redes sociales abiertas, profesionales o mixtas?	87	11	1	0	1
13. ¿Critica de manera irresponsable y sin argumentos productos o proyectos de la competencia?	95	3	0	0	2
Totales	906	212	111	59	12

A continuación, en la tabla 263 se exponen las puntuaciones totales obtenidas en la tabla anterior y a las que se les ha aplicado un valor o factor de ponderación multiplicador que va desde el número 1 hasta el número 5, en función del riesgo de cibervictimización estimado.

Tabla 263. *Resultados ponderados ítems 1-13*

Puntuaciones totales ítems (1-13)	906	212	111	59	12	
Factores de ponderación	1	2	3	4	5	
Resultados ponderados	906	424	333	236	60	
Total ponderado						**1959**

En la tabla 264, podemos observar los resultados de las puntuaciones totales obtenidas en los hechos o conductas reseñados de los ítems número 14 a 20, respectivamente, en las que los participantes tenían como opción cinco posibles respuestas:

1=NUNCA: Cero veces.

2=POCAS VECES: Una o dos ocasiones o veces en un año.

3=ALGUNAS VECES: Tres o cuatro ocasiones o veces en un año.

4=MUCHAS VECES: Desde cinco hasta diez ocasiones o veces en un año.

5=SIEMPRE: Habitualmente o con mucha frecuencia (diez o más veces) en un año.

Tabla 264. *Ítems para evaluación de ciberriesgos con valores de ponderación (5-1)*

Hechos o conductas	Escala de frecuencia conductual				
	1	**2**	**3**	**4**	**5**
14. ¿Evita entrar en debates y discusiones con clientes o potenciales clientes a través de las redes sociales?	25	4	4	1	66
15. ¿Evita dar información confidencial sobre su negocio que pueda usar la competencia?	14	7	10	5	64
16. ¿Elimina de forma segura la información confidencial archivada que no necesita?	12	12	11	9	56
17. ¿Cifra la información confidencial?	44	12	5	7	32
18. ¿Utiliza los servicios de almacenamiento en la nube?	38	14	20	11	17
19. ¿Realiza copias de seguridad en otro soporte de la información almacenada en el teléfono móvil, ordenador, tableta, etc.?	16	14	14	11	45
20. ¿Utiliza códigos de desbloqueo de pantalla (código numérico o patrón) en su teléfono móvil, tableta,	12	7	6	7	68

ordenador, etc.?

TOTALES	161	70	70	51	348

Igualmente, procedemos con las puntuaciones totales de los ítems desde el número 14 hasta el 20, respectivamente, de la encuesta, aplicándoles un valor o factor de ponderación multiplicador desde el número 5 hasta el número 1, en función del riesgo de cibervictimización estimado, tal y como se exponen en la tabla 265.

Tabla 265. *Resultados ponderados ítems 14-20*

Puntuaciones totales ítems (14-20)	161	70	70	51	348	
Factores de ponderación	5	4	3	2	1	
Resultados ponderados	805	280	210	102	348	
Total ponderado						**1745**

Posteriormente, procedemos a la suma del resultado total ponderado que hemos obtenido de las tablas 247 (1959) y 249 (1745), arrojando un resultado de 3704 puntos.

A continuación, comprobamos que los 3704 puntos obtenidos, se encuentran en el rango de puntuación de nivel de riesgo (3600-4400) de la tabla 266 contempla el baremo de evaluación de riesgos de cibervictimización generalizado.

Según el rango de clasificación reseñado, el riesgo de cibervictimización generalizado sería moderado, de probabilidad media y de impacto medio con una estimación de riesgo de 4.

Tabla 266. *Baremo de evaluación de ciberriesgos de victimización generalizado*

Rango Puntuación Nivel Riesgo	Tolerabilidad	Probabilidad	Impacto	Estimación Riesgo	Prioridad de acción
2000-2800	Trivial	Baja (1)	Bajo (1)	1	Prioridad Baja, plazo de hasta 1 año para implantar las

					medidas preventivas propuestas.
2800-3600	Tolerable	Media (2)	Medio (2)	4	Prioridad media, hasta 6 meses de plazo para adoptar medidas preventivas.
3600-4400	Moderado	Media (2)	Medio (2)	4	
4400-5200	Importante	Alta (3)	Alto (3)	9	Prioridad alta, los ciberriesgos requieren acción preventiva inmediata o, en su caso, en el plazo máximo de hasta 3 meses.
5200-6000	Intolerable	Alta (3)	Alto (3)	9	

En este orden de cosas, como la estimación del riesgo generalizado es igual a 4, la prioridad de acción es media, cosa que supondría que en un plazo máximo de hasta 6 meses, se deberían tomar medidas preventivas tanto desde la perspectiva de la prevención de ciberriesgos laborales como desde una perspectiva analítica del daño, pérdida o perjuicio económico que pudiera sufrir la empresa, que en el estudio presente, se centra en la figura del autónomo y de la microempresa o micropyme, en su caso.

V. DISCUSIÓN.

V.1. Discusión estudio cibercriminalidad social.

En primer lugar, si realizamos una comparativa respecto al género y edad de los participantes menores de edad, en este estudio de investigación y que pertenecen a los centros educativos: Colegio Nuestra Señora de la Consolación, Colegio Nuestra Señora Divina Providencia, IES José Vilaplana e IES Leopoldo Querol, respectivamente, podemos observar con relación al género la siguiente comparativa:

-curso 1º de la ESO, según tabla 267 y figura 349, los centros educativos que más chicos tienen en dicho curso son el Colegio Nª. Sª. Consolación y el IES Sanchis Vilaplana.

A contrario sensu, el centro educativo que más chicas tiene cursando 1º de la ESO con diferencia es el Colegio Nª. Sª. Divina Providencia.

Tabla 267. *Comparativa género participantes 1º ESO.*

Curso académico	chicos	chicas
1º ESO Consolación	17	10
1º ESO Divina Providencia	12	19
1º ESO Leopoldo Querol	13	13
1º ESO Sanchis y Vilaplana	16	11
Total	**58**	**53**

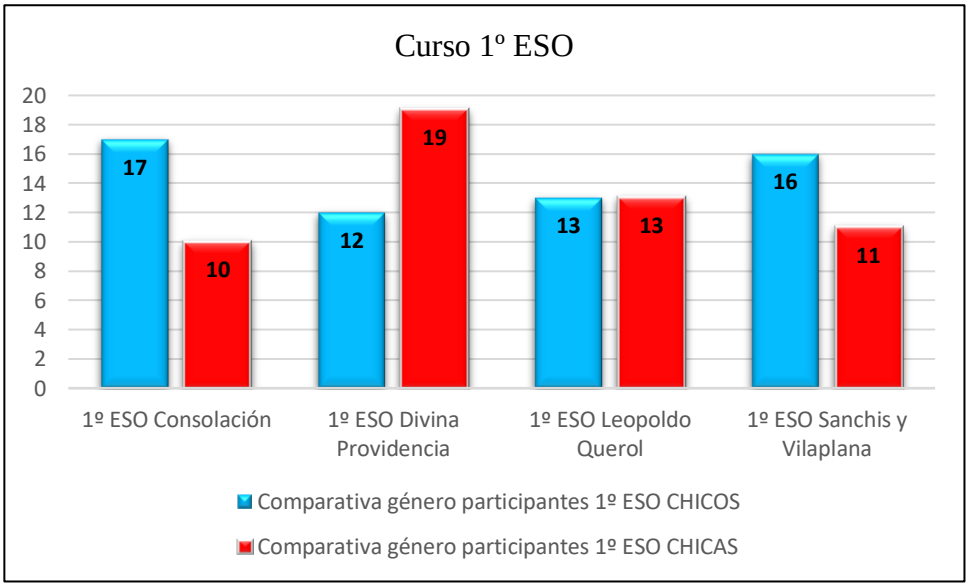

Figura 349. Comparativa género participantes 1º ESO.

-curso 2º de la ESO, según tabla 268 y figura 350, el centro educativo que más chicos tiene en el curso reseñado es el Colegio Nª. Sª Divina Providencia y los que tienen más chicas son el Colegio Nª. Sª Consolación y el IES Leopoldo Querol.

Tabla 268. *Comparativa género participantes 2º ESO.*

Curso académico	chicos	chicas
2º ESO Consolación	10	17
2º ESO Divina Providencia	18	9
2º ESO Leopoldo Querol	14	17
2º ESO Sanchis y Vilaplana	13	13
Total	**52**	**56**

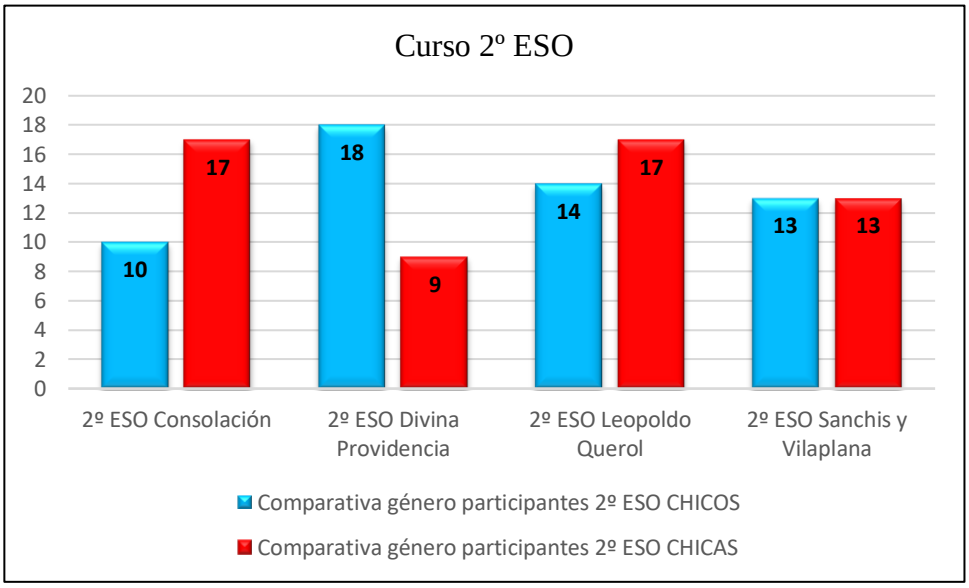

Figura 350. Comparativa género participantes 2º ESO.

-curso 3º de la ESO, según tabla 269 y figura 351, podemos destacar que los cuatro centros educativos participantes en el estudio tienen más chicas que chicos en el curso mencionado.

Tabla 269. *Comparativa género participantes 3º ESO.*

Curso académico	chicos	chicas
3º ESO Consolación	12	16
3º ESO Divina Providencia	10	16
3º ESO Leopoldo Querol	8	18
3º ESO Sanchis y Vilaplana	12	15
Total	**42**	**65**

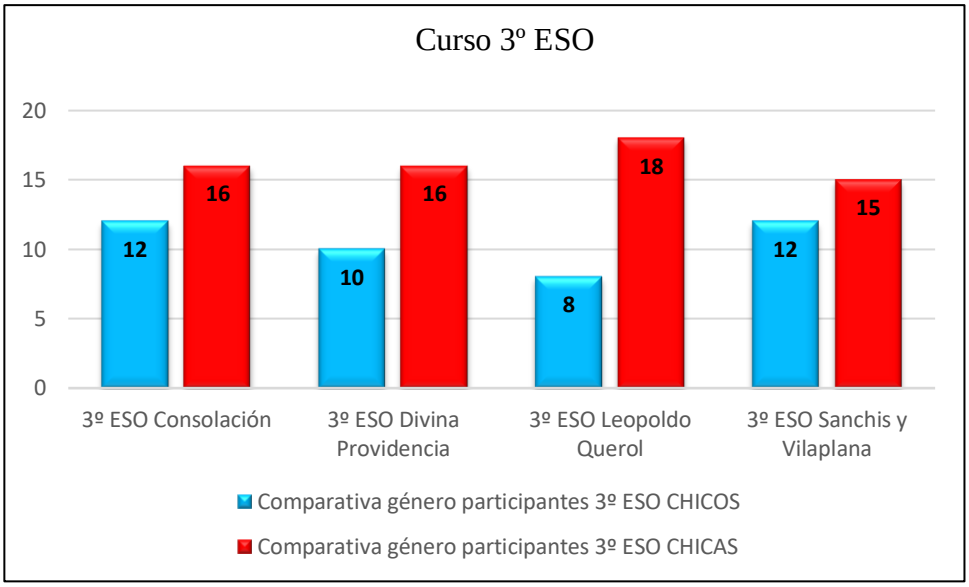

Figura 351. Comparativa género participantes 3º ESO.

-curso 4º de la ESO, según tabla 270 y figura 352, el centro educativo que más chicos tiene en el curso referenciado es el Colegio Nª. Sª. Divina Providencia y el que tiene más chicas es el IES Sanchis y Vilaplana.

Tabla 270. *Comparativa género participantes 4º ESO.*

Curso académico	chicos	chicas
4º ESO Consolación	10	17
4º ESO Divina Providencia	16	9
4º ESO Leopoldo Querol	11	15
4º ESO Sanchis y Vilaplana	6	23
Total	43	64

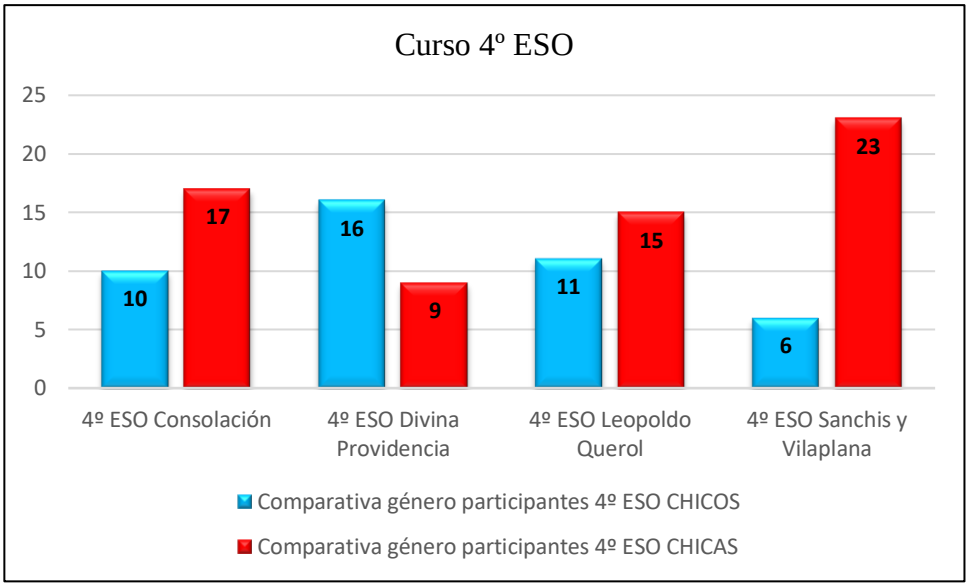

Figura 352. Comparativa género participantes 4º ESO.

En segundo lugar, con relación a la edad de los menores participantes, podemos deducir por los rangos de edad de los participantes que el centro educativo que posee más alumnos con diecisiete años cursando 3º y 4º de la ESO respectivamente, es el IES Sanchis y Vilaplana, y el que tiene más alumnos con once años cursando 1º de la ESO es el Colegio Nª. Sª. Consolación.

Por otra parte, si analizamos los datos obtenidos con relación a la interacción con las TIC de los menores participantes en los cuatro centros educativos, en su caso, podemos observar en los resultados arrojados y plasmados anteriormente, que la mayoría tienen ordenador y teléfono móvil, cuenta de correo electrónico, utilizan programas de mensajería instantánea y redes sociales, evidencias que nos indican que su interacción con las TIC es elevada y por ende con Internet.

En este sentido, en virtud de los resultados obtenidos, hay que destacar que la mayoría de los menores participantes han manifestado utilizar muy poco los blogs y foros en Internet.

Por lo que respecta al uso del ordenador, en la tabla 271 y la figura 353, podemos apreciar como la mayoría de los menores participantes de 1º a 4º de la ESO del Colegio Nª. Sª. de la Consolación, tapan la webcam cuando no la utilizan.

Tabla 271. *Comparativa 1º a 4º ESO Colegio Nª. Sª. Consolación (uso webcam).*

¿Tapas la webcam cuando no la utilizas?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Si	37%	85%	39%	59%
No	30%	11%	36%	26%
No tengo	33%	4%	25%	15%

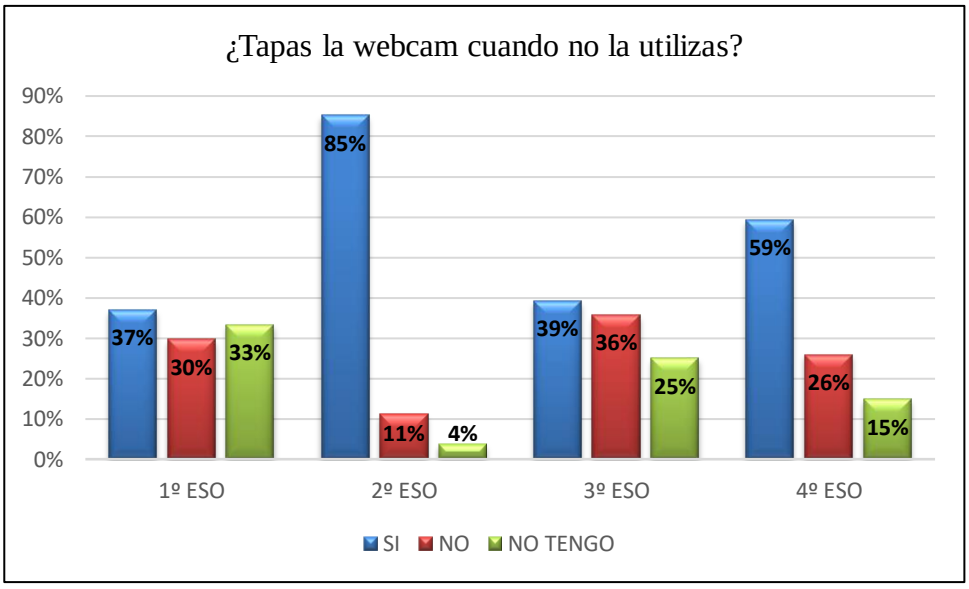

Figura 353. Comparativa 1º a 4º ESO Colegio Nª. Sª. Consolación (uso webcam).

Por el contrario, en los tres centros educativos restantes no ocurre lo mismo, tal y como podemos ver en la comparativa contemplada en las tablas 272 a 274 y en las figuras 354 a 356, respectivamente, así:

Tabla 272. *Comparativa 1º a 4º ESO Colegio Nª. Sª. Divina Providencia (uso webcam).*

¿Tapas la webcam cuando no la utilizas?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Si	45%	22%	46%	40%
No	19%	37%	19%	32%
No tengo	35%	41%	35%	28%

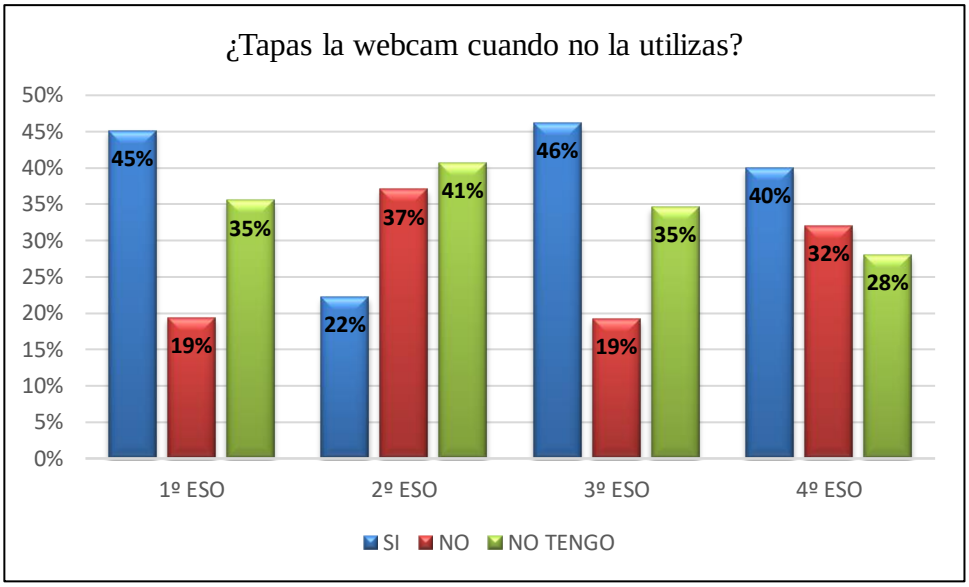

Figura 354. Comparativa 1º a 4º ESO Colegio Nª. Sª. Divina Providencia (uso webcam).

En los resultados obtenidos correspondientes al Colegio Nª. Sª. de la Divina Providencia, cabe destacar que de los menores participantes de 2º de la ESO, un 22% manifiesta que sí tapa la webcam cuando no la utiliza, frente a un 37% que no la tapa cuando no la usa, y el 41% restante no posee.

Tabla 273. *Comparativa 1º a 4º ESO IES Leopoldo Querol (uso webcam).*

¿Tapas la webcam cuando no la utilizas?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Si	31%	26%	38%	27%
No	8%	29%	19%	46%
No tengo	62%	45%	42%	27%

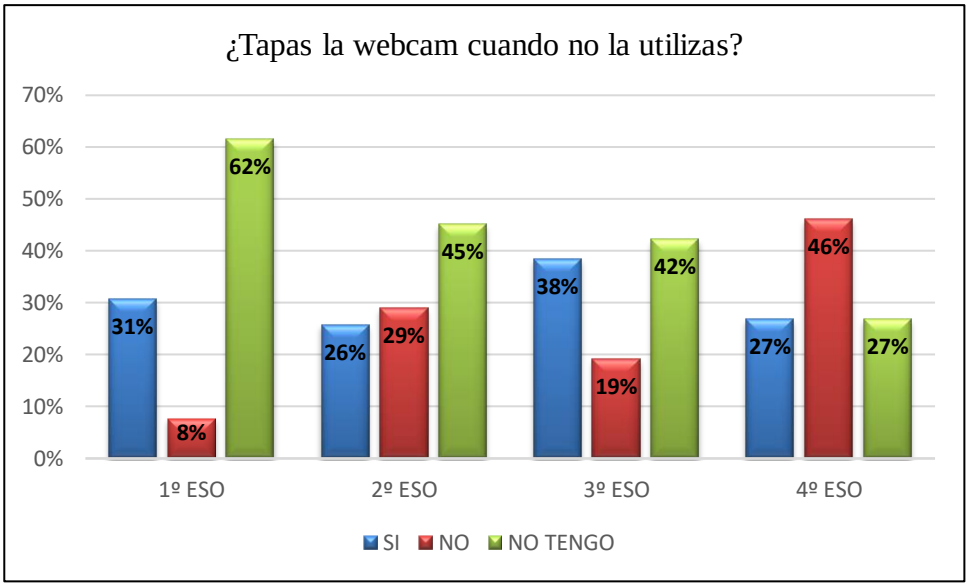

Figura 355. Comparativa 1º a 4º ESO IES Leopoldo Querol (uso webcam).

En los resultados obtenidos correspondientes al IES Leopoldo Querol, cabe destacar que de los menores participantes de 4º de la ESO, un 27% manifiesta que sí tapa la webcam cuando no la utiliza, frente a un 46% que no la tapa cuando no la usa, y el 27% restante no posee.

Tabla 274. *Comparativa 1º a 4º ESO IES Sanchis y Vilaplana (uso webcam).*

¿Tapas la webcam cuando no la utilizas?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Si	30%	19%	33%	38%
No	33%	27%	30%	34%
No tengo	37%	54%	37%	28%

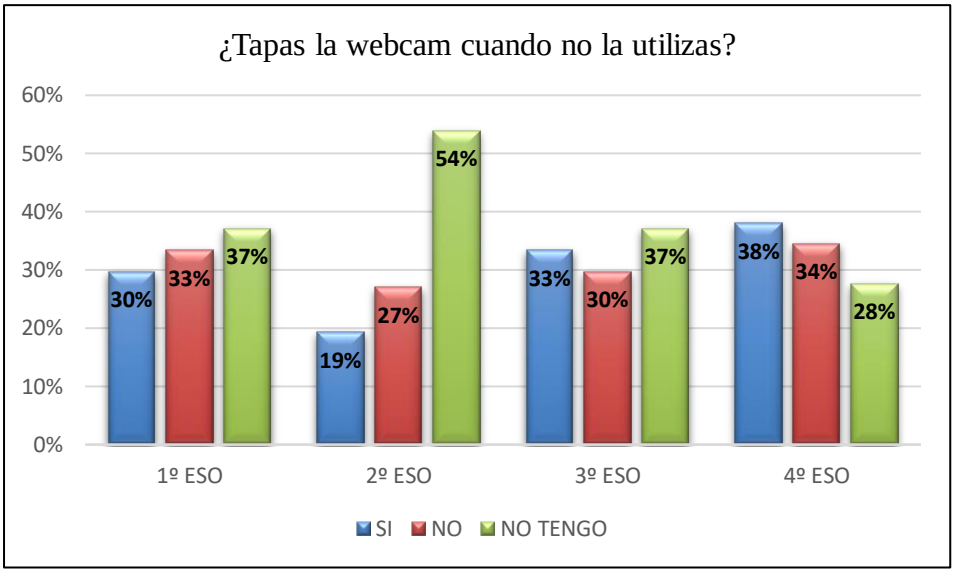

Figura 356. Comparativa 1º a 4º ESO IES Sanchis y Vilaplana (uso webcam).

En los resultados obtenidos correspondientes al IES Sanchis y Vilaplana, cabe destacar que de los menores participantes de 1 a 4º de la ESO, la mayoría se encuentran prácticamente equiparados entre los que manifiestan que sí tapan la webcam cuando no la utilizan, frente a los que no la tapan cuando no la usan, excepto los participantes de 2º de la ESO, de los que un 19% manifiesta que sí tapa la webcam cuando no la utiliza, frente a un 27% que no la tapa cuando no la usa, y el 54% restante no posee.

Por lo que respecta al lugar donde tienen ubicado los menores su ordenador, podemos observar en la comparativa de las tablas 275 a 278 y en las figuras 357 a 360, respectivamente, que de los participantes de:

a) Colegio Nª. Sª. Consolación: destacaremos el curso de 2º de la ESO con relación al resto de cursos del mismo centro educativo (1º, 3º y 4º de la ESO), donde un 67% ubica su ordenador en su habitación frente a un 33% que lo tiene en una zona común de su domicilio.

Tabla 275. *Comparativa 1º a 4º ESO Colegio Nª. Sª. Consolación (ubicación ordenador).*

¿Dónde tienes ubicado el ordenador?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Habitación	52%	67%	50%	48%
Zona común	44%	33%	50%	48%
No tengo	4%	0%	0%	4%

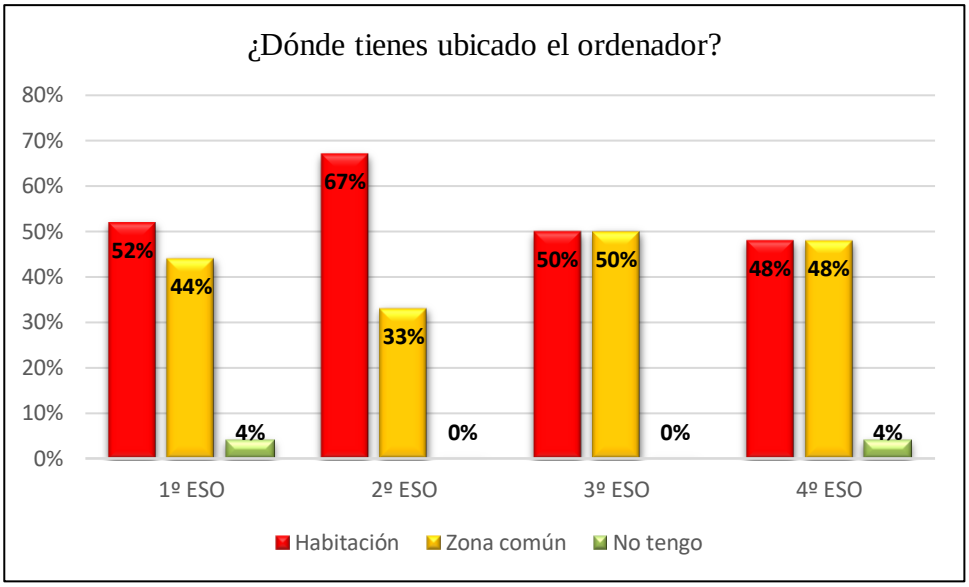

Figura 357. Comparativa 1º a 4º ESO Colegio Nª. Sª. Consolación (ubicación ordenador).

b) Colegio Nª. Sª. Divina Providencia: en los resultados obtenidos en este centro podemos apreciar y destacar como los participantes de 1º y 2º de la ESO manifestaron, mayoritariamente, tener el ordenador en su habitación (61% y 59%) frente a los que lo dijeron tenerlo ubicado en una zona común de su casa (35% y 30%).

Por el contrario, en los cursos de 3º y 4º de la ESO la mayoría de los participantes manifestaron tener el ordenador en una zona común de su morada (62% y 60%) frente a los que lo tenían ubicado en su habitación (38% y 36%).

Tabla 276. *Comparativa 1º a 4º ESO Colegio Nª. Sª. Divina Providencia (ubicación ordenador).*

¿Dónde tienes ubicado el ordenador?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Habitación	61%	59%	38%	36%
Zona común	35%	30%	62%	60%
No tengo	3%	11%	0%	4%

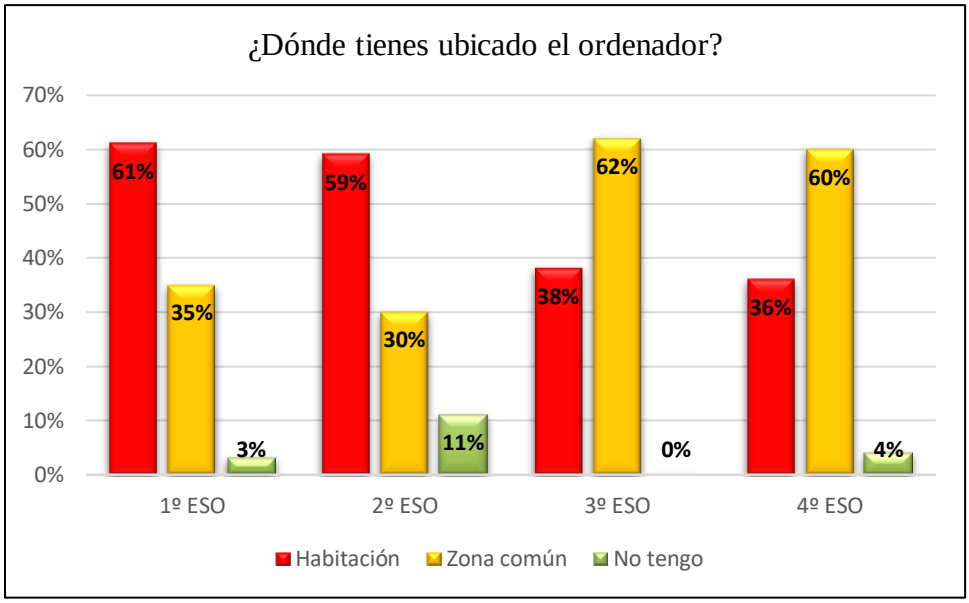

Figura 358. Comparativa 1º a 4º ESO Colegio Nª. Sª. Divina Providencia (ubicación ordenador).

c) IES Leopoldo Querol: en este centro educativo cabe destacar, entre los resultados obtenidos, los referentes al curso de 1º de la ESO que participaron en un 58%, ubicar el ordenador en una zona común frente a un 23% que manifestó tenerlo en su habitación.

Tabla 277. *Comparativa 1º a 4º ESO IES Leopoldo Querol (ubicación ordenador).*

¿Dónde tienes ubicado el ordenador?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Habitación	23%	45%	38%	54%
Zona común	58%	48%	54%	46%
No tengo	19%	6%	8%	0%

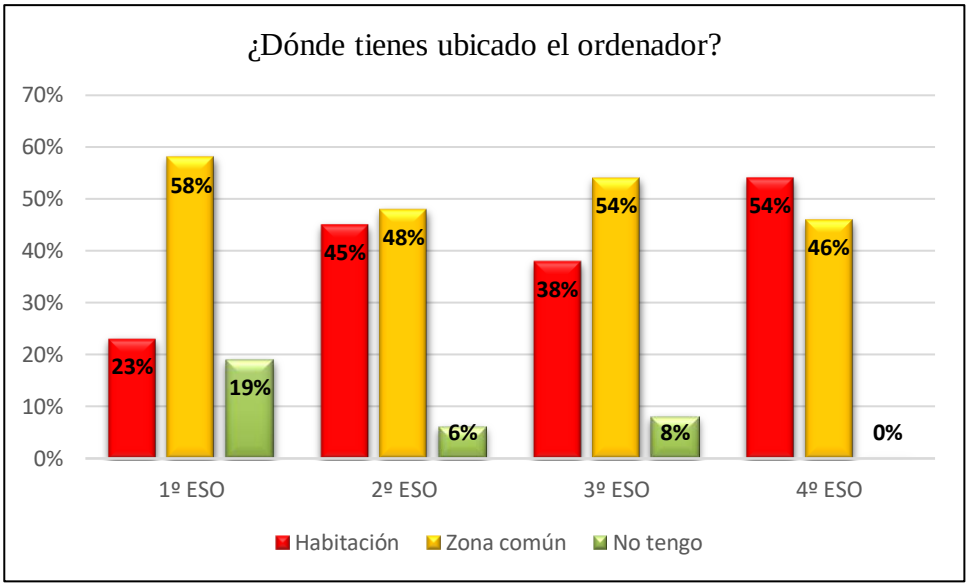

Figura 359. Comparativa 1º a 4º ESO IES Leopoldo Querol (ubicación ordenador).

d) IES Sanchis y Vilaplana: de este centro educativo cabe hacer mención de los resultados obtenidos en los cursos 1º y 2º de la ESO, observando que en el primero curso los participantes indicaron con un 59% que tenían ubicado el ordenador en su habitación frente a un 30% que lo tenía en una zona común de su casa.

A contrario sensu, en el segundo curso un 15% participó tener ubicado el ordenador en su habitación frente a un 73% que manifestó tenerlo en una zona común de su lugar de residencia.

Tabla 278. *Comparativa 1º a 4º ESO IES Sanchis y Vilaplana (ubicación ordenador).*

¿Dónde tienes ubicado el ordenador?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Habitación	59%	15%	52%	45%
Zona común	30%	73%	44%	48%
No tengo	11%	12%	4%	7%

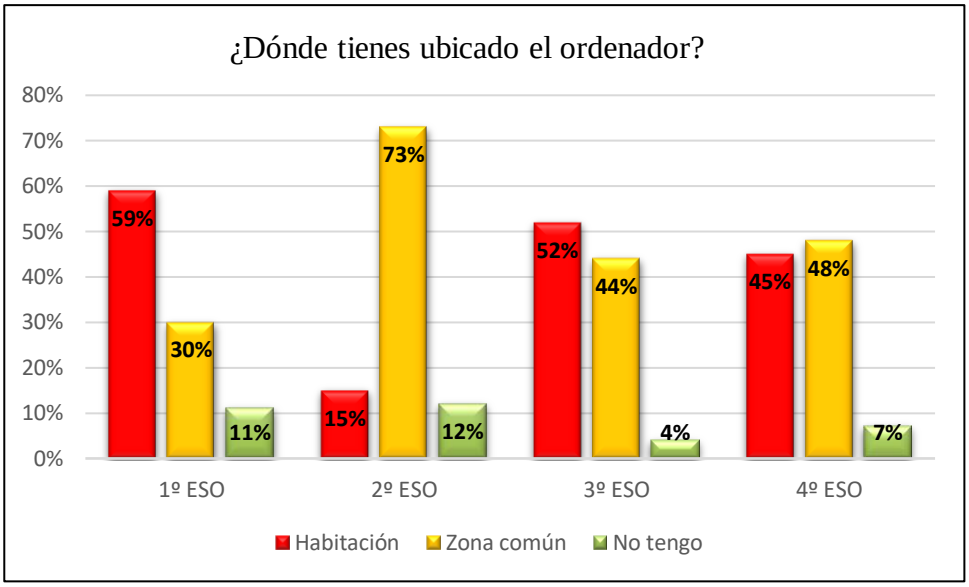

Figura 360. Comparativa 1º a 4º ESO IES Sanchis y Vilaplana (ubicación ordenador).

En lo atinente a la cuestión sobre si los participantes guardan información personal en el teléfono móvil, podemos observar en la comparativa plasmada por centros educativos en las tablas 279 a 282 y en las figuras 361 a 364, respectivamente, como la mayoría de los que sí poseen teléfono móvil guardan información personal o sensible en sus dispositivos.

Tabla 279. *Comparativa 1º a 4º ESO Colegio Nª. Sª. Consolación (info teléfono móvil).*

¿Guardas información personal en el teléfono móvil?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Si	63%	89%	75%	78%
No	37%	11%	25%	22%
No tengo	0%	0%	0%	0%

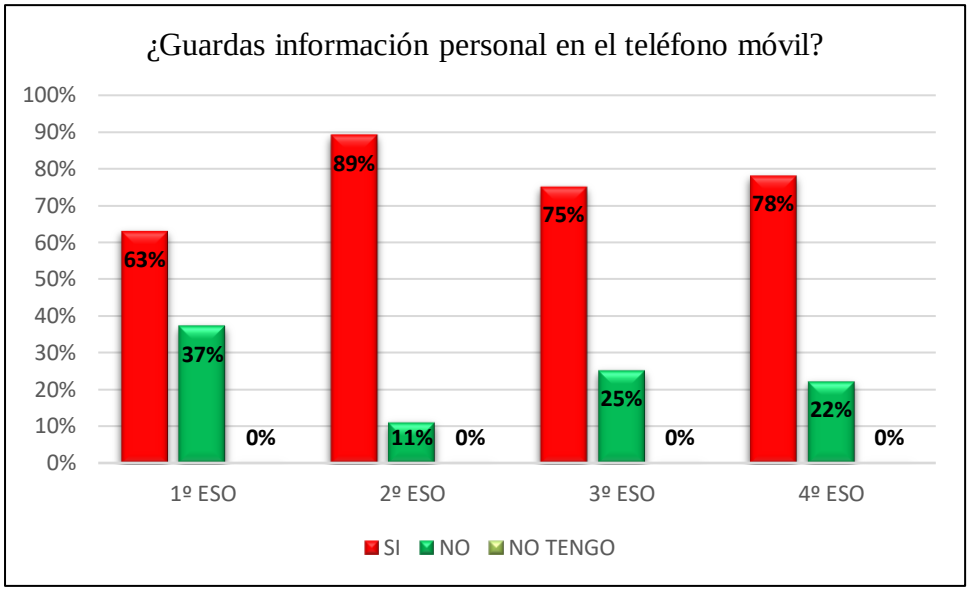

Figura 361. Comparativa 1º a 4º ESO Colegio Nª. Sª. Consolación (info teléfono móvil).

Tabla 280. *Comparativa 1º a 4º ESO Colegio Nª. Sª. Divina Providencia (info teléfono móvil).*

¿Guardas información personal en el teléfono móvil?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Si	52%	63%	88%	76%
No	39%	37%	12%	24%
No tengo	10%	0%	0%	0%

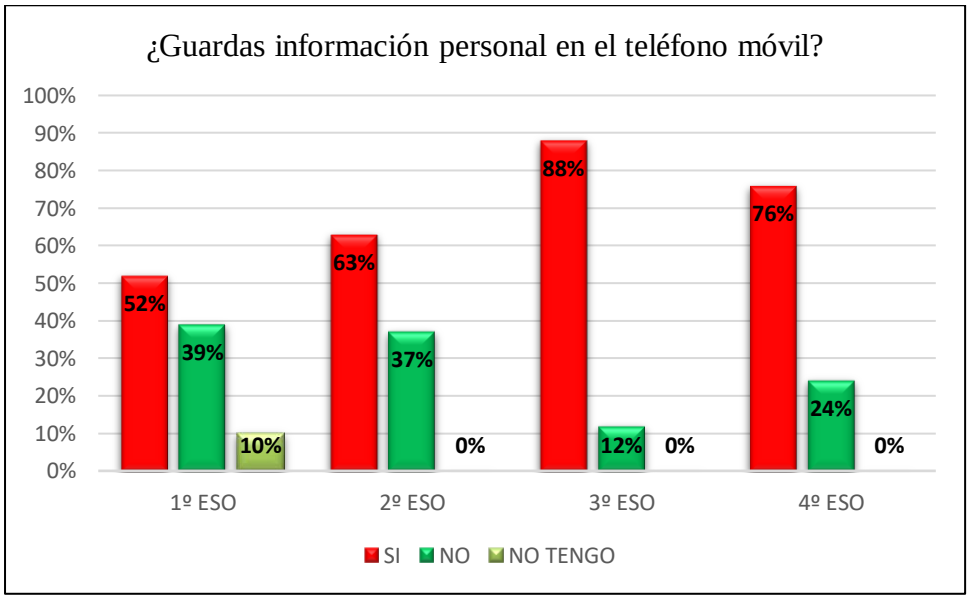

Figura 362. Comparativa 1º a 4º ESO Colegio Nª. Sª. Divina Providencia (info teléfono móvil).

Tabla 281. *Comparativa 1º a 4º ESO IES Leopoldo Querol (info teléfono móvil).*

¿Guardas información personal en el teléfono móvil?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Si	54%	77%	81%	85%
No	46%	23%	19%	15%
No tengo	0%	0%	0%	0%

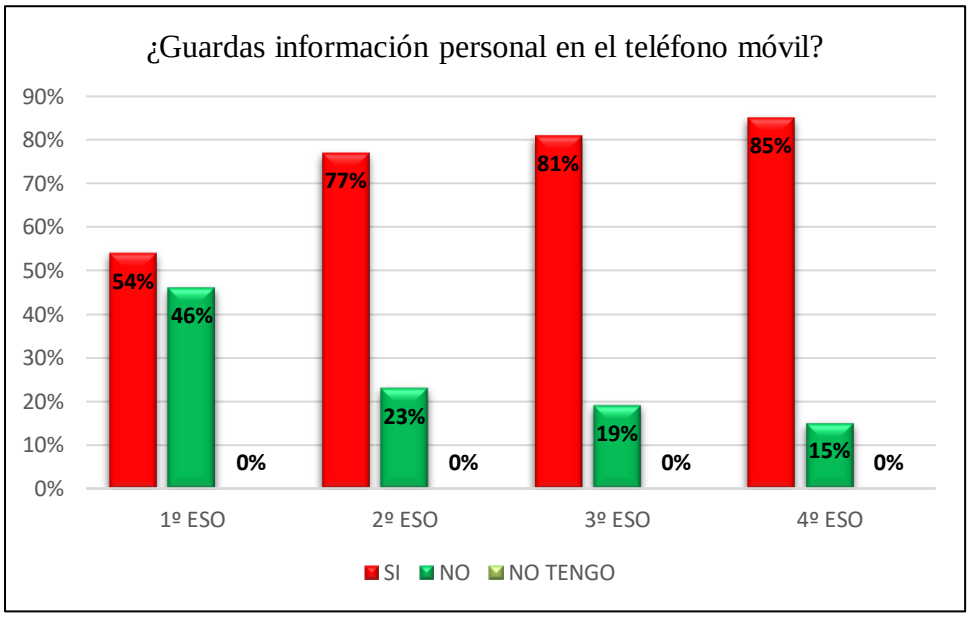

Figura 363. Comparativa 1º a 4º ESO IES Leopoldo Querol (info teléfono móvil).

Tabla 282. *Comparativa 1º a 4º ESO IES Sanchis y Vilaplana (info teléfono móvil).*

¿Guardas información personal en el teléfono móvil?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Si	78%	65%	93%	72%
No	22%	31%	4%	28%
No tengo	0%	4%	4%	0%

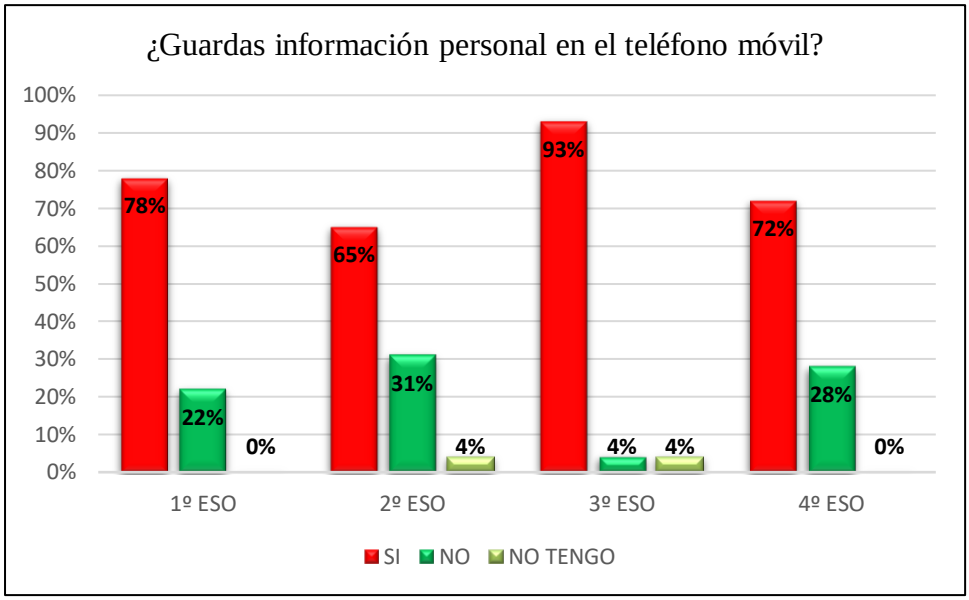

Figura 364. Comparativa 1º a 4º ESO IES Sanchis y Vilaplana (info teléfono móvil).

Por otra parte, en relación con el tiempo que dedicaban diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc., los menores participantes, podemos observar en la comparativa de resultados arrojados y plasmados en las tablas 283 a 286 y las figuras 365 a 368, respectivamente, que en los cuatro centros educativos objeto de estudio destacan con notoriedad los porcentajes de los cursos 3º y 4º de la ESO por dedicar tres horas o más a interaccionar en el ciberespacio, especialmente, el Colegio Nª. Sª. Consolación con un 71% los participantes de 3º de la ESO y con un 63% los de 4º de la ESO, así como el Colegio Nª. Sª. Divina Providencia con un 73% los participantes de 3º de la ESO y con un 60% los de 4º de la ESO, respectivamente.

Por el contrario, los participantes de 1º de ESO destacan por dedicar menos tiempo a ello, es decir, entre una hora y dos, salvo el IES Sanchis y Vilaplana que, mayoritariamente, dedican tres o más horas.

Tabla 283. *Comparativa 1º a 4º ESO Colegio Nª. Sª. Consolación (tiempo dedicado Internet, RRSS, etc.).*

¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

	1º ESO	2º ESO	3º ESO	4º ESO
Respuestas				
Menos de 1 hora	19%	11%	7%	0%
Entre 1 y 2 horas	52%	37%	21%	37%
3 horas o más	30%	52%	71%	63%

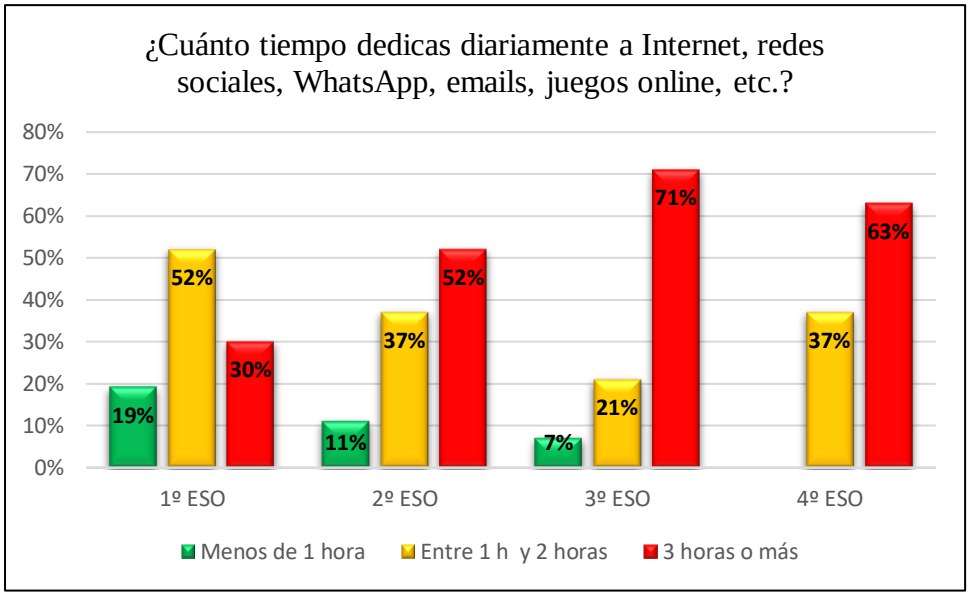

Figura 365. Comparativa 1º a 4º ESO Colegio Nª.Sª. Consolación (tiempo dedicado Internet, RRSS, etc.).

Tabla 284. *Comparativa 1º a 4º ESO Colegio Nª.Sª. Divina Providencia (tiempo dedicado Internet, RRSS, etc.).*

¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

Respuestas	1º ESO	2º ESO	3º ESO	4º ESO
Menos de 1 hora	26%	15%	15%	4%
Entre 1 y 2 horas	48%	33%	12%	36%
3 horas o más	26%	52%	73%	60%

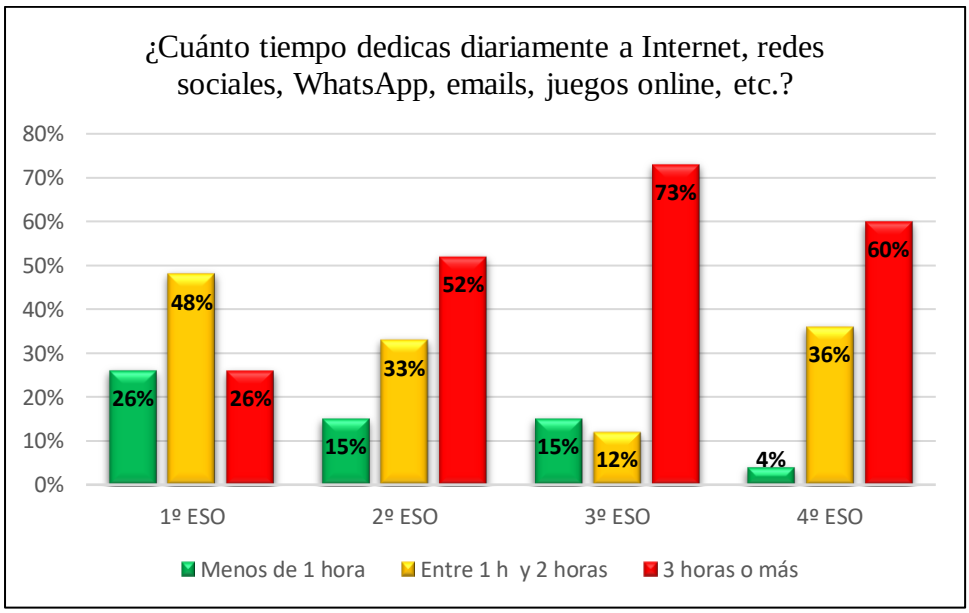

Figura 366. Comparativa 1º a 4º ESO Colegio Nª.Sª. Divina Providencia (tiempo dedicado Internet, RRSS, etc.).

Tabla 285. *Comparativa 1º a 4º ESO IES Leopoldo Querol (tiempo dedicado Internet, RRSS, etc.).*

¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

	1º ESO	2º ESO	3º ESO	4º ESO
Respuestas				
Menos de 1 hora	38%	10%	8%	0%
Entre 1 y 2 horas	42%	58%	27%	50%
3 horas o más	19%	32%	65%	50%

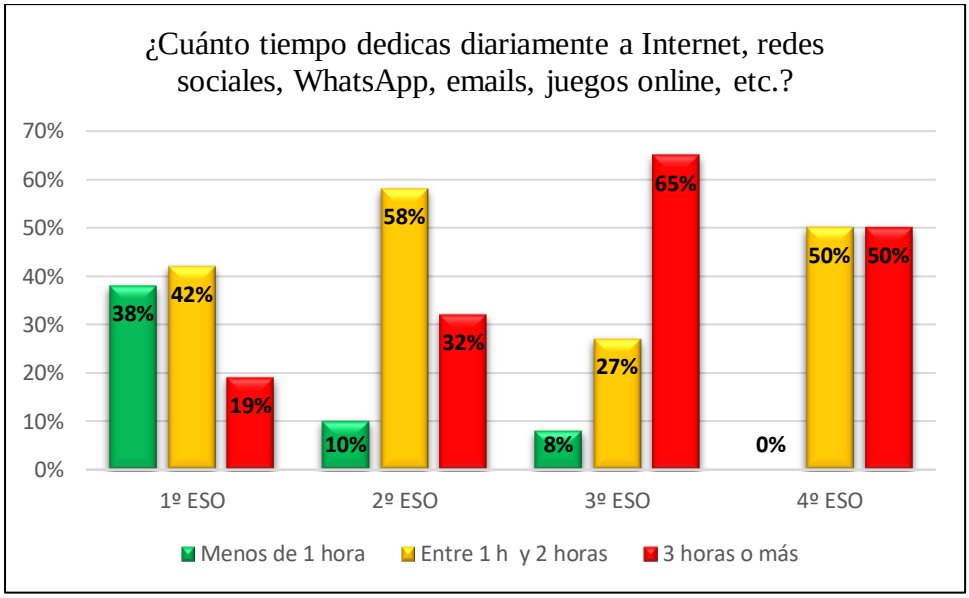

Figura 367. Comparativa 1º a 4º ESO IES Leopoldo Querol (tiempo dedicado Internet, RRSS, etc.).

Tabla 286. *Comparativa 1º a 4º ESO IES Sanchis y Vilaplana (tiempo dedicado Internet, RRSS, etc.).*

¿Cuánto tiempo dedicas diariamente a Internet, redes sociales, WhatsApp, emails, juegos online, etc.?

	1º ESO	2º ESO	3º ESO	4º ESO
Respuestas				
Menos de 1 hora	7%	12%	0%	21%
Entre 1 y 2 horas	44%	46%	37%	28%
3 horas o más	48%	42%	63%	52%

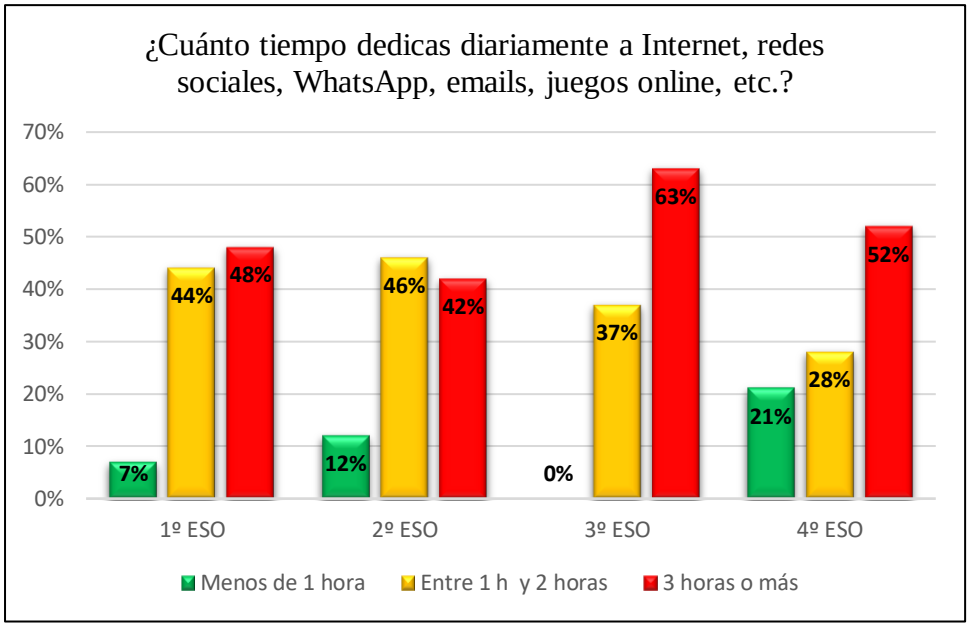

Figura 368. Comparativa 1º a 4º ESO IES Sanchis y Vilaplana (tiempo dedicado Internet, RRSS, etc.).

En este orden de cosas, debemos tener presente que hay personas que poseen conocimientos para poder hackear[28] la webcam[29] de nuestros ordenadores incluso la cámara integrada en nuestros teléfonos móviles, de manera que podrían grabarnos o hacernos fotografías en contra de nuestra voluntad o sin nuestro consentimiento que a posteriori podrían utilizar para extorsionarnos y/o difundir en las redes sociales con el objeto de causarnos un daño moral o psicológico, en su caso.

Por lo tanto, determinadas actividades cotidianas como no tapar la webcam cuando no se está utilizando o tener el ordenador en nuestra habitación, guardar información personal en el teléfono móvil, así como dedicar más de tres horas diariamente a Internet, redes sociales, programas de mensajería instantánea como WhatsApp, emails, juegos online, etc., constituyen factores de riesgo asociados al uso de las TIC.

A contrario sensu, determinadas actividades cotidianas como sí tapar la webcam cuando no se utiliza o tener el ordenador en una zona común de nuestro domicilio en la que los menores pueden tener mayor control parental, no guardar información sensible o personal en el teléfono móvil, así como dedicar entre una y dos horas o menos tiempo, en su caso, diariamente a Internet, redes sociales, programas de mensajería instantánea como WhatsApp, emails, juegos online, etc., constituyen factores de protección asociados al

[28] https://elpais.com/tecnologia/2015/07/10/actualidad/1436529318_258218.html

[29] https://www.youtube.com/watch?v=4Ji__pf3Ir4

uso de las TIC.

Por otra parte, respecto a la frecuencia con la que protagonizan los menores participantes los hechos o llevan a cabo las conductas contempladas en los ítems 1 a 20, respectivamente, como víctimas o victimarios, en su caso, y tras analizar los resultados obtenidos, podemos observar comparativamente, en las tablas 287 a 290 y figuras 369 a 372, por cursos académicos de la ESO de los cuatro centros educativos, individualmente, lo siguiente:

-1º de la ESO:

Tabla 287. *Comparativa valores de riesgo ponderados 1º ESO.*

Curso	Resultado ponderado
1º ESO Consolación	557
1º ESO Divina Providencia	651
1º ESO Leopoldo Querol	504
1º ESO Sanchis y Vilaplana	603

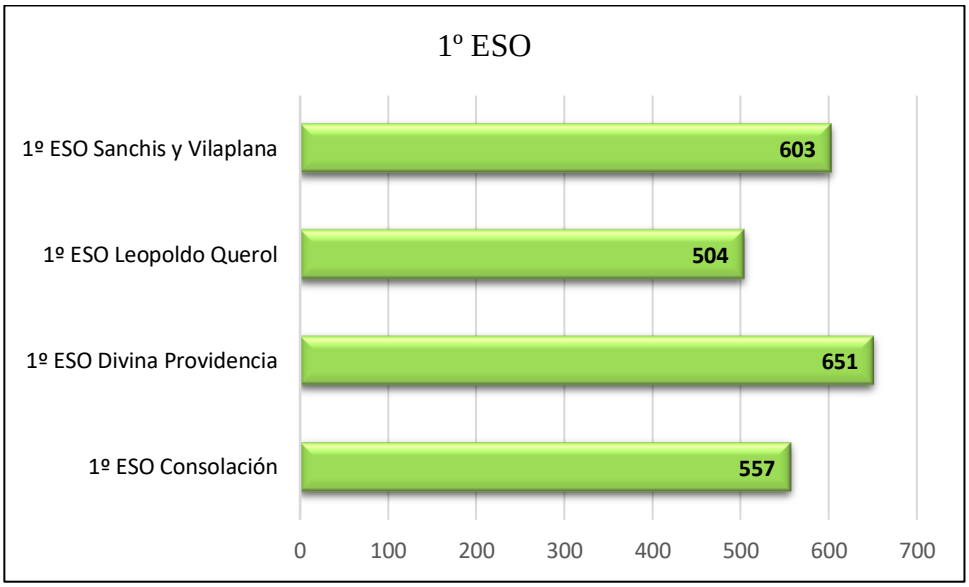

Figura 369. Comparativa valores de riesgo ponderados 1º ESO.

En primer lugar, con un resultado ponderado de 651 y 603, respectivamente, destacaremos los cursos de 1º de la ESO del Colegio Nª. Sª. Divina Providencia y el IES Sanchis y Vilaplana, al encontrarse dentro del rango de puntuación de nivel de riesgo (600-800) correspondiente a la tabla 12, cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es media, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-2º de la ESO:

Tabla 288. *Comparativa valores de riesgo ponderados 2º ESO.*

Curso	Resultado ponderado
2º ESO Consolación	581
2º ESO Divina Providencia	590
2º ESO Leopoldo Querol	659
2º ESO Sanchis y Vilaplana	681

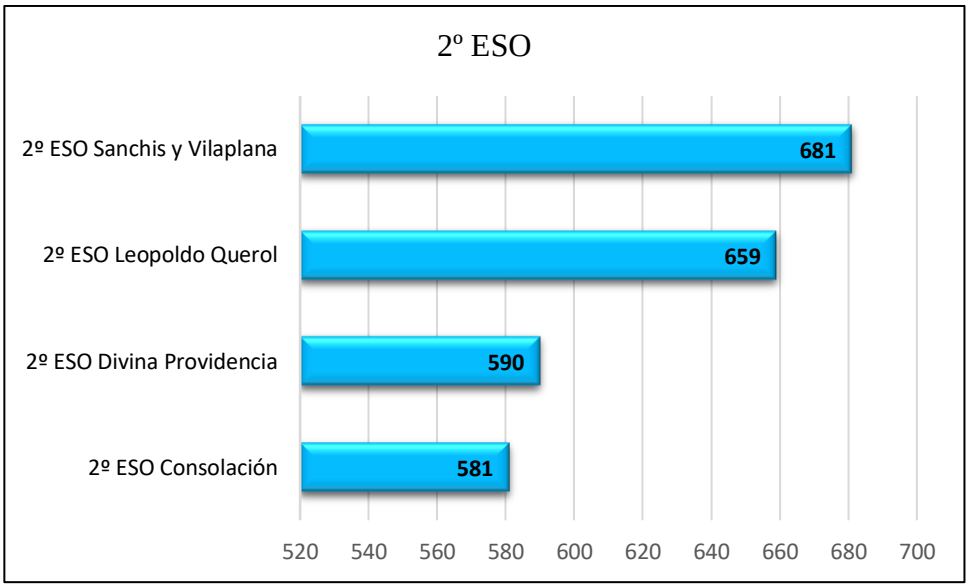

Figura 370. Comparativa valores de riesgo ponderados 2º ESO.

En segundo lugar, con un resultado ponderado de 681 y 659, respectivamente, destacaremos los cursos de 2º de la ESO de los IES Sanchis y Vilaplana y Leopoldo Querol, al encontrarse dentro del rango de puntuación de nivel de riesgo (600-800) correspondiente a la tabla 12, cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es media, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-3º de la ESO:

Tabla 289. *Comparativa valores de riesgo ponderados 3º ESO.*

Curso	Resultado ponderado
3º ESO Consolación	630
3º ESO Divina Providencia	619
3º ESO Leopoldo Querol	617
3º ESO Sanchis y Vilaplana	649

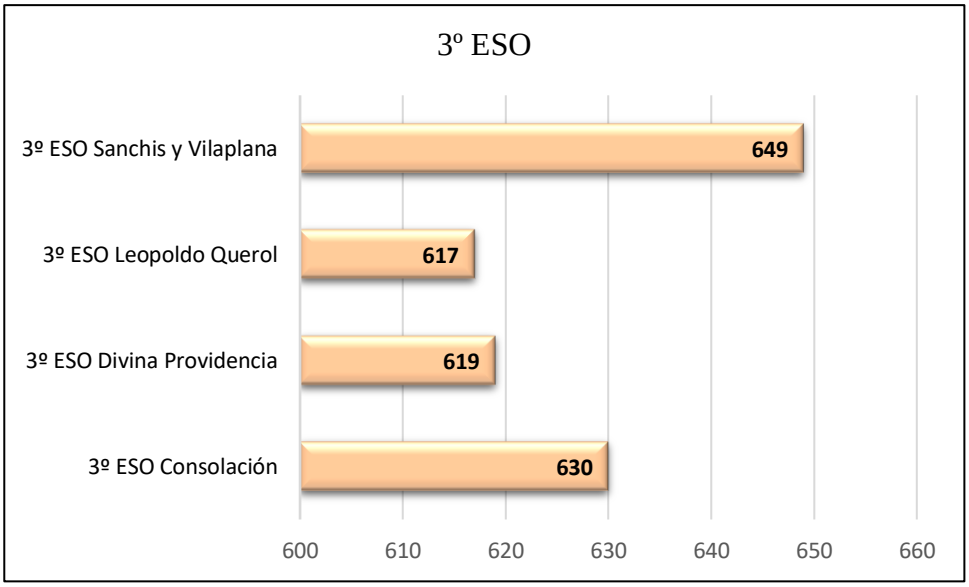

Figura 371. Comparativa valores de riesgo ponderados 3º ESO.

En tercer lugar, con unos resultados ponderados de 649, 630, 619 y 617, respectivamente, destacaremos los cursos de 3º de la ESO de los cuatro centros educativos del presente estudio, al encontrarse todos dentro del rango de puntuación de nivel de riesgo (600-800) correspondiente a la tabla 12, cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es media, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

-4º de la ESO:

Tabla 290. *Comparativa valores de riesgo ponderados 4º ESO.*

Curso	Resultado ponderado
4º ESO Consolación	605
4º ESO Divina Providencia	592
4º ESO Leopoldo Querol	561
4º ESO Sanchis y Vilaplana	663

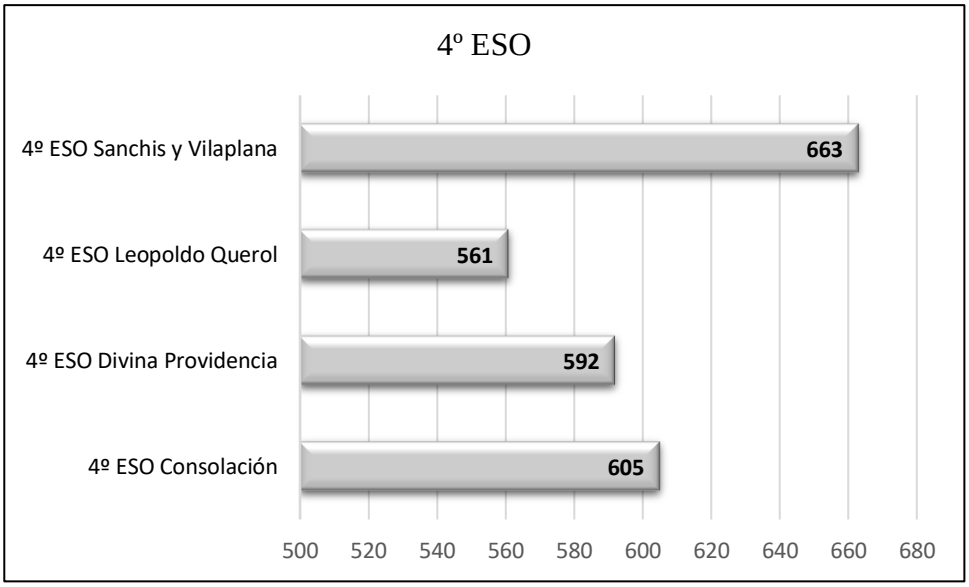

Figura 372. Comparativa valores de riesgo ponderados 4º ESO.

En cuarto lugar, con un resultado ponderado de 663 y 605, respectivamente, destacaremos los cursos de 4º de la ESO del IES Sanchis y Vilaplana y del Colegio Nª. Sª. Consolación, al encontrarse dentro del rango de puntuación de nivel de riesgo (600-800) correspondiente a la tabla 12, cuya VPR y probabilidad individualizada de ser víctima o victimario, en su caso, es media, siendo recomendable como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para los menores que cursan la ESO.

Por otra parte, con relación a la pregunta formulada a los participantes en la encuesta de victimización sobre a quién comunicarían en el supuesto de observar y/o protagonizar alguno de los hechos o conductas mencionados como víctima o victimario, en su caso, podemos observar en la comparativa por cursos de los cuatro centros educativos contenida en las tablas 291 a 294 y en las figuras 373 a 376, respectivamente, que la mayoría de los menores participantes de los cursos 1º a 4º de la ESO pertenecientes a los cuatro centros educativos se decantarían por mayoría, por la opción de comunicarlo en primera instancia a los padres.

Tabla 291. *Comparativa resultados comunicación ciberacoso 1º ESO.*

Respuestas	1º ESO Consolación	1º ESO Divina P.	1º ESO Leopoldo Q.	1º ESO Sanchis y Vilaplana
Compañeros	18%	14%	13%	14%
Padres	63%	57%	63%	59%
Profesores	13%	25%	13%	17%
A nadie	5%	5%	10%	10%

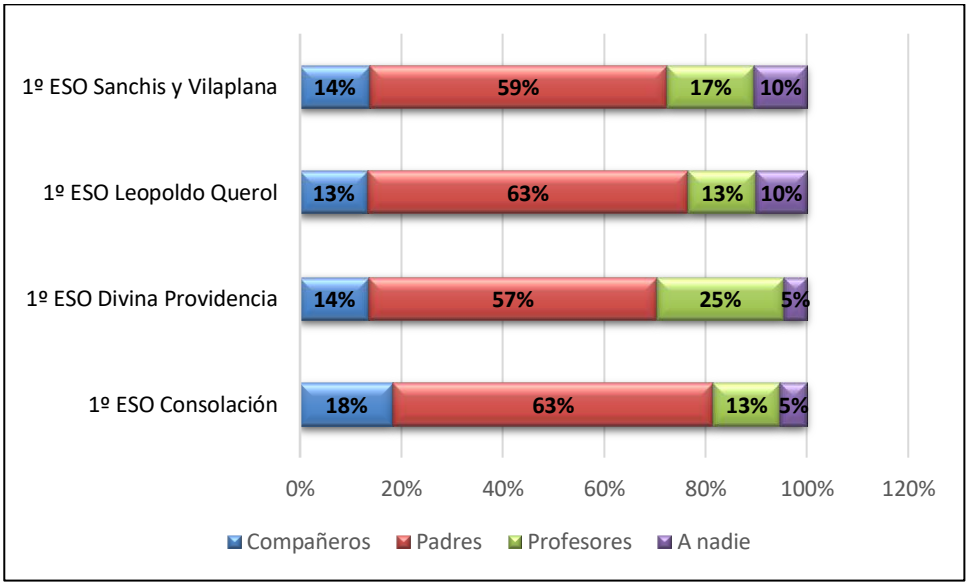

Figura 373. Comparativa resultados comunicación ciberacoso 1º ESO.

Tabla 292. *Comparativa resultados comunicación ciberacoso 2º ESO.*

Respuestas	2º ESO Consolación	2º ESO Divina P.	2º ESO Leopoldo Q.	2º ESO Sanchis y Vilaplana
Compañeros	22%	27%	18%	23%
Padres	64%	49%	61%	54%
Profesores	11%	16%	18%	17%
A nadie	3%	8%	2%	6%

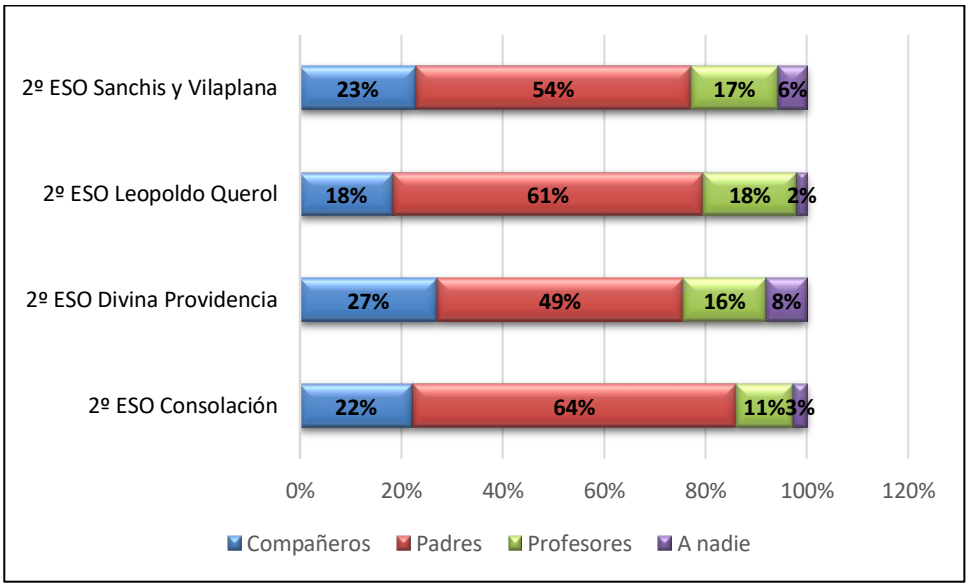

Figura 374. Comparativa resultados comunicación ciberacoso 2º ESO.

Tabla 293. *Comparativa resultados comunicación ciberacoso 3º ESO.*

Respuestas	3º ESO Consolación	3º ESO Divina P.	3º ESO Leopoldo Q.	3º ESO Sanchis y Vilaplana
Compañeros	31%	34%	31%	31%
Padres	44%	43%	56%	51%
Profesores	20%	9%	3%	14%
A nadie	4%	14%	9%	3%

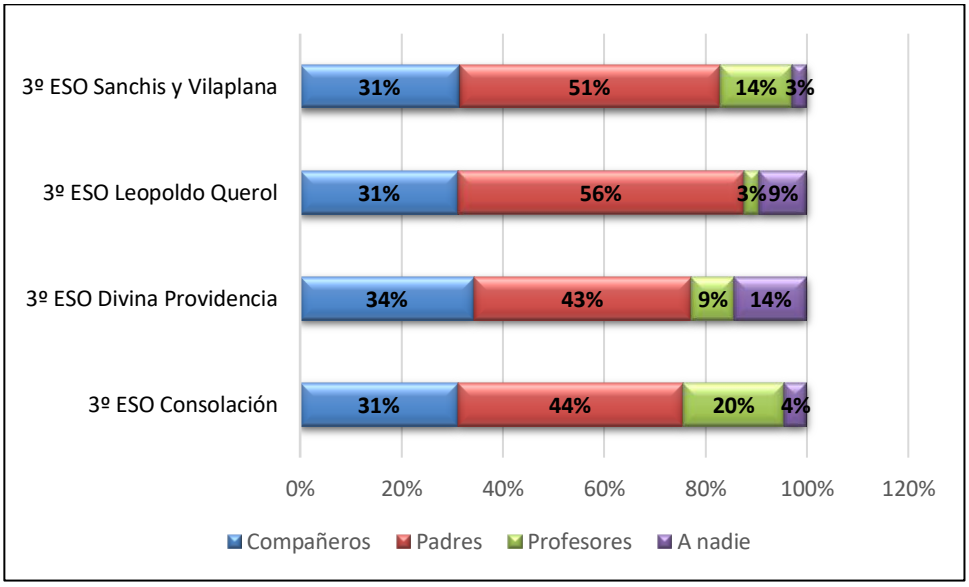

Figura 375. Comparativa resultados comunicación ciberacoso 3º ESO.

Tabla 294. *Comparativa resultados comunicación ciberacoso 4º ESO.*

Respuestas	4º ESO Consolación	4º ESO Divina P.	4º ESO Leopoldo Q.	4º ESO Sanchis y Vilaplana
Compañeros	23%	19%	21%	24%
Padres	77%	52%	56%	55%
Profesores	0%	13%	15%	16%
A nadie	0%	16%	9%	5%

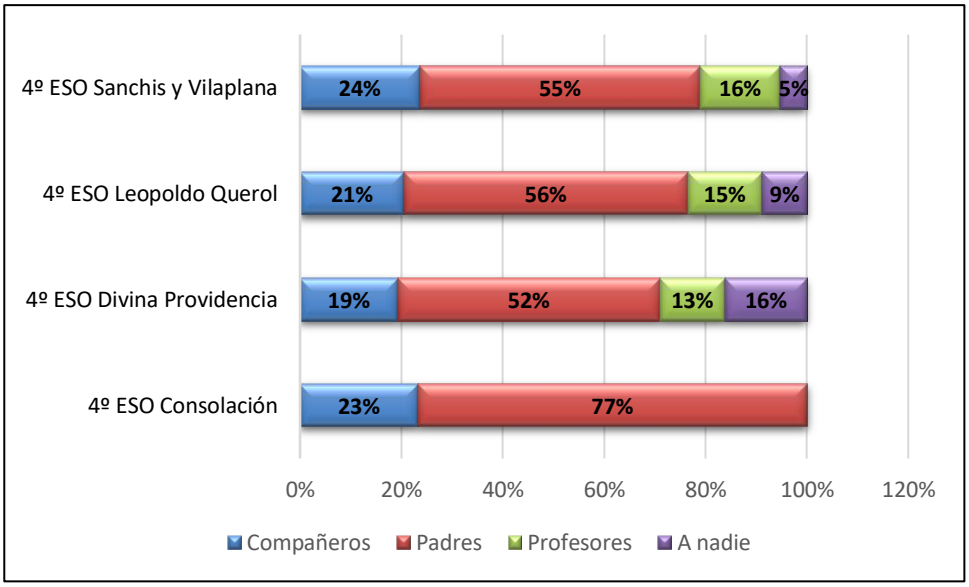

Figura 376. Comparativa resultados comunicación ciberacoso 4º ESO.

Por último, con relación a los resultados obtenidos sobre qué actividades preventivas han propuesto los menores participantes frente a hechos o conductas de ciberacoso, podemos observar en la comparativa por cursos de los cuatro centros educativos expuesta en las tablas 295 a 298 y en las figuras 377 a 380, respectivamente, que la mayoría de los menores participantes de los cursos 1º a 4º de la ESO pertenecientes a los cuatro centros educativos abogan, mayoritariamente, por las opciones de comunicar los hechos a personas adultas y denunciarlos a la policía, en su caso.

Tabla 295. *Comparativa resultados propuestas preventivas ciberacoso 1º ESO.*

Respuestas	1º ESO Nª. Sª. Consolación	1º ESO Nª. Sª. Divina Providencia	1º ESO Leopoldo Querol	1º ESO Sanchis y Vilaplana
Comunicar adultos	45%	41%	40%	33%
Denunciar a la policía	26%	35%	28%	35%
Ignorar ciberacoso	6%	2%	0%	8%
Mediar con el ciberacosador	4%	2%	0%	2%
Pedir ayuda	19%	16%	23%	17%
Otras	0%	4%	10%	4%

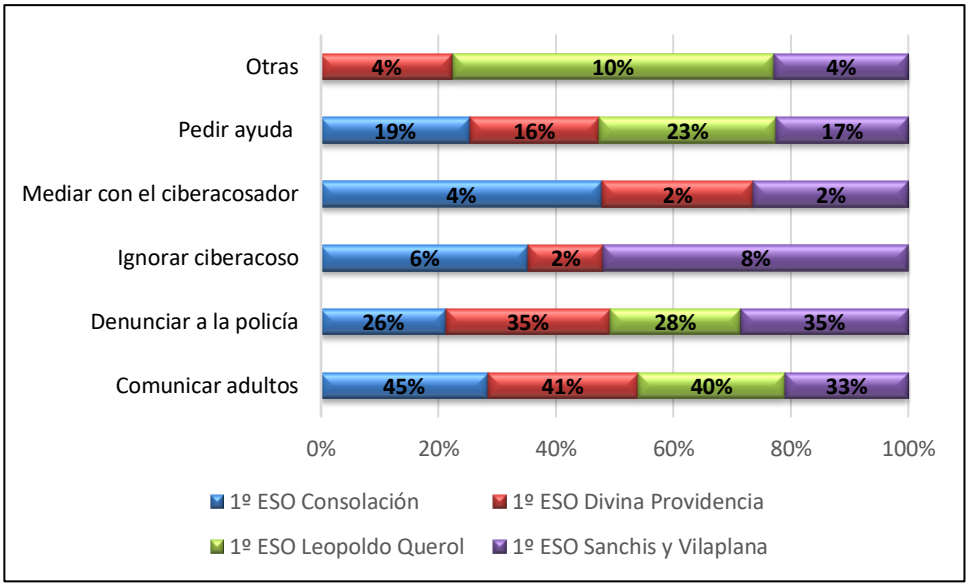

Figura 377. Comparativa resultados propuestas preventivas ciberacoso 1º ESO.

Tabla 296. *Comparativa resultados propuestas preventivas ciberacoso 2º ESO.*

Respuestas	2º ESO Nª. Sª. Consolación	2º ESO Nª. Sª. Divina Providencia	2º ESO Leopoldo Querol	2º ESO Sanchis y Vilaplana
Comunicar adultos	33%	37%	32%	33%
Denunciar a la policía	35%	32%	31%	22%
Ignorar ciberacoso	0%	0%	3%	5%
Mediar con el ciberacosador	4%	5%	10%	9%
Pedir ayuda	22%	25%	21%	24%
Otras	6%	0%	3%	7%

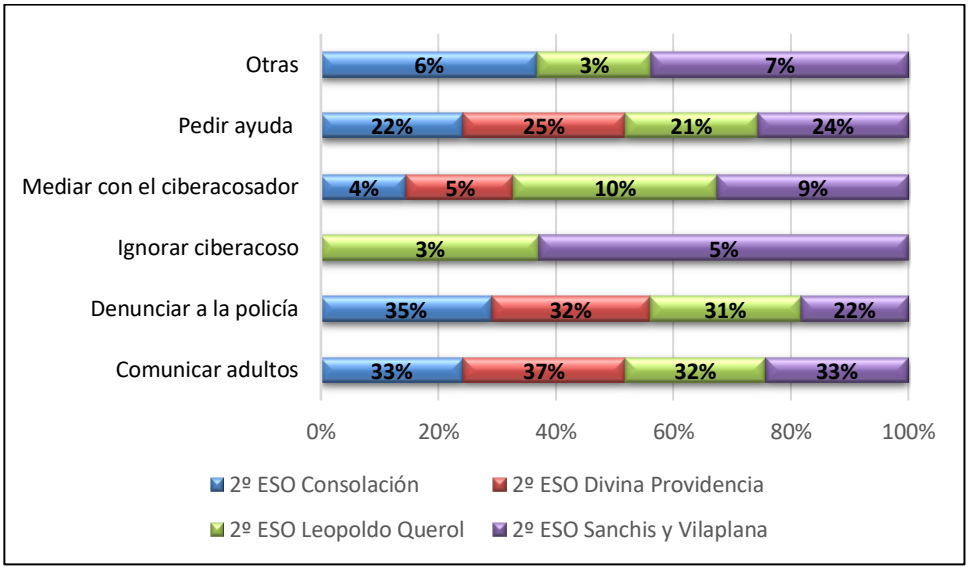

Figura 378. Comparativa resultados propuestas preventivas ciberacoso 2º ESO.

Tabla 297. *Comparativa resultados propuestas preventivas ciberacoso 3º ESO.*

Respuestas	3º ESO Nª. Sª. Consolación	3º ESO Nª. Sª. Divina Providencia	3º ESO Leopoldo Querol	3º ESO Sanchis y Vilaplana
Comunicar adultos	34%	30%	31%	26%
Denunciar a la policía	31%	23%	33%	35%
Ignorar ciberacoso	3%	3%	6%	6%
Mediar con el ciberacosador	3%	11%	4%	2%
Pedir ayuda	25%	26%	18%	24%
Otras	3%	8%	8%	7%

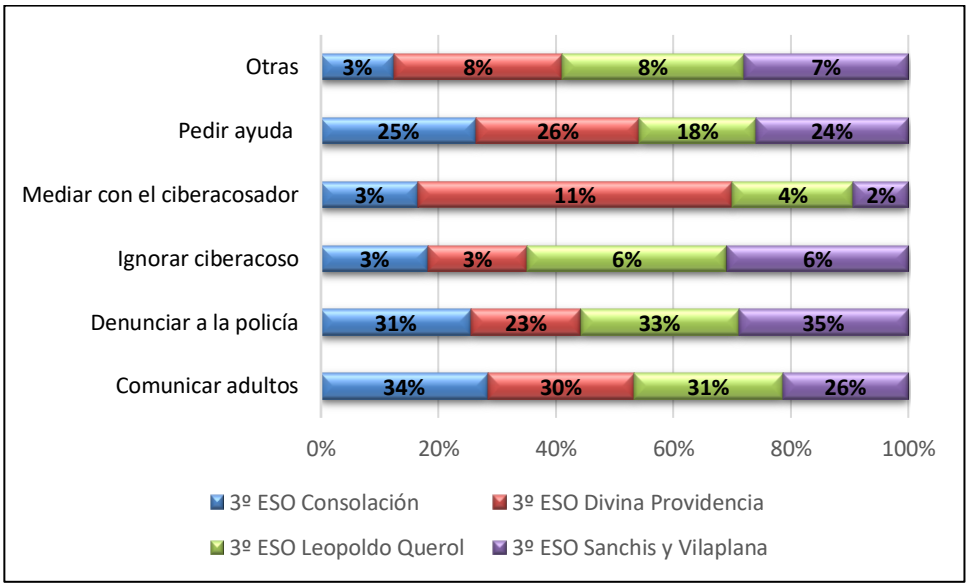

Figura 379. Comparativa resultados propuestas preventivas ciberacoso 3º ESO.

Tabla 298. *Comparativa resultados propuestas preventivas ciberacoso 4º ESO.*

Respuestas	4º ESO Nª. Sª. Consolación	4º ESO Nª. Sª. Divina Providencia	4º ESO Leopoldo Querol	4º ESO Sanchis y Vilaplana
Comunicar adultos	27%	30%	40%	27%
Denunciar a la policía	35%	27%	36%	31%
Ignorar ciberacoso	0%	5%	2%	2%
Mediar con el ciberacosador	2%	7%	2%	4%
Pedir ayuda	33%	25%	17%	25%
Otras	4%	7%	2%	12%

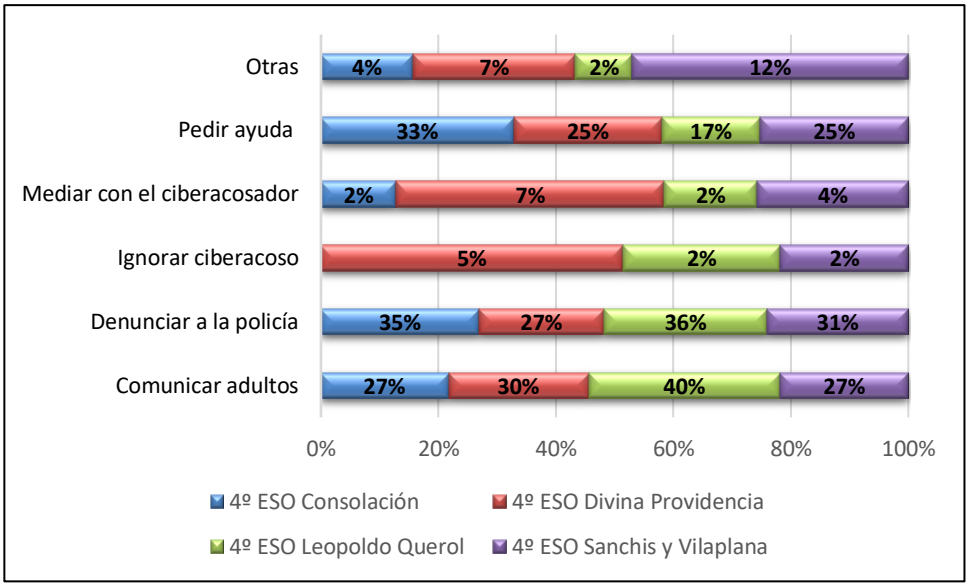

Figura 380. Comparativa resultados propuestas preventivas ciberacoso 4º ESO.

No obstante, de la comparativa expuesta también destacar que, entre las respuestas opcionales, la propuesta preventiva consistente en mediar con el ciberacosador ha obtenido unos resultados catastróficos en el estudio, es decir, unos porcentajes muy bajos, constituyendo una evidencia de que la mayoría de los menores participantes no cree o no ven una funcionalidad eficaz en la figura de la mediación para la resolución de conflictos interpersonales en el ámbito del ciberacoso, a pesar de contemplarse en el artículo 10 de Orden 62/2014, de 28 de julio, de la Conselleria de Educación, Cultura y Deporte, por la que se actualiza la normativa que regula la elaboración de los planes de convivencia en los centros educativos de la Comunidad Valenciana y se establecen los protocolos de actuación e intervención ante supuestos de violencia escolar, al amparo del artículo 7 del Decreto 39/2008, de 4 de abril, del Consell, sobre la convivencia en los centros docentes no universitarios sostenidos con fondos públicos y sobre los derechos y deberes del alumnado, padres, madres, tutores o tutoras, profesorado y personal de administración y servicios.

Así que, vistos los resultados obtenidos en el presente estudio, si tuviésemos que evaluar la eficacia de las dos normas reseñadas con relación a la figura del docente mediador o de equipos de mediación específicos, en su caso, en aras de resolver conflictos interpersonales en el ámbito del ciberacoso en los que se otorgue participación al alumnado así como la implementación de otros mecanismos para incentivar la resolución de los conflictos en el ámbito interno de los centros escolares, dotándolos de medios humanos y materiales necesarios para fomentar la participación de las familias en el

proceso de detección y resolución de los conflictos, perfectamente, podríamos darle un suspenso rotundo.

V.2. Discusión estudio cibercriminalidad económica.

En primer lugar, respecto al género y edad de los participantes, el 50% son hombres y el otro 50% mujeres, siendo la media de edad de los hombres de 45,44 años frente a la media de edad de las mujeres de 43,18 años.

Si analizamos los datos obtenidos con relación a la interacción con las TIC de los regentes de los comercios, establecimientos públicos y/o microempresas, en su caso, podemos observar en los resultados arrojados que la mayoría tienen ordenador en casa (84%) y en su negocio o empresa (92%) y también poseen teléfono móvil (100%), evidencias que nos indican que su interacción con las TIC es elevada y por ende con Internet.

Que más del 50% de los participantes manifestaran guardar información personal y/o confidencial del negocio en el teléfono móvil nos indica que, ante la pérdida o sustracción de éste, podrían tener un mayor riesgo de ser cibervictimizados, por el uso, en su caso, que terceras personas podrían hacer con la información sensible que contengan sus dispositivos móviles.

Que el 74% de los participantes hayan manifestado tener una cuenta de correo electrónico con fines comerciales, nos indica que el riesgo de ser víctima de la cibercriminalidad económica aumenta al interaccionar con sus clientes, proveedores, etc., por este medio.

Que el 54% de los participantes tengan página web de su negocio o empresa, un 67% utilice programas de mensajería instantánea como WhatsApp y un 77% utilice redes sociales con fines comerciales constituye una evidencia clara de que la mayoría ha apostado por la digitalización de sus negocios lo que conlleva una serie de ciberriesgos económicos inherentes.

A contrario sensu, únicamente un 25% de los participantes ha manifestado utilizar blogs, foros en Internet con fines comerciales, cuando también es una buena herramienta digital para conocer opiniones de clientes e interactuar con ellos, en su caso.

En este orden de cosas, si analizamos los resultados obtenidos en la encuesta de cibercriminalidad económica con relación al ítem sobre el conocimiento de los regentes de los establecimientos públicos y comercios de la existencia de una serie determinada de

tecnologías biométricas, podemos observar que en general hay más participantes que no conocen las tecnologías biométricas, es decir, un 55% frente a un 45% que sí las conocen, hecho que nos indica que los participantes se encuentran más expuestos en sus actividades cotidianas, y por tanto tienen más riesgo de cibervictimización al constituir las tecnologías biométricas reseñadas una herramienta de autoprotección en ciberseguridad que, evidentemente, no solo basta con conocerlas sino también en aplicarlas, en su caso.

Respecto a la frecuencia con qué protagonizan los participantes los hechos o lleva a cabo las conductas contempladas en los ítems 1 a 20, respectivamente, podemos observar que:

1º) en el ítem 1, la frecuencia con la que los participantes han perdido alguna vez el teléfono, tableta, ordenador portátil, etc., oscila de uno (nunca) a tres (algunas veces), siendo la media de 1,41.

2º) en el ítem 2, la frecuencia con la que a los participantes les han sustraído alguna vez el teléfono móvil, tableta, ordenador portátil, etc., oscila de uno (nunca) a tres (algunas veces), siendo la media de 1,30.

3º) en el ítem 3, la frecuencia con la que los participantes han perdido alguna vez un pendrive con información confidencial de su negocio y/o particular, oscila de uno (nunca) a tres (algunas veces), siendo la media de 1,11.

4º) en el ítem 4, la frecuencia con la que a los participantes se les ha infectado alguna vez su ordenador, teléfono móvil, tableta, etc., con algún virus o programa maligno, oscila de uno (nunca) a cuatro (muchas veces), siendo la media de 2,16.

5º) en el ítem 5, la frecuencia con la que los participantes han perdido archivos de su negocio por infección de programas malignos oscila de uno (nunca) a tres (algunas veces), siendo la media de 1,34.

6º) en el ítem 6, la frecuencia con la que los participantes han recibido alguna vez mensajes por WhatsApp, correo electrónico, redes sociales, etc., en la que se prometen grandes cantidades de dinero a cambio de pequeñas transferencias, oscila de uno (nunca) a cinco (siempre), siendo la media de 2,11.

7º) en el ítem 7, la frecuencia con la que los participantes han recibido alguna vez masivamente correos electrónicos no deseados de publicidad (spam), oscila de uno (nunca) a cinco (siempre), siendo la media de 3,21.

8º) en el ítem 8, la frecuencia con la que a los participantes les han suplantado la página web, Facebook, etc., oscila de uno (nunca) a tres (algunas veces), de su negocio, siendo la media de 1,06.

9º) en el ítem 9, la frecuencia con la que los participantes al contactar telemáticamente con proveedores o clientes, en su caso, les han sustraído contraseñas, datos personales de la tarjeta de crédito, etc., oscila de uno (nunca) a tres (algunas veces), de su negocio, siendo la media de 1,11.

10º) en el ítem 10, la frecuencia con la que los participantes al efectuar una compraventa en su negocio un cliente ha utilizado una tarjeta de crédito sustraída, oscila de uno (nunca) a tres (algunas veces), de su negocio, siendo la media de 1,25.

11º) en el ítem 11, la frecuencia con la que los participantes han sido víctimas de algún tipo de fraude online, extorsión, etc., oscila de uno (nunca) a cuatro (muchas veces), de su negocio, siendo la media de 1,25.

12º) en el ítem 12, la frecuencia con la que los participantes emiten opiniones de carácter político, religioso o ideológico en redes sociales abiertas, profesionales o mixtas, varía de uno (nunca) a cinco (siempre), siendo la media de 1,17.

13º) en el ítem 13, la frecuencia con la que los participantes critican de manera irresponsable y sin argumentos productos o proyectos de la competencia, varía de uno (nunca) a cinco (siempre), siendo la media de 1,11.

14º) en el ítem 14, la frecuencia con la que los participantes evitan entrar en debates y discusiones con clientes o potenciales clientes a través de las redes sociales varía de uno (nunca) a cinco (siempre), siendo la media de 3,79.

15º) en el ítem 15, la frecuencia con la que los participantes evitan dar información confidencial sobre su negocio que pueda usar la competencia, oscila de uno (nunca) a cinco (siempre), siendo la media de 3,98.

16º) en el ítem 16, la frecuencia con la que los participantes eliminan de forma segura la información confidencial archivada que no necesita, oscila de uno (nunca) a cinco (siempre), siendo la media de 3,85.

17º) en el ítem 17, la frecuencia con la que los participantes cifran la información confidencial oscila de uno (nunca) a cinco (siempre), siendo la media de 2,71.

18º) en el ítem 18, la frecuencia con la que los participantes utilizan los servicios de almacenamiento en la nube oscila de uno (nunca) a cinco (siempre), siendo la media de 2,55.

19º) en el ítem 19, la frecuencia con la que los participantes realizan copias de seguridad en otro soporte de la información almacenada en el teléfono móvil, ordenador, tableta, etc., varía de uno (nunca) a cinco (siempre), siendo la media de 3,55.

20º) en el ítem 20, la frecuencia con la que los participantes utilizan códigos de

desbloqueo de pantalla (código numérico o patrón) en su teléfono móvil, tableta, ordenador, etc., varía de uno (nunca) a cinco (siempre), siendo la media de 4,12.

En este orden de cosas, como podemos apreciar en los ítems 1 a 13 referenciados, cuanto más elevada sea la frecuencia de las conductas o hechos protagonizados por los participantes conllevará un mayor riesgo de cibervictimización.

A contrario sensu, en los ítems 14 a 20 reseñados, cuanto más elevada sea la frecuencia de las conductas o hechos protagonizados por los participantes conllevará un menor riesgo de cibervictimización.

Por último, tenemos que destacar que los 3704 puntos obtenidos, se encuentran en el rango de puntuación de nivel de riesgo (3600-4400) de la tabla 250.

En virtud del rango de clasificación mencionado, el riesgo de cibervictimización generalizado de los autónomos y microempresas de la ciudad de Vinaròs participantes en el estudio sería moderado, de probabilidad media y de impacto medio con una estimación de riesgo de 4.

VI. CONCLUSIONES.

VI.1. Conclusiones estudio cibercriminalidad social.

Primera. La interacción con las TIC e Internet de los menores participantes de los cuatro centros educativos objeto de este estudio es elevada constituyendo un factor probabilístico de mayor riesgo de ser víctima o victimario, en su caso, de la cibercriminalidad social.

Segunda. La probabilidad de riesgo de cibervictimización de los menores aumenta cuando menor sea el control parental en la supervisión de sus interacciones con las TIC.

Tercera. La probabilidad de riesgo de cibervictimización de los menores aumenta al guardar información personal o sensible en sus teléfonos móviles.

Cuarta. Determinadas actividades cotidianas llevadas a cabo por los menores como no tapar la webcam cuando no se está utilizando, tener el ordenador en su habitación, guardar información personal en el teléfono móvil, así como dedicar más de tres horas diariamente a Internet, redes sociales, programas de mensajería instantánea como WhatsApp, emails, juegos online, etc., constituyen factores de mayor riesgo de cibervictimización.

Quinta. Podemos afirmar en base al estudio realizado que cuanto más elevada sea

la frecuencia de las conductas o hechos protagonizados por los menores participantes relacionados con los ítems 1 a 20 de la encuesta de victimización, mayor riesgo tendrán de ser víctimas o victimarios, en su caso, de la cibercriminalidad social.

Sexta. En general, se recomienda como medida de autoprotección la formación e información en ciberseguridad sobre uso seguro de las TIC y redes sociales para todos los menores que cursan la ESO en la ciudad de Vinaròs, destacando como resultado de este estudio que los cursos de 3º de la ESO pertenecientes a los cuatro centros educativos, son los que han arrojado en su totalidad un resultado de riesgo ponderado individualizado de ser víctima o victimario, en su caso, medio.

Séptima. En el supuesto de observar y/o protagonizar alguno de los hechos o conductas relacionados con el ciberacoso como víctima o victimario, en su caso, la mayoría de los menores participantes que cursan la ESO objeto de este estudio, se decantarían en primera instancia, por la opción de comunicarlo a sus padres.

Octava. La mayoría de los menores participantes que cursan la ESO han propuesto como actividades o medidas preventivas frente a hechos o conductas relacionadas con las distintas modalidades de ciberacoso, las opciones de comunicar los hechos a personas adultas y denunciarlos a la policía, en su caso, es decir, priorizan una judicialización del conflicto frente a otras opciones extrajudiciales como la mediación para su resolución.

Novena. La mayoría de los menores participantes que cursan la ESO en Vinaròs, no cree o no ven una funcionalidad eficaz en la figura de la mediación para la resolución de conflictos interpersonales en el ámbito del ciberacoso, a pesar de contemplarse en el artículo 10 de Orden 62/2014, de 28 de julio, de la Conselleria de Educación, Cultura y Deporte, por la que se actualiza la normativa que regula la elaboración de los planes de convivencia en los centros educativos de la Comunidad Valenciana y se establecen los protocolos de actuación e intervención ante supuestos de violencia escolar, al amparo del artículo 7 del Decreto 39/2008, de 4 de abril, del Consell, sobre la convivencia en los centros docentes no universitarios sostenidos con fondos públicos y sobre los derechos y deberes del alumnado, padres, madres, tutores o tutoras, profesorado y personal de administración y servicios.

Décima. Anualmente, debería evaluarse tanto a nivel autonómico como municipal, la eficacia de las dos normas reseñadas en la novena conclusión, con relación a la figura del docente mediador o de equipos de mediación específicos, en su caso, en aras de resolver conflictos interpersonales en el ámbito del ciberacoso en los que se

otorgue participación al alumnado así como en la implementación de otros mecanismos para incentivar la resolución de los conflictos en el ámbito interno de los centros escolares, dotándolos de medios humanos y materiales necesarios para fomentar la participación de las familias en el proceso de detección y resolución de los conflictos.

V I.2. Conclusiones cibercriminalidad económica.

Primera. La interacción con las TIC de los regentes de los comercios, establecimientos públicos y/o microempresas, en su caso, en el ámbito de sus actividades rutinarias es elevada y por ende con Internet, aumentando la probabilidad y/o riesgo de ser víctimas de la cibercriminalidad económica.

Segunda. El hecho de que haya un 55% de los participantes que desconozcan las tecnologías biométricas frente a un 45% que sí las conozcan, constituye un factor de riesgo de cibervictimización al encontrarse más expuestos en sus actividades cotidianas y que, además, deberán saber aplicar o utilizar, en su caso, máxime cuando más del 50% de los participantes manifestaron guardar información personal y/o confidencial de su negocio en el teléfono móvil.

Tercera. El hecho de haber obtenido una media de 3,21 con relación a la frecuencia con la que los participantes han recibido alguna vez masivamente correos electrónicos no deseados de publicidad (spam), constituye un factor de riesgo de cibervictimización de conductas delictivas tales como el *phishing*.

Cuarta. El hecho de haber obtenido una media de 3,55 con relación a la frecuencia con la que los participantes realizan copias de seguridad en otro soporte de la información almacenada en el teléfono móvil, ordenador, tableta, etc., constituye un factor de protección frente a la cibervictimización económica.

Quinta. El hecho de haber obtenido una media de 4,12 con relación a la frecuencia con la que los participantes utilizan códigos de desbloqueo de pantalla (código numérico o patrón) en su teléfono móvil, tableta, ordenador, etc., constituye un factor de protección frente a la cibervictimización económica.

Sexta. El hecho de haber obtenido una media de 3,79 con relación a la frecuencia con la que los participantes evitan entrar en debates y discusiones con clientes o potenciales clientes a través de las redes sociales constituye un factor de protección frente a la cibervictimización económica.

Séptima. El hecho de haber obtenido una media de 3,85 con relación a la frecuencia con la que los participantes eliminan de forma segura la información

confidencial archivada que no necesita, constituye un factor de protección frente a la cibervictimización económica.

Octava. Las variables sociodemográficas obtenidas en el presente estudio no son relevantes con relación a una mayor o menor probabilidad, en su caso, de ser víctimas de la cibercriminalidad económica.

Novena. Desde una perspectiva criminológica preventiva, se debe fomentar la formación e información en el ámbito de la ciberseguridad e interacción con las TIC tanto para trabajadores autónomos, microempresas y sus empleados, en su caso, de la ciudad de Vinaròs, aunque la estimación de riesgo de cibervictimización obtenida en la puntuación del presente estudio haya sido moderada.

BIBLIOGRAFÍA.

Antón, J.I. (2007). *El delito como cuestión social*. Editorial Salamanca: Ciencias de la Seguridad Universidad de Salamanca.

Ayerbe, A. (2020). La ciberseguridad y su relación con la inteligencia artificial (noticia blog). Recuperado de https://www.realinstitutoelcano.org/analisis/la-ciberseguridad-y-su-relacion-con-la-inteligencia-artificial/

BBC Mundo (2013, 7 de junio). Cómo te pueden hackear la webcam de tu computadora [archivo de vídeo]. Recuperado de https://www.youtube.com/watch?v=4Ji__pf3Ir4

Brantingham, P.J. y Brantingham, P.L. (1994). *Environmental Criminology Prospect Heights*. OH: Waveland.

Betancourt, A. (2022, 5 de marzo). Tres apps para la seguridad de las mujeres. Recuperado de https://www.enter.co/chips-bits/apps-software/tres-apps-para-la-seguridad-de-las-mujeres/

Biurrun, A. (2021, 23 de diciembre). Phishing: el INCIBE alerta del envío de facturas falsas a clientes de Iberdrola. La Razón. Recuperado de https://www.larazon.es/tecnologia/20211223/hqsdicgrjre63oajfllmdwgfri.html

Bocij, P. y McFarlane, L. (2003). Seven fallacies about cyberstaking. *Prison Service Journal*, *149*, 37-42.

BOE (2016, 22 de enero). Circular 1/2016, de 22 de enero, sobre la responsabilidad penal

de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015. Recuperado de https://www.boe.es/buscar/doc.php?id=FIS-C-2016-00001

Burrueco, A. (2021, 30 de noviembre). Día Internacional de la Ciberseguridad: ¿Qué opinan de ella los expertos? Recuperado de https://cybersecuritynews.es/dia-internacional-de-la-ciberseguridad-que-opinan-de-ella-los-expertos/

Calvete, E., Orue, I., Estévez, A., Villardón, L., y Padilla, P. (2010). Cyberbullying in adolescents: modalities and aggressors' profile. *Computers in Human Behavior, 26*(5), 1128-1135. Recovered from https://www.researchgate.net/publication/220495959_Cyberbullying_in_adolescents_Modalities_and_aggressors%27_profile

Calmaestra, J. (2011). *Cyberbullying: prevalencia y características de un nuevo tipo de bullying indirecto*. (Tesis doctoral). Universidad de Córdoba. Recuperado de https://helvia.uco.es/xmlui/handle/10396/5717

Calmaestra, J. et al. (2016). Yo a eso no juego. Bullying y Ciberbullying en la infancia. Recuperado de https://www.savethechildren.es/sites/default/files/imce/docs/yo_a_eso_no_juego.pdf

Cano Paños, M.A. (2008). Internet y terrorismo islamista aspectos criminológicos y legales. Internet y terrorismo islamista. Aspectos criminológicos y legales. Eguzkilore: Cuaderno del Instituto Vasco de Criminología, 22, 67-88. Recuperado de https://www.ehu.eus/es/web/ivac/cuaderno-eguzkilore-22

Cañas, E., Estévez, E., Marzo, J.C., y Piqueras, J.A. (2019). Ajuste psicológico en cibervíctimas y ciberagresores en educación secundaria. Anales de Psicología, 35(3), 434-443. https://doi.org/10.6018/analesps.35.3.323151

CCN-CERT (2022, 31 de marzo). Aprobado el Plan Nacional de Ciberseguridad. Recuperado de Aprobado el Plan Nacional de Ciberseguridad (cni.es)

Climent, C; Garrido, V; Guardiola, J. (2012). *El informe criminológico forense: teoría y práctica*. Valencia: Editorial Tirant Lo Blanch.

Confederación Canaria de Empresarios (2019). Guía compliance para pymes. Recuperado de https://www.ccelpa.org/wp-

content/uploads/2019/12/Gu%C3%ADa-Compliance-para-PYMES.pdf

Constitución Española de 31 de octubre de 1978. Boletín Oficial del Estado, nº 311.1, 1978, 29 diciembre.

Decreto 39/2008, de 4 de abril, del Consell, sobre la convivencia en los centros docentes no universitarios sostenidos con fondos públicos y sobre los derechos y deberes del alumnado, padres, madres, tutores o tutoras, profesorado y personal de administración y servicio. *DOCV (Diario Oficial de la Comunitat Valenciana)*, 5738, de 9 de abril de 2008, 55906-55931.

Defensor del Pueblo (2007). Violencia escolar: el maltrato entre iguales en la educación secundaria obligatoria 1999-2006. *Publicaciones de la oficina del Defensor del Pueblo.* Recuperado de https://www.defensordelpueblo.es/informe-monografico/violencia-escolar-el-maltrato-entre-iguales-en-la-educacion-secundaria-obligatoria-1999-2006-nuevo-estudio-y-actualizacion-del-informe-2000-2007/

De Pedro, S. (2020). Inteligencia artificial, nueva arma para cibercriminales (noticia blog). Recuperado dehttps://gaptain.com/blog/inteligencia-artificial-la-nueva-arma-de-los-cibercriminales/

Desurmont, N. (2009). La géocriminologie en contexte de gang-stalking. *International e-journal of criminal sciences*, *3*, 1-28. Récupéré dans https://ojs.ehu.eus/index.php/inecs/article/view/259

El País (2015). Así de fácil pueden 'hackear' tu webcam. Recuperado de https://elpais.com/tecnologia/2015/07/10/actualidad/1436529318_258218.html

Europa press (2022). El Observatorio Nacional de Tecnología pide considerar la violencia de género digital en el ordenamiento jurídico. Recuperado de https://www.europapress.es/epsocial/igualdad/noticia-observatorio-nacional-tecnologia-pide-considerar-violencia-genero-digital-ordenamiento-juridico-20220412173343.html

Expósito Aguirre, O. (2019). *Programa de prevención para la ciberviolencia de género en adolescentes.* (Trabajo Fin de Grado). Universidad de Almería. Recuperado de http://repositorio.ual.es/handle/10835/9719

Faes, I. (2021). Europa impone más obligaciones de ciberseguridad a las empresas. *El*

economista.es. Recuperado de https://www.eleconomista.es/legislacion/noticias/11476429/11/21/Europa-impone-mas-obligaciones-de-ciberseguridad-a-las-empresas.html

Faustino, D. (2021). La protección total en ciberseguridad no existe. El economista.es. Recuperado de https://revistas.eleconomista.es/digital/2021/septiembre/la-proteccion-total-en-ciberseguridad-no-existe-AJ8975398

Felson, M. & Clarke, R.V. (1998). La ocasión hace al ladrón. Teoría práctica para la prevención del delito. *Serie Claves del Gobierno Local*, 6, pp.193-233. Recuperado de http://repositorio.gobiernolocal.es/xmlui/bitstream/handle/10873/855/claves06_09_felson_clarke.pdf

Fernández, M.G. (2022, 17 de febrero). Más de 850 adolescentes de 14 a 17 años tienen protección policial por sufrir violencia de género. Recuperado de https://www.elespanol.com/mujer/actualidad/20220217/adolescentes-anos-proteccion-policial-sufrir-violencia-genero-delito/650935242_0.html

Fernández, S.A. (2020, 22 de abril). Las nuevas tecnologías y la responsabilidad por culpa *in vigilando* (artículo de un blog). Recuperado de https://prevencionar.com/2020/04/22/las-nuevas-tecnologias-y-la-responsabilidad-por-culpa-in-vigilando/

Fiscal.es (2019). Las estafas son los delitos que más se denuncian en la red. Recuperado de https://www.fiscal.es/web/fiscal/-/elvira-tejada-fiscal-de-sala-de-criminalidad-informatica-las-estafas-son-los-delitos-que-mas-se-denuncian-en-la-red-

Garaigordobil, M. (2011). Prevalencia y consecuencias del cyberbullying: una revisión. *International journal of psychology and psychological therapy, 11*(2), 233-254. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=3655565

Garrido, V., Stangeland, P, y Redondo, S. (2001). *Principios de Criminología*. Valencia: Tirant lo Blanch.

Garrido, V. (2012). *Perfiles criminales: un recorrido por el lado oscuro del ser humano*. Barcelona: Editorial Planeta.

Giménez Pérez, A. (2020). The Hazards on the Network from a Criminological

Perspective: *Internet Madness. International Journal of Forensic Sciences*, 4 (*5*), 1-5. DOI: 10.23880/ijfsc-16000208

García Guilabert, N. (2014). Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio (tesis doctoral). Universidad de Murcia, Escuela Internacional de Doctorado, Murcia. Recuperado de https://dialnet.unirioja.es/servlet/tesis?codigo=50240

Gómez Blanco, A. (2022, 15 de febrero). QRishing, el phishing oculto en códigos QR. Recuperado de https://www.bbva.com/es/qrishing-el-phishing-oculto-en-codigos-qr/

González Arévalo, B. (2015). Los observadores ante el ciberacoso. *Investigación en la Escuela,* 87, 81-90. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=5608900

González Rus, J.J. (2022). Recensión del libro de Javier Valls Prieto, Inteligencia artificial, Derechos Humanos y bienes jurídicos. *Revista Electrónica de Ciencia Penal y Criminología: RECPC, 24 (r2)*, 1-10. Recuperado de https://dialnet.unirioja.es/buscar/documentos?querysDismax.DOCUMENTAL_TODO=recension+del+libro+de+Javier+Valls

INCIBE (2016). Manual curso de ciberseguridad para micropymes y autónomos. Recuperado de https://www.incibe.es/formacion/ciberseguridad-para-micropymes-y-autonomos

INCIBE (2017, 9 de mayo). El eslabón más importante de la ciberseguridad: tus empleados (noticia blog). Recuperado de https://www.incibe.es/protege-tu-empresa/blog/el-eslabon-mas-importante-ciberseguridad-tus-empleados

INE (2020). Notas de prensa. Estadística de Violencia Doméstica y Violencia de Género (EVDVG) Año 2020. Recuperado de https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176866&menu=ultiDatos&idp=1254735573206

INSST (1996). Evaluación de riesgos laborales. *Textos técnicos.* Recuperado de https://www.insst.es/textos-tecnicos/-/asset_publisher/Af6M6IuiLPta/content/evaluacion-de-riesgos-laborales-ano-1996?inheritRedirect=false

Instrucción 1/2017, de la Secretaría de Estado de la Seguridad por la que se actualiza el protocolo de actuación policial con menores. Recuperado de https://www.bienestaryproteccioninfantil.es/fuentes1.asp?sec=40&subs=596&cod=4024&page=

Instrucción 4/2019, de la Secretaría de Estado de Seguridad, por la que se establece un nuevo protocolo para la valoración policial del nivel de riesgo de violencia de género (Ley Orgánica 1/2004), la gestión de la seguridad de las víctimas y seguimiento de los casos a través del sistema de seguimiento integral de los casos de violencia de género (Sistema VIOGÉN). Recuperado de https://www.poderjudicial.es/cgpj/es/Temas/Violencia-domestica-y-de-genero/Guias-y-Protocolos-de-actuacion/Protocolos/Instruccion-4-2019--de-la-Secretaria-de-Estado-de-Seguridad--por-la-que-se-establece-un-nuevo-protocolo-para-la-valoracion-policial-del-nivel-de-riesgo-de-violencia-de-genero--Ley-Organica-1-2004---la-gestion-de-la-seguridad-de-las-victimas-y-seguimiento-de-los-casos-a-traves-del-sistema-de-seguimiento-integral-de-los-casos-de-violencia-de-genero--Sistema-VIOGEN-

Iriondo, I. (2020). Manual del investigador/perito experto en la elaboración de informes criminológicos en el ámbito judicial y extrajudicial. Palma de Mallorca: Addpol formación.

IVASPE (2016). Guía práctica del IVASPE para charlas en centros educativos. Cheste (Valencia): Instituto Valenciano de Seguridad Pública y Emergencias.

Juvonen, J., & Gross, E. F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School health, 78*(9), 496-505.

Kowalski, R.M., y Limber, S.P. (2007). Electronic bullying among middle school students. *Journal of adolescent health, 41*(6), S22-S30.

Laguna, S. (2010). *Manual de victimología*. Editorial Salamanca: Ciencias de la Seguridad Universidad de Salamanca.

Larrauri, E.; Zorrilla, N. (2014). Informe social y supervisión efectiva en la comunidad: especial referencia a delitos de violencia de género ocasional. *Revista para el análisis del derecho Indret* (3). Recuperado de https://indret.com/wp-content/themes/indret/pdf/1058_es.pdf

Lenhart, A. (2009). Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging. Recovered from https://www.pewresearch.org/internet/2009/12/15/teens-and-sexting/

Ley 31/95, de 8 de noviembre, de Prevención de Riesgos Laborales. *BOE* (*Boletín Oficial del Estado)*, 269, de 10 noviembre de 1995.

Ley 20/2007, de 11 de julio, del Estatuto del trabajo autónomo. *BOE* (*Boletín Oficial del Estado)*, 166, de 12 de julio de 2007, 29968.

Ley 4/2015, de 27 de abril, del Estatuto de la víctima del delito. *BOE (Boletín Oficial del Estado)*, 101, de 28 de abril de 2015, 36575-36590.

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. *BOE (Boletín Oficial del Estado)*, 236, de 2 de octubre de 2015, 89437-89440.

Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. *BOE* (*Boletín Oficial del Estado)*, 63, de 14 de marzo 1986.

Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil. *BOE* (*Boletín Oficial del Estado)*, 15, de 17 de enero 1996.

Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. *BOE (Boletín Oficial del Estado)*, 11, de 13 de enero de 2000, pp.1425-1439.

Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. *BOE (Boletín Oficial del Estado)*, 313, de 29 de diciembre de 2004, 42168.

Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *BOE* (*Boletín Oficial del Estado*), 77, de 31 de marzo de 2015, 27086.

Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia. *BOE* (*Boletín Oficial del Estado)*, 180, de 29 de julio de 2015, 64558.

Ley 2/2021, de 26 de marzo, del *Síndic de Greuges* de la Comunitat Valenciana. *BOE* (*Boletín Oficial del Estado)*, 91, de 16 de abril de 2021, 43685.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *BOE* (*Boletín Oficial del Estado)*, 294, de 6 diciembre de 1995.

Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia. *BOE* (*Boletín Oficial del Estado)*, 134, de 5 de junio de 2021.

Ley Orgánica 6/2022, de 12 de julio, complementaria de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, de modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *BOE* (*Boletín Oficial del Estado)*, 167, de 13 de julio de 2022.

Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual. *BOE (Boletín Oficial del Estado)*, 215, de 7 de septiembre de 2022.

Ley Orgánica 14/2022, de 22 de diciembre, de transposición de directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la Unión Europea, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso. *BOE (Boletín Oficial del Estado)*, 307, de 23 de diciembre de 2022.

Li, Q. (2007). Bullying in the new playground: research into cyberbullying and cybervictimization. *Australasian Journal of Educational Technology*, *23*(4).

Mason, K.L. (2008). Cyberbullying: a preliminary assessment for school personnel. *Psychology in the Schools*, *45*(4), 323-348.

Ministerio del Interior (2018). Datos estadísticos de cibercriminalidad. Estudio sobre cibercriminalidad en España. Recuperado de www.interior.gob.es/es/prensa/balances-e-informes/2018

Miró Llinares, F. (2012). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. (p.301). Madrid: Marcial Pons.

Miró et al. (2014). CiberApp. Aprender, Prevenir, Proteger. Estudio sobre el alcance de la cibercriminalidad contra menores de la provincia de Alicante. Elche: Crímina.

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007). Youth Internet users at risk for the most serious online sexual solicitations. *American Journal of Preventive Medicine, 32*(6), 532-537.

Morillas Fernández, D.L. (2023). Implicaciones de la inteligencia artificial en el ámbito del Derecho Penal. J.M. Peris y A. Massaro. *Derecho penal, inteligencia artificial y neurociencias* (pp. 51-91). Roma, Italia: Roma TrE-Press.

Muñoz Ruiz, J. (2016). Factores de riesgo en el acoso escolar y el ciberacoso: implicaciones educativas y respuesta penal en el ordenamiento jurídico español. *Criminalidad, 3* (58), 71-86. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=5763562

ONTSI (2022). Violencia digital de género: una realidad invisible. *Policy brief* para abordar su impacto en la sociedad. Recuperado de https://www.ontsi.es/es/publicaciones/violencia-digital-de-genero-una-realidad-invisible-2022

OSI (2016). Guía de privacidad y seguridad en Internet. Recuperado de https://www.osi.es/es/guia-de-privacidad-y-seguridad-en-internet

OSI (2020). Guía de ciberataques. Todo lo que debes saber a nivel usuario. Recuperado de https://www.osi.es/es/guia-ciberataques

Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. *BOD (Boletín Oficial de Defensa),* 40, de 26 de febrero de 2013, 4154-4155.

Orden 62/2014, de 28 de julio, de la Consellería de Educación, Cultura y Deporte, por la que se actualiza la normativa que regula la elaboración de los planes de convivencia en los centros educativos de la Comunitat Valenciana y se establecen los protocolos de actuación e intervención ante supuestos de violencia escolar. *DOCV (Diario Oficial de la Comunitat Valenciana),* 7330, de 1 de agosto de 2014, 19267-19284.

Ordenanza de Protección a la Infancia y Adolescencia del Ayuntamiento de Rafelbunyol. *BOP* (*Boletín Oficial de la Provincia de Valencia),* 199, de 14 de octubre de 2021.

Ortega, R., Calmaestra, J., y Mora-Merchán, J. (2008). Cyberbullying. *International Journal of Psychology and Psychological Therapy, 8* (2), 183-192. Recovered from https://www.ijpsy.com/volumen8/num2/194.html

Olweus, D. (2005). A useful evaluation design, and effects of the Olweus Bullying Prevention Program. *Psychology, Crime & Law, 11*(4), 389-402.

Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth violence and juvenile justice, 4*(2), 148-169.

Prat, T.C., Holfreter, K., y Reisig, M.D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. Journal of Research in Crime and Delinquency, 3 (47), 281. Recovered from https://www.researchgate.net/publication/237090930_Routine_Online_Activity_and_Internet_Fraud_Targeting_Extending_the_Generality_of_Routine_Activity_Theory/link/5cffec5ca6fdccd13093d184/download

Pinguelo, F.M. y Muller, B. W. (2011). *Virtual Crimes, Real Damages: A Primer On Cybercrimes In The United States and Efforts to Combat Cybercriminals*. VJLT.

RAE (2020). *Diccionario de la lengua española*. Recuperado de https://www.rae.es/

Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. *Gaceta de Madrid*, 206, de 25 de julio 1889.

Real Decreto 769/1987, de 19 de junio, sobre regulación de la Policía Judicial. *BOE (Boletín Oficial del Estado)*, 150, de 24 de junio 1987.

Rebollo, C. (2021, 16 de septiembre). Los ciberdelincuentes se reinventan durante la pandemia a través de los códigos QR. El País. Recuperado de https://elpais.com/tecnologia/2021-09-16/los-ciberdelincuentes-se-reinventan-durante-la-pandemia-a-traves-de-los-codigos-qr.html

Red Seguridad (2022, 5 de mayo). Casi un millón de españoles utiliza la combinación "12345" como contraseña. Recuperado de https://www.redseguridad.com/actualidad/dia-mundial-de-la-contrasena-casi-un-millon-de-espanoles-utiliza-la-combinacion-12345-como-contrasena_20220505.html

Reglamento (UE) nº 651/2014 de la Comisión, de 17 de junio de 2014. *DOUE (Diario Oficial de la Unión Europe*a), 187, de 17 de junio de 2014.

Reglamento (UE) nº 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. *DOUE (Diario Oficial de la Unión Europe*a), 119, de 27 de abril de 2016.

Rodríguez, Fernández, y Bautista (2017). Prevención de la cibervictimización en menores de la provincia de Alicante. *Revista Española de Investigación Criminológica: REIC*, 15, 1696-9219, Recuperado de

https://dialnet.unirioja.es/servlet/articulo?codigo=6226914

Rubio del Castillo, M. (2022, 19 de agosto). Primer centro público para tratar las adicciones a las nuevas tecnologías. Recuperado de https://www.mujerymadrehoy.com/primer-centro-publico-para-tratar-las-adicciones-a-las-nuevas-tecnologias/

Sedeño Rivero, M.A. (2017). Manual Perito Judicial Experto en Ciberdelincuencia y Conducta Criminal en la Web. Madrid: Fundación Uned.

Síndic de Greuges de la Comunidad Valenciana (2016). Informe a las Cortes Valencianas 2016. Recuperado de https://www.elsindic.com/informes-anuales/

Síndic de Greuges de la Comunidad Valenciana (2022). El Síndic pide a Educación medidas más efectivas para atajar el acoso escolar. Recuperado de https://www.elsindic.com/actualidad/el-sindic-pide-a-educacion-medidas-mas-efectivas-para-atajar-el-acoso-escolar/

Slonje, R., y Smith, P.K. (2008). Cyberbullying: another main type of bullying? *Scandinavian journal of psychology*, *49*(2), 147-154.

Valls Prieto, J. (2022). Sobre la responsabilidad penal por la utilización de sistemas inteligentes. *Revista Electrónica de Ciencia Penal y Criminología: RECPC, 24*, 1-35. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=8587635

Vandebosch, H., & Van Cleemput, K. (2009). Cyberbullying among youngsters: Profiles of bullies and victims. *New media & society*, *11*(8), 1349-1371.

Walrave, M., y Wannes, H. (2011). Cyberbullying: predicting victimization and perpetration. *Children & Society*, *25*(1), 59-72.

Wolak, J., Finkelhor, D., Mitchell, L. J. & Ybarra, M.L. (2010). Online predators and their victims: myths, realities and implications for prevention and treatment. *American Psychologist* *63*(2), 111-28. Recovered from https://www.researchgate.net/publication/5568459_Online_Predators_and_Their_Victims_Myths_Realities_and_Implications_for_Prevention_and_Treatment/link/0c960534996b0c6000000000/download

Young, K.S. (2005). Profiling online sex offenders, cyber-predators, and pedophiles. *Journal of Behavioral Profiling, 5*(1), 1-18.

Zapata, A. (2017). *Criminología empresarial. Manual de intervención criminológica en las empresas.* México: E/A.

ÍNDICE DE TABLAS.

ÍNDICE DE FIGURAS.

ANEXO I: Encuesta de victimización cibercriminalidad social.

Encuesta de Victimización

-Centro Educativo: _____

-Curso: _____ -Edad: _____

-Soy chico ☐ Soy chica ☐

-Tengo ordenador en casa: SI ☐ NO ☐ (EN CASO AFIRMATIVO*)
***¿Dónde lo tienes ubicado?**

***-En mi habitación ☐**

***-En una zona común de mi casa (Comedor, cocina, etc.) ☐**

-Tapo la webcam cuando no la utilizo: SI ☐ NO ☐ NO TENGO ☐

-Tengo teléfono móvil: SI ☐ NO ☐ (EN CASO AFIRMATIVO*)
***-Guardo información personal en el teléfono móvil: SI ☐ NO ☐**

-Tengo una cuenta de correo electrónico: SI ☐ NO ☐

-Utilizo programas de mensajería instantánea como WhatsApp, Telegram, etc.: SI ☐ NO ☐

-Utilizo redes sociales tales como Facebook, Twitter, etc.: SI ☐ NO ☐

-Utilizo blogs, foros en Internet: SI ☐ NO ☐

-Cuanto tiempo dedicas al día a Internet, redes sociales, envío de WhatsApp, emails, juegos online, etc.:
Menos de 1 hora ☐ Entre 1 y 2 horas ☐ 3 horas o más ☐

A continuación, señala con una cruz (X) con qué frecuencia protagonizas los hechos que a continuación se presentan. Por favor, en cada enunciado elige sólo una de las opciones ofrecidas y no dejes ninguna sin contestar.

1= Nunca; 2 = Pocas veces; 3 = Algunas veces; 4 = Muchas veces; 5 =Siempre

Hechos o conductas:	1	2	3	4	5
1.Realizar mensajes y/o llamadas ofensivas a través de teléfono móvil y/o Internet.					
2.Colgar en Internet una pelea, agresión o burla que ha sido grabada.					
3.Realizar comportamientos de tipo sexual a través de la webcam.					
4.Difundir vídeos y/o fotos privadas o comprometidas vía teléfono móvil o Internet.					
5.Colgar vídeos y/o fotos robadas en Internet o difundirlos a través del teléfono móvil.					
6.Realizar llamadas anónimas para asustar o intimidar.					
7.Realizar amenazas o chantajes a través de mensajes y/o llamadas.					
8.Acosar sexualmente a través del teléfono móvil y/o Internet.					
9.Suplantar a una persona para difamar, mentir o contar sus secretos.					
10.Robar la contraseña de una persona.					
11.Trucar fotos y vídeos para difundirlos y humillar vía teléfono móvil y/o Internet.					
12.Acosar a alguien para aislarle de sus contactos en las redes sociales.					
13.Chantajear a cambio de no divulgar información íntima vía teléfono móvil y/o Internet.					
14.Amenazar de muerte a alguien a través de teléfono móvil y/o Internet.					
15.Difundir y/o difamar con rumores para hacer daño vía teléfono móvil y/o Internet.					
16. Contactar con un adulto que se ha ganado tu confianza en las redes sociales.					
17.Controlar amigos / as en redes sociales, mensajes, WhatsApp, etc., de tu pareja.					
18.Pedir a tu pareja que retire fotos o comentarios de redes sociales, WhatsApp, etc.					
19.Pedir a tu pareja que suprima o borre a amigos / as en redes sociales, etc.					
20.Obligar a tu pareja a realizar comportamientos de tipo sexual a través de la webcam.					

En el caso de observar y/o protagonizar alguno de los hechos o conductas mencionados, ¿A quién lo comunicarías?

Compañeros	
Padres	
Profesores	
A nadie	

¿Qué actividades preventivas propones frente a hechos o conductas de ciberacoso?

Comunicar adultos	
Denunciar a la policía	
Ignorar ciberacoso	
Mediar con el ciberacosador	
Pedir ayuda	
Otras	

MUCHAS GRACIAS POR TU COLABORACION

ANEXO II: Encuesta de victimización cibercriminalidad económica.

Encuesta de Victimización

-Tipo de establecimiento: _____

-Edad: _____ Hombre ☐ Mujer ☐

-Tengo ordenador en casa: SI ☐ NO ☐

-Tengo ordenador en mi negocio o empresa: SI ☐ NO ☐

-Tengo teléfono móvil: SI ☐ NO ☐

-Guardo información personal y/o confidencial de mi negocio u empresa en el teléfono móvil: SI ☐ NO ☐

-Tengo una cuenta de correo electrónico con fines comerciales:

SI ☐ NO ☐

-Tengo una página web de mi negocio u empresa: SI ☐ NO ☐

-Utilizo programas de mensajería instantánea como WhatsApp, Telegram, etc., con fines comerciales: SI ☐ NO ☐

-Utilizo redes sociales tales como Facebook, Twitter, etc., con fines comerciales: SI ☐ NO ☐

-Utilizo blogs, foros en Internet con fines comerciales: SI ☐ NO ☐

Actualmente, existen diversas tecnologías biométricas aplicadas a la ciberseguridad con el fin de proteger la información confidencial de teléfonos móviles, ordenadores, tabletas, etc. ¿Sabía de la existencia de alguna de ellas? Indíquelas con una cruz (X).

S= SI; N= NO

Tipología Tecnologías biométricas		
	S	N
Huella dactilar		
Reconocimiento facial		
Reconocimiento de iris		
Reconocimiento de la geometría de la mano		
Reconocimiento de firma		
Reconocimiento de voz		
Reconocimiento vascular		
Reconocimiento de escritura		
Otras formas de biometría		

A continuación, señale con una cruz (X) con qué frecuencia protagoniza los hechos o lleva a cabo las conductas que a continuación se presentan. Por favor, en cada enunciado elija sólo una de las opciones ofrecidas y no deje ninguna sin contestar.

1= Nunca; 2 = Pocas veces; 3 = Algunas veces; 4 = Muchas veces; 5 =Siempre

Hechos o conductas:	**1**	**2**	**3**	**4**	**5**
1. ¿Ha perdido alguna vez el teléfono móvil, tableta, ordenador portátil, etc.?					
2. ¿Le han sustraído alguna vez el teléfono móvil, tableta, ordenador portátil, etc.?					
3. ¿Ha perdido alguna vez un pendrive con información confidencial de su negocio y/o particular de usted?					
4. ¿Se le ha infectado alguna vez su ordenador, teléfono móvil, tableta, etc., con algún virus o malware?					
5. ¿Alguna vez ha perdido archivos de su negocio por infección de malware?					
6. ¿Ha recibido alguna vez mensajes por WhatsApp, correo electrónico, redes sociales, etc., en la que se prometen grandes cantidades de dinero a cambio de pequeñas transferencias relacionadas con la lotería, trabajo, etc. (scam)?					
7. ¿Ha recibido alguna vez masivamente correos electrónicos no deseados de publicidad (spam)?					
8. ¿Alguna vez han suplantado la página web, Facebook, etc., de su negocio?					
9. Al contactar telemáticamente con proveedores o clientes, en su caso, ¿le han sustraído contraseñas, datos personales de la tarjeta de crédito y/o cuenta bancaria mediante diferentes técnicas tales como correos electrónicos que llevan a páginas falsas en las que se solicita la introducción de estos datos, o mediante infección por virus?					
10. Al efectuar una compraventa en su negocio, ¿alguna vez un cliente ha utilizado una tarjeta de crédito sustraída?					
11. ¿Ha sido víctima de algún tipo de fraude online, extorsión, etc.?					
12. ¿Emite opiniones personales de carácter político, religioso o ideológico en redes sociales abiertas, profesionales o mixtas?					
13. ¿Critica de manera irresponsable y sin argumentos productos o proyectos de la competencia?					
14. ¿Evita entrar en debates y discusiones con clientes o potenciales clientes a través de las redes sociales?					
15. ¿Evita dar información confidencial sobre su negocio que pueda usar la competencia?					
16. ¿Elimina de forma segura la información confidencial archivada que no necesita?					
17. ¿Cifra la información confidencial?					
18. ¿Utiliza los servicios de almacenamiento en la nube?					
19. ¿Realiza copias de seguridad en otro soporte de la información almacenada en el teléfono móvil, ordenador, tableta, etc.?					
20. ¿Utiliza códigos de desbloqueo de pantalla (código numérico o patrón) en su teléfono móvil, tableta, ordenador, etc.?					

MUCHAS GRACIAS POR SU COLABORACION

ANEXO III: Informe criminológico cibercriminalidad social.

Ajuntament de Vinaròs

Ref.: Informe nº 1/2022

INFORME CRIMINOLÓGICO DE RIESGO DE CIBERCRIMINALIDAD SOCIAL DE LOS MENORES QUE CURSAN LA ESO EN LA CIUDAD DE VINARÒS

POLICIA LOCAL VINAROS

REALIZADO POR: ADRIÁN GIMÉNEZ PÉREZ

DIRIGIDO A: JEFATURA DE POLICÍA LOCAL / SR. ALCALDE-PRESIDENTE DEL AYUNTAMIENTO DE VINARÒS

El presente informe criminológico contendría la información resultante de la parte de esta tesis doctoral sobre cibercriminalidad social, cuya estructura, a parte de la carátula, podría ser la siguiente:

a) índice.
b) introducción.
c) objetivos generales y específicos.
d) material y métodos utilizados.
e) resultados.
f) conclusiones.
g) bibliografía.

ANEXO IV: Informe criminológico cibercriminalidad económica.

Ajuntament de Vinaròs

Ref.: Informe nº 2/2022

INFORME CRIMINOLÓGICO DE RIESGO DE CIBERCRIMINALIDAD ECONÓMICA DE AUTÓNOMOS Y MICROEMPRESAS DE LA CIUDAD DE VINARÒS.

REALIZADO POR: ADRIÁN GIMÉNEZ PÉREZ

DIRIGIDO A: JEFATURA DE POLICÍA LOCAL / SR. ALCALDE-PRESIDENTE DEL AYUNTAMIENTO DE VINARÒS

El presente informe criminológico contendría la información resultante de la parte de esta tesis doctoral sobre cibercriminalidad económica, cuya estructura, a parte de la carátula, podría ser la siguiente:

a) índice.
b) introducción.
c) objetivos generales y específicos.
d) material y métodos utilizados.
e) resultados.
f) conclusiones.
g) bibliografía.