

**Acciones y peligros al usar internet (estudiantes de grado décimo liceo psicopedagógico
mundo activo y colegio san francisco de asís)**

Leonard Santiago Salinas Aguilar

Código: 2012101064

Universidad Pedagógica Nacional

Facultad de ciencia y tecnología

Licenciatura en diseño tecnológico

Bogotá

2017

**Acciones y peligros al usar internet (estudiantes de grado décimo liceo psicopedagógico
mundo activo y colegio san francisco de asís)**

Leonard Santiago Salinas Aguilar

Trabajo de grado para optar por el título de licenciado en diseño tecnológico

Dirigido por

Evelio Ortiz Ch


Universidad Pedagógica Nacional

Facultad de ciencia y tecnología

Licenciatura en diseño tecnológico

Bogotá

2017

 UNIVERSIDAD PEDAGÓGICA NACIONAL <small>Educación de excelencia</small>	FORMATO	
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE	
Código: FOR020GIB	Versión: 01	
Fecha de Aprobación: 10-10-2012	Página 3 de 5	

1. Información General	
Tipo de documento	Trabajo de grado
Acceso al documento	Universidad Pedagógica Nacional. Biblioteca Central
Título del documento	Acciones y peligros al usar internet (estudiantes de grado décimo liceo psicopedagógico mundo activo y colegio san francisco de asís)
Autor(es)	Salinas Aguilar, Leonard Santiago
Director	Ortiz, Evelio
Publicación	Bogotá. Universidad Pedagógica Nacional. 2017. 161.p
Unidad Patrocinante	Universidad Pedagógica Nacional
Palabras Claves	PELIGROS DE INTERNET, ACCIONES EN INTERNET, EDUCACIÓN EN TECNOLOGÍA, ACCIONES DE LOS ESTUDIANTES EN EL USO DE INTERNET, MATERIAL EDUCATIVO COMPUTACIONAL

2. Descripción
<p>El siguiente trabajo de grado tiene como temática central ciertas acciones que pueden exponer a un estudiante a ser víctima de peligros como el Sexting, grooming y los códigos maliciosos (virus, gusanos, troyanos, keyloggers, spywares), teniendo en cuenta estas temáticas durante este proyecto se plantea desarrollar un material educativo computacional el cual se trabaja con un grupo de estudiantes donde la finalidad es que dicho material educativo genere una incidencia sobre los</p>

estudiantes de tal manera que estos generen cambios en las acciones que los pueden exponer a los peligros.

Entre las acciones específicas que se trabajan con los estudiantes se encuentra

- No intercambiar fotos íntimas con la pareja
- No intercambiar fotos íntimas con un desconocido
- No leer los términos y condiciones al instalar un software que fue descargado gratis de internet
- Tener como públicas fotos en las redes sociales cuyo contenido no deberían ver todas las personas.
- Tener demasiada información como pública en la redes sociales
- No fijarse en los permisos que se le dan a las aplicaciones conectadas a Facebook
- No fijarse en el tipo de instalación que se selecciona cuando se va a instalar un software
- No manejar configuraciones de privacidad para las fotos que se postean en internet

En el material educativo computacional propuesto se plantean ejercicios acompañados con teoría, videos e imágenes a partir de los cuales se plantea generar cambios en las acciones nombradas, al finalizar se plantea un post-test donde se pretende evidenciar esos cambios y generar los resultados y conclusiones

3. Fuentes

Administración del estado, (2016), *Temario. Vol. 2 Actividad administrativa y ofimática*, Sevilla, España: Ediciones Rodio

Anónimo, (1998), *Máxima seguridad en internet*, Madrid, España: Anaya multimedia

Avilés, Á.-P. (2013). *XIRED+SEGURA*. España.

Bustamante, K & Iedesmas, Y (2014). METODOLOGIA PARA LA ENSEÑANZA DE LA NETIQUETA, EN EL AREA DE INFORMATICA EN EL GRADO 10 EN LA INSTITUCION EDUCATIVA ALFONZO LÒPEZ PUMAREJO DEL MUNICIPIO DE LA VIRGINIA RISARALDA. Colombia: Universidad Tecnológica de Pereira. Recuperado de: <http://repositorio.utp.edu.co/dspace/handle/11059/4581> consultado el (7 de abril de 2016)

Bono Cabré, R. *DISEÑOS CUASI-EXPERIMENTALES Y LONGITUDINALES* (p. 3). Barcelona. Recuperado de:
<http://diposit.ub.edu/dspace/bitstream/2445/30783/1/D.%20cuasi%20y%20longitudinales.pdf>
consultado el (25 de agosto de 2016)

CNN en español. (2013). *Nativos digitales: ¿Quiénes son y qué significa?*. CNN. Recuperado de:
<http://cnnespanol.cnn.com/2013/01/25/nativos-digitales-quienes-son-y-que-significa/>

Colombia tic. (s.f). Colombia tic vive digital. Bogotá Recuperado de:
<http://colombiatic.mintic.gov.co/estadisticas/stats.php?&pres=content&jer=1&cod=&id=34#TTC>
(consultado el 10 de marzo de 2016)

Cuerda.J.L. Colegios tendrían nueva cátedra de seguridad digital para fomentar el uso responsable de TIC, *RCN RADIO*, [en línea]. 21 de enero de 2016, recuperado de:
<http://www.rcnradio.com/tecnologia/colegios-tendrian-nueva-catedra-seguridad-digital-fomentar-uso-responsable-tic/>. (consultado el 18 de mayo de 2016)

Da cunha. T, Luviano. R, Revuelta. B, Sánchez. R, (2007), *Globalización, Derechos Humanos y Sociedad de la Información*, México, Facultad de Derecho y Ciencias Sociales / UMSNH

Educación Bogotá (2015). COLEGIOS PÚBLICOS DE BOGOTA: CONECTADOS Y A TODA VELOCIDAD. [en línea]. Recuperado de : <http://www.educacionbogota.edu.co/es/sitios-de-interes/nuestros-sitios/agencia-de-medios/noticias-institucionales/colegios-publicos-de-bogota-conectados-y-a-toda-velocidad>. (consultado el 20 de marzo de 2016)

EFE. (25 de julio de 2012). 'Sexting' no está asociado con problemas psicológicos, según estudio. *EL tiempo*.

Galvis, A. (1992) *ingeniería de software educativo*. Santafé de Bogotá. Colombia. Universidad de los andes

Gil, A.M, (2015), *¿Privacidad del menor en internet? : "me gusta" ; ; ; todas las imágenes de "mis amigos" a mi alcance con un simple "click" ; ; ;*, navarra, España: Editorial Aranzadi S.A

Gómez, M & Polania, N. (2008). *ESTILOS DE ENSEÑANZA Y MODELOS PEDAGÓGICOS: Un estudio con profesores del Programa de Ingeniería Financiera de la Universidad Piloto de Colombia*. (tesis de maestría). Universidad de la Salle. Bogotá

Goodman. M, (s.f), *los delitos del futuro*, España: Editorial Ariel

Ibáñez. N, (2010), *CIBERPUTEADORES EN INTERNET*, España, NORBOOKSEDITIONES (consultado el 22 de julio de 2016)

javier fernandez, A. P. (2015). hàbitos de uso y conductas de riesgo en internet en la preadolescencia. *comunicar revista científica de comunicaciòn y educaciòn* , 113-120.

Jimènèz, A. G. (2011). una perspectiva sobre los riesgos y usos de internet en la adolescencia. *icono 14*, 396-411.

Leguizamón, M (s.f). DISEÑO Y DESARROLLO DE MATERIALES EDUCATIVOS COMPUTARIZADOS (MEC´S): UNA POSIBILIDAD PARA INTEGRAR LA INFORMÁTICA CON LAS DEMÁS ÁREAS DEL CURRÍCULO. UPTC. [En línea]. Recuperado de:
http://www.colombiaaprende.edu.co/html/mediateca/1607/articles-106492_archivo.pdf

Ley 679. Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. Bogotá, Colombia 3 de agosto de 2001. [En línea]. Recuperado de:
<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=18309>

Ley 1336. Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Bogotá, Colombia. 21 de julio de 2009. [En línea]. Recuperado de:
<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36877>

Ley 1341. POR LA CUAL SE DEFINEN PRINCIPIOS Y CONCEPTOS SOBRE LA SOCIEDAD DE LA INFORMACIÓN Y LA ORGANIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - TIC-, SE CREA LA AGENCIA NACIONAL DE ESPECTRO. Bogotá, Colombia. 30 de julio de 2009.[En línea]. Recuperado de: http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

Ley 1620. "POR LA CUAL SE CREA EL SISTEMA NACIONAL DE CONVIVENCIA ESCOLAR Y FORMACIÓN PARA EL EJERCICIO DE LOS DERECHOS HUMANOS, LA EDUCACIÓN PARA LA SEXUALIDAD Y LA PREVENCIÓN Y MITIGACIÓN DE LA VIOLENCIA ESCOLAR". Bogotá, Colombia. 15 de marzo de 2013[En línea]. Recuperado de:
<http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201620%20DEL%2015%20DE%20MARZO%20DE%202013.pdf>

Manterola, Carlos, & Otzen, Tamara. (2015). Estudios Experimentales 2 Parte: Estudios Cuasi-Experimentales. *International Journal of Morphology*, 33(1), 382-387. Recuperado de:
<http://www.scielo.cl/pdf/ijmorphol/v33n1/art60.pdf>. (Consultado el 22 de julio de 2016)

MARCELO, J. & MARTÍN. E (2010). Protege a tus hijos de los riesgos de Internet y otras tecnologías. Madrid. Ediciones Anaya.

Marañon, G. À. (2009). *¿QUE SABEMOS DE? Còmo protegernos de los peligros de internet*. madrid: los libros de la catarata.

NAVARRO-MANCILLA, Álvaro Andrés and RUEDA-JAIMES, Germán Eduardo. Adicción a Internet: revisión crítica de la literatura. *rev.colomb.psiquiatr.* [online]. 2007, vol.36, n.4, pp.691-700. ISSN 0034-7450.

Oxman.V, Nicolas.A, Estafas informáticas a través de internet: acerca de la imputación penal del "phising" y el "pharming", *Revista de Derecho (Valparaíso)*, [en línea], 2013 n° 41, consultado el 1 de junio de 2016, recuperado de: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-68512013000200007#back

Prensky, M. (2001). *Nativos e Inmigrantes Digitales*. [En línea]. Recuperado de: [http://www.marcprensky.com/writing/Prensky-NATIVOS%20E%20INMIGRANTES%20DIGITALES%20\(SEK\).pdf](http://www.marcprensky.com/writing/Prensky-NATIVOS%20E%20INMIGRANTES%20DIGITALES%20(SEK).pdf)

Puchades. Pardo, M. P. (2013). Internet y adolescencia: guía on line para educadores. España: Universidad Politécnica de Valencia. Recuperado de: <https://riunet.upv.es/bitstream/handle/10251/32867/Memoria.pdf?...1> (consultado el 31 de marzo de 2016)

Requesens, E. E. (2012). *Adicción a las redes sociales y nuevas tecnologías en niños y adolescentes*. piramide.

Sierra, D. M. (2013). Las redes sociales, sus riesgos y la manera de protegerse. Colombia: Universidad CES. Recuperado de: <http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1285/2/Articulo%20de%20grado%20de%20las%20redes%20sociales%20aprobado.pdf> (consultado el 31 de marzo de 2016)

Tünnermann Bernheim, C. (2011). El constructivismo y el aprendizaje de los estudiantes. Universidades, Enero-Marzo, 21-32. [En línea]. Recuperado de: <http://www.redalyc.org/pdf/373/37319199005.pdf>

Vanderhoven, E. Schellens, T. Valcke, M. (2014). Enseñar a los adolescentes los riesgos de las redes sociales: una propuesta de intervención en secundaria. *Revista comunicar*, 22, (43), 123-132
voces, p. (2006). *internet sano para todos*. bogota: dupligráficas.

4. Contenidos

El presente trabajo de grado se divide en seis capítulos de la siguiente manera.

Capítulo 1 Componentes iniciales del problema: En este capítulo se plantea el problema que se va a trabajar a lo largo del proyecto y del documento, a su vez también se enuncia la pregunta

problema la cual se desea solucionar continuando en este capítulo se encontrara la justificación en donde se dan a conocer las razones de porque es importante y necesario el desarrollo del trabajo, también en este capítulo se plantean los objetivos donde se plantea un objetivo general y tres objetivos específicos luego para finalizar este capítulo se encuentran los antecedentes locales, nacionales e internacionales que se tuvieron en cuenta.

Capítulo 2 Marco legal y teórico: A lo largo de este capítulo se encuentra una lista de leyes en las cuales se habla sobre las temáticas trabajadas en este proyecto, posteriormente se encuentra el marco teórico en donde se trata la información tenida en cuenta para el desarrollo del proyecto dicha información va desde temas generales hasta temáticas particulares.

Capítulo 3 metodología: En este capítulo esta la información referente a la metodología utilizada para el desarrollo de este trabajo de grado donde se encuentra el tipo de investigación utilizada la cual para este caso fue investigación cuasi-experimental, seguidamente se expone la hipótesis y variables propuestas a continuación de esto se hace la descripción de la población con la que se trabajó y para finalizar el capítulo se enuncian los instrumentos de recolección de datos y se hace una descripción de la aplicación de los mismos

Capítulo 4 Material propuesto: Este capítulo hace referencia al material propuesto para trabajar con la población en la realización de este trabajo de grado, allí se plantea el desarrollo del material a partir de cuatro componentes como lo son el entorno, un componente educativo, el componente de comunicación o interfaz y finalmente se encuentra el componente computacional

Capítulo 5 Análisis de datos: En este capítulo se muestra como se realizó el respectivo análisis de datos, se muestran unas gráficas de los datos obtenidos, dichos datos y gráficas van acompañados de una explicación teórica

Capítulo 6 conclusiones: Este es el capítulo final del trabajo de grado, allí se encuentran las conclusiones las cuales surgen del respectivo análisis de datos y de los objetivos planteados para el proyecto.

En la parte final de este documento se encuentra la bibliografía donde esta las referencias de cada elemento utilizado para el desarrollo de este documento y finalmente se encuentran unos anexos en donde se encuentran unos pantallazos del material educativo computacional propuesto y unas graficas de las respuestas obtenidas en la encuesta trabajada.

5. Metodología

La metodología utilizada durante este proyecto fue metodología cuasi-experimental, de la cual se utilizó el diseño de grupo control no equivalente a su vez y para el desarrollo del mismo se utilizaron 3 instrumentos.

1. **Encuesta:** con esta se obtuvo información de los estudiantes como peligros a los que están expuestos y las acciones que estos tienen cuando usan internet
2. **Material educativo computacional:** el propuesto por el investigador
3. **Post-test:** aquí se proponían ejercicios con los cuales se pretendía evidenciar que cambios hubo en las acciones de los estudiantes

6. Conclusiones

- Los datos obtenidos a partir de la realización de la encuesta ayudaron a identificar que la población con la que se desarrolló el proyecto podrían ser víctimas de peligros como el grooming, el Sexting y los códigos maliciosos (virus, gusanos, troyanos, keyloggers, spywares), lo que motivo a desarrollar un material educativo donde se trabajaran estas temáticas. (ver tabla 8, p.85)
- La orientación sobre los estudiantes genera una mayor incidencia cuando se les plantean situaciones con las que la población se sienta identificada, aquí el impacto fue sobre ciertas acciones particulares como la disminución en la cantidad de estudiantes que aceptarían enviar y recibir fotos insinuantes con su pareja, la configuración de cierta información que los

estudiantes tenían en su red social (Facebook) a la vista de cualquier persona, la configuración de privacidad de las fotos que se publican en las redes sociales según su contenido, el comprender que ciertas aplicaciones que se conectan a la cuenta de Facebook pueden tener acceso a la información que el usuario tiene en esta red social y el aumento en la cantidad de estudiantes que leen los términos y condiciones a la hora de instalar un programa.

- a partir del análisis se observa que las acciones sobre las que más incidencia generó el material fueron el escoger siempre que se va a instalar un software el tipo de instalación como personalizada (60%) la de leer los términos y condiciones al momento de instalar un software (50%), y la acción de configurar los permisos de acceso que tienen las aplicaciones conectadas a Facebook sobre la información de un usuario (52%), las acciones sobre las que se generó poca incidencia fueron la no práctica del Sexting (38%), la configuración de cierta información para que no quedara a la vista de cualquier persona (10%), y la acción sobre la que no se generó ninguna incidencia fue la práctica del grooming (0%).

Elaborado por:	Salinas Aguilar, Leonard Santiago
Revisado por:	Ortiz, Evelio

Fecha de elaboración del Resumen:	13	06	2017
--	----	----	------

Tabla de contenido

	Pág.
Capítulo 1 Componentes iniciales del problema	1
1.1 Planteamiento del problema.....	1
1.2 Pregunta problema	3
1.3 Justificación.....	3
1.4 Objetivos.....	6
1.4.1 Objetivo general.....	6
1.4.2 Objetivos específicos.....	6
1.5 antecedentes.....	7
1.5.1 local.....	7
1.5.2 nacional.....	8
1.5.3 internacional.....	11
Capítulo 2 marco legal y teórico	16
2.1 marco legal.....	16
2.1.1 ley 1620 del 15 de marzo del 2013.....	16
2.1.2 ley 679 del 2001.....	17
2.1.3 ley 1336 del 2009.....	18
2.1.4 ley 1341 de 2009.....	19
2.2 marco teórico.....	21
2.2.1 Componente educativo.....	21
2.2.1.1 el papel de la educación.....	21
2.2.1.2 el modelo pedagógico conductista.....	23

2.2.1.3 modelo pedagógico constructivista	24
2.2.1.3.1 aprendizaje significativo.....	25
2.2.1.4 ¿Qué es un material educativo?.....	26
2.2.1.5 ¿Qué es un material educativo computacional?.....	26
2.2.1.5.1 sistemas tutoriales.....	27
2.2.1.5.2 sistemas de ejercitación y practica.....	27
2.2.1.5.3. Simuladores y juegos educativos.....	27
2.2.1.5.4 sistemas expertos con fines educativos.....	27
2.2.1.5.5 sistemas tutoriales inteligentes.....	28
2.2.2 los nativos digitales.....	28
2.2.3 ¿es internet peligroso?.....	30
2.2.4 la privacidad en internet.....	31
2.2.5 riesgos en internet.....	33
2.2.5.1 Cyberbullying.....	34
2.2.5.2 Grooming.....	34
2.2.5.2.1 algunos casos de grooming en Colombia.....	35
2.2.5.3 Sexting.....	36
2.2.5.4 pornografía infantil.....	37
2.2.5.5 el phishing.....	38
2.2.5.6 Acceso a material inadecuado.....	39
2.2.5.7 los códigos maliciosos.....	40
2.2.5.7.1 los virus.....	41
2.2.5.7.2 los gusanos.....	41

2.2.5.7.3 los troyanos.....	42
2.2.5.7.4 los exploit.....	42
2.2.5.7.5 los keyloggers.....	43
2.2.5.8 la adicción a internet.....	44
2.2.6 peligros en las redes sociales.....	46
2.2.7 Acciones en internet.....	46
Capítulo 3 metodología.....	49
3.1 el tipo de investigación.....	49
3.1.1 cuasi-experimental.....	49
3.2 hipótesis.....	50
3.3 variables.....	50
3.3.1 variable independiente.....	50
3.3.2 variable dependiente.....	50
3.4 Categorías de análisis.....	51
3.4.1 los peligros en internet.....	51
3.4.2 las acciones de los usuarios en internet que los exponen a los peligros.....	52
3.5 Población objeto de estudio.....	54
3.6 Instrumentos y técnicas de recolección de datos.....	55
3.6.1 la encuesta.....	55
3.6.2 El material educativo digital propuesto y trabajado con la población.....	56
3.6.3 El post-test.....	56
3.7 Etapas para la recolección de datos.....	56
3.7.1 Etapa 1: Desarrollo y aplicación de la encuesta para seleccionar las temáticas a.....	56

trabajar en el material digital	
3.7.1.1 Planificación y creación de la encuesta.....	57
3.7.1.2 Prueba piloto.....	57
3.7.1.3 Aplicación de la encuesta.....	58
3.7.2 Etapa 2: Construcción, prueba piloto y aplicación del material educativo.....	58
computacional.	
3.7.2.1 Construcción del material educativo.....	59
3.7.2.2 prueba piloto del material educativo.....	59
3.7.2.3 aplicación del material educativo computacional.....	60
3.7.3 Etapa 3: Elaboración y aplicación del material post-test.....	61
3.7.3.1 Elaboración del post-test.....	61
3.7.3.2 Aplicación del post-test.....	62
Capítulo 4 Material propuesto.....	63
4.1 El entorno.....	64
4.2 Diseño educativo (componente pedagógico).....	65
4.3 Diseño de comunicación o interfaz.....	70
4.3.1 Menú principal.....	70
4.3.2 Fuente de letra.....	71
4.3.3 Elementos gifs.....	71
4.3.4 los botones de avance y retroceso.....	72
4.3.5 Actividades.....	73
4.3.6 videos.....	74
4.4 Diseño computacional.....	74

Capítulo 5 análisis de datos.....	75
5.1 la encuesta.....	75
5.2 Análisis de datos pre-test post-test.....	81
5.2.1 Análisis de datos tema “privacidad en internet”.....	82
5.2.1.1 Configuración de datos perfil simulado.....	82
5.2.1.2 la información que cada alumno tiene en su perfil de Facebook.....	85
5.2.1.3 Privacidad en las fotos según el contenido de estas.....	89
5.2.1.4 Conectar aplicaciones a las redes sociales.....	91
5.2.2 Análisis de datos tema “grooming”.....	94
5.2.2.1 Pre-test (grooming).....	94
5.2.2.3 Post-test (grooming).....	96
5.2.3 Análisis de datos tema “sexting”.....	97
5.2.4 Análisis de datos tema “códigos maliciosos”.....	99
5.2.4.1 Tipo de instalación de un software.....	99
5.3 Análisis de datos de la categoría 2 acciones en internet.....	102
Capítulo 6 conclusiones.....	108
Bibliografía.....	110
Anexos.....	113
Anexo 1 encuesta aplicada a la población.....	113
Anexo 2 pantallazos del material educativo computacional.....	143

LISTA DE TABLAS

	Pág.
Tabla 1: Información sobre la aplicación de la respectiva prueba piloto.....	60
Tabla 2: Información de la aplicación del material educativo computacional.....	61
Tabla 3: Información de la aplicación del material educativo computacional (post-test).....	62
Tabla 4: Interrogantes planteados por Galvis para el desarrollo del entorno.....	64
Tabla 5: otros elementos del material educativo computacional propuesto.....	66
Tabla 6 : algunas de las respuestas de la pregunta 2 de la encuesta.....	76
Tabla 7: Clasificación de las preguntas según el peligro al que aportan información.....	77
Tabla 8: Cantidad de estudiantes que podrían ser víctimas de cada peligro.....	79
Tabla 9: Tipo de configuración de privacidad según el perfil simulado.....	83
Tabla 10: Comparación de resultados de post-test grupo experimental con grupo control.....	84
Ejercicio 1 del post-test	
Tabla 11: Resultados pre-test post-test información que tienen los estudiantes en su perfil de red social.....	87
Tabla 12: Comparación de datos post-test grupo experimental y post-test grupo control, información que tienen los estudiantes en el perfil de la red social.....	88
Tabla 13: Configuración de privacidad de fotos según el contenido de estas, comparación entre grupo experimental y grupo control.....	90
Tabla 14: Estudiantes que inician sesión en ciertas aplicaciones usando su red social.....	93
Facebook	
Tabla 15: Datos ejercicio post-test grooming grupo experimental y control.....	96
Tabla 16: Pre-test post-test tema sexting.....	98
Tabla 17: Comparación post-test grupo control y grupo experimental (sexting).....	99
Tabla 18: Análisis de datos códigos maliciosos.....	100

Introducción

Este trabajo de grado se realiza partiendo del hecho que la internet al igual que el mundo real está lleno de peligros, esto debido a que los seres humanos que son los encargados de subir información a la red, también se encargan de que el internet se vuelva peligroso, es decir, una persona que en la vida real se dedique a estafar puede tranquilamente utilizar el internet para cumplir sus propósitos, una persona que trabaje haciendo cualquier acto delictivo puede usar el internet para cometer sus delitos allí, y así sucesivamente.

Sabiendo entonces esto y teniendo en cuenta que como docentes tenemos la función de enseñar entonces por qué no enseñarle a los estudiantes acerca de esos peligros a los que ellos en algún momento se pueden enfrentar.

Ninguna persona que use internet está exento de ser víctima de alguno de los peligros que hay allí, pero una persona informada y con conocimientos puede evitar ser víctima de esos peligros es entonces cuando se hace necesario que los estudiantes sepan cuáles son esos peligros, conozcan cómo es que funcionan , y como se pueden evitar, acerca de este tema es que se trata este documento, además aquí se plantea un material educativo computacional el cual se pretende trabajar con un grupo de estudiantes, en dicho material se le dan a los estudiantes una serie de orientaciones y se le proponen unos ejercicios prácticos los cuales tienen el fin de que el alumno cambie ciertas acciones que lo pueden llevar a ser víctima de los diversos peligros que hay en internet.

Capítulo 1. Componentes iniciales del problema

1.1 Planteamiento del problema

Actualmente el acceso a internet por parte de los jóvenes es más frecuente, a este se puede acceder desde diversos lugares (la casa, los centros comerciales, los parques, el colegio, etc.), a través de distintos dispositivos (computador, celular, Tablet, televisor, etc.) donde la conexión se puede hacer por cable o a través de la red wifi. Teniendo en cuenta la facilidad de acceso y conexión a internet, resulta pertinente considerar algunas estadísticas.

De acuerdo con cifras actuales que ofrece MINTIC¹, el tercer Trimestre del 2015 se registraron en total 12.266.069 suscriptores a internet cifra que aumento en el mismo trimestre pero del 2016, un año después arrojando la cifra 15.130.185 suscriptores, aumento que se vio reflejado en casi 2.864.116 personas con acceso a internet.

De estas cifras es significativo tener un dato de Bogotá, donde se registró en ese mismo periodo de tiempo un aumento de 117.486 suscriptores a internet², cifras que pueden ser insignificantes pero que demuestran el alto impacto del internet en los hogares donde los jóvenes son beneficiarios.

Es posible que estas estadísticas nombradas anteriormente hayan aumentado para el cuarto trimestre del año 2016, pero actualmente de estos no se tiene informe³. Teniendo conocimiento

¹ Siglas pertenecientes al ministerio de tecnologías de la información y la comunicación

² Según las estadísticas consultadas las cifras fueron de 1.597.190 suscriptores en 2015 (3 trimestre) y de 1.714.676 suscriptores en 2016 (3 trimestre)

³ Esto se afirma teniendo en cuenta que se hace una última consulta el día 24 de mayo del 2017 al sitio de donde se sacaron estas estadísticas y estas no han sido actualizadas.

de los datos anteriores se puede decir que el avance en el tema de internet en nuestro país es cada vez más imprescindible en la conexión global del servicio a internet, pero como todo lo bueno tiene sus problemas, el solo hacer una inversión a nivel estructural y de conexión, deja aislado a problemas que cobijan a la mayoría de la población en el uso apropiado de la internet y los peligros cibernéticos a los que actualmente la juventud se ve expuesta.

Pero cuál ha sido el alcance que ha tenido la educación en ámbitos de acceso a internet, de acuerdo con la Secretaria de educación del distrito (2015).

“Al inicio del gobierno de la Bogotá Humana, tan solo 200 sedes de colegios oficiales tenían conexión a internet de alta velocidad. Hoy, de las 706 sedes con las que cuenta la educación pública de Bogotá, 621 ya cuentan con 30 megas para navegar. Esto beneficia a más 800 mil estudiantes y cerca de 30 mil maestros.”

A partir de esto resulta oportuno tener en cuenta que en las clases de informática de algunos colegios los temas de enseñanza principalmente son enfocados a la ofimática, el uso y enseñanza de software de programación y la realización de algunas actividades en internet, ya sea la creación de un blog, una wiki o una cuenta de correo, lo cual es necesario de cierta manera, pero si como se enuncia anteriormente que casi 621 colegios de Bogotá tiene conexión a internet; se podría pensar que si a estos estudiantes no se les orienta sobre los riesgos que se podrían encontrar en la web, algunos de estos serían vulnerables frente a estos peligros.

Es probable que muchos de los jóvenes que tienen acceso a la web no se preocupen por lo que se puedan encontrar allí, quizás por que consideren que no les afecte o porque ellos no lo vean como peligroso, pero es importante instruirlos y darles a conocer que el internet es otro mundo,

pero de forma virtual el cual a su vez tiene sus peligros como el mundo real. A partir de toda la información anterior se plantea la siguiente pregunta problema.

1.2 Pregunta problema

¿Cambian algunas acciones de los estudiantes en el uso del internet después de orientarlos sobre los peligros a los que pueden estar expuestos?

Es importante tener en cuenta que el internet siendo prácticamente un mundo entramado de flujo de datos, allí las personas se ven expuestas a muchos de los peligros como ataques cibernéticos y posibles suplantaciones de identidades. Aunque el proyecto no evita que la población se exponga, si busca orientarlos sobre los malos hábitos y posibles riesgos de internet a los que se puedan enfrentar en algún momento de su vida.

1.3 Justificación

Considerando que la gran mayoría de los dispositivos conectados a internet son manejados por personas y teniendo en cuenta que no todas las personas conectadas a la web tienen buenas intenciones sería lógico pensar que estos sujetos pongan en práctica sus malas intenciones usando internet, lo que significa que cuando un usuario se conecta a la web puede llegar a ser víctima de algún peligro de internet. Es entonces cuando se puede creer que son muy pocas las personas que navegan en la web y a la vez están pensando en que se pueden exponer a alguno de los peligros existentes en la red de redes.

Es aquí cuando se ve la necesidad de dar a conocer a los estudiantes cuáles son los peligros a los que se puede estar expuesto en la red y ese es uno de los propósitos de este proyecto de

grado, revisando el documento CONPES 3854, se encuentran varios ítems referentes a la seguridad digital, entre ellos se encuentra una estrategia titulada “Promover en los diferentes niveles de formación comportamientos responsables en el entorno digital (DE5)” en la cual se enuncia que el fin de esta es capacitar a estudiantes y docentes sobre los riesgos de la seguridad digital, de manera puntual se afirma.

“El Gobierno nacional, a través del Ministerio de Educación Nacional, creará contenidos educativos complementarios relacionados con la gestión de riesgos de seguridad digital, y capacitará a los estudiantes de educación básica y media, y a los estudiantes de educación superior, a estos últimos a través del Portal Educativo Colombia Aprende”. CONPES 3854 (2016).

Basado en el párrafo anterior se puede entender que todos los estudiantes deberían tener conocimientos sobre los riesgos digitales, además se habla de la creación de contenidos donde se trabajen estas temáticas, a partir de esto se puede evidenciar que el proyecto a trabajar es viable ya que con el desarrollo de este se contribuye a esta estrategia planteada por el Ministerio de Educación Nacional (MEN), a partir de este mismo documento (CONPES 3854), se entiende que cada vez más el gobierno de Colombia se ha venido preocupando por la seguridad digital de las personas y que el tema está en auge, esta es una razón más que lleva a considerar el trabajar esta temática.

Teniendo en cuenta que en dicho documento se habla de una creación de contenidos por parte del gobierno nacional lo más adecuado es revisar dichos contenidos ya que a partir de ellos se puede realizar el material que en este proyecto se desea trabajar con los estudiantes, pero en la búsqueda de dichos contenidos estos no se encuentran quizás la razón de esto sea que en el

apartado de recomendaciones del CONPES 3854 se plantea que dichos contenidos deben ser creados e implementados a partir de enero del 2017.

Por otro lado se encuentra un artículo periodístico de RCN radio (2016), titulado “Colegios tendrían nueva cátedra de seguridad digital para fomentar el uso responsable de TIC” allí Fernando Bejarano⁴ afirma

Tenemos laboratorios de informática pero es muy poco lo que realmente aprenden ellos en términos de riesgos de seguridad digital, por ejemplo que hagan buen uso de las redes sociales, de dispositivos móviles y cómo usarlos de manera adecuada. Es un tema donde tienen que conocer aspectos básicos.

Con respecto a las palabras del señor Bejarano se nota que este proyecto cada vez es más viable, ya que este de cierta manera da a entender que es necesario el trabajar con los estudiantes sobre los diversos riesgos que cualquier persona se puede encontrar en la red y mucho más un joven que de cierta manera se preocupa menos por esto.

Ahora es importante entender que con este trabajo no se pretende enseñarle a los estudiantes la teoría existente sobre los diversos riesgos encontrados en la red ya que información teórica respecto a este tema existe en libros, en videos, en diversas páginas de internet, etc. aquí la finalidad que se tiene, es que los estudiantes a través de diversos ejercicios propuestos en el material educativo computacional y en el post-test se den cuenta que a partir de ciertas acciones que tienen mientras usan internet, pueden estar expuestos a alguno de los peligros existentes en la web, es decir, información sobre los diversos peligros de internet se puede encontrar en

⁴ Fernando bejarano es el director de estándares y arquitectura de tecnologías de la información del Ministerio TIC. Quien concedió estas palabras para RCN radio, las cuales se encuentran plasmadas en el artículo titulado “Colegios tendrían nueva cátedra de seguridad digital para fomentar el uso responsable de TIC”

muchas partes, pero ejercicios referentes al tema no se encuentran mucho y menos ejercicios parecidos a los que se proponen en este trabajo de grado.

Para culminar este apartado es significativo considerar que un profesor puede influir en cada uno de sus alumnos, lo que significa que como docentes al trabajar este tipo de temas con los educandos se podría lograr que ellos se interesaran más por conocer sobre la importancia de tener ciertas precauciones cada vez que se usa internet, para de esta manera lograr que en un futuro estos alumnos no se expongan a caer en alguno de los riesgos de la red.

1.4 Objetivos

1.4.1 Objetivo general: Analizar los cambios en los estudiantes al actuar en internet después de haberlos orientado en los peligros con los que se pueden encontrar.

1.4.2 Objetivos específicos:

- Identificar los peligros de internet a los que se ve expuesta la población objeto de estudio
- Orientar a los estudiantes como utilizar internet de manera segura, buscando que estos sepan cómo actuar en caso de encontrarse con los peligros aquí trabajados.
- Evidenciar la incidencia que tiene el material educativo en los estudiantes a partir de la aplicación de este.

1.5 Antecedentes

Durante la búsqueda de antecedentes se observa que gran parte de la información se enfoca más a las redes sociales y no a otros campos del internet como la búsqueda de información, el manejo de correo electrónico, sitios de descarga y visualización de videos, teniendo en cuenta esto, se decide optar por buscar antecedentes en los cuales se trabaje el comportamiento de los jóvenes en internet.

Los antecedentes de este proyecto están organizados de la siguiente manera: local, nacional e internacional.

1.5.1 Local:

1. Nombre del trabajo: Investigación revela completa radiografía del uso de Internet de los adolescentes en Bogotá.

Autor: Universidad de la Sabana.

Año: 2014

Este es un estudio de la universidad anteriormente nombrada que consistió en una consulta a una población de 180 estudiantes con unas edades de 12 y 18 años los cuales son de estratos 4, 5 y 6.

El objetivo de dicha investigación era resolver algunas preguntas que ellos se habían planteado, tales como “¿cuáles son los principales riesgos y beneficios a los que se ven expuestos los adolescentes en Bogotá por el uso de esta herramienta?, ¿Cómo la están utilizando? y ¿Qué percepción tienen de ella?”

Respecto a los resultados obtenidos por ellos lo que podría aportar a este trabajo es:

- El referente a las aplicaciones o sitios más utilizados y cuyos resultados son
 “Las aplicaciones que más utilizan están relacionadas con las comunidades virtuales y las redes sociales. El 27% de los entrevistados afirmó que entra frecuentemente a Facebook, el 23% a Skype Messenger, el 17% a Google, el 11% a YouTube, el 10% a Hotmail, el 6% chatea, el 3% juega en línea, el 2% ve pornografía y el 1% hace apuestas.”
- El referente al para que usan internet, este según Martin, el director de la investigación.
 “En promedio, el 45% de los adolescentes se conectan a Internet para estar en contacto con otros, el 19% por distracción, el 13% para descargar música o videos, el 12% por fines académicos, el 7% para buscar información de interés personal, el 3% para conocer gente y sólo el 1% para escapar de la cotidianidad”
- El referente a las percepciones de los peligros en internet:
 “En cuanto a las percepciones de los riesgos que tiene Internet, los entrevistados sostuvieron que temen ser víctimas de chismes en el 95% de los casos, de críticas (89%), de inseguridad (87%), de burlas (86%), de pornografía (83%), de rencores (68%), de depresión (43%) y de aislamiento social (42%).”

1.5.2 Nacional: los siguientes antecedentes son de documentos e investigaciones realizadas en nuestro país:

1. Nombre del trabajo: METODOLOGÍA PARA LA ENSEÑANZA DE LA NETIQUETA, EN EL ÁREA DE INFORMÁTICA EN GRADO 10 EN LA INSTITUCIÓN EDUCATIVA ALFONSO LÓPEZ PUMAREJO DEL MUNICIPIO DE LA VIRGINIA RISARALDA.

Autor: Bustamante y Ledesma

Año: 2014

Este trabajo tuvo como finalidad la enseñanza de la netiqueta en los estudiantes de grado decimo de un colegio de Pereira, según el documento la enseñanza del tema se pretendía realizar por medio de un grupo en Facebook. En resumen la metodología utilizada por ellas en este trabajo lo dividen en dos momentos.

En el primer momento hablan de un trabajo sin interacción con Facebook donde la idea es saber que saben los estudiantes sobre el tema, hacen grupos de trabajo para que entre los estudiantes discutan sobre el tema, donde Bustamante y Ledesma expresan que no importa si los aportes de los estudiantes sobre el tema, son correctas o no, si no que a parir la idea es que entre todos construyan el concepto. Para terminar este primer momento las autoras les dan una introducción a los estudiantes sobre lo que se hará en el segundo momento, como en este caso ellas utilizan Facebook como una herramienta entonces le hablan a los chicos de cómo será la interacción con este.

En el segundo momento pasan a la utilización de Facebook como herramienta, donde publicaran los temas a trabajar, desarrollo de actividades y competencias que adquirirán los estudiantes, además de la utilización de las herramientas que da Facebook como el chat, y las publicaciones en el muro.

Ellas también hablan de que su observación es participante, teniendo en cuenta que ellas intervendrán ya sea dando instrucciones, guiando actividades y demás, ellas observaron lo siguiente en su documento: uso de las herramientas, apropiación del tema, participación conjunta y responsabilidad individual, para finalizar este antecedente Bustamante y Ledesma (2014) dicen entre sus conclusiones.

“Mediante la metodología diseñada para la enseñanza de la netiqueta en el área de informática, se estableció una secuencia didáctica que permitió reconocer el estado en que se encontraban los estudiantes frente al tema planteado (netiqueta), un proceso a seguir y las reacciones encontradas durante la implementación de la metodología y el aprendizaje. En consecuencia, la secuencia didáctica permitió establecer parámetros a seguir, acciones frente a las situaciones presentadas antes, durante y después de la aplicación en el entorno y el reconocimiento de la adquisición de los nuevos conocimientos mediante un tipo de aprendizaje colaborativo.” (pág. 123).

2 . Nombre del trabajo: LAS REDES SOCIALES, SUS RIESGOS Y LA MANERA DE PROTEGERSE

Autor: Sierra del valle

Año: 2013

Este artículo el autor lo divide en seis partes, que son: 1.) concepto de redes sociales, 2.) clasificación de las redes sociales, 3.) la historia cronológica de las redes sociales, 4.) el auge de las redes sociales en la sociedad actual, 5.) riesgos de las redes sociales en internet, 6.) normatividad en Colombia referente a la protección de la información y termina con las respectivas conclusiones.

De este artículo el aporte principalmente como antecedentes es la quinta y sexta parte donde el autor trabaja los riesgos de las redes sociales en internet y la normatividad en Colombia referente a la protección de la información. Si se habla un poco de este artículo se observa que el

aporte que brinda este artículo sería los riesgos que se pueden encontrar en las redes sociales según el Comité Económico y Social Europeo citado por Sierra del Valle (2013) son:

“Los riesgos psicológicos derivados de insultos transmitidos por esos medios,

El acoso sexual a niños y jóvenes,

La exhibición en formatos multimedia de adolescentes desnudos,

Los anuncios de prostitución,

La violación de la privacidad,

La honra y la dignidad personal,

Los atentados contra la salud física y mental de los usuarios,

Los llamamientos a la xenofobia,

El racismo o la violencia,

Divulgación del ideario fascista o nacionalsocialista, y

La creación de situaciones extremas que puedan llevar al suicidio a determinadas personas”⁵.

1.5.3 Internacional: los antecedentes siguientes son de investigaciones, artículos y demás realizados en otros países.

1. Nombre del trabajo: una perspectiva sobre los riesgos y usos de internet en la adolescencia

⁵ Esta cita se puso de esta manera ya que así aparece en el documento de donde fue tomada

Autor: García Jiménez

Año: 2011

Este documento consiste en la investigación sobre los usos y consumos de medios y redes sociales de los adolescentes madrileños y detectar las prácticas de riesgo que llevan asociados. La forma en la que se desarrolló este proyecto fue utilizando encuestas y grupos de discusión, allí se trabajaron dos grupos según su edad los cuales son de 12 a 14 años y de 15 a 17 años.

A partir de dicho estudio García Jiménez (2011) da a conocer los siguientes resultados.

“al 76,3% de los entrevistados afirma haber entrado en contacto con algún contenido no recomendado de forma involuntaria. Por ejemplo, el 15,4% afirma tener acceso frecuente, de modo inconsciente, a contenidos sexuales fuertes y el 9,5% a escenas de violencia. Por otra parte, el 44,6% de los jóvenes afirma que ha recibido la petición de algún desconocido para contactar por teléfono o por correo electrónico y también una proporción relevante, un 17,1%, dice haber recibido peticiones para encuentros cara a cara. En este sentido, un 10,4% se declara responsable de haber solicitado a algún desconocido contactar por teléfono o tener un encuentro cara a cara”.

En la parte de las conclusiones se encuentra que “Ya sean en la escuela o en casa, la formación, la educomunicación, la regulación positiva y responsabilidad deben convivir con Internet, entendido como el lugar para un nuevo modelo de comunicación interpersonal, especialmente de las nuevas generaciones.”(García, 2011, pág. 409).

2. nombre del trabajo: INTERNET Y ADOLESCENCIA: GUIA ON LINE PARA EDUCADORES

Autor: Puchades

Año: 2013

Durante la revisión de este documento se encuentra en la parte inicial que Puchades (2013) dice:

“**la motivación de este estudio** ha sido en centrarnos en el adolescente en internet, la influencia de su uso en aspectos muy importantes de sus vidas, como por ejemplo, el ámbito escolar, el entorno familiar, tiempo de uso de pantallas y la valoración de los posibles peligros que puede entrañar. Ya el hecho, de lo que podríamos en un principio suponer una simple conexión y que resulta no ser lo inocente que esperábamos. (p.9)”

A su vez en este documento se observa que el autor divide este en cuatro partes, la primera es la brecha digital, la segunda parte es el ciberacoso donde el autor trata y define todos los temas respecto a lo que se quiere tratar en este trabajo, estos temas son Ciberbullying, grooming sexting, phishing, pedofilia y pornografía infantil.

En la tercera parte se encuentra un apartado para padres y educadores, y en la última parte el autor se refiere a la parte legal, conclusiones y consejos. A su vez vemos en el documento que el autor obtuvo como material un blog el cual se encuentra en <https://adolescentinternet.wordpress.com/> y en el cual trata temas respecto al acoso en internet.

Cuando Puchades llega a las conclusiones de este documento (2013) dice:

“El adolescente es una persona muy vulnerable y necesita sentirse incluido en esta sociedad, e incluso ellos, reciben o realizan parte de sus tareas escolares mediante el uso de esta tecnología, por lo tanto, ya sea educadores o familiares del adolescente, deben de asegurar dentro de la medida de lo posible la máxima seguridad en el uso de internet por el adolescente, aplicando las herramientas indispensables de protección en la red contra los fenómenos como el grooming o Ciberbullying.”(p. 78).

Este autor durante su documento habla ciertas cosas acerca de dos peligros de internet como lo son el grooming y el Ciberbullying, este sería el aporte de ese autor, en las demás conclusiones el autor se refiere a que es importante enfocar a los niños y orientarlos durante el uso del internet.

3. Nombre del trabajo: Hábitos de usos y conductas de riesgo en internet en la preadolescencia

Autor: Fernández, Peñalva e Irazábal

Año: 2015

El artículo es basado en un estudio realizado a una población de entre 10 y 13 años quienes cursan sexto año escolar y son de la ciudad de Navarra España, el total de sujetos con los que se hizo la investigación fueron 364 (206 niños y 158 niñas).

Esta investigación se ve importante tenerla en cuenta como antecedente de este trabajo no solo por el hecho de que tenga que ver con internet, sino que también entre sus resultados se muestran algunos comportamientos frente a las tics, especialmente hacia el internet.

En la página 114 de la revista comunicar (2015), se puede evidenciar que el objetivo principal de dicho estudio es “conocer las características del uso de Internet en una muestra de preadolescentes de sexto curso de Educación Primaria. Se trata de determinar el grado real de penetración que las TIC, y principalmente Internet, tiene en estas edades.”

Estos investigadores recogieron la información de este estudio a partir de la elaboración de 142 preguntas en las cuales Fernández, Peñalva e Irazabal (2015), trabajaron 11 temáticas referentes a las nuevas tecnologías, que fueron:

“introducción de las TIC en los hogares, introducción de Internet en los hogares, lugar que ocupa Internet en la vida cotidiana del niño, formación recibida en TIC (reglada y no reglada), grado de alfabetización digital conceptual, grado de alfabetización digital procedimental, grado de alfabetización digital actitudinal, perfil de los usuarios de Internet, características de los usuarios de teléfono móvil, acceso y creación de contenidos en Internet, y actividades desarrolladas en Internet.”.(p.115)

Lo interesante de este artículo de estudio, son los resultados obtenidos y más que todos los referentes a los comportamientos de los estudiantes y sus conductas en internet; en donde Fernández, Peñalva e Irazabal (2015) manifiestan que:

“Las principales conductas llevadas a cabo a través de la red se relacionan con el desarrollo de las relaciones sociales. En este sentido, Internet se utiliza para quedar o hacer planes con los amigos, agregarlos a los perfiles sociales, enviarles mensajes o conversar con ellos en tiempo real.

Por otra parte, se observan comportamientos que, aun siendo menos frecuentes, son importantes de destacar. Así, entre el 20% y el 30% de la muestra miente a través de la

red diciendo que tiene más edad de la real o, incluso, diciendo que su apariencia física es distinta.”

A su vez en este mismo apartado de resultados, los autores nombran algunas conductas de riesgos que obtuvieron en su estudio y que fueron “enviar fotografías o vídeos a desconocidos, añadir personas desconocidas a la lista de amigos, dar el número de teléfono o cualquier otro tipo de dato personal, enviar fotografías o vídeos a través de la Red o, lo que es más peligroso, quedar directamente con desconocidos.” (Fernández, Peñalva e Irazabal, 2015, p. 116).

Capítulo 2 marco legal y teórico

2.1 Marco legal

Cuando se habla de internet muchas veces se puede pensar en libertad o en que en este se puede hacer lo que se quiera, esta forma de ver al internet se presenta más que todo en los jóvenes quienes la gran mayoría de veces navegan en la red sin medir las consecuencias de lo que están haciendo. Es aquí cuando se hace necesario conocer que en el país si existen varias leyes respecto al tema (internet) las cuales es necesario conocer para el desarrollo de este proyecto,

Algunas de las leyes que existen en nuestro país y que de cierta manera están vinculados con el uso de internet son las siguientes.

2.1.1 Ley 1620 del 15 de marzo del 2013: esta ley se crea en base a la ya existente ley 115 de 1994 (ley general de educación), en esta ley se tratan temas como “creación del sistema nacional de convivencia escolar y formación para el ejercicio de los derechos humanos, la educación para la sexualidad y la prevención y mitigación de la violencia escolar.”

Esta ley es importante en este marco legal debido a que en ella se trata el tema de Ciberbullying que es definido en esta como “forma de intimidación con uso deliberado de tecnologías de información (Internet, redes sociales virtuales, telefonía móvil y video juegos online) para ejercer maltrato psicológico y continuado.”(Pag 2.) Asimismo se considera el numeral 9 del artículo 8 que dice “Coordinar la creación de mecanismos de denuncia y seguimiento en Internet, redes sociales y demás tecnologías de información a los casos de ciberbullying.”(Pag 6.)

2.1.2 Ley 679 del 2001: esta ley tiene por objeto según el congreso de la republica (2001):

“**ARTÍCULO 1o. OBJETO.** Esta ley tiene por objeto dictar medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio, y la expedición de otras disposiciones en desarrollo del artículo 44 de la Constitución.”

La presente ley tiene importancia en este trabajo, si es asociada con uno de los peligros aquí desarrollados, en este caso con el “Grooming” (descrito y trabajado en este documento más adelante), esto se afirma teniendo en cuenta que según un artículo de MinTIC (2015) dice que:

“En Colombia el Grooming no está tipificado como delito, sin embargo cuando un victimario establece contacto con un menor de 18 años con fines sexuales, se considera pornografía infantil y esto sí es considerado un delito. Desde el 2013 se han recibido más

de 17 mil denuncias de las cuales casi la mitad están relacionados con pornografía infantil.”

De la presente ley se considera que los artículos que aportan a este trabajo y que son importantes tener en cuenta son el artículo 7(prohibiciones), 8(deberes) y 10 (sanciones) que son los artículos en donde se evidencia una relación a internet.

2.1.3 Ley 1336 de 2009 (julio 21): esta ley fue desarrollada con el fin de robustecer la ya existente ley 679 del 2001, revisando esta ley se encuentra que el artículo 24 aporta información importante a este trabajo; el artículo dice lo siguiente:

ARTÍCULO 24. El artículo 218 de la ley 599 quedara así:

Artículo 218. *Pornografía con personas menores de 18 años.* El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, incurrirá en prisión de 10 a 20 años y multa de 150 a 1.500 salarios mínimos legales mensuales vigentes. Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro.

2.1.4 Ley 1341 de 2009 (13 de julio): durante la revisión de esta ley se contempla que es una de las más completas en lo que respecta al ámbito de las TIC⁶, esto es percibido en el artículo 1 de la ley mencionada, con el siguiente objetivo

Artículo 1.- OBJETO. La presente Ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información. (Ley 1341, 2009, pág. 1).

Como se observa anteriormente esta ley cobija todo el ámbito de las TIC en el país, incluyendo hechos como la brecha digital, los aportes al Ministerio de educación, el acceso a las tics por parte de todos los habitantes de Colombia y demás temas, pero los únicos que sirven como influencias en el presente trabajo de grado son los tres temas nombrados anteriormente.

Para este proyecto también es de suma importancia el **artículo 6** de la ley mencionada; ya que se presenta una definición concreta de las tics.

⁶ Durante todo este documento se nombrara a las tecnologías de la información y la comunicación como TIC Y no como TICS, ya que la forma correcta de escribirlo en plural es agregándole el artículo en plural (las tic o algunas tic) información sacada de <http://www.fundeu.es/recomendacion/las-tic-mejor-que-las-tics-o-las-tics/>

ARTÍCULO 6.-DEFINICIÓN DE TIC: Las Tecnologías de la Información y las Comunicaciones (en adelante TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, vídeo e imágenes.

El Ministerio de Tecnologías de la Información y las Comunicaciones junto con la CRC, deberán expedir el glosario de definiciones acordes con los postulados de la UIT y otros organismos internacionales con los cuales sea Colombia firmante de protocolos referidos a estas materias. (Ley 1341, 2009, pág. 4).

Otro de los artículos a tener en consideración es que tiene que ver con la parte educativa, esto teniendo en cuenta que este proyecto se desarrollara en dos colegios, el artículo que se refiere a este tema es el **ARTÍCULO 39** titulado **Articulación DEL PLAN DE TIC**, el cual se compone de 5 numerales tal cual como se observa a continuación:

ARTÍCULO 39.- ARTICULACIÓN DEL PLAN DE TIC: El Ministerio de Tecnologías de la Información y las Comunicaciones coordinará la articulación del Plan de TIC, con el Plan de Educación y los demás planes sectoriales, para facilitar la concatenación de las acciones, eficiencia en la utilización de los recursos y avanzar hacia los mismos objetivos.

Apoyará al Ministerio de Educación Nacional para:

1. Fomentar el emprendimiento en TIC, desde los establecimientos educativos, con alto contenido en innovación
2. Poner en marcha un Sistema Nacional de alfabetización digital.
3. Capacitar en TIC a docentes de todos los niveles.

4. Incluir la cátedra de TIC en todo el sistema educativo, desde la infancia.
5. Ejercer mayor control en los cafés Internet para seguridad de los niños (Ley 1341, 2009, pág.20).

2.2 Marco teórico

El marco teórico plantea las temáticas de lo general a lo particular, los temas tratados a nivel general son: el componente educativo, el significado del término comportamiento, por qué el internet es peligroso, la libertad y la privacidad en internet.

Después de haber tratado los temas generales lo siguiente es tratar los temas particulares tales como cada uno de los peligros más frecuentes a los que se puede exponer una persona cuando navega en internet entre dichos peligros se trabaja en este documento lo que es el Ciberbullying, el phishing, el grooming, algunos códigos maliciosos (virus, gusanos, troyanos, exploit, etc.) y demás.

2.2.1 Componente educativo. A partir de conocer que este proyecto tiene como fin más que observar ciertas acciones de los estudiantes, el enseñarles a estos una temática en particular, es entonces pertinente iniciar el marco teórico con lo referente a la educación.

2.2.1.1 El papel de la educación. Existen diferentes autores que hablan sobre el papel de la educación escolar para crear conciencia de los peligros existentes en internet. Sobre este apartado del papel de la educación sobre los riesgos de internet, se tiene en cuenta a Vanderhoven, Schellens y Valcke (2014), quienes basados en (Patchin & Hinduja, 2010; Tejedor & Pulido, 2012), afirman “Parece que las escuelas se encuentran en una posición ideal para

promover la educación sobre la seguridad en línea, ya que llegan a casi todos los adolescentes al mismo tiempo” (p.3).

Respecto a lo afirmado anteriormente por los autores se debe tener en cuenta que mucho más que las propias escuelas la influencia sobre los estudiantes inicia desde el profesor, teniendo en cuenta que el docente sigue un currículo establecido por la institución donde este labore.

Es el docente quien está en primera instancia y en contacto directo con los estudiantes enseñándoles cierta temática, por otra parte hay que tener en cuenta que un profesor cuando realiza una clase, le está transmitiendo nuevos conocimientos a más de un estudiante dentro del aula, en efecto se podría decir que enseñarle a los educandos sobre los diversos peligros de internet puede tener un buen resultado cuando esta enseñanza se da en la escuela ya que el conocimiento no se le está transmitiendo a una persona sino que en las instituciones educativas el conocimiento se da a un grupo de sujetos.

Asimismo es sustancial no olvidar que en muchas ocasiones, este conocimiento no llega a todos los estudiantes que están presentes en el salón de clase esto se puede presentar porque en muchos casos a los estudiantes no les interesa el tema lo que indica que en el momento de aplicar el material que va a surgir como muestra de este trabajo es significativo lograr que los estudiantes vean dicho material como interesante.

Continuando la línea del presente marco teórico, el siguiente tema a tratar hace referencia a los modelos pedagógicos esto debido a que el material que se va a desarrollar estará basado en un modelo pedagógico.

2.2.1.2. El modelo pedagógico conductista. De manera puntual en el marco teórico solo se tratara el modelo pedagógico conductista ya que basado en este es que se desarrollara el material fruto de este trabajo de grado.

Gómez y Polania (2008) anuncia que “el conductista considera que la función de la escuela es la de transmitir saberes aceptados socialmente, pero en este modelo el aprendizaje es el resultado de cambios más o menos permanentes de conducta”.

A su vez Gómez y Polania (2008) afirman que

“La función del maestro apunta en este contexto, a la de un diseñador de situaciones de aprendizaje en las cuales -tanto los estímulos como los reforzadores-, se programan para lograr las conductas deseadas. Por esta razón enseña para el logro de objetivos de aprendizaje que ha establecido previamente con claridad, y los diseña de tal modo que cualquier aprendizaje pueda medirse a través de la evaluación del nivel de logro.” (p. 57)

Por otra parte y teniendo en cuenta que la manera en la que se va a plantear el material es siguiendo la lógica de que el estudiante con el que se trabajara primeramente recibirá un estímulo (videos, imágenes, teoría contenidas dentro del material) para luego pedirle una respuesta y a partir de dicha respuesta el alumno recibirá un refuerzo, es entonces importante en este orden de ideas aclarar que aquí se estaría hablando de un condicionamiento operante, el cual es planteado por skinner, ahora es significativo tener en cuenta a Mejía (s.f) que basada en skinner afirma.

“Se entiende por operante a la serie de acciones que realiza el individuo y que generan consecuencias o respuestas de las mismas, las cuales pueden cambiarse o modificarse a través de lo se conoce como reforzadores. Los reforzadores, como su nombre lo indica, refuerzan la respuesta a la que se espera llegue el individuo” (p. 52).

Ahora es importante dejar claro que no todo el trabajo se desarrollara bajo este modelo ya que en muchas ocasiones uno puede llegar a utilizar varios modelos, pero el principal a utilizar en el desarrollo y aplicación del material educativo será el modelo pedagógico conductista.

Considerando que páginas más adelante se afirma que no todo el material ni el trabajo están enfocados en el modelo conductista, el otro modelo pedagógico que acompaña este trabajo es el constructivista, esto se afirma ya que existe la posibilidad de que los alumnos ya tengan conocimientos previos sobre las temáticas que se van a trabajar y en el momento que se trabaje el material con los educandos, estos construyan un nuevo conocimiento.

2.2.1.3 modelo pedagógico constructivista. A pesar de que el aprendizaje de conceptos por parte de los estudiantes no es un objetivo de este proyecto y si el que los alumnos cambien ciertas acciones que los pueden exponer a los peligros de internet, se debe tener en cuenta que durante la interacción del alumno con el material que se propondrá existe la posibilidad de que el estudiante adquiera o refuerce los conocimientos sobre la temática de peligros de internet y acciones que lo exponen a este, partiendo entonces de lo anterior se hace importante trabajar el modelo constructivista ya que en este se encuentra la teoría del aprendizaje significativo y de cierta manera dicha teoría se podría ver aplicada en el presente proyecto.

Ahora entrando a la referencia teórica sobre este modelo, se encuentra Tünnermann (2011) quien citando a Piaget afirma “el mecanismo básico de adquisición de conocimientos consiste en un proceso en el que las nuevas informaciones se incorporan a los esquemas o estructuras preexistentes en la mente de las personas, que se modifican y reorganizan según un mecanismo de asimilación y acomodación facilitado por la actividad del alumno”

Por otra parte Soler (2006) citando a Doolittle afirma “el constructivismo se centra en la creación y modificación activa de pensamientos, ideas, y modelos acerca de los fenómenos y afirma que el aprendizaje está influenciado por el contexto sociocultural en que está inmerso el aprendiz”

Dentro de este modelo se pueden encontrar diversas teorías que aportan al mismo, en este documento solo se tratara la teoría del aprendizaje significativo ya que esta aporta al proyecto.

2.2.1.3.1 aprendizaje significativo Romero (2009) basada en Ausubel plantea:

El aprendizaje significativo, se refiere a que el proceso de construcción de significados es el elemento central del proceso de enseñanza-aprendizaje. El alumno aprende un contenido cualquiera cuando es capaz de atribuirle un significado. Por eso lo que procede es intentar que los aprendizajes que lleven a cabo sean, en cada momento de la escolaridad, lo más significativo posible, para lo cual la enseñanza debe actuar de forma que los alumnos profundicen y amplíen los significados que construyen mediante su participación en las actividades de aprendizaje. En este sentido, las nuevas tecnologías que han ido desarrollándose en los últimos tiempos y siendo aplicadas a la educación juegan un papel vital. (p.2).

Por otra parte y referente a este tema se encuentra que para que se considere que un aprendizaje es significativo según Romero (2009) se deben considerar tres condiciones.

- El estudiante debe tener unos conocimientos previos frente a lo que se va a trabajar, para que de esta manera el alumno pueda relacionar lo que se le está enseñando con los conocimientos previos que tiene este.
- El contenido debe poseer una estructura

- El alumno debe tener actitud para aprender lo que se le desea enseñar

2.2.1.4 ¿Qué es un material educativo? Para decir que se va a desarrollar un material educativo, como parte de este proyecto; se hace necesario comprender que es un material educativo, para esto se toma como apoyo el concepto de Ospina (s.f) quien afirma:

Los materiales educativos están constituidos por todos los instrumentos de apoyo, herramientas y ayudas didácticas (guías, libros, materiales impresos y no impresos, esquemas, videos, diapositivas, imágenes, etc.) que construimos o seleccionamos con el fin de acercar a nuestros estudiantes al conocimiento y a la construcción de los conceptos para facilitar de esta manera el aprendizaje. Ahora bien, los materiales educativos realizados con la utilización de las tecnologías de la información y la comunicación, son todos los anteriormente enunciados (exceptuado los impresos), con la característica fundamental de ser representados en formato digital y transmitidos por medio de sistemas de telecomunicación.

Sabiendo que los materiales educativos son de diversos tipos como los impresos, los no impresos, ayudas didácticas, materiales digitales entre otros, el material que se va a desarrollar para este trabajo de grado será un Material Educativo Computacional (MEC).

2.2.1.5 ¿Qué es un material educativo computacional? Para Galvis, citado por Leguizamón (1996)

“Material educativo computarizado (MEC) es pues, la denominación otorgada a las diferentes aplicaciones informáticas cuyo objetivo terminal es apoyar el aprendizaje. Se caracterizan

porque es el alumno quien controla el ritmo de aprendizaje, la cantidad de ejercicios, decide cuando abandonar y reiniciar, interactuar reiteradas veces, en fin son muchos los beneficios. Por su parte el docente encuentra en ellos una ayuda significativa, pues en muchos casos en los MECs se registra toda la actividad del estudiante.” (p.2)

A su vez según Galvis (1992), los MECs se clasifican según su función, dicha clasificación es:

2.2.1.5.1 sistemas tutoriales. Este sistema tiene la característica de poseer cuatro fases las cuales hacen parte del proceso de enseñanza-aprendizaje. Dichas fases son la introductoria, la orientación inicial, la aplicación y la retroalimentación.

2.2.1.5.2 sistemas de ejercitación y práctica. Este sistema consiste en brindarle unos conocimientos previos a los estudiantes antes de que ellos tengan la respectiva interacción con el MEC, para Galvis (1992), en este sistema “deben conjugarse tres condiciones: cantidad de ejercicios, variedad en los formatos con que se presentan y retroinformación que reoriente con luz directa la acción del aprendiz”.

2.2.1.5.3 simuladores y juegos educativos. “Ambos poseen la cualidad de apoyar el aprendizaje de tipo experiencial y conjetural, como base para lograr aprendizaje por descubrimiento. La interacción con un micromundo, en forma semejante a la que se tendría en una situación real, es la fuente de conocimiento” (Galvis, 1992. p.26)

2.2.1.5.4 sistemas expertos con fines educativos. Para Galvis (1992)

“Una clase muy particular de sistemas para aprendizaje heurístico son los llamados sistemas expertos (SE). Estos son sistemas de computación capaces de representar y razonar acerca de algún dominio rico en conocimientos, con el ánimo de resolver problemas y dar consejo a quienes no son expertos en la materia” (p.29)

2.2.1.5.5 sistemas tutoriales inteligentes. Este “se caracteriza por mostrar un comportamiento inteligentemente adaptativo, es decir, adapta el tratamiento educativo en función de aquello que se desea aprender y de las características y desempeños del aprendiz” (Galvis, 1992, p. 31)

Después de tratar este apartado referente a la educación, se puede pasar al siguiente escalón, en el cual se habla sobre ciertas características de la población actual de los colegios, esos estudiantes que tienen contacto con la tecnología unos con mucha frecuencia, otros pocas veces, pero en conjunto son denominados nativos digitales.

2.2.2 Los nativos digitales. Este tema es imperioso tratarlo debido a que la población que se encuentra actualmente en las diferentes instituciones educativas, podrían ser considerados en su mayoría como nativos digitales. ¿Pero quizás usted se pregunte que significa este término?.

(Prensky, 2001) define a este tipo de población, como aquellos que han nacido y se han formado en su forma de pensar a partir de la “lengua digital” de los juegos de video en computador y el internet.

Respecto al párrafo anterior es importante el hecho de que no se puede considerar como nativo digital a todas las personas que han nacido durante esta época del boom de la tecnologías digitales, y esto se puede afirmar a partir de un artículo de CNN en español (2013), donde en uno de sus párrafos se enuncia.

Definir a los nativos y a los inmigrantes por generación es una “preocupación seria, dijo a CNN el director en el Centro para Internet y Sociedad en India, Nishant Shah. “Las observaciones (de Prensky) pueden describir una brecha generacional que Estados Unidos

enfrentó, pero si trasladas esa misma definición a otras partes del mundo, a veces los nativos son indistinguibles de los inmigrantes”.

Con respecto a lo anterior se puede afirmar que una persona es considerada como nativo digital, no solo por haber nacido en esta época de las tecnologías digitales, sino que también se considera así a las personas que han estado en contacto con ellas durante gran parte de su vida.

Siguiendo con esta temática es relevante tener en cuenta que según Prensky⁷ (2001), los nativos digitales:

- Quieren recibir información de forma ágil e inmediata
- Se sienten atraídos por las multitareas
- Prefieren los gráficos a los textos.
- Funcionan mejor y rinden más cuando trabajan en red
- Prefieren instruirse de forma lúdica a embarcarse en el rigor del trabajo tradicional.

A partir de conocer que es y cuando es una persona un nativo digital, se presenta importante considerar el hecho que la población con la que se desarrollara este proyecto son considerados como nativos digitales, lo que conlleva a tener en cuenta las características enunciadas para la aplicación del material educativo y la intervención con los estudiantes.

El tema anterior es significativo ya que lleva a focalizar un poco más sobre la población a encontrar en las instituciones educativas.

⁷ La información enunciada respecto a este autor es sacada de un texto pasado al español, el texto original es escrito en inglés y titulado “Digital Natives, Digital Immigrants”, por otra parte los puntos enunciados en esta página fueron sacados del texto traducido y se encuentran en la página 6

2.2.3 ¿Es internet peligroso? El título de este apartado podría dar a pensar que el internet es peligroso en todo momento, quizás sea así como quizás no, antes de entrar a tratar la temática de los peligros en internet es necesario tener en cuenta la información contenida en esta sección del trabajo, que tiene como propósito dar a conocer un poco que tan seguro es internet.

Se inicia esta sección a partir del libro titulado *máxima seguridad en internet*, anónimo⁸ (1998⁹). Allí el autor afirma que una de las causas para ver el internet como peligroso es “La naturaleza humana. El ser humano es perezoso. La mayoría de los usuarios prefieren pensar que la seguridad es un tema que hay que dejar en manos de los expertos” (pág. 120.).

Asimismo el autor nombra como otro de los posibles factores que pueden llevar a encontrarse con estas amenazas existentes en internet, es la curiosidad. En la vida descubrir cosas nuevas es una gran experiencia para todo ser humano, y como humanos siempre estamos descubriendo algo, esto se presenta desde el momento que se nace, durante este proceso de descubrimiento siempre se presenta un intercambio de información y mientras las personas mantengan este pensamiento de estar intercambiando información, el internet no será seguro. (Anónimo, 1998)

Pero a partir de un solo autor no es posible considerar que el internet sea del todo inseguro, Ibañez (2010), afirma que:

En cuanto al tema de la conflictividad o peligrosidad de internet no me es posible señalar a grupos o países concretos como origen de que internet este contaminado de peligros y amenazas; porque internet la hacemos todos, y en parte es el reflejo de cada uno de nuestros

⁸ Durante la lectura de este libro se puede encontrar en sus primeras páginas, que se da a entender que el autor se presenta como anónimo ya que este fue un hacker que cuando escribió dicho libro no quería revelar su identidad.

⁹ Se puede llegar a pensar que citar un libro de 1998 en este trabajo llegue a ser algo viejo, pero este se hace con el fin de mostrar que los peligros de internet existen desde hace bastante tiempo, quizás desde el mismo momento que inicio el funcionamiento del internet.

actos o influencias por muy pequeña que sea nuestra participación desde cualquier rincón del planeta. Cada uno de nosotros está haciendo a cada momento que internet cambie en unos bytes, lo cual es en realidad, un milagro de la tecnología virtual porque a su vez esos bytes de información cambian la mente de alguna persona en algún rincón del planeta (p. 170).

Adicional a lo anterior se debe también saber que la libertad en internet es prácticamente incensurable, donde cualquiera puede acceder así sus intenciones y lo que agregue a internet sea bueno o malo, esto es posible por razones como que no existe un ente regulador, no es una propiedad privada y casi cualquier persona puede hacer lo que quiera en el (Ibañez, 2010).

Por otra parte también es necesario considerar que actualmente muchos países ya presentan regulaciones sobre el internet, pero lo que en muchas ocasiones no es posible es el hecho de monitorizar y vigilar que hace cada usuario de internet.

Es posible que a partir de lo dicho por los dos autores mencionados en esta sección se tenga un poco más claro, el por qué en el internet existen peligros, se puede apreciar que ambos autores y quizás otros también hayan tratado este tema estén de acuerdo en que el peligro en la red parte desde la esencia humana, de las personas que alojan en internet cualquier archivo con el fin de causarle algún daño a otro usuario de este gran mundo virtual.

2.2.4 La privacidad en internet. La privacidad es lo que más se pierde cuando los usuarios se exponen a cualquiera de los peligros de internet.

Actualmente cada vez más con el paso del tiempo se va perdiendo la privacidad de una persona en internet, y para afirmar esto se toma como apoyo lo siguiente:

La privacidad está cada vez más expuesta y, en ocasiones, ni siquiera exige un comportamiento intencionado por parte del usuario para hacerlo. El rastro que deja una persona al moverse por internet constituye por sí mismo una pieza de información valiosísima, que permite la oferta de servicios adaptados a las particulares circunstancias del usuario y que sin duda desvela nuestra vida privada , gustos, preferencias, fotografías, viajes, foros, conversaciones, etc. (gil,2015, pág. 99.)

Es entonces cuando a partir de lo expuesto en el párrafo anterior se puede llegar a generar una gran preocupación sobre el uso que le dan a internet todos los jóvenes, y de forma particular a la población con la que se realizara este trabajo de grado.

Con el paso del tiempo se puede observar en los jóvenes un cambio sobre el concepto de privacidad en internet, ya que con el uso del internet muchos jóvenes revelan información personal en muchos casos de forma involuntaria y sin pensar las consecuencias de este hecho.

Gil (2015), en su libro “¿privacidad del menor en internet?”, plantea una pregunta que se puede considerar importante, la cual es. ¿Pero cómo es posible proteger a quien voluntariamente revela en la RED su privacidad?, para esta pregunta el autor trata de cierta manera de responderla de la siguiente manera: no se trata de prohibir o marginar a los menores que utilicen las TIC, teniendo en cuenta las ventajas que estas brindan a el conocimiento, nuevos saberes y la comunicación, lo que se debe hacer en este caso es buscar la manera de concienciar y educar sobre estas ya que a esto se añade que actualmente estamos en un mundo global donde los niños y jóvenes de la época actual están acostumbrados a la presencia de algún artefacto tecnológico(gil, 2015).

A causa de estar en este apartado hablando de la privacidad como otro de los factores que tiene relación con los peligros existentes en internet, se es relevante señalar que “privacidad y seguridad son dos caras de una misma moneda, o más bien, la privacidad debería ser entendida como uno de los pilares para construir la seguridad.”(Gil, 2015, pág. 102)

La privacidad de todos y en especial la de los menores se encuentra al desnudo en todo momento y en tiempo real, contenido como fotografías, videos, imágenes, opiniones, un ME GUSTA, y hasta el contenido retwittiado puede llegar a ser muy revelador de información para terceros que buscan información de una persona en específico.(Gil, 2015).

A partir de las temáticas anteriores se puede pasar a trabajar las temáticas más específicas del proyecto, los peligros que existen actualmente en internet, y a los cuales toda persona que accede a internet está expuesto.

2.2.5 Riesgos en internet. Internet proporciona todo un universo de cosas nuevas por descubrir, a todos los usuarios donde se encuentran incluidos los menores, este brinda diversión, información, complementa la educación y sirve como espacio de comunicación, pero no todos los usuarios en tienen buenas intenciones, por lo que a medida que aumenta su uso también aumenta la exposición a un peligro, a partir de acciones básicas como acceso a contenido poco apropiado y tener contacto con personas inescrupulosas (proyecto voces, 2006 pág. 13)

Al igual que en la vida real, en este universo virtual existen peligros como Cyberbullying, grooming, sexting, phishing, códigos maliciosos, adicción a internet entre otros.

2.2.5.1 Ciberbullying: el bullying siempre ha estado presente en las aulas de clase desde bastante tiempo atrás; pero actualmente con el uso de internet este ha trascendido las paredes de un salón de clase, para llegar a cualquier parte del mundo donde se cuente con acceso a internet. Ahora este peligro recibe el nombre de Ciberbullying; el cual de forma breve según CIBERAPP (2014) “hace referencia al uso de las TIC por parte de un menor o de un grupo de menores, para acosar de manera repetida e intencional a otro menor.” (P.10)

2.2.5.2 Grooming: de este peligro se ha hablado en algunos programas de televisión en nuestro país y se han hecho algunos artículos periodísticos de noticias de hechos que han sucedido en nuestro país.

Según la Unicef y otros (2014) se define el grooming como “la acción deliberada de un adulto de acosar sexualmente a un niño o niña mediante el uso de internet” (pág. 2), según esta misma entidad se dice que:

“el mecanismo del grooming suele incluir un pedido de foto o video de índole sexual o erótica (pedido por el adulto, utilizando el perfil falso). Cuando consigue la foto o el video, comienza un periodo de chantaje en el que se amenaza a la víctima con hacer público ese material si no entrega nuevos videos o fotos o si no accede a un encuentro personal”

A propósito del párrafo anterior se es evidente que los estudiantes puedan ser afectados por este riesgo, esto se dice partiendo del hecho de que aunque a los jóvenes muchas veces se les ha aconsejado el no chatear con extraños, estos muchas veces no siguen las advertencias que les da un adulto.

Si se observa las redes sociales más conocidas como Facebook y twitter se puede apreciar que crear un perfil falso en alguna de estas redes mencionadas es bastante fácil, pues lo único necesario es crear una cuenta de correo electrónico y poner información y fotos falsas que pueden ser de otra persona; en este caso de un niño.

2.2.5.2.1 Algunos casos de grooming en Colombia: los siguientes son dos casos de los muchos que hay actualmente en nuestro entorno cercano, según enticconfio (2016) se nombran los siguientes:

“**El imitador de cantantes:** Este hombre de 23 años –sin identificar aún por parte de las autoridades– contaba con dos perfiles falsos en Facebook, a nombre del cantante Maluma. A través de estas presencias en línea se ganaba la confianza de niñas de entre 9 y 12 años, a quienes pedía fotografías y videos en que aparecieran desnudas o en ropa interior. Una vez las menores de edad le enviaban el material que él solicitaba, las amenazaba con publicar las imágenes o enviárselas a sus padres a menos que accedieran a sostener relaciones sexuales con él.”

Otro de los casos también aquí mencionado es: “**Un delincuente con dos perfiles falsos:** Periodista de 27 años de edad. Entre los años 2011 y 2015, utilizó dos perfiles falsos de Facebook, en los cuales se presentaba como una mujer llamada *Juliana Salazar*, para contactar a estudiantes de colegios de estratos altos, de entre 13 y 16 años. Después de ganar su confianza les pedía fotos en las que estuvieran desnudos o en diferentes poses sugestivas. Luego, a través de otro perfil falso a nombre de *Andrés Monsalve*, extorsionaba para no revelar estas fotografías y videos. En estos casos, les pedía más imágenes o que accedieran a encontrarse con él. Las autoridades estiman que cerca de 150 niños habrían sido víctimas de esta persona.”

2.2.5.3 Sexting: este peligro es entendido como la acción de enviar y recibir videos o fotos insinuantes o desnudas, este se puede observar como un peligro muchas veces, como puede que en otras no; esto se afirma a partir de que es muy común esta práctica entre novios o amigos.

Según el TIEMPO (2012) “Investigadores de la Universidad de Michigan (UM) analizaron el comportamiento de 3.447 jóvenes con edades de entre 18 a 24 años, y encontraron que, si bien el sexting es muy común, a su vez también encontraron que casi la mitad de los encuestados respondieron que participaba en sexting y la mayoría de los que dijeron que habían recibido este tipo de mensaje señaló que también los había enviado, lo que sugiere que el sexting es recíproco y probablemente ocurre entre parejas románticas”

Si se sigue hablando de este tema es importante saber que una fotografía o video que se envía muchas veces a través de internet de forma inocente puede ser un peligro, no solamente por el contenido de la imagen si no también la información que pueda llevar esta, tal como lo dice Avilés (2013).

“Esas imágenes que circulan libremente por la Red pueden caer en manos de cualquiera y esto es un verdadero peligro ante el cual la mayoría de los menores son inconscientes, el enviar fotografías explícitas que pueden ser armas utilizadas por ciberdepredadores¹⁰, con el peligro añadido de que una fotografía puede aportar más datos que los que solo se ven. Una fotografía puede contener, en la información oculta (metadatos) los datos exactos de donde se tomó la misma, un Smartphone es capaz de guardar esa información en las fotografías que se hacen con este tipo de terminales.”

¹⁰ El autor define el término **ciberdepredador** para denominar a la persona adulta que padece una parafilia (**desvío de índole sexual**) en la que el objeto sexual elegido para la excitación y relación sexual es un menor y que como forma de acercamiento y acceso a los niños utiliza Internet.

2.2.5.4 Pornografía infantil. Se entiende por pornografía infantil todo material audiovisual que utiliza niños en un contexto sexual con contenidos de características groseras, lúdicas o libidinosas, dedicadas a actividades sexuales explícitas, reales o simuladas, que persigan la excitación o satisfacción sexual (proyecto voces, 2006, p. 17), este tema no se toma por el lado de que las personas con las que va a desarrollar este trabajo visualicen o no pornografía, la importancia del tema está en darles a conocer a estos jóvenes que pueden ser víctimas de este peligro, que muchas veces puede traspasar el sentido virtual y presentarse en la vida real. Una mejor explicación a esto se puede dar a entender con el siguiente texto que trata el tema de las fotografías como medio de difusión, según proyecto voces (2006) “uno de los materiales con más demanda en el mercado sexual son las fotografías de niños y, sobre todo, de niñas. Los proveedores necesitan continuamente nuevas caras y nuevos cuerpos que ofrecer.” (pág. 20).

Pero lo que más interesa y se debe tener en cuenta del peligro de las fotografías se presenta con el caso de

Las fotografías familiares de niños y niñas que muchos padres insertan en sus páginas web. Si alguna es lo suficientemente atractiva para el comercio, se pueden utilizar de varias maneras: una, robarla de su página original para intercambiarla, y otra, mucho más peligrosa, conseguir la dirección postal, que a veces los padres incluyen en la página, y de ese modo llegar al secuestro físico. (Proyecto voces, 2006, pág. 20)

A partir del texto anterior se puede observar que cualquier persona que publique una fotografía está expuesto a ser víctima de un tercero el cual use sus fotos en páginas pornográficas. Si se enfoca esto al ámbito de los jóvenes se pueden llegar a visualizar un peligro para el caso de este tema a partir del siguiente ejemplo.

Muchos jóvenes tienen cuentas en redes sociales y en las cuales publican fotos de todo lo que hacen como en los descansos del colegio, con los amigos y cuando salen de paseo, si el paseo es a piscina lo más lógico sería que estos publicaran fotos en vestido de baño, se podría entonces considerar que estas fotografías en traje de baño serían las más adecuadas para ser utilizadas como material de estos ciberdepredadores.

2.2.5.5 El phishing. Según un artículo de la revista de derecho de Valparaíso titulado “Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming"” (2013), se dice que:

Este tipo de fraude informático que ha aparecido desde mediados de la década pasada, tiene como finalidad apoderarse de información personal de un usuario de Internet, para acceder a sus cuentas de correo o de redes sociales y obtener adicionalmente datos de sus contactos virtuales, a fin de comerciarlos ilícitamente, o bien, conseguir claves de "e-banking" para de este modo ingresar a las cuentas corrientes bancarias de los titulares y disponer del dinero que en ellas se encuentra.

Por otro lado se encuentra que:

El objetivo del phishing consiste en el robo de identidad digital para obtener un lucro indebido. Para mayor concreción, se trata de un ciberataque en el cual un atacante (el *phisher*) se hace pasar por una compañía o institución financiera de reconocido prestigio, enviando mensajes de forma masiva (el primer cebo), habitualmente a través del correo electrónico (aunque podría utilizar otros canales), como mensajes instantáneos, mensajes en foros o en salas de *chat* o incluso en documentos de Word o en pdf. Sirve cualquier

soporte donde aparezca un hiperenlace sobre el que se pueda hacer clic. Los mensajes están dirigidos a potenciales clientes (phish,) de la organización suplantada, con la esperanza de que muerdan el anzuelo y sea redirigidos a un sitio web idéntico al original (el segundo cebo) encargado de recolectar la información personal que constituye su identidad digital, típicamente un nombre de usuario y contraseña o los datos de la tarjeta de crédito. (Álvarez, 2009, pag.43).

Continuando con este tema es significativo anunciar lo que expresa Solís(2013) a continuación “entre las amenazas que más pérdidas causan a los usuarios de la banca en línea y comercios electrónicos es el phishing, éste explota las vulnerabilidades humanas para obtener información sensible”(pág. 73), a su vez con este tipo de delito se es posible realizarlo y que una persona muerda el anzuelo a partir de que los delincuentes dedicados a este, crean unos sitios similares a los del banco real, con estos sitios se pretende tener acceso a los datos personales, números de tarjetas de crédito, usuarios y contraseñas de acceso a instituciones bancarias.

Sabiendo que el phishing va enfocado al engaño de las personas para principalmente hacer el robo de dinero, y durante la búsqueda de información se da a conocer que este peligro, se hace efectivo por razones como el poco conocimiento de las tecnologías, engaños visuales y la falta de atención de los usuarios que realizan este tipo de transacciones bancarias a través de internet (revista sistemas, 2013)

2.2.5.6 Acceso a material inadecuado. Cuando se habla de internet, se hace referencia a todo un mundo virtual donde se puede encontrar cualquier tipo de información, desde información valiosa para cualquier cosa que se quiere realizar hasta un contenido nocivo e ilegal, en la gran mayoría de los casos el contenido que cada persona está visualizando en el dispositivo del que

accede a internet es por qué lo ha buscado de forma voluntaria, pero a su vez también en muchos casos de manera espontánea y automática se puede apreciar un contenido no muy agradable.

Los términos nombrados anteriormente (contenido nocivo y contenido ilegal), son conceptos muy diferentes, ya que la concepción de contenido ilegal o también llamado por otros como contenido ilícito es descrito como “aquel que es constituido de delito por sí mismo p. ej. (Apología del terrorismo, incitación a la rebelión y al desorden, publicación de secretos militares y delitos contra los derechos de autor)”. (Da cunha, Luviano, Revuelta y Sánchez, 2009, pág.222)¹¹.

Mientras por otro lado el termino contenido nocivo hace alusión al contenido que puede llegar a causar algún daño en la persona que lo recibe, pero en este tipo de contenido se debe tener en cuenta cosas como la persona y su pensamiento individual ya que quizás lo que para unos sea nocivo, para otros no (García y Bringué, 2007)

2.2.5.7 Los códigos maliciosos. Otro de los diversos peligros con los que se puede encontrar una persona en internet son los llamados códigos maliciosos, de los cuales a continuación se da una breve explicación de los diversos que existen, entonces se hace importante saber que este tipo de códigos crece cada día más. Por lo tanto es importante es este tema (Marcelo y Martín, 2010) que nombran como este tipo de código a: “los virus, los gusanos, los troyanos, las puertas traseras, exploit, los keyloggers, ladillas, spyware, adware, rootkit y los redireccionadores del navegador”

¹¹ Los autores dan esta definición al término contenido ilícito, a partir de un informe de la comisión europea titulado *libro verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información*.

2.2.5.7.1 Los virus. Este es un tipo de código el cual “necesitan infiltrarse en el código de otros programas para poder propagar la infección. Se contagian sobre todo mediante el intercambio de programas y ficheros” (Marcelo y Martin, 2010, p. 40), este tipo de código se puede considerar como uno de los más frecuentes en internet.

Adicional a lo anterior se debe tener en cuenta que este tipo de códigos necesitan una interacción del usuario para poder actuar, generalmente los virus se obtienen a través del intercambio de archivos en USB, mensajes de correo electrónico o la descarga de programas de internet. (Álvarez, 2009)

“Los objetivos de los virus suelen ser los programas ejecutables (ficheros con extensión .EXE o .COM). Sin embargo, también pueden infectar otros tipos de ficheros, como páginas Web (.HTML), documentos de Word (.DOC), hojas de cálculo (.XLS), etc.”(pandasecurity.com, s.f., párr.5).

2.2.5.7.2 Los gusanos. Este es otro de los diferentes códigos maliciosos existentes, el cual presenta cierta diferencia con los virus ya que estos no necesitan infiltrarse en otros códigos ya existentes, esto se debe a que usan técnicas mucho más llamativas para los usuarios que tienden a frecuentar internet, como ejemplo se puede tener en cuenta que “ofrecen al usuario contenidos de un cierto interés, como las fotos de un famoso o famosa, o el video de un político haciendo el ridículo. Cuando la gente ejecuta dicho video o dichas fotos, esta además contaminando su sistema” (Marcelo y Martin, 2010, p. 41).

Es posible que en muchas ocasiones se tienda a confundir este código malicioso con el nombrado anteriormente (virus y gusanos), sin embargo una de las principales diferencias entre estos dos, es el hecho que

Un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas den la red (aunque sea simplemente consumiendo ancho de banda) mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan. (Administración del estado¹², 2016, p.180)

Respecto a este código malicioso se puede pensar en el hecho de que en muchas ocasiones casi nadie se fija en el peligro que existe en todo el contenido llamativo y multimedia que se encuentra en internet.

2.2.5.7.3 Troyanos. de este código se tiene en cuenta el hecho de que tienden a camuflarse en alguna otra aplicación útil, los cuales cuando ya se encuentran dentro del computador buscan permitir el acceso a otras personas de forma remota, a partir de esto se tiene en cuenta que estos presentan una diferencia respecto a los virus y la cual es que los troyanos actúan a partir de una orden humana y no de manera automática como los virus. (Marcelo y Martin, 2010)

Respecto a los troyanos es considerable conocer que “estos no se reproducen infectando otros archivos en sí, sino que se propagan engatusando a los usuarios para que hagan clic en un archivo o abran un fichero adjunto a un correo electrónico infectado”. (Goodman, s.f)

2.2.5.7.4 Los exploit Posiblemente este término sea desconocido para muchas personas que poco saben de informática; para entender mejor este tipo de código hay que partir del hecho de saber que todos los sistemas operativos están hechos en base a líneas de códigos de programación, las cuales en muchas ocasiones pueden presentar ciertos errores que son considerados como vulnerabilidades del sistema. (Marcelo y Martin, 2010)

¹² Esta administración del estado es perteneciente al país de España

Sabiendo de las vulnerabilidades que pueden presentar algunos códigos de programación, es importante saber que, “hay listillos que crean aplicaciones específicas para explotar esas debilidades, e infectar el máximo número de ordenadores posible, estas piezas de software se llaman *exploit*, y suele ser parte de otros códigos maliciosos como los gusanos” (Marcelo y Martin, 2010, p. 41).

2.2.5.7.5 Keyloggers También llamados capturadores de teclado, su inicio se da como una herramienta de los piratas informáticos, la cual actualmente es posible que sea usada por personas del común, (Marcelo y Martin, 2010) sabiendo que los keyloggers a su vez también son llamados capturadores de teclado, se da a entender de manera obvia que la función de este tipo de programa es capturar lo que escribe otra persona en el computador que se haya introducido un keyloggers.

En el momento que se dice que este tipo de programa lo puede usar cualquier tipo de persona se hace referencia a los siguientes ejemplos:

- Padres que introduce este tipo de programas en los computadores de sus hijos para monitorear lo que hacen estos
- Jefes de una empresa que monitorean a sus empleados.

Se puede observar que en los ejemplos anteriores hay más que solo capturar teclas, se habla de monitorizar un equipo de manera remota, esto es posible gracias a que cada vez con el paso del tiempo estos softwares no solo capturan lo que teclea un usuario, sino que también “permite hacer un seguimiento de todas las acciones del usuario en el ordenador y en internet, de ahí su interés en aplicaciones de espionaje doméstico” (Marcelo y Martin, 2010, p. 43).

Quizás en el párrafo anterior no se evidencie mucho los keyloggers como un peligro, sino como una herramienta útil, por lo tanto se puede pensar en que estos software son peligrosos dependiendo las intenciones que tenga la persona que lo esté utilizando, ya que un usuario de internet con malas intenciones utilizaría este para saber las claves de las tarjetas de crédito de quien este vigilando, las contraseñas de acceso a redes sociales y cuentas de correo y demás; es decir si uno se pone a pensar y analizar este tipo de software en malas manos son demasiado peligrosos.

Un ejemplo que se podría tener sobre el peligro de un keyloggers y aterrizándolo a la población objetivo de este trabajo de grado que son estudiantes, sería el tener acceso a las claves de las redes sociales de dicho estudiante, que después pueden llevar a un chantaje o una extorsión por parte de quien robo estas contraseñas a sus víctimas.

2.2.5.8 La adicción a internet: Otro de los peligros a los que se puede estar expuesto cuando se conecta a internet es el de la adicción a internet o también llamado por algunos autores y entidades como ciberadicción, este riesgo es bien definido por la Revista Argentina de Clínica Neuropsiquiátrica (2006), donde se especifica a un ciberadicto como “Alguien que teniendo una trayectoria de vida en la que el uso de Internet representaba una actividad compatible con sus relaciones personales, con su trabajo y no le producía sentimientos de culpabilidad,”. A su vez también se encuentra que.

La AI¹³ surge cuando las personas que emplean demasiado tiempo navegando en Internet generan un estado de excitación cuyos resultados serán pocas horas de sueño, hiporexia¹⁴

¹³ Esta sigla significa Adicción a Internet

¹⁴ Esta palabra es desconocida y para mayor comprensión del texto esta se define según efesalud.com como “disminución del apetito; así como la anorexia sería una falta absoluta de apetito, la hiporexia sería una disminución, de cualquier causa”

durante largos periodos y poca actividad física, con lo cual desencadenarán problemas en la salud física y mental. Estos usuarios de Internet tienden a estar menos tiempo con las personas y, por lo tanto, tendrán dificultades para relacionarse. (Navarro y Rueda, 2007, pág. 692).

La AI es una dependencia psicológica caracterizada por un incremento en las actividades que se realizan por este medio, con malestar cuando la persona no está en línea, tolerancia y negación de su problemática. El término adictivo se usa para describir los problemas que causan las sustancias como el alcohol, el cigarrillo y las drogas ilegales. Sin embargo, se ha popularizado también para otras conductas, como el sexo, las compras, el ejercicio o el juego, y ahora para Internet. (Navarro y Rueda, 2007, pág. 693).

Pero para reafirmar más esta temática de la adicción como otro de los peligros de internet, se puede recurrir a lo que dice Echeburua y requesens (2012)

Estar enganchado a internet puede actuar como una droga estimulante que produce cambios fisiológicos en el cerebro que implican el aumento de la dopamina y de otros neurotransmisores vinculados al circuito del placer. El uso de estos dispositivos sirve para alterar nuestro estado de ánimo y la conciencia y, por tanto, puede producir un *subidón* similar al generado por la cocaína. Para algunas personas, el abuso de internet es tal que su privación puede causarles síntomas de abstinencia, como, por ejemplo, un humor depresivo, irritabilidad, inquietud psicomotriz, deterioro en la concentración y trastornos del sueño. Llegados a este punto, los jóvenes sienten una necesidad imperiosa de engancharse a la red a costa de lo que sea. (pág. 51)

Si se piensa bien este peligro de internet no se evidencia de forma tan inmediata, pero con el paso del tiempo puede traer grandes consecuencias de manera física a la persona que sea víctima de este peligro.

2.2.6 Peligros en las redes sociales:

Los peligros tratados anteriormente se pueden evidenciar en cualquier sitio de internet, pero es probable que algunos se presenten más que otros en determinado sitio, esto puede suceder dependiendo el contenido de dicho sitio web.

Conociendo entonces que la población objetivo de este proyecto son jóvenes, no se puede dejar de lado las redes sociales, que son algunos de los sitios que más visitan los jóvenes y en este caso la población objetivo

Son muchas las redes sociales existentes actualmente y con el paso del tiempo se puede observar que van apareciendo más, por lo tanto trabajar todas las redes sociales tomaría mucho tiempo, lo que indica que se debe entonces solo tener en cuenta alguna de las muchas existentes como Facebook, twitter e Instagram.

Para finalizar este pequeño apartado, cabe resaltar que muchas veces las personas mismas se encargan de exponerse a estos peligros dependiendo de algunos factores que manejan en sus redes como la configuración de privacidad, el contenido que publican y que buscan, las aplicaciones externas que manejan conectadas a sus redes sociales y demás.

2.2.7 Acciones en internet. Las Acciones que realiza un usuario mientras utiliza internet, en algunas ocasiones podrían llevar a que este usuario fuera víctima de alguno de los diversos peligros nombrados anteriormente, a continuación se encuentra una lista general de acciones las

cuales fueron identificadas con una encuesta y también fueron tomadas de los diferentes referentes teóricos consultados.

Acciones peligrosas (pueden ponernos en peligro)

- El interactuar con personas desconocidas a través de internet
- El enviar archivos multimedia de la vida íntima y privada de una persona a alguien conocido o desconocido.
- El realizar descargas de cualquier archivo utilizando alguno de los sitios gratuitos existentes en internet.
- Instalar programas gratuitos sin fijarse en que archivos secundarios u ocultos se puedan estar instalando.
- No tener un antivirus con licencia activado en el computador de la casa.
- El usar la misma contraseña y códigos de seguridad para todas las cuentas que se tengan creadas ya sea en redes sociales u otros sitios de internet.
- Acceder a sitios con cierto contenido llamativo.
- Publicar en internet todo lo que hace a diario.
- No utilizar los filtros de privacidad que ofrecen ciertas redes sociales
- No leer los permisos que se le dan a una aplicación cuando se va a utilizar
- No leer los términos y condiciones de algún sitio o programa al que se desee acceder.
- El dar clic en algún enlace que alguien envié ya sea una persona conocida o desconocida.

Acciones no peligrosas (a partir de estas acciones un usuario evita estar en peligro mientras usa internet)

- Utilizar programas que hayan sido comprados en tiendas o descargados con licencia de sitios oficiales.
- Tener cuidado con quien se interactúa en internet
- Tener un antivirus con licencia activo
- Fijarse en que herramientas se están instalando a parte del programa que se desee instalar, y más si dicho programa fue descargado de un sitio gratuito.
- Tener cuidado en que sitios se visitan cuando se navega por internet
- No enviar ningún tipo de archivo de multimedia que tenga contenido de la vida privada de una persona
- Utilizar las diferentes características de privacidad y seguridad que ofrecen los sitios de internet donde se crea una cuenta (redes sociales, tiendas de música, sitios de archivos en la nube, correos, etc.)
- Estar pendiente de que tipo de páginas de internet se visitan

Antes de continuar es pertinente saber que de las acciones nombradas anteriormente solo se buscó generar cambio en algunas, este proceso usted lo observará en páginas más adelante.

Capítulo 3 metodología

3.1 El tipo de investigación

A partir de la consulta previa de los diversos tipos de investigación existentes, el presente trabajo de grado se realiza basado en la metodología cuasi-experimental

3.1.1 Cuasi-experimental. Según Hedrick et al. (1993) citado por Bono, R (s.f) “Los diseños cuasi-experimentales tienen el mismo propósito que los estudios experimentales: probar la existencia de una relación causal entre dos o más variables. Cuando la asignación aleatoria es imposible, los cuasi-experimentos (semejantes a los experimentos) permiten estimar los impactos del tratamiento o programa”, (p.3), a su vez Hernández R, (2006), afirma que “en los diseños cuasi-experimentales los sujetos no se asignan al azar a los grupos ni se emparejan, sino que dichos grupos ya están formados antes del experimento” (p.203).

Teniendo en cuenta lo anterior y que la metodología cuasi-experimental se clasifica en diversos diseños, para el caso puntual de esta investigación el diseño usado es el llamado “diseño de grupo control no equivalente”, el cual según Manterola & Otzen (2015) “consiste en un estudio en el que a uno o varios grupos se les aplica una intervención (variable independiente); y se comparan con uno o varios grupos control, que no reciben la intervención.” (p.384)

Avanzado con el tema también se hace importante expresar que en toda investigación en la cual se usa la metodología cuasi-experimental se debe tener en cuenta una o más variables independientes que se relacionan con una o más variables dependientes, según Buendía y Hernández (2001), la variable independiente (VI) “Es la variable que el investigador manipula o

selecciona para determinar su relación con el fenómeno” y la variable dependiente (VD) “es el factor que aparece, desaparece, varía, etc., como consecuencia de la manipulación que el investigador hace de la variable independiente”. A partir de estos autores y teniendo en cuenta la manera en la que se va a desarrollar este proyecto se infiere que esta es la metodología adecuada para el presente trabajo de grado.

3.2 Hipótesis.

Los estudiantes participantes de este proyecto que interactuaron con el material educativo en el cual se tratan las temáticas de privacidad en internet, grooming, Sexting y códigos maliciosos presentarán cambios en sus acciones al usar internet, los cuales se evidenciarán a través de la aplicación de un instrumento post-test.

3.3 Variables

3.3.1 Variable independiente: orientación dada a los estudiantes a partir de la aplicación del Material Educativo Computacional

Definición conceptual: en el material propuesto se trabajarán temáticas como los peligros de internet (sexting, grooming, códigos maliciosos) y las acciones que exponen a los estudiantes a estos peligros, a partir de que los estudiantes interactúen con el material se pretende que se evidencien cambios en las acciones que tienen los mismos al momento de usar internet.

3.3.2 Variable dependiente: acciones en internet que exponen a los estudiantes a peligros como el sexting, grooming, códigos maliciosos.

Definición conceptual: son diversas las acciones que tiene un usuario de internet las que lo pueden exponer a los peligros del mismo, pero si se tiene en cuenta que aquí solo se trabajaran tres peligros las acciones sobre las que el material tendrá incidencia son:

- Intercambiar fotos intimas con la pareja
- Intercambiar fotos intimas con un desconocido
- Descargar softwares de manera gratuita
- Entablar conversaciones con extraños
- No leer los términos y condiciones al instalar un software que fue descargado gratis de internet
- Tener como publicas fotos en las redes sociales cuyo contenido no deberían ver todas las personas.
- Tener demasiada información como publica en la redes sociales
- Instalar un software seleccionando la opción “instalación personalizada”, ya que esta es la opción más adecuada

3.4 Categorías de análisis.

En este proyecto se tienen en cuenta unas categorías de análisis en las cuales se resume la problemática a tratar. Dichas categorías son:

3.4.1 Los peligros de internet En internet al igual que en la vida real son diversos los peligros existentes,

En esta categoría se encuentran unas sub categorías que son:

- Los peligros que se dan a partir de una interacción con otro usuario. (Sexting, grooming, Ciberbullying).
- Los diversos códigos maliciosos (virus, gusanos, keyloggers, spywares, los troyanos)
- Otros peligros (phishing, adicción a internet).

De esta categoría es necesario aclarar que según los resultados de la encuesta (**anexo 1**) y el respectivo análisis de datos (**capítulo 5**), los peligros que se trabajan y que dan en esta categoría son:

- Los peligros que se dan a partir de una interacción con otro usuario. (Sexting, grooming,)
- Los diversos códigos maliciosos (virus, gusanos, keyloggers, spyware, los troyanos)

3.4.2 Las acciones de los usuarios en internet que los exponen a los peligros. Cada vez que se usa internet un usuario puede tener buenas acciones o malas acciones, por lo tanto esta clasificación de acciones se toma como unas subcategorías.

Acciones peligrosas (pueden ponernos en peligro)

- El interactuar con personas desconocidas a través de internet
 - El enviar archivos multimedia de la vida íntima y privada de una persona a alguien conocido o desconocido.
 - El realizar descargas de cualquier archivo utilizando alguno de los sitios gratuitos existentes en internet.
 - Instalar programas gratuitos sin fijarse en que archivos secundarios u ocultos se puedan estar instalando.

- No tener un antivirus con licencia activado en el computador de la casa.
- El usar la misma contraseña y códigos de seguridad para todas las cuentas que se tengan creadas ya sea en redes sociales u otros sitios de internet.
- Acceder a sitios con cierto contenido llamativo.
- Publicar en internet todo lo que hace a diario.
- No utilizar los filtros de privacidad que ofrecen ciertas redes sociales
- No leer los permisos que se le dan a una aplicación cuando se va a utilizar
- No leer los términos y condiciones de algún sitio o programa al que se desee acceder.
- El dar clic en algún enlace que alguien envié ya sea una persona conocida o desconocida.

Acciones no peligrosas (a partir de esta acciones un usuario evita estar en peligro mientras usa internet)

- Utilizar programas que hayan sido comprados en tiendas o descargados con licencia de sitios oficiales.
- Tener cuidado con quien se interactúa en internet
- Tener un antivirus con licencia activo
- Fijarse en que herramientas se están instalando a parte del programa que se desee instalar, y más si dicho programa fue descargado de un sitio gratuito.
- Tener cuidado en que sitios se visitan cuando se navega por internet
- No enviar ningún tipo de archivo de multimedia que tenga contenido de la vida privada de una persona

- Utilizar las diferentes características de privacidad y seguridad que ofrecen los sitios de internet donde se crea una cuenta (redes sociales, tiendas de música, sitios de archivos en la nube, correos, etc.)
- Estar pendiente de que tipo de páginas de internet se visitan

3.5 Población objeto de estudio

Este proyecto se realiza con tres grupos de estudiantes todos de décimo grado y pertenecientes a dos instituciones educativas como lo son el liceo psicopedagógico mundo activo (16 estudiantes) institución de índole privado ubicado en el municipio de Soacha, en el cual solo se trabajó con un grupo de alumnos. El segundo es el colegio distrital san francisco de asís (34 estudiantes¹⁵) ubicado en la localidad de Antonio Nariño en la ciudad de Bogotá en el cual se trabajó con dos cursos que son 10-01 y 10-03, estos estudiantes se encuentran en edades de 15 a 18 años, por otra parte, el hecho de que un colegio sea de índole privado y el otro público no afecta en nada esta investigación ya que con esta no se pretende comparar resultados entre colegios, se trabajan en estos dos colegios, ya que fueron las dos instituciones en donde se permitió trabajar con los estudiantes.

De la población participe en general se sabe que son de estratos socio económicos 1, 2 y 3. La gran mayoría tiene internet en sus hogares, desde dispositivos como computadores, tablets y teléfonos móviles.

¹⁵ En este colegio la cantidad total de estudiantes es de 55 pero teniendo en cuenta que el desarrollo de este proyecto es individual, solo se tuvieron en cuenta los estudiantes que trabajaron de manera individual, los resultados de los estudiantes que trabajaron en parejas no se tuvieron en cuenta.

3.6 Instrumentos y técnicas de recolección de datos.

Para la recolección de la información en el desarrollo del proyecto se usó:

- La encuesta
- El material educativo digital propuesto y trabajado con la población.
- El post test

3.6.1 La encuesta (ver anexo 1). Una de las herramientas más eficaces para la recolección de datos son las encuestas, según Torres M, Paz K y Salazar F enuncian algunas razones para afirmar que todo fenómeno puede ser estudiado por medio de encuestas:

1. Las técnicas de encuesta se adaptan a todo tipo de información y a cualquier población.
2. Las encuestas permiten recuperar información sobre sucesos acontecidos a los entrevistados
3. Las encuestas permiten estandarizar los datos para un análisis posterior, obteniendo gran cantidad de datos a un precio bajo y en un corto periodo de tiempo.

Considerando que el propósito de esta encuesta es obtener información de la población sobre cuáles de los peligros existentes en internet están más expuestos ellos se plantean las preguntas enfocadas en las dos categorías de investigación (peligros de internet, acciones de los estudiantes en internet)

Para terminar esta sección es pertinente mencionar que en la encuesta planteada hay unas preguntas con respuesta de selección múltiple y otras de respuesta abierta, para estas últimas lo que se realiza para analizar sus resultados es el proceso de codificación, según Rincón (2014) “el propósito de la codificación es reducir toda la variedad de respuestas dadas para una pregunta, a pocos tipos de contestaciones que pueden ser tabuladas y luego analizadas”. (p. 142).

3.6.2 El material educativo digital propuesto y trabajado con la población: el material educativo en si no es instrumento de recolección de datos propiamente dicho ya que con este se pretende orientar a los estudiantes sobre los temas contenidos en él, pero considerando que dentro del material digital se plantean unas preguntas y unos ejercicios con los que se recogen datos sobre la población, se toma el material educativo computacional como parte de los instrumento de recolección de datos.

3.6.3 El post-test. Para determinar si la interacción de los estudiantes con el material educativo tuvo alguna incidencia sobre ellos se plantea un post-test con unos ejercicios que presentan relación con cada una de las temáticas tratadas en el material, con el desarrollo de este post-test por parte de los estudiantes se obtendrán unos datos los cuales se compararan con los datos proporcionados por los alumnos en las sesiones de clase anteriores donde se trabajó con el material educativo. A su vez es pertinente enunciar que el post-test presenta ejercicios que están basados en acciones que hacen los estudiantes cuando están en internet.

3.7 Etapas para la recolección de datos y aplicación de instrumentos

3.7.1 Etapa 1: Desarrollo y aplicación de encuesta para seleccionar las temáticas a trabajar en el material digital. En la primera etapa del proyecto lo que se busca es obtener información de los estudiantes, el tipo de información que se busca aquí es, ¿que saben los participantes respecto al tema de los peligros de internet?, es decir, que tan expuestos pueden

estar a los diversos riesgos existentes en la web. Frente a esta situación el instrumento más adecuado para el desarrollo de esta etapa es una encuesta.

3.7.1.1 Planificación y creación de la encuesta. Para poder crear la encuesta fue necesario tener en cuenta los peligros que se pueden encontrar en internet, (Ciberbullying, grooming, Sexting, pornografía infantil, phishing, acceso a material inadecuado, códigos maliciosos y adicción a internet.) y ciertas acciones predeterminadas de los usuarios (chatear, descargar archivos, publicar contenido en sus redes sociales, ver contenido multimedia, entre otros.), a partir de tener clara la información sobre cada una de las temáticas, se procede a la redacción de las preguntas que contendrá la encuesta.

Luego para proceder a crear la encuesta se hace una revisión y corrección de las preguntas, entre dichas correcciones se tiene en cuenta la redacción de las mismas y el agregarle imágenes de apoyo a ciertas preguntas, esto con el fin de que haya una mejor comprensión.

A partir de las respectivas rectificaciones de los interrogantes se procede a la creación del instrumento, esto se hace utilizando la herramienta de google forms, en esta encuesta se tienen dos grandes temáticas a desarrollar, la primera es: el uso seguro e inseguro de internet y la segunda las acciones de los estudiantes en internet, adicional a esto se hace importante enunciar que en el instrumento se encuentran preguntas de respuesta múltiple y preguntas abiertas (Encuesta planteada al estudiante disponible en <https://goo.gl/forms/sHP3d0Hzcj1tAO913>.)

3.7.1.2 Prueba piloto: previo a la aplicación de la encuesta se hace la respectiva prueba piloto de la misma, donde la intención de hacer una primera prueba es ver que tan efectivas son las preguntas a partir de dicha prueba piloto se obtiene que hay que mejorar la redacción de ciertas preguntas debido a que hay algunas que los estudiantes no entienden, aquí también se evidencia

que hay que agregar más preguntas ya que habían temáticas que no se abordaron en primera instancia

3.7.1.3 Aplicación de la encuesta. Posterior a la corrección de los detalles y mejoras que se hicieron a partir de la prueba piloto, se procede a La aplicación de la encuesta la cual se realiza con los estudiantes durante una sección de clase donde la población se tomó un tiempo de hora y media para el desarrollo de la misma, esta encuesta consta de un total de 49 preguntas de las cuales 17 de ellas son de respuesta abierta y 32 de opción múltiple. Con la aplicación de esta encuesta se pretendía:

Tema 1 de la encuesta: peligros en internet

Objetivo: establecer los peligros específicos a trabajar con los estudiantes en el desarrollo de esta investigación, los cuales surgen a partir de una encuesta enfocada a estos.

Tema 2 de la encuesta: acciones de los estudiantes en internet.

Objetivo: identificar las acciones que realizan los estudiantes en internet, las cuales hacen que estos estén expuestos a los diversos peligros existentes allí.

En el (**capítulo 5**) se muestra como se planteó en análisis de datos de la encuesta, para ver los resultados de la misma vaya a (**anexo 1**)

3.7.2 Etapa 2: Construcción, prueba piloto y aplicación del material educativo computacional. Posterior a la aplicación, la obtención y análisis de las respuestas de las diversas preguntas de la encuesta (etapa 1), se obtiene que las temáticas que se deben tratar en el material digital que se creara en esta etapa 2 son:

1. La privacidad en internet
2. El grooming
3. Sexting

4. Los códigos maliciosos.

3.7.2.1 Construcción del material educativo: el desarrollo del material es basado en el diseño de Materiales Educativos Computacionales (MECs) planteado por Galvis (1992), quien propone que se tengan en cuenta 4 elementos que son el entorno, el diseño educativo, diseño de comunicación y diseño computacional (**ver capítulo 4**).

3.7.2.2 Prueba piloto del material educativo: después de desarrollar el respectivo material educativo computacional se hace necesario probar el material (prueba piloto), para este caso el material que se desarrolló se probó en el colegio liceo psicopedagógico mundo activo con una población de 12 estudiantes, con esta prueba se pretendían varias cosas como probar si el material desarrollado funcionaba perfectamente en los equipos de cómputo, ver si los estudiantes entendían el contenido planteado en el material (contenido teórico y ejercicios), observar si los estudiantes comprendían la manera en la que se navega a través del material, ver si el tamaño de la letra era el adecuado, si los colores trabajados eran los ideales, entre otros. Saber si los botones estaban en un sitio adecuado para la navegabilidad del estudiante.

Durante esta prueba se hizo una observación y se tomaron apuntes de lo que los estudiantes pensaban del material, esta prueba fue de suma importancia porque permitió evidenciar que detalles se debían corregir, entre ellos se encontró que había botones que no funcionaban, algunas preguntas que estaban repetidas, los estudiantes dijeron que el tamaño de la letra era ideal, sobre el fondo también se hizo una recomendación.

Tabla 1***Información sobre la aplicación de la respectiva prueba piloto***

Tipo de prueba	Población participe	Fecha	Finalidad de la prueba
Prueba piloto	12 estudiantes	2 semana de marzo	<ul style="list-style-type: none"> • Observar si el material educativo computacional que se aplicara con los estudiantes funciona bien en diferentes equipos • Ver si los estudiantes comprenden el contenido propuesto en el material. • tener en cuenta la información que proporcionan los estudiantes sobre que fallos encontraron en la materialidad para realizar las respectivas correcciones

Elaboración propia.

3.7.2.3 Aplicación del material educativo computacional. Posterior a la aplicación de la prueba piloto y el debido ajuste de los detalles a corregir se procede a realizar la aplicación con los estudiantes del colegio liceo psicopedagógico mundo activo y el colegio san francisco de asís, Por otra parte es importante enunciar que el material se trabajó con cada grupo durante dos secciones de clase con una duración de 1 hora y 45 minutos cada sesión.

Tabla 2***Información de la aplicación del material educativo computacional***

Tipo de prueba	Población partcipe	Fecha	Finalidad de la aplicación
Aplicación del material educativo computacional	16 estudiantes del colegio liceo psicopedagógico mundo activo del grado decimo	Viernes 31 de marzo y viernes 7 de abril del 2017	La finalidad de trabajar este material con la población es primeramente que estos a partir del contenido y los ejercicios que se le proponen allí se afecten las acciones que de cierta manera expondrían en algún momento al estudiante frente a algún peligro.
	23 Estudiantes del colegio san francisco de asís del grado decimo (10-01)	Miércoles 29 de marzo y miércoles 5 de abril del 2017	
	17 Estudiantes del colegio san francisco de asís del grado decimo (10-03)	Viernes 31 de marzo y viernes 7 de abril del 2017	

Nota importante: El tiempo de duración de las sesiones de clase es de 2 horas, pero si se tiene en cuenta el tiempo que los estudiantes toman en organizarsen, en prender los equipos y demás se llega a que el tiempo de aplicación real fue de 1 hora y 45 minutos

Elaboración propia.

3.7.3 Etapa 3 elaboración y aplicación del material post-test. Luego de la aplicación del material educativo y dado que en los objetivos se plantea el observar si este material aplicado con los estudiantes genero una incidencia en los mismos, se proponen unos ejercicios que tienen como finalidad el dar a conocer en que estudiantes se observó un cambio y en que temáticas.

3.7.3.1 Elaboración del post-test. Durante la primera y segunda semana del mes de abril del año 2017 el investigador procede a la elaboración del post-test, teniendo en cuenta las temáticas trabajadas en el material, para el caso de la temática de privacidad se piensa en simular un perfil

el cual configure el estudiante con sus datos, para el grooming y Sexting los ejercicios son una conversación simulada y para los códigos maliciosos el ejercicio es la simulación de una descarga y el manejo de ciertos permisos por parte del usuario (estudiante), entre otros.

A partir de este pos-test se evidenciara si se generó algún cambio en los estudiantes con los que se realizó la debida intervención.

3.7.3.2 Aplicación del post-test.

Tabla 3

Información de la aplicación del material educativo computacional (post-test)

Tipo de prueba	Población partícipe	Fecha	Finalidad de la aplicación
Aplicación del post-test.	14 estudiantes del colegio liceo Psicopedagógico Mundo Activo del grado décimo	Viernes 5 de mayo del 2017	Con la aplicación de esta prueba se pretende obtener unos datos los cuales darán a conocer si el educativo computacional desarrollado y aplicado a la población genero una incidencia sobre ellos.
	23 Estudiantes del colegio san francisco de Asís del grado decimo (10-01)	Miércoles 3 de mayo del 2017	Con esto se puede identificar si se generaron cambios en las acciones de los estudiantes del grupo experimental.
	13 Estudiantes del colegio san francisco de Asís del grado decimo (10-03)	Viernes 28 de abril del 2017	Además como en esta prueba participa otro grupo (control), se puede comparar los resultados entre las dos poblaciones.
	25 estudiantes del colegio san francisco de Asís (grupo comparativo, este grupo no trabajo con el material educativo)	Viernes 5 de mayo del 2017	

NOTA: En esta tabla aparece la información de la aplicación de la prueba post-test, en dicha tabla se observa que hay un grupo más que es la población comparativa, es decir la población con la que no se trabajó el material educativo solo se les aplico el post-test.

Elaboración propia.

A partir de la tabla anterior es importante observar el hecho de que el día que se aplicó el post-test faltaron estudiantes que habían trabajado con el material educativo computacional (etapa 2), lo que trae como consecuencia para el caso de la población experimental solo se consideren los datos de la población que estuvo en el desarrollo del material educativo y el post-test.

Capítulo 4 Material propuesto

Antes de iniciar la lectura de este capítulo es importante saber que el material educativo computacional se encuentra en el siguiente enlace

<https://drive.google.com/open?id=0B5JyK0N3zJKvNXJ3Vmo2WIJHRGc> si este link no funciona intente con el siguiente

<https://www.dropbox.com/sh/0i4yrozz4f47maq/AAD8PoMzvIkeG4VTBBbQrj-ka?dl=0>

En caso de que ninguno de los enlaces funcione comuníquese a los siguientes correos

dte_lsalinas002@pedagogica.edu.co o santi-65@hotmail.com

Para trabajar con la población participe se crea un material educativo con el cual los estudiantes tendrán una interacción, a partir de dicha interacción material-alumno se espera que los estudiantes luego de trabajar las temáticas y las situaciones allí propuestas estos generen cambios en sus acciones durante el uso de internet. Con esto no se quiere decir que los

estudiantes solo trabajaron con el material, pues el investigador durante el trabajo con el material participo dando ciertas orientaciones previas y explicaciones de dudas que de pronto le surgían a algún educando. Además como se dice este es un material educativo el cual es utilizado como apoyo por parte del investigador y que en una clase seria apoyo para el docente trabajar estas temáticas.

El material educativo computacional se desarrolló tomando como base 4 ítems propuestos por Galvis (1992), como son el entorno, diseño educativo, diseño de comunicación y diseño computacional, además de otros ítems como lo son el contenido a trabajar en el material el cual surge de la encuesta previamente desarrollada.

4.1 El entorno.

Referente a este ítem Galvis (1992) plantea varios interrogantes los cuales se encuentran en la tabla 4.

Tabla 4

Interrogantes planteados por Galvis para el desarrollo del entorno

¿Qué características tienen los destinatarios?	Todos los estudiantes con los que se trabajara el material educativo son pertenecientes al grado decimo de dos colegios diferentes, con una edad promedio de 15 años, ninguna de las personas que participaran tiene algún tipo de discapacidad. Lo que indica que este MEC solo está diseñado para personas que no tengan discapacidades.
¿Qué problemas se pretenden resolver con el MEC?	Con este material educativo se pretende que los estudiantes adquieran cierto conocimiento sobre los peligros de internet a los que se pueden exponer a partir de ciertas acciones que estos hacen cuando están usando internet (ver información más detallada en la tabla 5)
¿Para un equipo con que características físicas y lógicas	El material se desarrolla para ser utilizado en diferentes equipos de cómputo, esto teniendo en cuenta que el material se trabajara en dos colegios, frente a esto se opta por diseñar el material en un software en el cual se pueda generar

conviene	un ejecutable que funcione en cualquier equipo, en este caso se usó el
desarrollar el MEC?	programa Visual Basic 6.0 (ver información más completa en el ítem 4.4)

Elaboración propia

4.2 Diseño educativo (componente pedagógico).

El material educativo se plantea tomando como base el modelo pedagógico conductista, en el cual plantean estímulos, respuestas y reforzadores, esto se ve reflejado en el material de la siguiente manera, el estímulo es la información que se le da al estudiante, las imágenes y algunos videos explicativos que se encuentran dentro del material, a partir de esto se esperan unas respuestas de los alumnos en las diversas actividades allí propuestas, las respuestas esperadas aquí corresponden a esas acciones que se le indicaron al estudiante las cuales no lo expondrían al peligro (no enviar fotos intimas a la pareja, no enviar fotos intimas a extraños, manejar privacidad en la información que se maneja en los perfiles de las diferentes redes sociales, manejar configuraciones de privacidad en las fotos que se postean en redes sociales, no fijarse en los permisos que se le conceden a las aplicaciones conectadas a Facebook, entre otras ver página 75 para observar la lista completa de acciones que debería tener el estudiante para no estar en peligro) y como reforzadores se encuentran algunos videos donde se muestran casos reales, en sí mismo las actividades también actuarían como reforzadores ya que allí se trata a través de un puntaje, de un punto rojo o verde o de un signo de más o de menos indicarle al alumno si la acción o la respuesta que escogió lo pondría en peligro.

Por otra parte se tiene en cuenta que “en el modelo pedagógico conductista los esfuerzos están orientados a fijar y controlar los contenidos y los objetivos instruccionales que han sido definidos con anterioridad por el profesor, el estudiante debe adquirir conocimientos, destrezas, y competencias bajo la forma de conductas observables, la mayoría de veces medibles

”(universidad del valle, 2005), para complementar esta información es oportuno expresar que en este modelo se enfatiza principalmente en los resultados y en los efectos que pueden surgir (Ruggiero, 1996).

Antes de continuar es necesario aclarar que a pesar de que el material educativo propuesto se hace basado en el modelo conductista estímulo-respuesta-reforzamiento, también existe la posibilidad de ver aplicada la teoría del aprendizaje significativo (modelo constructivista), esto se afirma a partir considerar que los estudiantes ya tienen conocimientos previos, entonces con los ejercicios y contenido teórico propuesto en el MEC existe la posibilidad que el estudiante genere un nuevo significado entre los conocimientos previos que posee este y los nuevos que se le están transmitiendo.

A continuación se encuentra la tabla 5 donde muestran otros elementos que hacen parte esencial del proceso de desarrollo del MEC, esta tabla se pone en este apartado ya que allí se enuncian algunos elementos pedagógicos como lo son los aprendizajes a adquirir con este y la evaluación que se puede realizar a partir del material propuesto.

Tabla 5

Otros elementos del material educativo computacional propuesto.

Nombre del material educativo	Estoy en peligro cuando uso internet
Descripción de contenidos	Este es un recurso digital, en el cual se trabajan cuatro temáticas que tienen que ver con los peligros que hay en internet, entre dichas temáticas se encuentran la privacidad en internet, el grooming, el Sexting y los códigos maliciosos (virus, gusanos, troyanos, keyloggers, spywares).

Propósito del material El propósito principal del material es lograr que los estudiantes cambien las acciones que lo pueden exponer a los diversos peligros, pero hay que tener claro que estos cambios no son automáticos por lo que el estudiante tendrá que comprender lo que se le está mostrando, el por qué algunas de sus acciones son peligrosas, para que este a partir de esos aprendizajes adquiridos cambie sus acciones.

Aprendizajes que se pueden obtener con este material educativo **Privacidad en internet.**

- Comprender el concepto de que es la privacidad en internet.
- Entender porque es importante tener ciertas configuraciones de privacidad sobre cualquier contenido que se quiera publicar en internet.
- Fijarse en que contenido es adecuado publicar en las redes sociales teniendo en cuenta que la gran mayoría de personas no conocen bien a esos amigos que tienen en las redes sociales.
- Comprender la importancia de leer los permisos que se le dan a las aplicaciones que se utilizan y más si algunas de estas apps están ligadas a alguna de mis redes sociales.

Grooming

- Aprender que es el grooming (persona que usa un perfil falso para obtener material con contenido erótico de alguna persona)
 - entender que si inicio una conversación con algún extraño esta charla virtual puede tomar otro rumbo y puedo terminar siendo víctima del grooming
 - considerar que muchas personas usan internet con algún perfil falso y tratan a través de un chat hacer creer que son una persona de confianza
-

Sexting

- Aprender que es el Sexting
- Comprender que a pesar de tener una pareja estable y se tenga mucha confianza con esta persona no es seguro poner en práctica el Sexting
- Asimilar que cualquier material de contenido sensual propio que se quiere compartir con alguna persona que se conoce, puede en algún momento caer en manos de algún desconocido.
- Conocer que han existido casos de personas que en algún momento han practicado el Sexting y cuando la relación se acaba hay personas que han sextorsionado a sus ex parejas.

Códigos maliciosos

- Entender que son los códigos maliciosos (virus, gusanos, troyanos, keyloggers, spyware) y como actúa cada uno de estos.
- Tener claro que casi siempre que se descarga algún contenido de internet y si generalmente es la versión gratuita esta puede traer oculto algún código malicioso
- Reconocer cuál es la importancia de leer los términos y condiciones de algún software que se desea descargar e instalar en nuestro computador

Uso del material educativo

Este material educativo esta creado para ser trabajado en el área de tecnología e informática o en alguna otra área donde el profesor desee trabajar el tema de los peligros de internet, esto es importante ya que en cualquier momento de su acción diaria en el uso de internet una persona puede estar expuesta a los diversos peligros de la red.

	<p>Este por ser un material educativo computacional solo puede trabajar en el computador.</p> <p>A su vez una vez cuando el estudiante este interactuando con el material se encontrara con cuatro temáticas de trabajo, una vez dentro de cada temática al estudiante se le brindara una información y el a partir de esa información que se le está dando constantemente, estará en la capacidad de realizar las diversas actividades y a la vez ir adquiriendo el conocimiento que se pretende que este aprenda.</p>
<p>¿Qué se puede evaluar a partir de este material educativo?</p>	<p>A partir de este material educativo se pueden evaluar conceptos adquiridos por los estudiantes, además se puede evidenciar en las siguientes acciones si se presentan esos cambios que se desean ver como la configuración adecuada de un perfil, llevar una conversación con un desconocido que le insinúa una situación y cuál sería la diferencia si la conversación es con la pareja sentimental, el tipo de privacidad para una foto según el contenido de esta, entre otros</p>
<p>Obtención del material educativo</p>	<p>Si usted como lector de este trabajo de grado desea observar el material educativo, usted puede comunicarse al correo dte_Isalinas002@pedagogica.edu.co o santi180594@gmail.com y yo le enviare el ejecutable del material educativo para que usted lo observe en su computador.</p>
<p>Forma de trabajar el material</p>	<p>Este material educativo está diseñado para trabajo individual donde el estudiante desarrolle los ejercicios de manera personal.</p> <p>Por otra parte también se plantea que el uso sea de manera individual considerando que generalmente en la vida cotidiana una persona usa los dispositivos con conexión a internet de manera personal.</p> <p>Adicional a esto y basado en las observaciones de la aplicación de la prueba piloto se presenta que cuando los estudiantes trabajan el material en parejas no toman el material con seriedad y se despistan buscando otras cosas cuando realizan puntualmente el ejercicio de su red social.</p>

Elaboración propia, esta tabla se presentó a los docentes de las instituciones educativas, ya que en esta se encuentra la información de lo que se iba a desarrollar con los estudiantes y las temáticas que contiene el material que se trabajó con los estudiantes.

Otras cuestiones que son necesarias dar a conocer antes de culminar este apartado, es el hecho de que a pesar de que el modelo base es el conductismo, con el material también se pretende que el estudiante tenga un papel activo e individual, que el estudiante escoja cualquiera de las temáticas que se le ofrecen y una vez seleccionada está él vaya trabajando a su ritmo, por otra parte en el material también se le muestran al estudiante casos reales pues a partir de estos el estudiante los asocie a su vida y de esta manera vaya comprendiendo como a partir de las acciones que quizás el haya hecho mientras usa internet podrían llevarlo a ser una víctimas de los riesgos de internet.

4.3 Diseño de comunicación o interfaz.

Los elementos que se tienen en cuenta en este ítem son el menú, botones de navegación, las características del texto y demás elementos visuales contenidos el material educativo computacional.

4.3.1 Menú principal El material posee un menú principal donde se encuentran seis botones, 4 de ellos son los que llevan a la ventana inicial de cada una de las temáticas, otro de los botones corresponde a la bibliografía y un último botón lleva a la ventana donde se encuentra la información del proyecto como por quien fue hecho el material, para que se hizo, entre otras cosas. Los botones que corresponden a cada una de las cuatro temáticas tienen una configuración desplegable, de tal forma que cuando se hace clic sobre alguno de estos, se despliegan unos subtemas. A su vez estos botones se encuentran ubicados en la parte superior con el fin de que los subtemas de cada uno se desplieguen hacia abajo.



Imagen 1, forma en la que se encuentra el menú principal

4.3.2 Fuente de letra. La letra usada en los textos del material es de fuente Tahona 16, ya que este es un tamaño en el que la letra es legible, El color de la letra a lo largo del material generalmente es de color negro, aunque en algunas actividades después de que el alumno responde es posible que salga un texto de color rojo en caso de que la respuesta seleccionada por el alumno no sea la más segura o de color verde si la respuesta es considerada segura, estos textos son de una letra de un tamaño menor

4.3.3 Elementos gifs. El material posee ciertas animaciones .gif, el candado que se observa en la siguiente imagen es uno de los gif, presentes en el material, el uso de estos elementos se hace con el propósito de que los estudiantes realicen ciertas asociaciones, por ejemplo en la imagen 2 se visualiza un candado el cual tiene la intención de ser asociado con el termino privacidad.



Imagen 2, ventana 1 de la temática privacidad en internet del material educativo computacional.

Respecto al gif mostrado en la imagen anterior, hay que aclarar que existe la posibilidad que este fuera un distractor para el estudiante, pero esto como elemento distractor no se tuvo en cuenta durante el desarrollo del proyecto.

4.3.4 los botones de avance y retroceso. Para la navegabilidad del estudiante a través de las diversas ventanas del material, se encuentran botones ubicados en la parte inferior de cada ventana, estas flechas dentro de cada temática son diferentes ya que con esto se pretende que el usuario distinga la temática donde se encuentra ubicado.

En el caso de la temática de Sexting, los botones de avance y retroceso usados son los siguientes, estos botones son imágenes .gif



Imagen 3, botones de avance y retroceso usados en la temática de Sexting

Otro de los tema tratados en el material es el grooming, a lo largo de este módulo los botones usados son los visualizados en la imagen 4



Imagen 4, botones de avance y retroceso que se usan en el módulo del grooming.

El último tema trabajado en este material corresponde a códigos maliciosos donde los respectivos botones son.



Imagen 5, botones de avance y retroceso que se usan en el tema de los códigos maliciosos.

A lo largo del material también se encuentra el siguiente botón de continuar que es tipo .gif



Imagen 6, botones de continuar que se encuentran en ciertas partes del material

4.3.5 Actividades en el material se plantean diversos ejercicios como algunos de responder preguntas abiertas, donde es necesario que el estudiante haga uso del teclado del computador, otras son preguntas de selección múltiple, de llenar espacios en blanco entre otros. A continuación se pueden ver unos ejemplos, en la imagen 7 se puede observar que corresponde a una actividad donde el estudiante debe seleccionar la respuesta más adecuada, mientras que en la imagen 8 la actividad planteada corresponde a observar una imagen y responder en el recuadro en blanco lo que observo el estudiante en la imagen.



Número de teléfono: 344 789 65xx	<input type="radio"/> público <input type="radio"/> solo mis contactos <input checked="" type="radio"/> privado "solo yo"
Fecha de nacimiento	<input type="radio"/> público <input type="radio"/> solo mis contactos <input checked="" type="radio"/> privado "solo yo"
Foto de perfil	<input type="radio"/> público <input type="radio"/> solo mis contactos <input checked="" type="radio"/> privado "solo yo"
Álbumes de fotos y videos	<input type="radio"/> público <input type="radio"/> solo mis contactos <input checked="" type="radio"/> privado "solo yo"

Imagen 7, ventana 2 del tema privacidad en internet, en esta ventana hay un ejercicio donde el estudiante debe seleccionar la respuesta que considere correcta.

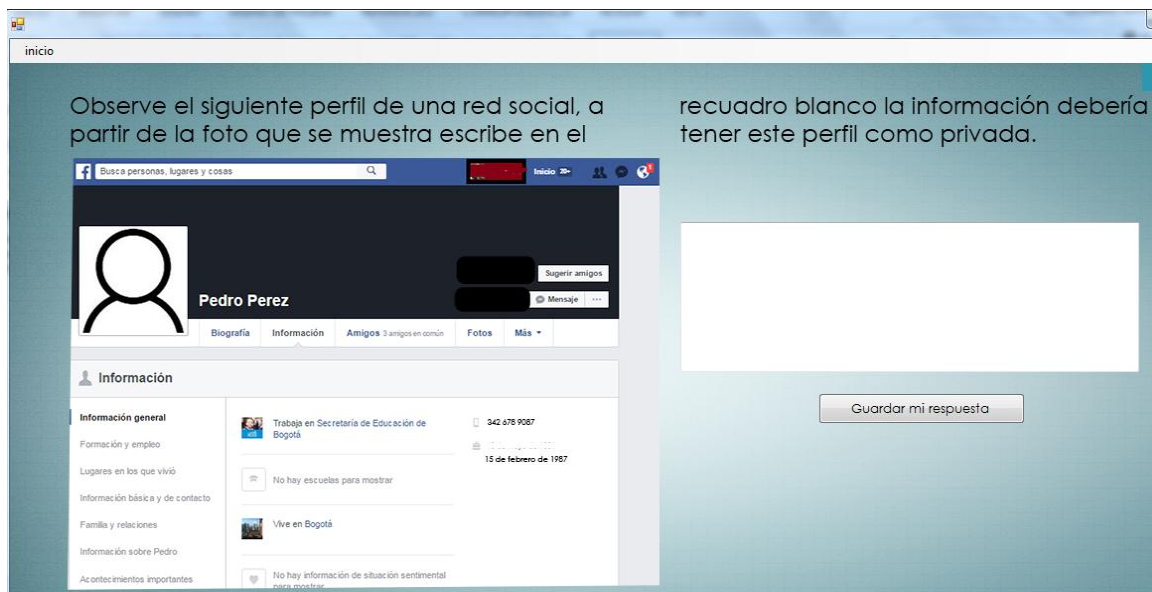


Imagen 8, en esta ventana los estudiantes deben responder lo que se les pide en el recuadro blanco, en caso de que el recuadro quede vacío el estudiante no le aparecerá el botón de continuar

4.3.6 videos. En el material se proponen unos videos para mostrar al estudiante casos reales de manera visual, un video es llamativo y genera atracción por parte de los estudiantes, estos generan motivación en el estudiante.

4.4 Diseño computacional

Para la creación del material digital se utilizó el software de Visual Basic 6.0, este programa se trabaja ya que es uno de los softwares de programación enseñado en la Universidad Pedagógica Nacional, adicional a esto se tiene en cuenta ya que permite plantear los ejercicios y el material que quiere desarrollar el investigador, otra de las consideraciones que tiene el investigador es que en este software es posible generar un ejecutable el cual pueda usarse en cualquier equipo de cómputo, esto se enuncia ya que el ejecutable que se genera aquí no requiere muchos requisitos para poder ser ejecutado en otros equipos.

El material desarrollado en Visual Basic 6.0 no tiene ningún problema en ser ejecutado en cualquier sistema operativo y al ser un ejecutable sencillo no exige que los computadores donde se va a ejecutar tengan muchos requisitos.

- Este ejecutable funciona en cualquier sistema operativo
- Funciona en equipos que tengan como mínimo 256 Mb de memoria RAM
- El ejecutable tiene un tamaño de 185 Mb
- Al tener videos como parte del contenido si es necesario que el computador donde se va a ejecutar cuente con el reproductor de video de Windows media player, ya que en otros reproductores no funcionara y esto sí podría causar un conflicto en la ejecución del material educativo.

Capítulo 5 análisis de datos

Posterior a la aplicación de los instrumentos y la debida recolección de datos de este trabajo de grado se procede al análisis de datos, en este capítulo se encuentra, cómo se analizaron los datos de la encuesta, y los datos del pre-test post-test, además de la comparación entre los datos obtenidos del post-test del grupo experimental con los datos post-test del grupo control.

5.1 la encuesta. (Ver respuestas en anexo 1) Como ya se enuncio en páginas anteriores la primera intervención que se realizó con los estudiantes fue una encuesta que contiene un total de 49 preguntas donde 17 de estas son de respuesta abierta y 32 de selección múltiple.

Para el caso de las preguntas con respuesta abierta lo que se hizo con estas fue un proceso de codificación donde se agruparon las respuestas a partir de las recurrencias a partir de cada una de estas.

Veamos a continuación un ejemplo de esto. Si nos vamos a la encuesta (ver anexo 1), se encuentra que la pregunta 2, que dice ¿Observa la siguiente imagen y piensa que el mensaje de la imagen es para ti, cual crees que sería tu reacción? En esta pregunta se muestra una imagen referente a un mensaje amenazante. Ahora si se miran algunas de las respuestas individuales que se encuentran en la base de datos para esta pregunta, nos encontramos con

Tabla 6

Algunas de las respuestas de la pregunta 2

De frustración pero primero se lo informaría a mis padres y si es el caso a las autoridades
Indiferencia. Hasta que no tenga pruebas de que lo haga no tomare ninguna otra actitud.
Yo simplemente hablaría cara a cara con el malnacido (a) y le dejaría bien en claro que ni con migo ni con mi familia se vaya o se le ocurra meterse.
me pondría mal, e intentaría hablar con la persona que mando dicho mensaje
Haría caso omiso a las palabras hirientes :'(
Decirle a mis papas.
Nada, pues suave, no me afecta
Es una estupidez
No respondería.
Le contaría a mis padres
No me interesa
No haría caso
Busco a esa persona

Respuestas tomadas de la base de datos de la encuesta aplicada a los estudiantes. Por eso se puede apreciar ciertos errores ortográficos en dicha tabla

A partir de las respuestas obtenidas se puede observar en la tabla 6 términos repetitivos como

“no haría nada”, “no respondería”, “le cuento a mis padres”, de esta manera fue que se realizó la respectiva codificación para cada una de las preguntas de respuesta abierta. (En el anexo 1 las respuestas están ya codificadas)

Después de que las respuestas abiertas son codificadas se procedió a clasificar las preguntas según el peligro al que pertenezca cada pregunta, dicha clasificación se encuentra en la tabla 7.

Tabla 7

Clasificación de las preguntas según el peligro al que aportan información.

Peligro (temática)	Preguntas que aportan a este peligro.
Sexting	4,46,47
Grooming	1,16,25,26,28
Phishing	18,19,48
Ciberbullying	2,3,34
Códigos maliciosos (virus, troyanos, gusanos, keyloggers, spywares)	5,6,7,8,9,11,12,13,14,30,32,40,41
Adicción a internet ¹⁶	35,36,37,38,39
Acceso a material inadecuado	20,21
Preguntas informativas que no aportan a ningún peligro ¹⁷ .	22,23,24,25,26,27,29,33

Posterior a tener clara la clasificación de las preguntas por temática el procedimiento que se realiza es empezar a analizar cada una de las respuestas de las preguntas planteadas para cada

¹⁶ Estas preguntas fueron tomadas textualmente de un test planteado por un psicólogo respecto a este tema de la adicción a internet.

¹⁷ Estas preguntas a pesar de que no aportan a los peligros de internet, se plantean con el fin de saber cuáles son las actividades que generalmente hace esta población en internet y a partir de esto se obtiene información sobre cuales son algunos de los comportamientos (acciones que tienen estos estudiantes en internet.)

temática, donde lo que se busca es mirar a partir de esas respuestas de cada temática a que peligro nos estarían expuestos los estudiantes.

Ahora si se observa en la tabla 7 se dice que las preguntas 4, 46 y 47 corresponden a la temática del Sexting, ahora si se miran los resultados para estas preguntas (anexo 1) se observa que a partir de las respuestas dadas por los estudiantes existe la posibilidad que estos llegarían a practicar el Sexting en algún momento lo que indica que esta temática debe ser trabajada en el material educativo.

En la misma tabla 7 se observa que las preguntas 18,19 y 48 pertenecen a la temática del phishing, si se va a las respuestas de esta temática se puede observar que ninguno de los estudiantes da a entender que ellos o un familiar directo (padre o madre), hacen uso de tarjetas para compras o transacciones bancarias usando internet, lo que nos indica que estos estudiantes nos podrían ser víctimas de este peligro bancario (phishing), es a partir de esto que se decide no tratar esta temática en el material.

Según esta misma tabla las preguntas 1, 16,25 y 26 apuntan al peligro del grooming, haciendo el mismo proceso de observar las respuestas de estas preguntas se obtiene que existen alumnos a los cuales en algún momento le han hecho algún tipo de propuesta indecente, existen alumnos que dan a entender con sus respuestas que aceptarían este tipo de propuestas entre otros y así de esta manera se toma la decisión de incluir esta temática en el material educativo que se va a desarrollar.

Así de esta manera fue que se realizó el análisis de cada pregunta y se tomó la decisión de incluir o de descartar las temáticas de ser trabajadas en el material a partir del proceso anterior

fue que se llegó a que los peligros que debían ser trabajados según el análisis de la encuesta son: el sexting, el grooming, y los diversos códigos maliciosos.

A continuación se muestran de manera general la cantidad de personas que según la encuesta podrían ser víctimas de cierto peligro.

Tabla 8

Cantidad de estudiantes que podrían ser víctimas de cada peligro.

Peligro (temática)	Cantidad de estudiantes que según sus respuestas serían víctimas de este peligro
Sexting	12 estudiantes
Grooming	12 estudiantes
Phishing	0 estudiantes
Ciberbullying	0 estudiantes
Códigos maliciosos (virus)	15 estudiantes
Códigos maliciosos (troyanos)	10 estudiantes
Códigos maliciosos (gusanos)	12 estudiantes
Códigos maliciosos (keyloggers)	5 estudiantes
Códigos maliciosos (spywares)	14 estudiantes
Adicción a internet ¹⁸	0 estudiantes
Acceso a material inadecuado	0 estudiantes

Elaboración propia.

Recordando que las categorías de análisis planteadas en este documento fueron “los peligros de internet”, y “las acciones de los estudiantes en el uso de internet” y que a partir de la encuesta se descartó el trabajar ciertos peligros lleva a dejar claro que las categorías de análisis definitivas de este proyecto fueron.

¹⁸ Estas preguntas fueron tomadas textualmente de un test planteado por un psicólogo respecto a este tema de la adicción a internet.

Categoría 1 peligros de internet

Subcategorías

- El sexting
- El grooming
- Códigos maliciosos

Categoría 2 acciones de los estudiantes en internet que los pueden exponer a los peligros nombrados en la categoría 1.

- Intercambiar fotos intimas con la pareja
- Intercambiar fotos intimas con un desconocido
- Descargar softwares de manera gratuita
- Entablar conversaciones con extraños
- No leer los términos y condiciones al instalar un software que fue descargado gratis de internet
- Tener como publicas fotos en las redes sociales cuyo contenido no deberían ver todas las personas.
- Tener demasiada información como publica en la redes sociales
- No Fijarse en los permisos que se le dan a las aplicaciones conectadas a Facebook
- No fijarse en el tipo de instalación que se selecciona cuando se va a instalar un software
- No manejar configuraciones de privacidad para las fotos que se postean en internet

En la categoría 2 se observa que se enuncia unas acciones, estas acciones son las que se tuvieron en cuenta y se trabajaron ya que son las que apuntan a los peligros de la categoría 1 (Sexting, grooming, códigos maliciosos)

Quizás usted se pregunte por que no se trataron en el material las temáticas de phishing, Cyberbullying, adicción a internet y acceso a contenido inadecuado, esto se debe a que en durante la revisión de las respuestas que apuntan a estas temáticas mencionadas se observó que ninguno de los estudiantes participes dio a entender con sus respuestas que podrían llegar a ser víctimas de estos peligros (**ver tabla 8**).

5.2 Análisis de datos pre-test post-test

Previo a iniciar este análisis es pertinente recordar que la población con la que se trabajo fue en total 50 personas donde se encuentran los 3 grupos con los cuales se realizó la intervención, pero para poder evidenciar si el trabajar el material con estos estudiantes genero unos cambios en ellos, lo que se realiza es una comparación entre los resultados obtenidos en el pre-test (ejercicios previos trabajados en el material educativo computacional que servirán como punto de comparación) y el respectivo post-test, luego para reafirmar que el material genero una incidencia se hace una comparación entre la información obtenida del post-test de la población experimental con los datos del post-test de un grupo control con el cual no se aplicó el material educativo computacional

Recordando que en este trabajo de grado se manejan 4 temáticas la información se mostrara dividida en dichos temas. (Privacidad en internet, grooming, Sexting, códigos maliciosos.)

5.2.1 Análisis de datos tema “privacidad en internet”.

5.2.1.1 Configuración de datos perfil simulado

En este ejercicio los estudiantes debían configurar un perfil con sus datos, pero lo que se quería observar en este punto no son los datos proporcionados por los estudiantes si no el tipo de configuración de privacidad que ellos escogieran para cada ítem. El resultado esperado con este ejercicio es que los alumnos en ninguno de los ítems seleccionaran la configuración como público ya que durante las sesiones de trabajo con estos se les había indicado que es peligroso el dejar que cualquier persona de una red social tenga acceso a cierta información. Los resultados obtenidos aquí son:



Imagen9 Ejercicio 1 propuesto en el post-test.

Tabla 9***Tipo de configuración de privacidad según el perfil simulado***

Estudiantes con los que se trabajó el material			
3 grupos (50 estudiantes en total)			
Ítem a configurar por los estudiantes.	Tipo de privacidad	Cantidad de estudiantes	Porcentaje de estudiantes
“Estudia en”	Público	9 estudiantes	18 %
	Solo yo	23 estudiantes	46 %
	Mis amigos	18 estudiantes	36 %
“Estudió en”	Público	9 estudiantes	18 %
	Solo yo	15 estudiantes	30%
	Mis amigos	26 estudiantes	52 %
“Trabaja en”	Público	14 estudiantes	28%
	Solo yo	23 estudiantes	46 %
	Mis amigos	13 estudiantes	26 %
“Vive en”	Público	9 estudiantes	18 %
	Solo yo	16 estudiantes	32 %
	Mis amigos	25 estudiantes	50 %
“Tiene una relación con”	Público	11 estudiantes	22 %
	Solo yo	28 estudiantes	56 %
	Mis amigos	11 estudiantes	22 %
“Número de teléfono”	Público	9 estudiantes	18%
	Solo yo	15 estudiantes	30%
	Mis amigos	26 estudiantes	52%
“Fecha de nacimiento”	Público	10 estudiantes	20%
	Solo yo	15 estudiantes	30%
	Mis amigos	25 estudiantes	50%

Elaboración propia.

Analizando la tabla anterior se puede observar que los estudiantes en este ejercicio simulado en promedio 20% de la población configuro los ítems como públicos, lo que indica que frente a

este ejercicio 10 de 50 estudiantes no les interesa o no comprendieron que en las redes sociales es peligroso dejar que cualquier persona pueda ver la información personal que se postea allí.

Ahora observemos la siguiente tabla en donde se hace la comparación entre los datos del grupo experimental y el grupo control.

Tabla 10

Comparación de resultados de post-test grupo experimental con grupo control ejercicio 1 del post-test

Ítem a configurar por los estudiantes.	Tipo de privacidad	Estudiantes con los que se trabajó el material 3 grupos (50 estudiantes en total)		Estudiantes a los que solo se les aplico el post-test 1 grupo (25 estudiantes en total)	
		Cantidad de estudiantes	Porcentaje de estudiantes	Cantidad de estudiantes	Porcentaje de estudiantes
“Estudia en”	Público	9 estudiantes	18 %	18 estudiantes	72 %
	Solo yo	23 estudiantes	46 %	2 estudiantes	8 %
	Mis amigos	18 estudiantes	36 %	5 estudiantes	20 %
“Estudió en”	Público	9 estudiantes	18 %	18 estudiantes	72 %
	Solo yo	15 estudiantes	30%	2 estudiantes	8 %
	Mis amigos	26 estudiantes	52 %	5 estudiantes	20 %
“Trabaja en”	Público	14 estudiantes	28%	16 estudiantes	64 %
	Solo yo	23 estudiantes	46 %	3 estudiantes	12 %
	Mis amigos	13 estudiantes	26 %	6 estudiantes	24 %
“Vive en”	Público	9 estudiantes	18 %	20 estudiantes	80%
	Solo yo	16 estudiantes	32 %	2 estudiantes	8%
	Mis amigos	25 estudiantes	50 %	3 estudiantes	12%
“Tiene una relación con”	Público	11 estudiantes	22 %	18 estudiantes	72%
	Solo yo	28 estudiantes	56 %	4 estudiantes	16%
	Mis amigos	11 estudiantes	22 %	3 estudiantes	12%
“Número de teléfono”	Público	9 estudiantes	18%	15 estudiantes	60%
	Solo yo	15 estudiantes	30%	8 estudiantes	32%

	Mis amigos	26 estudiantes	52%	2 estudiantes	8%
“Fecha de nacimiento”	Público	10 estudiantes	20%	10 estudiantes	40%
	Solo yo	15	30%	7 estudiantes	28%
	Mis amigos	25	50%	8 estudiantes	32%

Elaboración propia.

A partir de la tabla anterior se puede ver que los estudiantes del grupo control configuraron más ítems como públicos a diferencia del grupo experimental, de esta tabla también se puede evidenciar que en el grupo control, el ítem que menos estudiantes escogieron como público fue la fecha de nacimiento, lo que indica que en este grupo control hubiera sido interesante aplicar el MEC ya que estos muestran que los resultados muestran que dicho grupo expone demasiada información. Es decir el grupo control muestra que entre sus acciones no se encuentra mucho la acción de configurar un perfil para que este sea seguro y no cualquier persona tenga acceso a la información de dicha cuenta.

5.2.1.2 la información que cada alumno tiene en su perfil de Facebook. Como ejercicio de pre-test en el material educativo computacional se les planteo a los estudiantes que entraran a su perfil de la red social Facebook y que le tomaran un pantallazo a la información de su perfil, luego durante la interacción con el material educativo se les pedía que entraran de nuevo a su red social pero en esta ocasión se les daban unas instrucciones para que los estudiantes pudieran observar a que información proporcionada por ellos en dicha red social podría tener acceso cualquier persona, por ultimo para finalizar este ejercicio en el post-test se le pedía al estudiante de nuevo un pantallazo de su perfil. Respecto a lo anterior lo que hizo fue una comparación entre los pantallazos proporcionados por cada uno de los estudiantes. Antes de ver los resultados obtenidos para este ejercicio observe el siguiente ejemplo.

En esta imagen se observa la información que tiene este estudiante en el perfil de su red social, este fue el pantallazo que se le pidió al sujeto en el pre-test

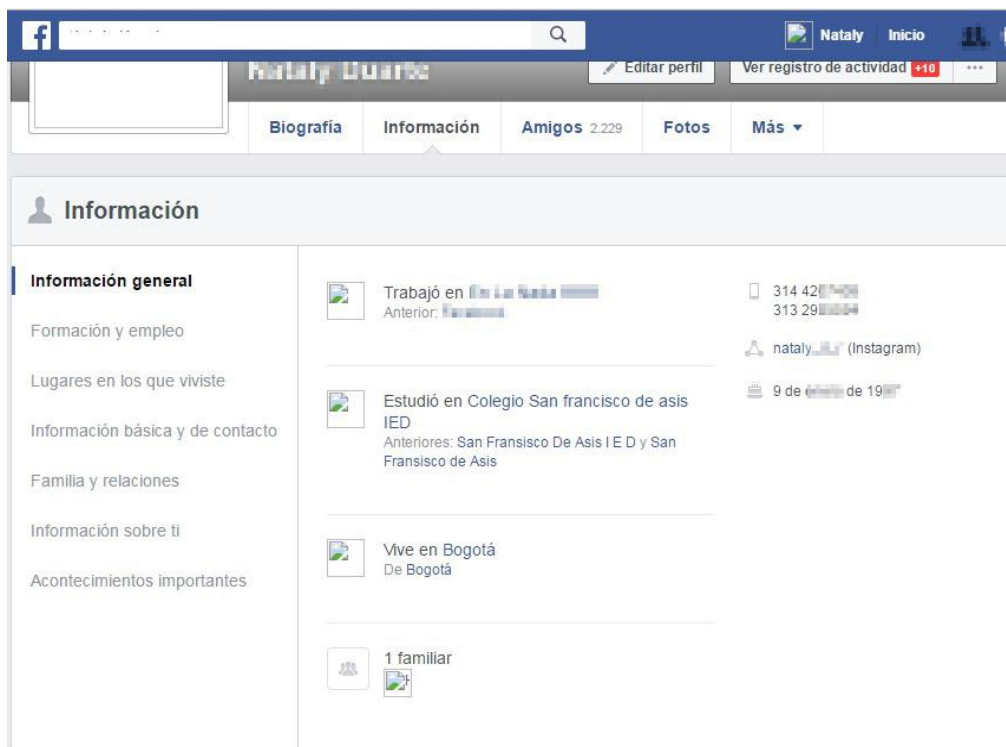


Imagen 10. Pantallazo del perfil pedido en el pre-test a uno de los estudiantes.

Luego lo que se hace es comparar el primer pantallazo dado por el estudiante, con el pantallazo obtenido en el post-test.



Imagen 11. Pantallazo del perfil pedido en el post-test a uno de los estudiantes

A partir de observar los dos pantallazos proporcionados por este sujeto del ejemplo, se puede visualizar que la única información que este estudiante tiene como no público son sus números de teléfono, esta comparación se hizo con cada uno de los estudiantes participantes y los resultados obtenidos fueron.

Tabla 11

Resultados pre-test post-test información que tienen los estudiantes en su perfil de red social

Ítem	Pre-test	Porcentaje de estudiantes	Post test	Porcentaje de estudiantes
Estudiantes que no tienen ningún ítem de información como público	35 estudiantes	70 %	40 estudiantes	80 %
Estudiantes que tienen algún ítem como público	15 estudiantes	30 %	10 estudiantes	20 %

Elaboración propia.

A partir de la tabla anterior se observa que la gran mayoría de estudiantes tenían configurados sus perfiles para que no cualquier persona pueda ver su información, de esta población se aprecia que en el pre-test 15 estudiantes tenían algún ítem de información en su perfil como público, pero si se observa bien de esos 15 estudiantes en el post-test son solo 10 los que siguieron mostrando algún tipo de información en sus red social Facebook, esto quiere decir que existe la posibilidad que el material hay contribuido a que 5 personas hubieran hecho cambios en la privacidad de su perfil.

Ahora veamos la tabla que es donde se proporcionan los datos de comparación obtenidos en el post-test para este ejercicio.

Tabla 12

Comparación de datos post-test grupo experimental y post-test grupo control, información que tienen los estudiantes en el perfil de la red social

	Estudiantes con los que se trabajó el material y se les aplico post-test 3 grupos (50 estudiantes en total)		Estudiantes a los que solo se les aplico el post-test 1 grupo (25 estudiantes en total)	
	Cantidad de estudiantes	Porcentaje de estudiantes	Cantidad de estudiantes	Porcentaje de estudiantes
Estudiantes que no tienen ningún ítem de información como publico	40 estudiantes	80 %	10	40%
Estudiantes que tienen algún ítem como publico	10 estudiantes	20 %	15	60%

Elaboración propia.

En esta tabla se puede percibir en cuestión de porcentajes que solo el 20% de la población experimental total tiene en su perfil de red la red social Facebook alguna ítem de información a

la vista de cualquier persona, mientras que en el grupo control se percibe que el 60 % de la población total perteneciente a este grupo tienen uno o varios datos de su información a la vista de cualquiera, por lo tanto el hecho de que el grupo experimental tenga un menor porcentaje de estudiantes que dejan información en su red social como público da a entender que la población experimental está más segura que la población del grupo control.

5.2.1.3 Privacidad en las fotos según el contenido de estas. Para este ejercicio los estudiantes debían seleccionar quien podría tener acceso a las fotos presentadas, previo a esto se les daba a entender a los estudiantes que las fotos son representativas de un hecho. Es decir la imagen 1 hace referencia a una foto con amigos, la imagen 2 a una foto donde salgan niños pequeños, la imagen 3 a fotos en ropa interior, la imagen 4 a fotos con amigos en situaciones que no se quieren dar a conocer a cualquier persona y la imagen 5 a fotos en algún gimnasio o haciendo deporte.

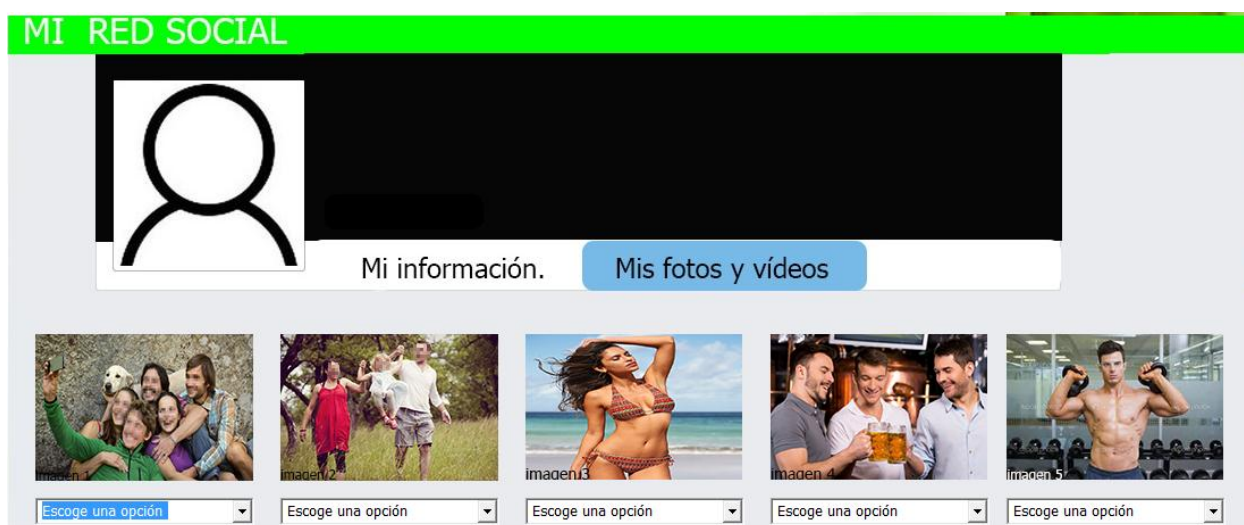


Imagen 12. Ejercicio numero 2 planteado en el post-test

Previo a la explicación anterior los resultados obtenidos aquí fueron.

Tabla 13

Configuración de privacidad de fotos según el contenido de estas, comparación entre grupo experimental y grupo control

Ítem a configurar por los estudiantes.	Tipo de privacidad	Estudiantes con los que se trabajó el material y se les aplico post-test 3 grupos (50 estudiantes en total)		Estudiantes a los que solo se les aplico el post-test 1 grupo (25 estudiantes en total)	
		Cantidad de estudiantes	Porcentaje de estudiantes	Cantidad de estudiantes	Porcentaje de estudiantes
Imagen 1	Público	22 estudiantes	44%	16 estudiantes	64%
	Solo yo	6 estudiantes	12%	1 estudiantes	4%
	Mis amigos	22 estudiantes	44%	8 estudiantes	32%
Imagen 2	Público	7 estudiantes	14%	14 estudiantes	56%
	Solo yo	17 estudiantes	34%	2 estudiantes	8%
	Mis amigos	26 estudiantes	52%	9 estudiantes	36%
Imagen 3	Público	3 estudiantes	6%	8 estudiantes	32%
	Solo yo	28 estudiantes	56%	10 estudiantes	40%
	Mis amigos	19 estudiantes	38%	7 estudiantes	28%
Imagen 4	Público	15 estudiantes	30%	5 estudiantes	20%
	Solo yo	6 estudiantes	12%	5 estudiantes	20%
	Mis amigos	29 amigos	57%	15 estudiantes	60%
Imagen 5	Público	7 estudiantes	14%	6 estudiantes	24%
	Solo yo	30 estudiantes	60%	13 estudiantes	52%
	Mis amigos	13 estudiantes	26%	6 estudiantes	24%

Elaboración propia.

Observando los resultados de la tabla 13 se puede apreciar que en promedio el 10% de los alumnos del grupo experimental no tuvieron en cuenta que las fotos en donde aparezcan niños pequeños y fotos en ropa interior no se deberían colocar como publicas ya que esto puede llegar

a ser bastante peligroso, esto indica que la parte del material educativo donde se les orienta a los alumnos sobre que fotos no deberían ser públicas en una red social no quedo clara para todos ellos. Por otra parte mirando los resultados del grupo control, se observa que para el caso de la imagen 2 (donde aparecen los niños pequeños) 14 estudiantes dejaron esta como publica (56 %) y la imagen 3(foto en ropa interior) 8 estudiantes seleccionaron esta como publica (32 %), lo que da a entender que como el grupo control no tuvo interacción con el material educativo posiblemente no estén informados acerca de que este tipo de fotografías es mejor no dejarlas a la vista de cualquier persona.

5.2.1.4 conectar aplicaciones a las redes sociales. Otro de los subtemas que se trabajó con los estudiantes fue el de conectar ciertas aplicaciones a las redes sociales. En este caso el ejercicio que se propuso a la población en el pre-test consistía en que estos debían seguir una serie de instrucciones para llegar al punto donde se encuentran ubicadas las aplicaciones que el estudiante en algún momento había ligado su red social (Facebook), allí lo que se pretendía evidenciar con el pre-test (por ejemplo ver imagen 13) era saber si los estudiantes se fijan en los permisos que le conceden a una app cada vez que la conectan con su cuenta de Facebook, para esto se les pidió a los alumnos que tomaran pantallazos a 3 aplicaciones de las diversas que quizás tienen enlazadas a su cuenta posterior a esto se les planteo en el post-test (ver imagen 14) un ejercicio donde los estudiantes tenían la posibilidad de deshabilitar estos permisos que les pedía una aplicación (de ejemplo y simulada) .

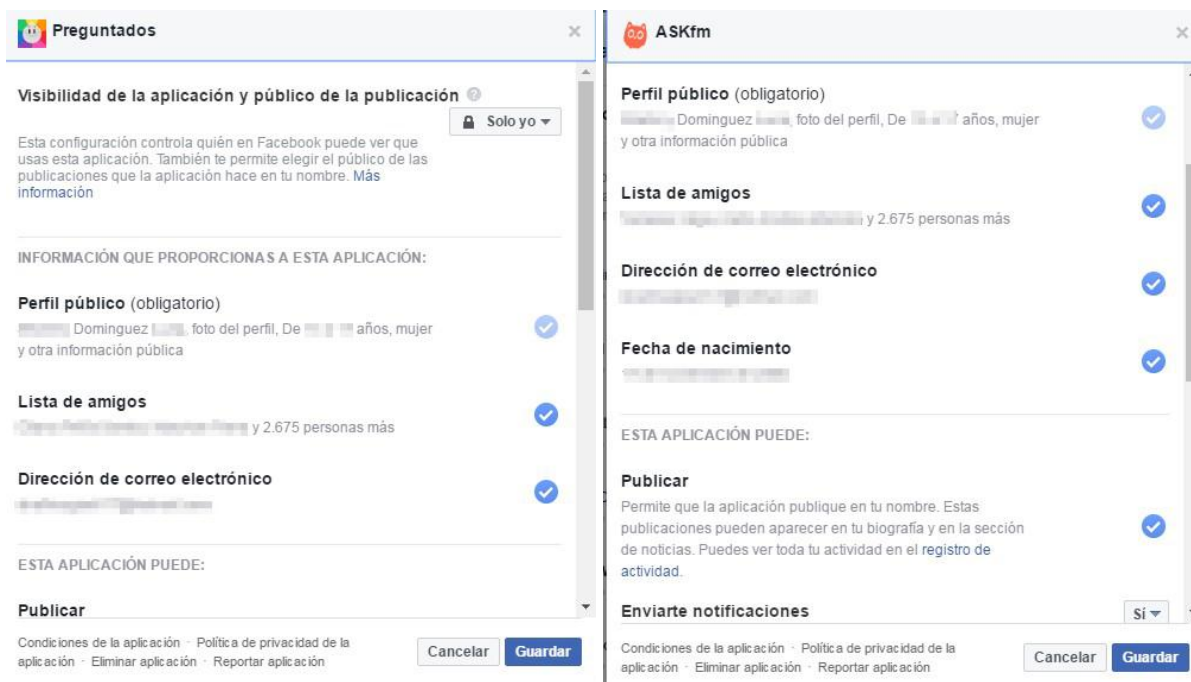


Imagen 13 Pantallazo de los permisos de algunas de las aplicaciones que usa una alumna y que están conectadas a su cuenta de Facebook

Ahora para el siguiente ejercicio es necesario que accedas a la siguiente aplicación, esta aplicación requiere registro con Facebook, por lo tanto teniendo en cuenta que ya

tiene su cuenta de Facebook abierta, solo es necesario que de clic [aquí](#) para que se pueda registrar en la app usando Facebook, esta app es necesaria para las actividades posteriores en este material.

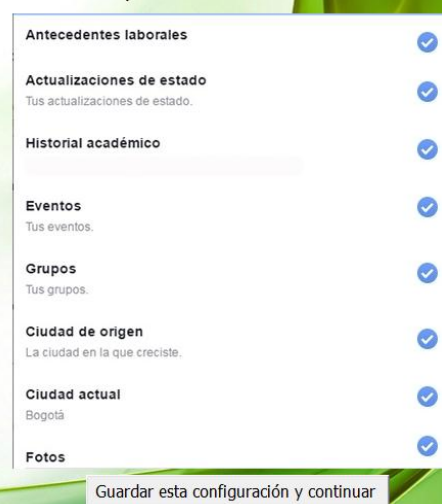


Imagen 14. Pantallazo del ejercicio propuesto en el post-test. Para hacer la respectiva comparación y evidenciar si hay cambios.

Los resultados obtenidos en este ejercicio fueron.

Tabla 14.

Estudiantes que inician sesión en ciertas aplicaciones usando su red social Facebook

	Grupo experimental (50 personas), interactúan con el material educativo y realizan post-test				Grupo control (25 estudiantes), solo se les aplica post-test	
	Pre-test	Porcentaje de estudiantes	Post-test	Porcentaje de estudiantes	Post-test	Porcentaje de estudiantes
Estudiantes que en sus pantallazos evidencian que le dieron permisos a las aplicaciones	50 alumnos	100 %	24 alumnos	48 %	21 Alumnos	84%
Estudiantes que evidencian con sus pantallazos que no conceden permisos a las aplicaciones que usan	0 alumnos	0 %	26 alumnos	52 %	4 Alumnos	16%

Elaboración propia.

Revisando los datos de la tabla 14 se ve que en la aplicación del pre-test a la población experimental ellos dieron a conocer con sus respectivos pantallazos que en las aplicaciones que tienen ligadas a su cuenta de Facebook, permiten que estas apps tengan acceso a cierta información y ciertos permisos sobre dicha cuenta de Facebook, pero si se observa nuevamente la tabla 14 es evidente que con este ejercicio se logró que el 52% del grupo experimental comprendiera que cuando se conecta cualquier app externa a una red social es necesario fijarse en qué tipo de información solicita una app sobre una persona y cual de esa información puede el

usuario no proporcionarle. Respecto a este dato se observa que con este ejercicio solo se logró la incidencia sobre un poco más de la mitad de la población experimental.

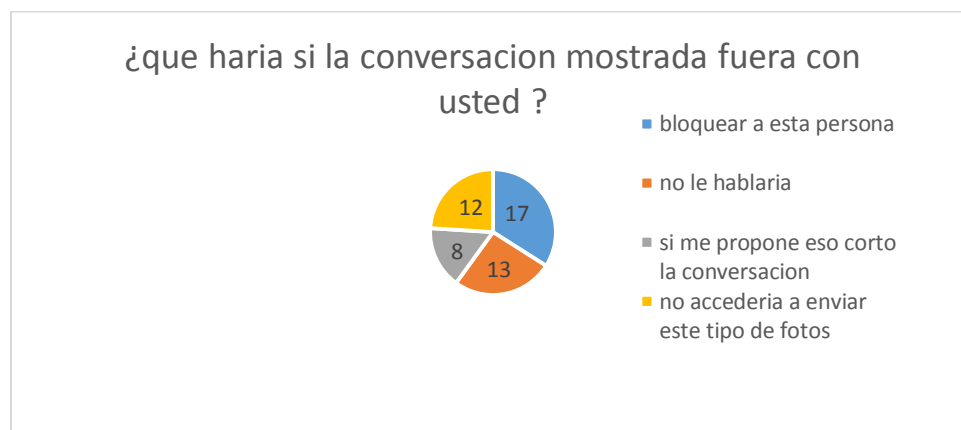
Por otro lado del grupo control se obtiene que el 84% de estos en el ejercicio que se les propuso **no** quitaron los permisos, esto puede indicar dos cosas la primera es que a este 84 % del grupo control no le interesa que una aplicación tenga acceso a cierta información sobre ellos, o la segunda opción es que existe la posibilidad que estas personas no entendieron el ejercicio planteado esto se dice teniendo en cuenta que durante la aplicación del post-test con este grupo control varios preguntaban sobre en qué consistía este ejercicio lo que a su vez indica que estos estudiantes nunca se han fijado en los permisos que conceden a una app.

5.2.2 Análisis de datos tema “grooming”. Frente a esta temática lo que se plantea en el pre-test es una conversación entre dos sujetos que son desconocidos en donde la finalidad de la conversación es que un sujeto le pide al otro fotos insinuantes a partir de esta conversación se les pregunta a los estudiantes que harían si la conversación fuera con ellos, sabiendo esto lo que se hará en este apartado será analizar la respuesta a esta pregunta con el resultado que arroja el ejercicio planteado en el post-test el cual fue una conversación simulada donde se le propone al estudiante que acceda a enviar fotos íntimas¹⁹, Los datos obtenidos para esta temática fueron.

5.2.2.1 pre-test (grooming) aquí se les muestra una conversación a los alumnos (ver imagen 15), luego se les plantea la siguiente pregunta, si fuera usted la persona que está teniendo esta conversación ¿qué haría usted?, teniendo en cuenta que esta pregunta es de respuesta abierta lo

¹⁹ Es pertinente que usted como lector conozca que los ejercicios propuestos en el post-test son simulados por lo tanto nunca hay un intercambio de fotos con este ejercicio solo se pretende saber si el alumno accedería o no a esta situación.

que se realiza es una codificación de las respuestas, para finalmente obtener que las respuestas fueron (ver grafica 1).



Grafica 1



Imagen 15. Parte de la conversación que se les mostro a los estudiantes en el pre-test

Según la gráfica 1 lo que se puede evidenciar en esta es que ninguno de los estudiantes del grupo experimental accedería a tener este tipo de conversaciones con un extraño y mucho menos a enviarle fotos a este.

5.2.2.3 post-test (grooming). El ejercicio planteado para esta temática en el post-test consiste en una simulación de una conversación, donde el estudiante a lo largo de la conversación tenía solo tres opciones entre ellas esta cortar la conversación después de iniciar, llegar al final de la conversación y aceptar o no aceptar lo que se le proponía.

Tabla 15

Datos ejercicio post-test grooming grupo experimental y control

	Estudiantes con los que se trabajó el material y se les aplico post-test 3 grupos (50 estudiantes en total)		Estudiantes a los que solo se les aplico el post-test 1 grupo (25 estudiantes en total)	
	Cantidad de estudiantes	Porcentaje de estudiantes	Cantidad de estudiantes	Porcentaje de estudiantes
Estudiantes que prefirieron terminar la conversación antes de que la simulación les hiciera la propuesta	40 estudiantes	80 %	22 estudiantes	88%
Estudiantes que llegaron al final de la conversación y no aceptaron la propuesta de enviar fotos intimas	10 estudiantes	20 %	2 estudiantes	8%
Estudiantes que llegaron al final de la conversación y aceptaron la propuesta de enviar fotos intimas	0 estudiantes	0%	1 estudiante	4%

Elaboración propia.

A partir de la tabla anterior se observa que frente a esta temática no es mucha la incidencia que tenga el material, ya que aparentemente según los datos los estudiantes del grupo experimental en ningún momento llegarían a ser víctimas del grooming y comparando estos datos con el grupo control se ve que solo una persona de este grupo según el ejercicio del post-

test podría llegar a ser víctima del grooming, teniendo en cuenta que tanto los datos del pre-test como del post-test para el grupo experimental es posible decir que en esta temática no se observara ningún cambio.

5.2.3 análisis de datos tema “sexting”. Frente a esta temática en el pre-test se le plantea la siguiente pregunta a la población (si usted tiene un novio(a) lo más lógico es que usted tenga demasiada confianza con esta persona, a partir de esto ¿al cuánto tiempo de relación consideraría enviarle fotos o videos con contenido erótico donde aparezca usted?), si se observa bien la pregunta esta tiene un sentido y es saber si los alumnos llegarían a aceptar en algún momento practicar sexting con su respectiva pareja sentimental, por otra parte en el post-test se plantea un ejercicio de una conversación simulada, pero en esta ocasión se le pide al estudiante que piense que esta conversación la está teniendo con su novio(a). Los resultados de este análisis se encuentran en la siguiente tabla.

Tabla 16

Pre-test post-test tema sexting

Pre-test				Post-test		
	¿Al cuánto tiempo de relación consideraría enviarle fotos o videos con contenido erótico donde aparezca usted?	Cantidad de estudiantes	Porcentaje de estudiantes	Según el ejercicio aceptarían practicar Sexting con su pareja	Cantidad de estudiantes	Porcentaje de estudiantes
No	nunca	20	40%	No	39	78%
		estudiantes			estudiantes	
Si	Entre 0 y 6 meses de relación	12	24 %	Si	11	22%
	Entre 7 meses y 1 año de relación	9 estudiantes	18%		estudiantes	
	Después de más de un año de relación	9 estudiantes	18%			

Elaboración propia.

A partir de la tabla 16 se puede percibir que en el pre-test un 60% de la población (grupo experimental) da a entender que en algún momento de la relación practicarían el sexting con sus respectivas parejas, por lo tanto lo que se pretendía con el material educativo respecto a este tema era dar a conocer a los estudiantes él porque es peligroso llegar a realizar en algún momento sexting con sus novios (as), posterior a esto se esperaba que cuando se les aplicara el post-test en el ejercicio propuesto sobre el sexting ninguno de los alumnos diera a entender con el resultado que practicarían el sexting.

Por otro lado observando los respectivos datos (pre-test comparado con post-test) se ve que se generó una incidencia en este tema sobre el 38% (19 alumnos).

Ahora se comparan los datos del post-test aplicado al grupo control y al grupo experimental.

Tabla 17

Comparación post-test grupo control y grupo experimental (sexting)

	Estudiantes con los que se trabajó el material y se les aplico post-test 3 grupos (50 estudiantes en total)		Estudiantes a los que solo se les aplico el post-test 1 grupo (25 estudiantes en total)	
	Cantidad de estudiantes	Porcentaje de estudiantes	Cantidad de estudiantes	Porcentaje de estudiantes
Estudiantes que practicarían el Sexting con su pareja	11 estudiantes	22 %	16 estudiantes	64%
Estudiantes que no practicarían Sexting con su pareja	39 estudiantes	78 %	9 estudiantes	36%

Elaboración propia.

Posterior a ver la tabla 17 se observa que el 64% de la población control practicaría el Sexting con su pareja mientras que en el grupo experimental solo el 22% lo haría, esto da a entender que a pesar de que a la población experimental se le trato de orientar sobre el peligro de practicar sexting a través del post-test se evidencio que solo el 78% de la población experimental comprendió esto.

5.2.4 análisis de datos tema “códigos maliciosos”.

5.2.4.1 Tipo de instalación de un software. Un ejercicio más aplicativo referente a este tema es el proceso de como instalan un programa los estudiantes. En este ejercicio se les preguntaba a los estudiantes si cuando instalaban algún programa leían los respectivos términos y condiciones

y por otra parte se les ponía un ejercicio en donde ellos debían seleccionar que opción escogen cuando van a instalar un software si la manera rápida o la personalizada, los datos obtenidos aquí se presentan en la siguiente tabla.

Tabla 18

Análisis de datos códigos maliciosos

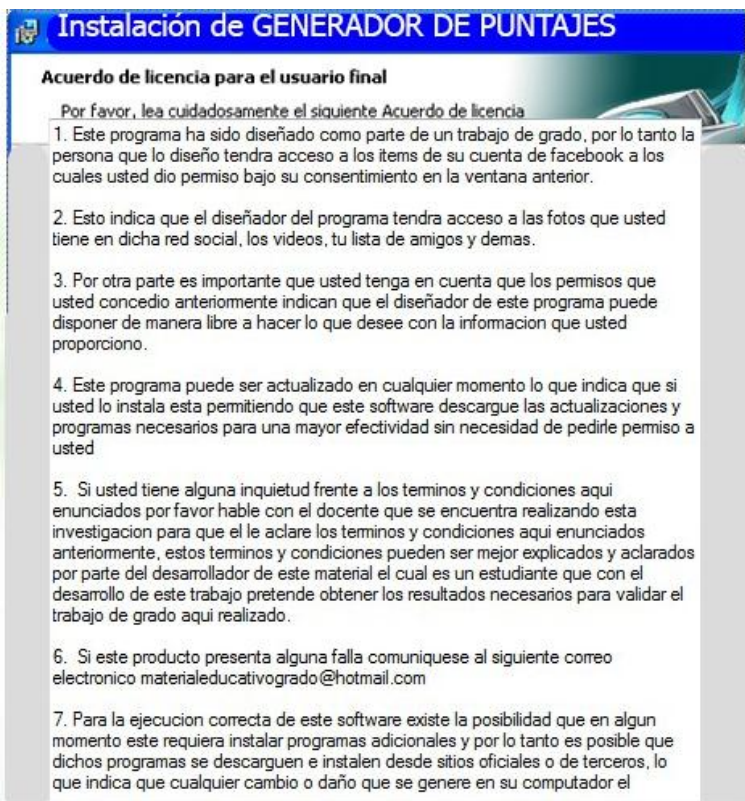
	Grupo experimental							
	Pre-test				Post-test			
	Tipo de instalación		Lee los términos y condiciones cuando va a instalar un software		Tipo de instalación		Lee los términos y condiciones cuando va a instalar un software	
	rápida	personalizada	si	no	rápida	personalizada	si	no
Cantidad de estudiantes	45	5	15	35	15	35	40	10
Porcentaje de estudiantes	90%	10%	30%	70%	30%	70%	80%	20%
	Grupo control							
	Tipo de instalación		Lee los términos y condiciones cuando va a instalar un software		Tipo de instalación		Lee los términos y condiciones cuando va a instalar un software	
	rápida	personalizada	si	no	rápida	personalizada	si	no
Cantidad de estudiantes	20	5	15	10				
Porcentaje de estudiantes	80%	20%	60%	40%				

De acuerdo a la tabla anterior es posible observar que en el ejercicio planteado sobre esta temática respecto a la forma en que los estudiantes instalan un programa se observa un cambio en esta acción sobre un 60% de la población (grupo experimental) lo que da a entender que los estudiantes comprendieron que una próxima ocasión que vayan a instalar algún software en sus computadores se deben fijar en detalles como el leer los términos y condiciones que trae dicho programa y la forma en la que se desea instalar el mismo.

Por otra parte se puede percibir que del grupo control el 80% de los estudiantes seleccionan que cuando instalan un software seleccionan la manera rápida lo que indica que estos no saben que esta es la manera menos recomendada cuando se va a instalar un programa y más si este fue descargado de internet de manera gratuita.

Para terminar es significativo anunciar que en el post-test para el ejercicio de los términos y condiciones los estudiantes podían escoger entre dos opciones leer los términos y condiciones o saltarse este paso y proceder a la respectiva simulación de instalación. En dicho ejercicio a los estudiantes se les mostraban los términos y condiciones²⁰ que aparecen en la siguiente imagen.

²⁰ Los términos y condiciones que se enuncian en la imagen mostrada hacen parte de la simulación del post-test lo que significa que estos no son ciertos.

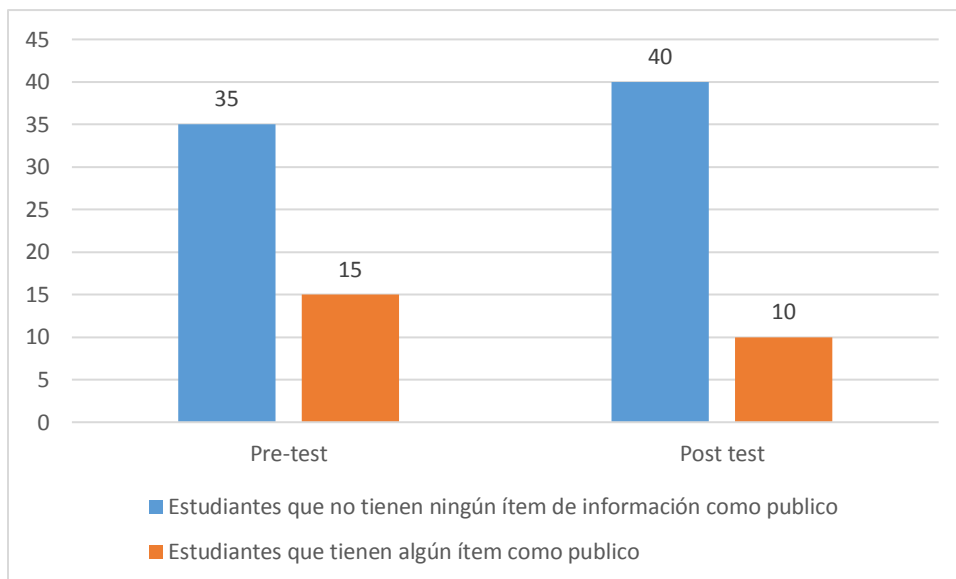


Dichos términos y condiciones se pusieron con el fin de saber si los estudiantes leían o no estos, esto fue posible evidenciarlo ya que había estudiantes que durante la aplicación del post-test se tomaron la molestia de preguntarle al investigador si era cierto o no lo que se indica allí.

5.3 Análisis de la categoría 2: acciones en internet.

Categoría 2: a partir del análisis previo de los resultados se puede entender de manera más precisa que las acciones particulares que se trabajaron en este proyecto fueron. Además si se tiene en cuenta que uno de los objetivos en generar cambios en las acciones de los estudiantes observe el siguiente análisis

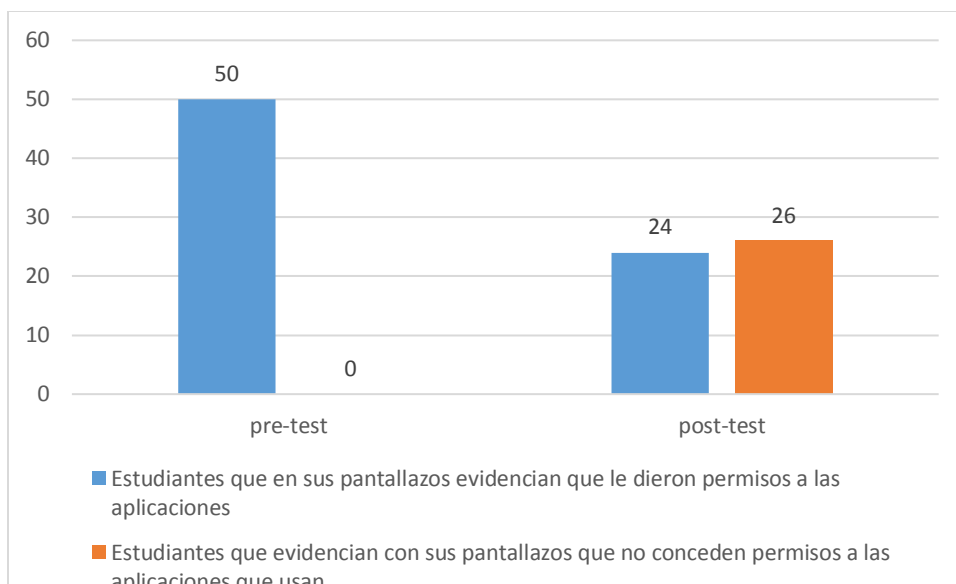
- **La configuración adecuada de un perfil de una red social evitando que dejar información a cualquier persona.** Para analizar esta acción se observa los perfiles de cada uno de los estudiantes buscando si estos tienen en su información algún ítem que pueda ver cualquier persona



Grafica 3

A partir de lo anterior si se observa la gráfica 3 se puede evidenciar que el material incidió en la configuración de la información de los perfiles de 5 estudiantes.

- **No Fijarse en los permisos que se le dan a las aplicaciones conectadas a Facebook.**
Los jóvenes se preocupan poco por leer los permisos que en muchas ocasiones les pide alguna aplicación en internet. A partir de esto es que se toma esta como otra de las acciones sobre las que se quiere incidir con este proyecto. sabiendo que anteriormente se enunció y se confirmó que son muchos los jóvenes que inician sesión en alguna aplicación usando Facebook.

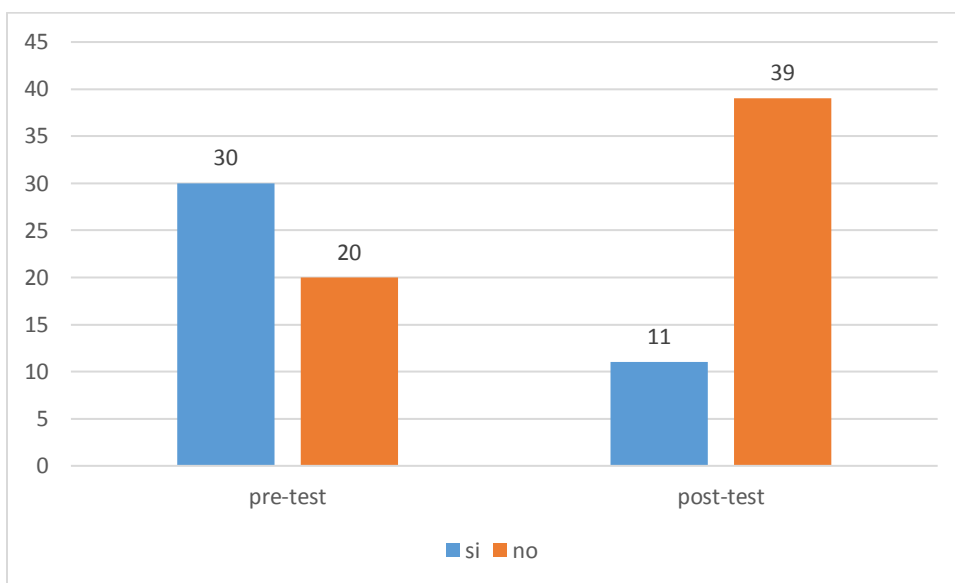


Grafica 4

Basado en la gráfica 4 se puede observar que la incidencia con respecto a esta acción hubo una incidencia sobre 26 estudiantes, si se tiene en cuenta que en el pre-test todos los estudiantes solo abrían sesión en alguna aplicación y no se fijaban en que al hacer esto esa app podía tener acceso a cierta información del usuario, ahora el post-test indica que los alumnos se fijan y se toman el trabajo de seleccionar si desean o no que esa app tenga acceso a cierta información sobre el usuario, continuando con el análisis de la gráfica 4 es preocupante saber que aún se hay estudiantes que cada vez que descargan o acceden a una app nueva y en dicha aplicación inician sesión con alguna red social, no se fijan en la información que esta app puede obtener sobre ellos. (El análisis de esta acción se hace tomando como base el ejercicio correspondiente a los permisos que se le conceden a las apps ligadas a la cuenta de Facebook de cada estudiante)

- **intercambiar fotos insinuantes con la pareja sentimental.** Actualmente son muchos los jóvenes que tienen acceso a un dispositivo con conexión a internet. Con estos dispositivos es muy fácil que los jóvenes generalmente parejas como parte de ese

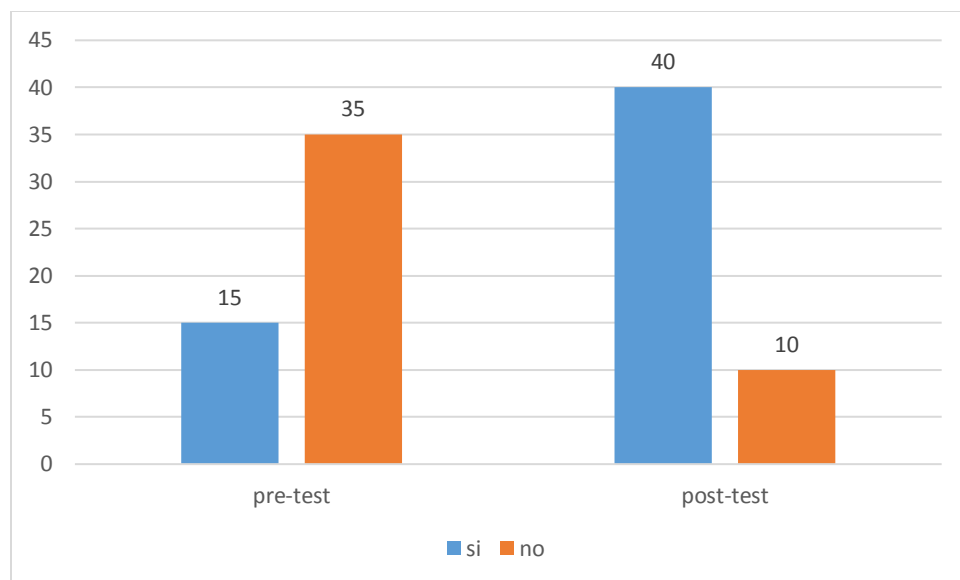
noviazgo hagan intercambio de fotos con cierto contenido erótico o insinuante. Al trabajar el material educativo con estos jóvenes se pretendía enseñarles que practicar el sexting puede ser peligroso. (el análisis de esta acción se hace teniendo en cuenta el ejercicio del sexting)



Grafica 5

En la gráfica 5 se muestra que en el pre-test 30 estudiantes aceptaron que intercambiarían fotos con su pareja, luego si se observa la barra correspondiente al post-test se evidencia que de esos 30 estudiantes se logró disminuir a 11 la cantidad

- **No leer los términos y condiciones siempre que se vaya a instalar un software y más si este fue descargado de internet de forma gratuito.** Generalmente cuando los estudiantes descargan un programa de internet a la hora de instalarlo no leen lo que les va diciendo el programa si no que lo que hacen estos es darle clic sobre el botón siguiente las veces que este aparezca. (este análisis se hace a partir del ejercicio propuesto acerca de los códigos maliciosos)

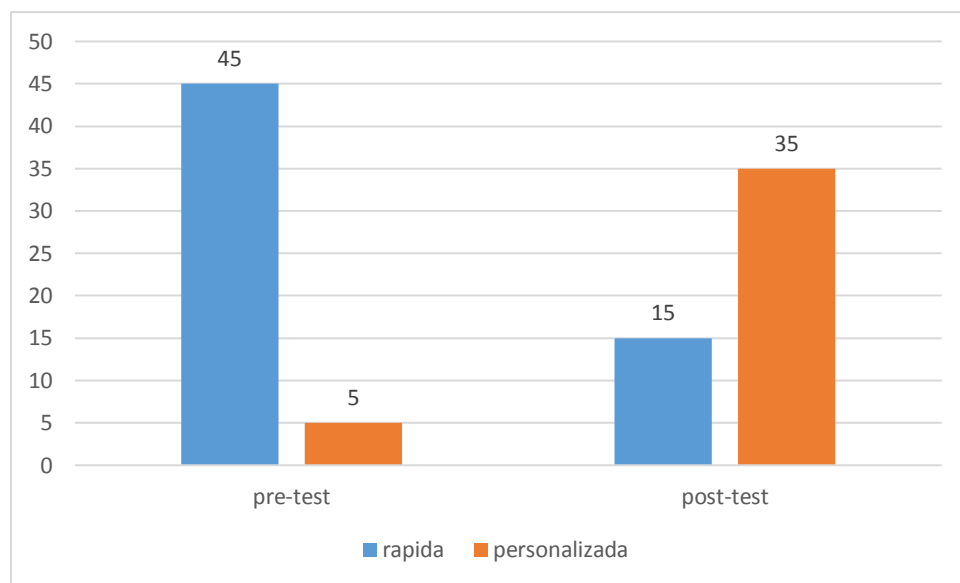


Grafica 6

Frente a esta acción se puede observar en la gráfica 6 que en el pre-test solo 15 estudiantes dijeron que cada vez que instalaban un software leían los términos y condiciones de este, en el post-test se evidencia que hubo un aumento de 25 personas que leen los términos y condiciones, este aumento se puede deber al hecho que a los estudiantes en la interacción con el material educativo se les insistió en que esto es necesario leerlo debido a que en muchas ocasiones allí dice lo que puede hacer este software en el equipo después de ser instalado y en muchas ocasiones en dichos términos y condiciones dice que el software puede instalar o hacer uso de programas de terceros, algo que no es muy confiable ya que generalmente esos programas de terceros son códigos maliciosos.

- **No fijarse en el tipo de instalación que se selecciona cuando se va a instalar un software.** Generalmente todos los softwares cuando van a ser instalados ofrecen dos maneras de instalación una rápida y una personalizada, cuando el usuario escoge la opción rápida este software se encarga de instalar todo lo que venga en el software

incluidos programas de terceros, mientras que cuando se escoge la opción de instalación personalizada es el usuario quien escoge si desea o no que se instalen programas de terceros que vienen incluidos generalmente en los softwares gratuitos.



Grafica 7

Según la gráfica 7 inicialmente solo 5 estudiantes dieron a conocer con el pre-test que esto instalaban un software usando la opción personalizada, luego cuando los estudiantes se les dio a conocer a través del MEC que de estas opciones la más adecuada siempre que se vaya a instalar un software es la opción personalizada debido a que de esta manera pueden escoger lo que desean instalar, se evidencia en los resultados del post-test que hubo una incidencia sobre 30 estudiantes los cuales dieron a conocer en el ejercicio del post-test que la opción que escogieron fue personalizada. En esta acción se logró una fuerte incidencia.

Tomando como base los gráficos anteriores se puede observar que el material cumplió uno de los objetivos del proyecto que era el generar cambios en las acciones de los estudiantes, a pesar de que según los gráficos se observa que estos cambios no fueron sobre la totalidad de la

población si se observan cambios lo cual indica que de cierta manera este proyecto tuvo una respuesta positiva.

Capítulo 6 Conclusiones

- Los datos obtenidos a partir de la realización de la encuesta ayudaron a identificar que la población con la que se desarrolló el proyecto podrían ser víctimas de peligros como el grooming, el Sexting y los códigos maliciosos (virus, gusanos, troyanos, keyloggers, spywares), lo que motivo a desarrollar un material educativo donde se trabajaran estas temáticas. (ver tabla 8, p.85)
- La orientación sobre los estudiantes genera una mayor incidencia cuando se les plantean situaciones con las que la población se sienta identificada, aquí el impacto fue sobre ciertas acciones particulares como la disminución en la cantidad de estudiantes que aceptarían enviar y recibir fotos insinuantes con su pareja, la configuración de cierta información que los estudiantes tenían en su red social (Facebook) a la vista de cualquier persona, la configuración de privacidad de las fotos que se publican en las redes sociales según su contenido, el comprender que ciertas aplicaciones que se conectan a la cuenta de Facebook pueden tener acceso a la información que el usuario tiene en esta red social y el aumento en la cantidad de estudiantes que leen los términos y condiciones a la hora de instalar un programa.
- a partir del análisis se observa que las acciones sobre las que más incidencia genero el material fueron el escoger siempre que se va a instalar un software el tipo de instalación como personalizada(60%) la de leer los términos y condiciones al momento de instalar un software (50%), y la acción de configurar los permisos de acceso que tienen las aplicaciones conectadas a Facebook sobre la información de un usuario (52 %), las acciones sobre las que

se generó poca incidencia fueron la no practica del Sexting (38%), la configuración de cierta información para que no quedara a la vista de cualquier persona (10%), y la acción sobre la que no se generó ninguna incidencia fue la práctica del grooming (0%).

- Basado en los resultados adquiridos durante el análisis se evidencio que la incidencia del material no fue sobre el 100%, lo cual podría llevar a pensar que factores como el solo poder trabajar el material educativo computacional con los estudiantes en dos sesiones de clase no fue suficiente para lograr que la incidencia del material fuera sobre todos los estudiantes.
- Trabajar en el aula de informática la temática de los peligros de internet de manera preventiva con los estudiantes puede ayudar a evitar que alguno de los estudiantes llegue a ser víctima de los peligros de internet o llevar a que este sepa actuar ante estos si llega a ser víctima de los mismos, así como con este trabajo se generó una incidencia no en el 100% de la población trabajada pero si en una parte de ella existe la posibilidad que este material también genere incidencia si se aplica con otros estudiantes.
- A pesar de que en este proyecto se planteó como base el modelo pedagógico conductista los resultados evidencian que este modelo escogido no fue el adecuado ya que en el modelo conductista los resultados obtenidos deberían ser del 100% de las acciones que se desean cambiar.

Bibliografía

Administración del estado, (2016), *Temario. Vol. 2 Actividad administrativa y ofimática*, Sevilla, España: Ediciones Rodio

Anónimo, (1998), *Máxima seguridad en internet*, Madrid, España: Anaya multimedia

Avilés, Á.-P. (2013). *XIRED+SEGURA*. España.

Bustamante, K & ledemas, Y (2014). METODOLOGIA PARA LA ENSEÑANZA DE LA NETIQUETA, EN EL AREA DE INFORMATICA EN EL GRADO 10 EN LA INSTITUCION EDUCATIVA ALFONZO LÓPEZ PUMAREJO DEL MUNICIPIO DE LA VIRGINIA RISARALDA. Colombia: Universidad Tecnológica de Pereira. Recuperado de: <http://repositorio.utp.edu.co/dspace/handle/11059/4581> consultado el (7 de abril de 2016)

Bono Cabré, R. *DISEÑOS CUASI-EXPERIMENTALES Y LONGITUDINALES* (p. 3). Barcelona. Recuperado de: <http://diposit.ub.edu/dspace/bitstream/2445/30783/1/D.%20cuasi%20y%20longitudinales.pdf> consultado el (25 de agosto de 2016)

CNN en español. (2013). *Nativos digitales: ¿Quiénes son y qué significa?*. CNN. Recuperado de: <http://cnnespanol.cnn.com/2013/01/25/nativos-digitales-quienes-son-y-que-significa/>

Colombia tic. (s.f). Colombia tic vive digital. Bogotá Recuperado de: <http://colombiatic.mintic.gov.co/estadisticas/stats.php?&pres=content&jer=1&cod=&id=34#TTC> (consultado el 10 de marzo de 2016)

Cuerda, J.L. Colegios tendrían nueva cátedra de seguridad digital para fomentar el uso responsable de TIC, *RCN RADIO*, [en línea]. 21 de enero de 2016, recuperado de: <http://www.rcnradio.com/tecnologia/colegios-tendrian-nueva-catedra-seguridad-digital-fomentar-uso-responsable-tic/>. (consultado el 18 de mayo de 2016)

Da cunha, T, Luviano, R, Revuelta, B, Sánchez, R, (2007), *Globalización, Derechos Humanos y Sociedad de la Información*, México, Facultad de Derecho y Ciencias Sociales / UMSNH

Educación Bogotá (2015). COLEGIOS PÚBLICOS DE BOGOTÁ: CONECTADOS Y A TODA VELOCIDAD. [en línea]. Recuperado de : <http://www.educacionbogota.edu.co/es/sitios-de-interes/nuestros-sitios/agencia-de-medios/noticias-institucionales/colegios-publicos-de-bogota-conectados-y-a-toda-velocidad>. (consultado el 20 de marzo de 2016)

EFE. (25 de julio de 2012). 'Sexting' no está asociado con problemas psicológicos, según estudio. *EL tiempo*.

Galvis, A. (1992) *ingeniería de software educativo*. Santafé de Bogotá. Colombia. Universidad de los andes

Gil, A.M, (2015), *¿Privacidad del menor en internet? : "me gusta" ¿¿todas las imágenes de "mis amigos" a mi alcance con un simple "click"¿¿¿*, navarra, España: Editorial Aranzadi S.A

Gómez, M & Polania, N. (2008). *ESTILOS DE ENSEÑANZA Y MODELOS PEDAGÓGICOS: Un estudio con profesores del Programa de Ingeniería Financiera de la Universidad Piloto de Colombia*. (tesis de maestría). Universidad de la Salle. Bogotá

Goodman. M, (s.f), *los delitos del futuro*, España: Editorial Ariel

Ibáñez. N, (2010), *CIBERPUTEADORES EN INTERNET*, España, NORBOOKSEDITIONES (consultado el 22 de julio de 2016)

javier fernandez, A. P. (2015). hábitos de uso y conductas de riesgo en internet en la preadolescencia. *comunicar revista científica de comunicaciòn y educaciòn* , 113-120.

Jiménez, A. G. (2011). una perspectiva sobre los riesgos y usos de internet en la adolescencia. *icono 14*, 396-411.

Leguizamón, M (s.f). **DISEÑO Y DESARROLLO DE MATERIALES EDUCATIVOS COMPUTARIZADOS (MEC's): UNA POSIBILIDAD PARA INTEGRAR LA INFORMÁTICA CON LAS DEMÁS ÁREAS DEL CURRÍCULO**. UPTC. [En línea].

Recuperado de: http://www.colombiaaprende.edu.co/html/mediateca/1607/articles-106492_archivo.pdf

Ley 679. Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. Bogotá, Colombia 3 de agosto de 2001. [En línea]. Recuperado de: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=18309>

Ley 1336. Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Bogotá, Colombia. 21 de julio de 2009. [En línea]. Recuperado de: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36877>

Ley 1341. **POR LA CUAL SE DEFINEN PRINCIPIOS Y CONCEPTOS SOBRE LA SOCIEDAD DE LA INFORMACIÓN Y LA ORGANIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - TIC-, SE CREA LA AGENCIA NACIONAL DE ESPECTRO**. Bogotá, Colombia. 30 de julio de 2009.[En línea]. Recuperado de: http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

Ley 1620. "POR LA CUAL SE CREA EL SISTEMA NACIONAL DE CONVIVENCIA ESCOLAR Y FORMACIÓN PARA EL EJERCICIO DE LOS DERECHOS HUMANOS, LA EDUCACIÓN PARA LA SEXUALIDAD Y LA PREVENCIÓN Y MITIGACIÓN DE LA VIOLENCIA ESCOLAR". Bogotá, Colombia. 15 de marzo de 2013[En línea]. Recuperado de: <http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201620%20DEL%2015%20DE%20MARZO%20DE%202013.pdf>

Manterola, Carlos, & Otzen, Tamara. (2015). Estudios Experimentales 2 Parte: Estudios Cuasi-Experimentales. *International Journal of Morphology*, 33(1), 382-387. Recuperado de: <http://www.scielo.cl/pdf/ijmorphol/v33n1/art60.pdf>. (Consultado el 22 de julio de 2016)

MARCELO, J. & MARTÍN. E (2010). Protege a tus hijos de los riesgos de Internet y otras tecnologías. Madrid. Ediciones Anaya.

Marañón, G. À. (2009). *¿QUE SABEMOS DE? Còmo protegernos de los peligros de internet*. madrid: los libros de la catarata.

NAVARRO-MANCILLA, Álvaro Andrés and RUEDA-JAIMES, Germán Eduardo. Adicción a Internet: revisión crítica de la literatura. *rev.colomb.psiquiatr.* [online]. 2007, vol.36, n.4, pp.691-700. ISSN 0034-7450.

Oxman.V, Nicolas.A, Estafas informáticas a través de internet: acerca de la imputación penal del "phising" y el "pharming", *Revista de Derecho (Valparaíso)*, [en línea], 2013 n° 41, consultado el 1 de junio de 2016, recuperado de: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-68512013000200007#back

Prensky, M. (2001). *Nativos e Inmigrantes Digitales*. [En línea]. Recuperado de: [http://www.marcprensky.com/writing/Prensky-NATIVOS%20E%20INMIGRANTES%20DIGITALES%20\(SEK\).pdf](http://www.marcprensky.com/writing/Prensky-NATIVOS%20E%20INMIGRANTES%20DIGITALES%20(SEK).pdf)

Puchades. Pardo, M. P. (2013). Internet y adolescencia: guía on line para educadores. España: Universidad Politécnica de Valencia. Recuperado de: <https://riunet.upv.es/bitstream/handle/10251/32867/Memoria.pdf?...1> (consultado el 31 de marzo de 2016)

Requesens, E. E. (2012). *Adicciòn a las redes sociales y nuevas tecnologías en niños y adolescentes*. piramide.

Sierra, D. M. (2013). Las redes sociales, sus riesgos y la manera de protegerse. Colombia: Universidad CES. Recuperado de: <http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1285/2/Articulo%20de%20grado%20de%20las%20redes%20sociales%20aprobado.pdf> (consultado el 31 de marzo de 2016)

Tünnermann Bernheim, C. (2011). El constructivismo y el aprendizaje de los estudiantes. *Universidades*, Enero-Marzo, 21-32. [En línea]. Recuperado de: <http://www.redalyc.org/pdf/373/37319199005.pdf>

Vanderhoven, E. Schellens, T. Valcke, M. (2014). Enseñar a los adolescentes los riesgos de las redes sociales: una propuesta de intervención en secundaria. *Revista comunicar*, 22, (43), 123-132

voces, p. (2006). *internet sano para todos* . bogota: dupligráficas.

Anexos

Anexo 1

Encuesta aplicada a la población

Respecto a este anexo es importante recordar que fueron 30 estudiantes los que desarrollaron la encuesta, ahora por otra parte es importante recordar que las preguntas de esta encuesta aportan a las 2 categorías de investigación a clasificación de estas es la siguiente.

1 = acciones en internet: las preguntas pertenecientes a esta categoría son los números (2,3,7,11,12,13,17,18,24,29,32,33,34,41,42,44,45)

2= detectar los peligros de internet a los que está expuesta la población. Las preguntas pertenecientes a esta categoría son las número (4, 5, 14,15, 16, 25, 35, 36, 37, 38,39)

3=pregunta que aporta a las 2 categorías anteriores (comportamientos en internet, detectar los peligros en internet) las preguntas pertenecientes a esta categoría son las número (1, 4,9, 10, 19, 26,28)

4= preguntas informativas que aportan a saber qué acciones tienen los estudiantes en el uso de internet , las preguntas pertenecientes a este ítem son (6,8,20,21,22,23,27,30,31,33,40,43,)

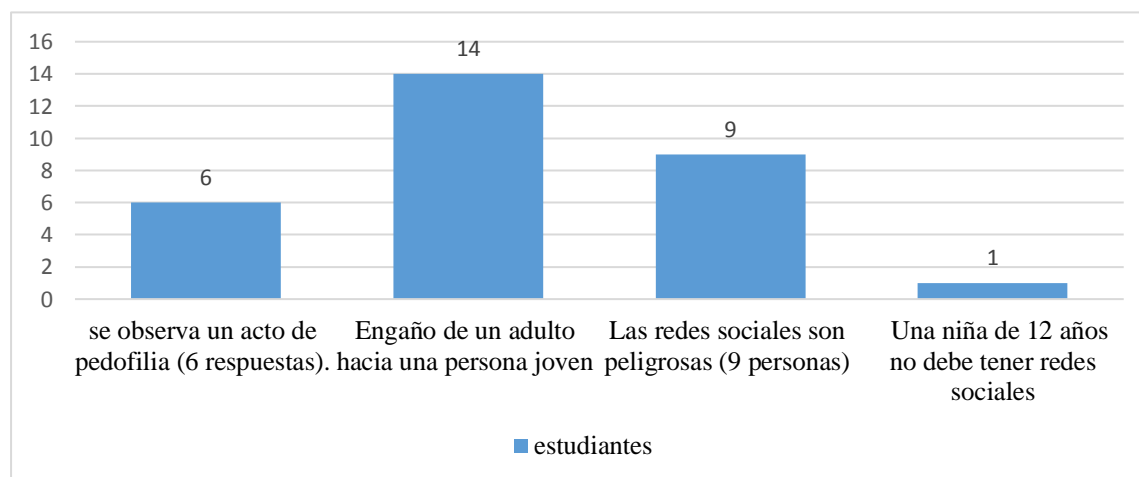
A continuación se encuentran las preguntas planteadas en la encuesta con las respuestas obtenidas de manera general

Pregunta 1	
Categoría a la que aporta	Aporta a las dos categorías
Tipo de respuesta	Respuesta abierta

Pregunta: Observe con mucha atención la siguiente imagen y escriba lo que observa y piensa sobre ella.



Respuestas obtenidas

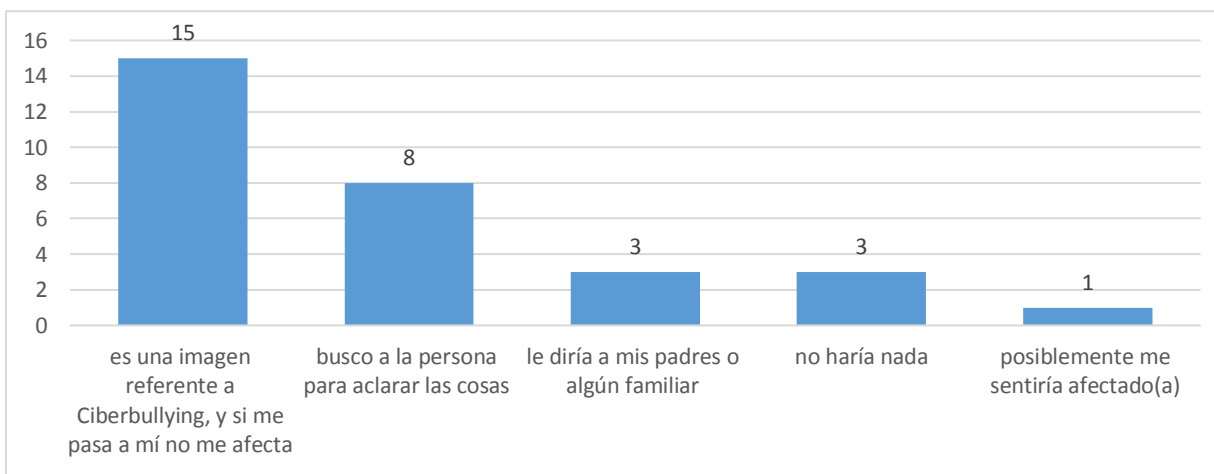


Pregunta 2	
Categoría a la que aporta	Comportamientos en internet
Tipo de respuesta	Respuesta abierta

Pregunta: Observa la siguiente imagen y piensa que el mensaje de la imagen es para ti, cual crees que sería tu reacción.

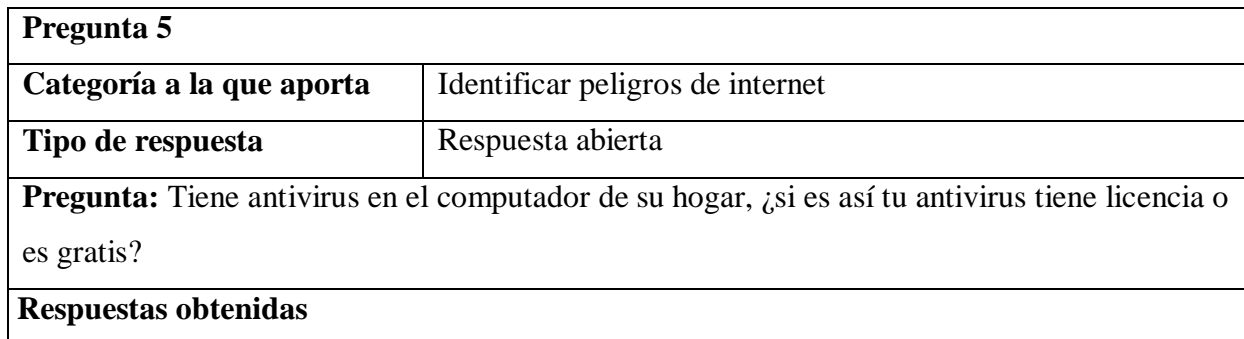
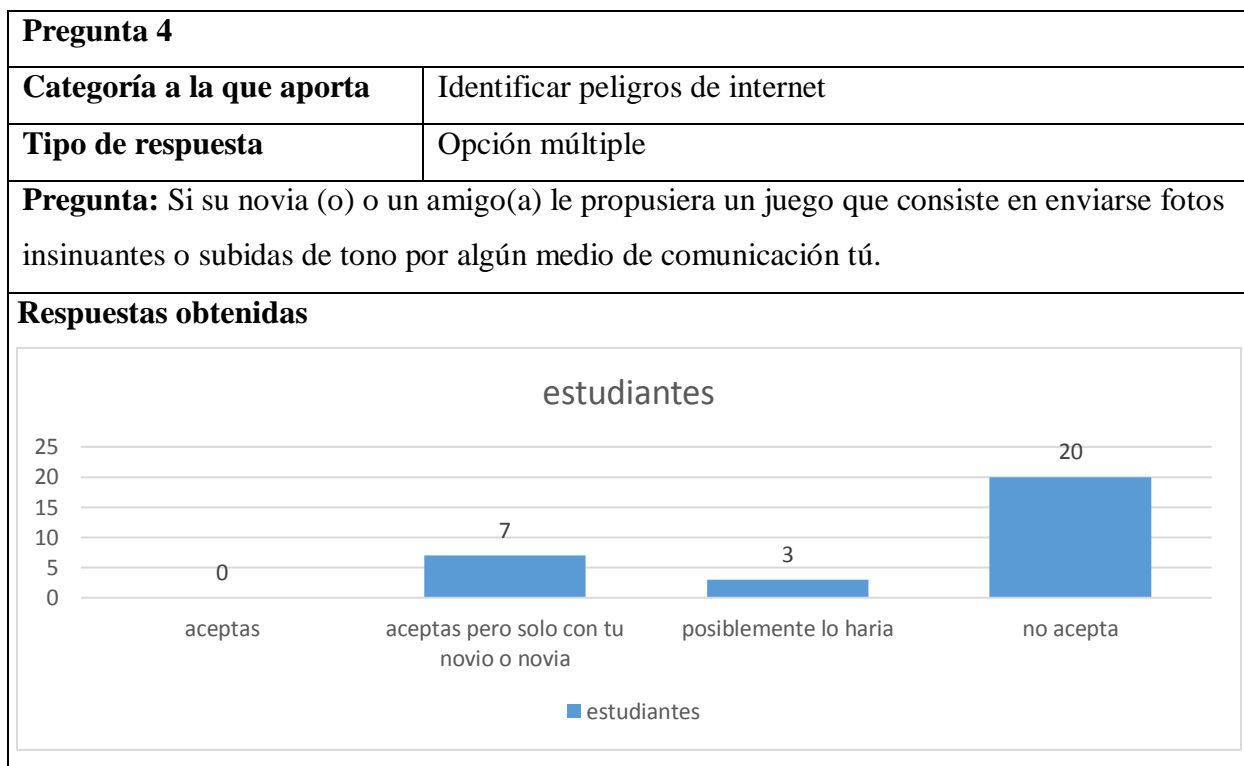
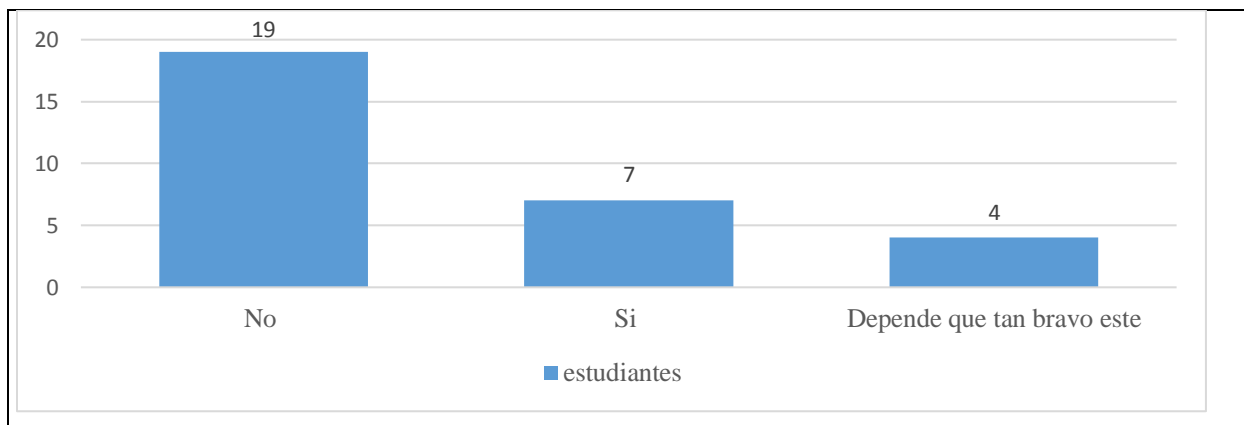


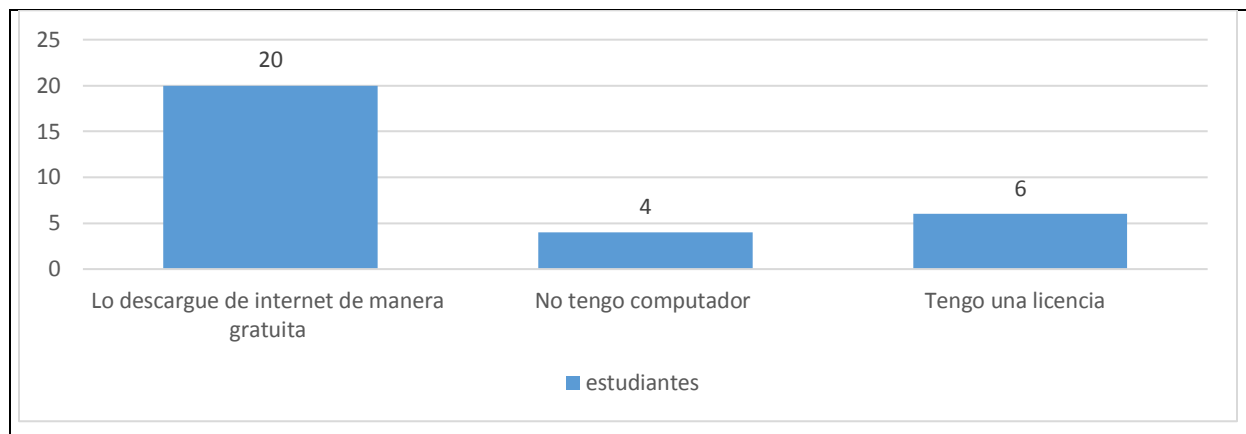
Respuestas obtenidas



Pregunta 3

Categoría a la que aporta	Aporta a las dos categorías
Tipo de respuesta	Respuesta abierta
Pregunta: ¿Si estas bravo u ofendido con alguien le enviarías mensajes ofensivos?	
Respuestas obtenidas	



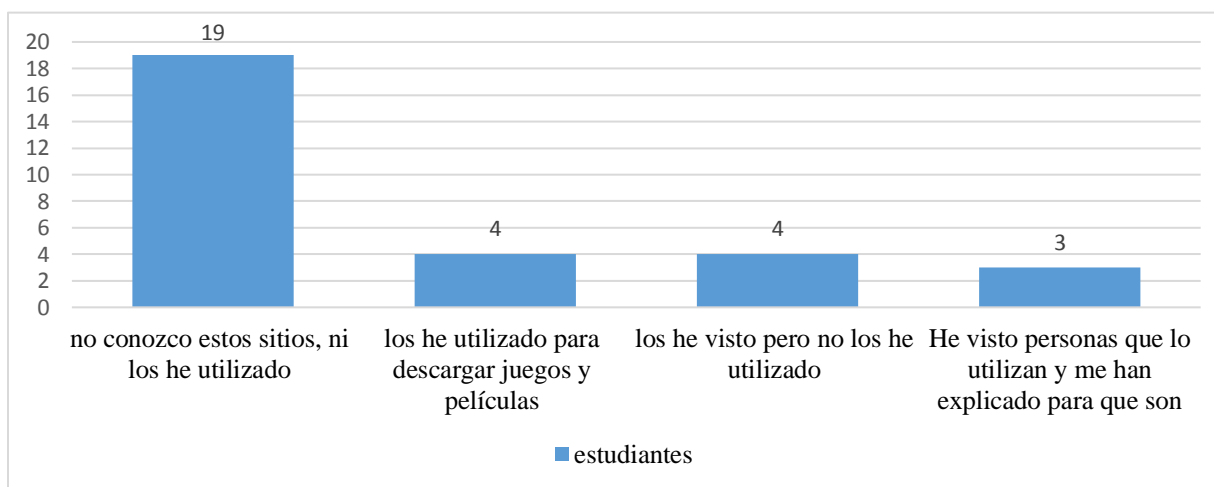


Pregunta 6															
Categoría a la que aporta	Pregunta informativa														
Tipo de respuesta	Pregunta de selección múltiple donde el estudiante podía seleccionar varias respuestas.														
Pregunta: ¿Qué tipo de archivos descargas de Internet?															
Respuestas obtenidas															
<p>A bar chart with a vertical axis from 0 to 40 in increments of 10. The horizontal axis lists six categories: 'música', 'videos', 'juegos y programas', 'imágenes', 'libros', and 'todas las anteriores'. The bars represent the number of students for each category: 26 for música, 20 for videos, 5 for juegos y programas, 30 for imágenes, 2 for libros, and 10 for todas las anteriores. A legend indicates that the blue bars represent 'estudiantes'.</p> <table border="1"> <thead> <tr> <th>Categoría</th> <th>Estudiantes</th> </tr> </thead> <tbody> <tr> <td>música</td> <td>26</td> </tr> <tr> <td>videos</td> <td>20</td> </tr> <tr> <td>juegos y programas</td> <td>5</td> </tr> <tr> <td>imágenes</td> <td>30</td> </tr> <tr> <td>libros</td> <td>2</td> </tr> <tr> <td>todas las anteriores</td> <td>10</td> </tr> </tbody> </table>		Categoría	Estudiantes	música	26	videos	20	juegos y programas	5	imágenes	30	libros	2	todas las anteriores	10
Categoría	Estudiantes														
música	26														
videos	20														
juegos y programas	5														
imágenes	30														
libros	2														
todas las anteriores	10														

Pregunta 7	
Categoría a la que aporta	Comportamientos en internet
Tipo de respuesta	Respuesta abierta
Pregunta: La siguiente imagen muestra los logos de ciertos sitios de Internet, ¿los ha usado?, si es así para que los ha utilizado.	



Respuestas obtenidas



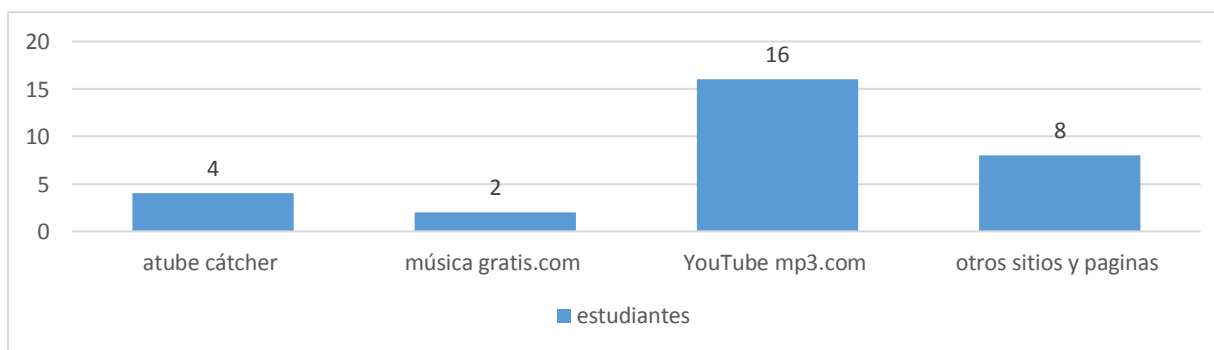
Pregunta 8

Categoría a la que aporta Pregunta informativa

Tipo de respuesta Respuesta abierta

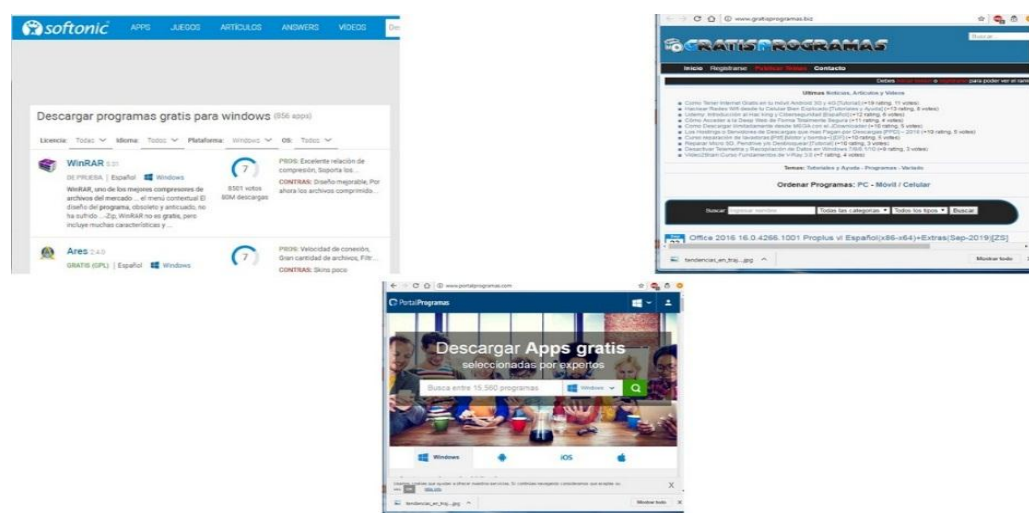
Pregunta: Descarga música desde su computador, si es así ¿cuál es el programa que usa usted para esto?

Respuestas obtenidas

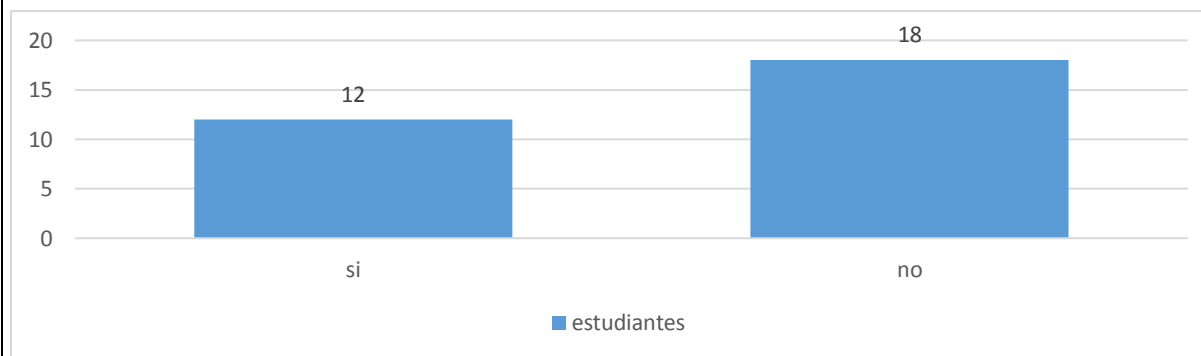


Pregunta 9	
Categoría a la que aporta	Aporta a las 2 categorías
Tipo de respuesta	Respuesta si o no

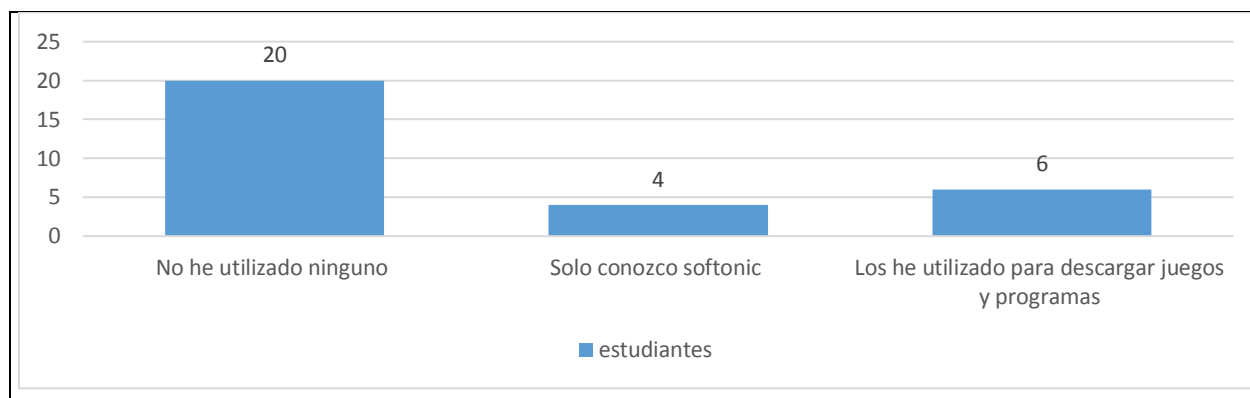
Pregunta: Conoces alguno de los programas que aparece en la siguiente imagen.



Respuestas obtenidas

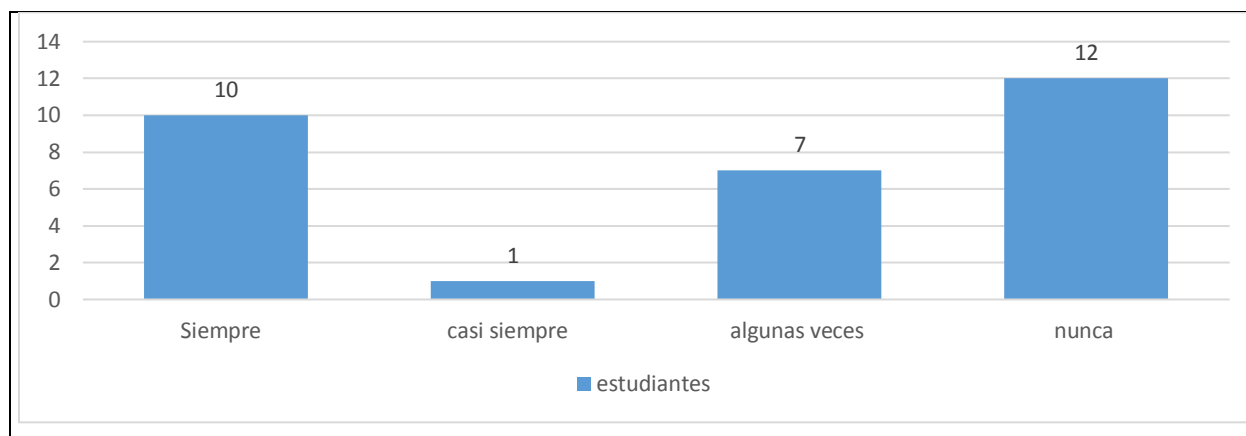


Pregunta 10	
Categoría a la que aporta	Aporta a las 2 categorías
Tipo de respuesta	Respuesta abierta
Pregunta: ha utilizado alguno de los programas presente en la imagen anterior, si su respuesta es sí explique para que los ha utilizado	
Respuestas obtenidas	



Pregunta 11											
Categoría a la que aporta	Comportamientos en internet										
Tipo de respuesta	Opción múltiple										
Pregunta: Si necesita o desea un programa o juego para su computador, tú lo compras en la tienda oficial.											
Respuestas obtenidas											
<table border="1"> <thead> <tr> <th>Categoría</th> <th>Estudiantes</th> </tr> </thead> <tbody> <tr> <td>Siempre</td> <td>2</td> </tr> <tr> <td>casi siempre</td> <td>4</td> </tr> <tr> <td>algunas veces</td> <td>13</td> </tr> <tr> <td>nunca</td> <td>11</td> </tr> </tbody> </table>		Categoría	Estudiantes	Siempre	2	casi siempre	4	algunas veces	13	nunca	11
Categoría	Estudiantes										
Siempre	2										
casi siempre	4										
algunas veces	13										
nunca	11										

Pregunta 12	
Categoría a la que aporta	Comportamientos en internet
Tipo de respuesta	Opción múltiple
Pregunta: Si necesita o desea un programa o juego para su computador, tú lo compras pirata.	
Respuestas obtenidas	



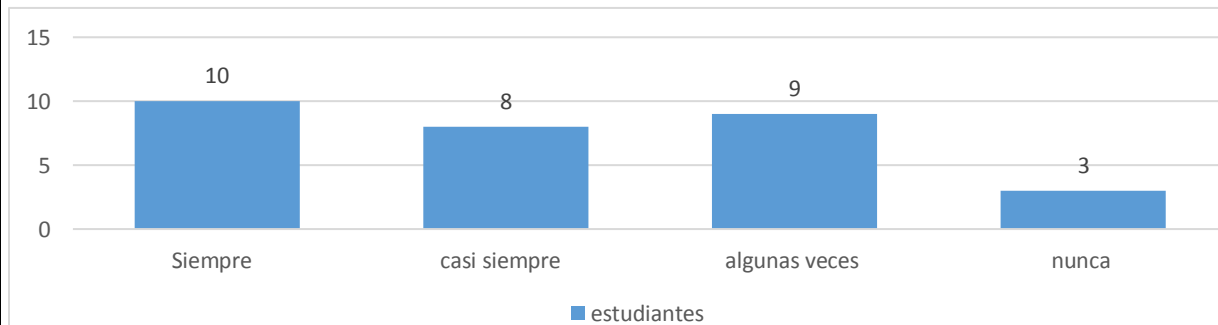
Pregunta 13

Categoría a la que aporta	Comportamientos en internet
----------------------------------	-----------------------------

Tipo de respuesta	Opción múltiple
--------------------------	-----------------

Pregunta: Si necesita o desea un programa o juego para su computador, tú lo descargas gratis de internet.

Respuestas obtenidas

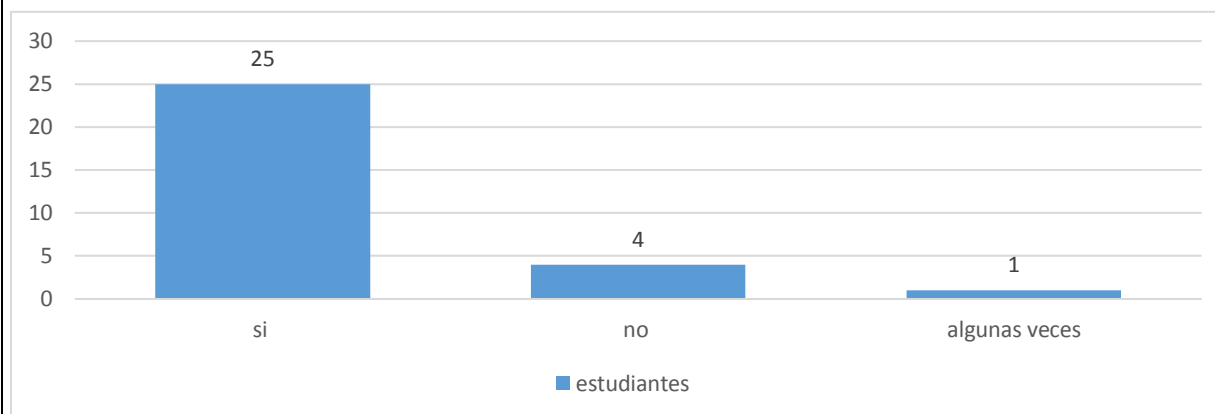


Pregunta 14

Categoría a la que aporta	Identificar peligros de internet
Tipo de respuesta	Respuesta abierta

Categoría a la que aporta	Identificar peligros de internet
Tipo de respuesta	Respuesta abierta

Le ha aparecido alguna vez en su pantalla algún anuncio publicitario de algo que usted no haya buscado.

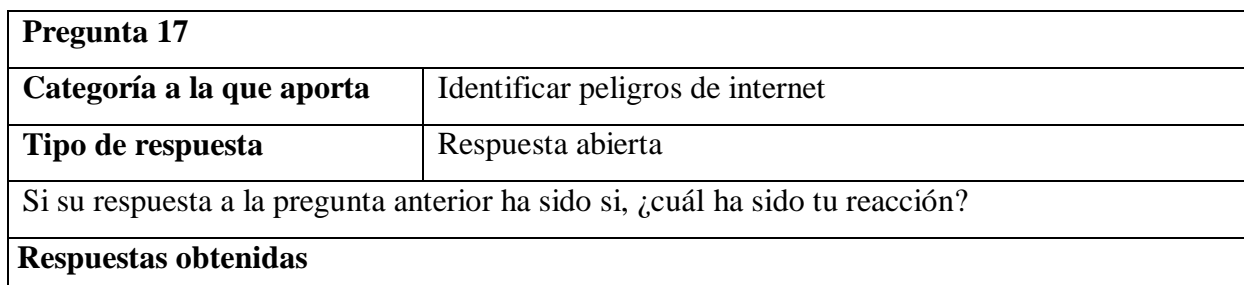
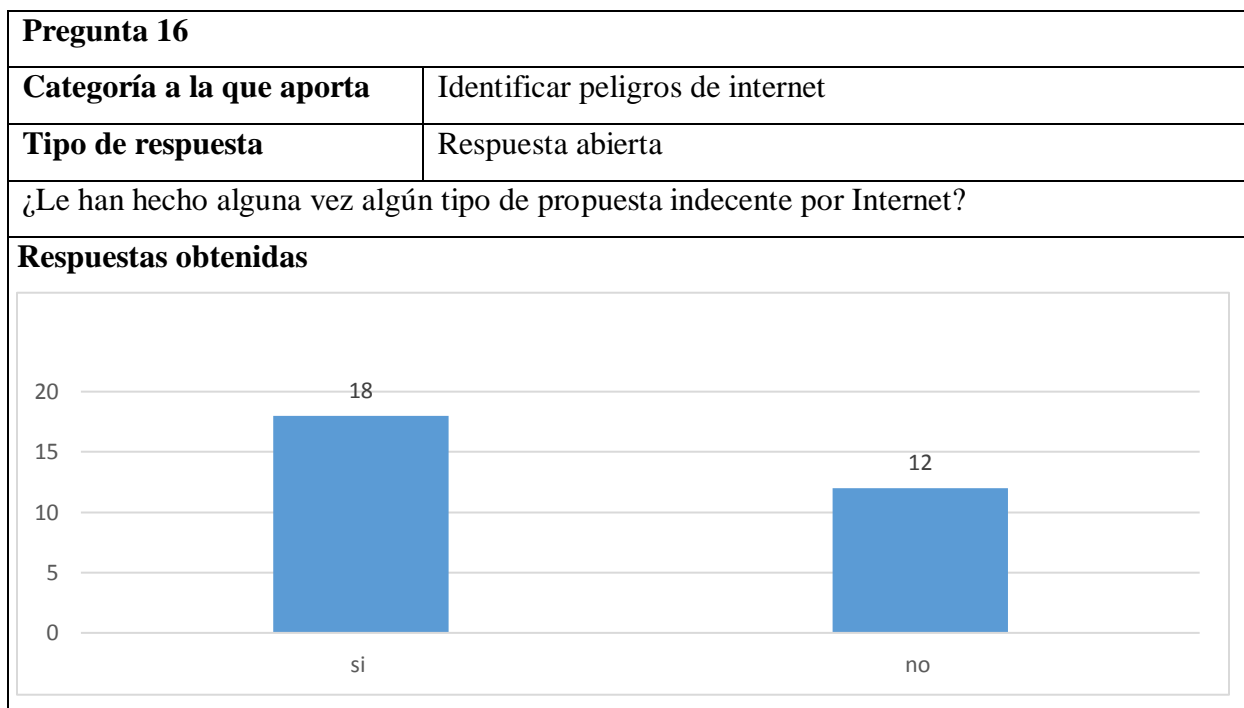
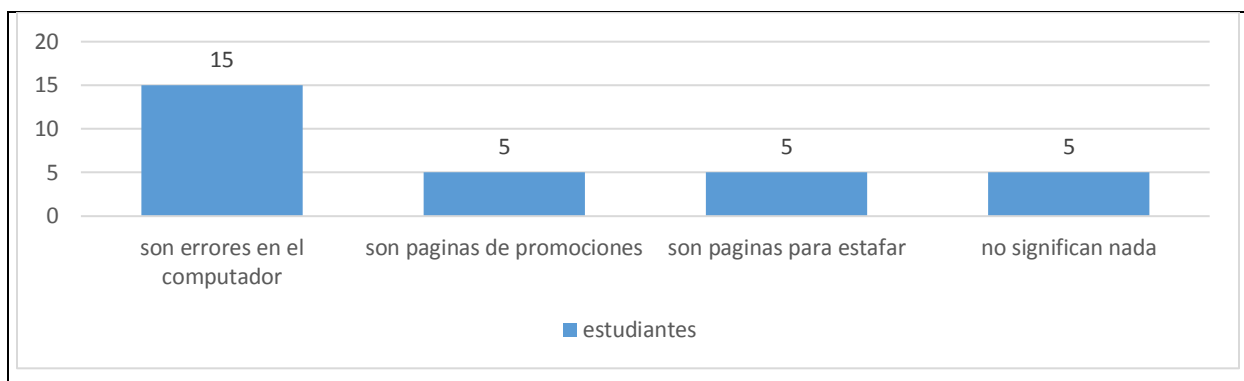
Respuestas obtenidas**Pregunta 15**

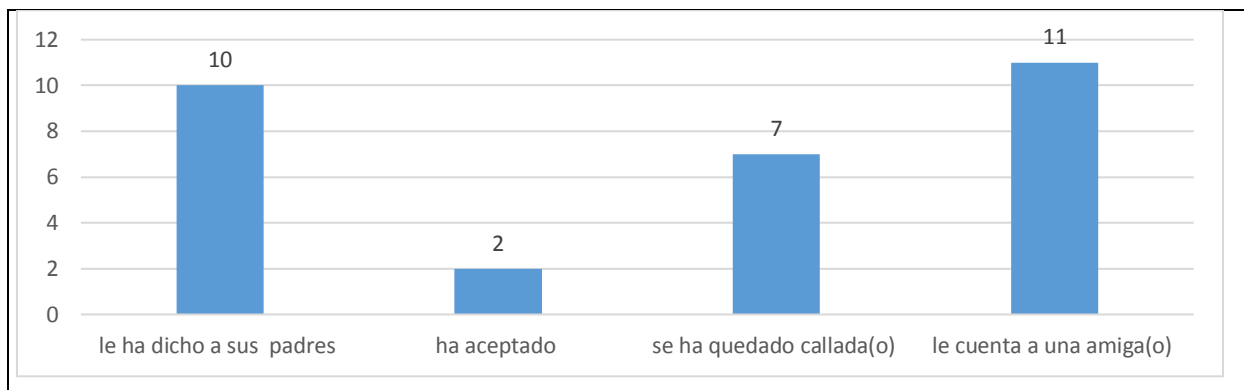
Categoría a la que aporta	Identificar peligros de internet
Tipo de respuesta	Respuesta abierta

Categoría a la que aporta	Identificar peligros de internet
Tipo de respuesta	Respuesta abierta

Desde su punto de vista y sus conocimientos, que piensa usted de la siguiente imagen

**Respuestas obtenidas**





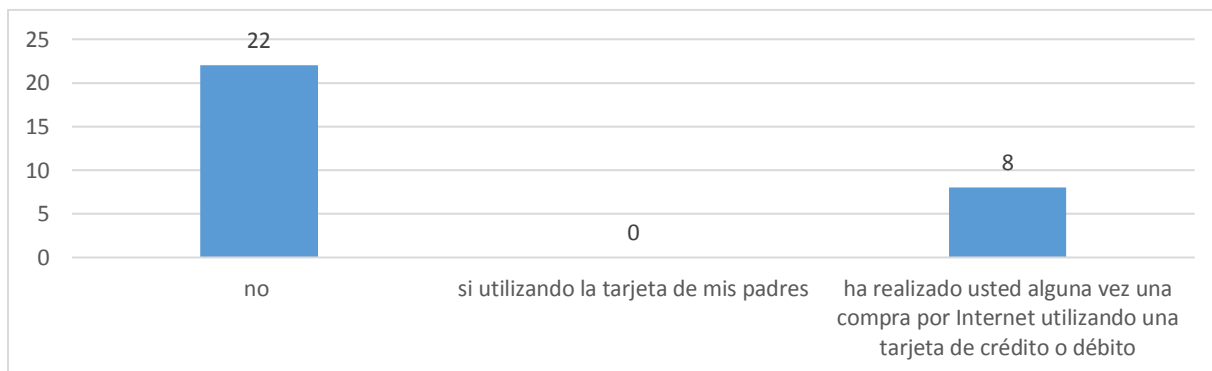
Pregunta 18

Categoría a la que aporta	Acciones en internet
----------------------------------	----------------------

Tipo de respuesta	Respuesta abierta
--------------------------	-------------------

ha realizado usted alguna vez una compra por Internet utilizando una tarjeta de crédito o débito

Respuestas obtenidas



Pregunta 19											
Categoría a la que aporta	Identificar peligros de internet										
Tipo de respuesta	Opcion multiple										
Reconoce usted alguno de los sitios de Internet que aparecen en la siguiente imagen.											
											
Respuestas obtenidas											
 <table border="1"> <caption>Data for the bar chart</caption> <thead> <tr> <th>Respuesta</th> <th>Cantidad</th> </tr> </thead> <tbody> <tr> <td>si</td> <td>0</td> </tr> <tr> <td>si y los he utilizado</td> <td>0</td> </tr> <tr> <td>no</td> <td>11</td> </tr> <tr> <td>se para que son pero no los he utilizado</td> <td>19</td> </tr> </tbody> </table>		Respuesta	Cantidad	si	0	si y los he utilizado	0	no	11	se para que son pero no los he utilizado	19
Respuesta	Cantidad										
si	0										
si y los he utilizado	0										
no	11										
se para que son pero no los he utilizado	19										

Pregunta 20	
Categoría a la que aporta	Identificar peligros de internet
Tipo de respuesta	Respuesta abierta
Cuando estas navegando en Internet y de manera voluntaria o involuntaria accedes a ver imágenes, vídeos o animaciones sobre peleas, agresiones a personas de distinta clase social o	

color, contenido sensual. ¿Te aparece un letrero como el de la siguiente imagen?



Atención

El acceso a esta página ha sido denegado.

Respuestas obtenidas



Pregunta 21

Categoría a la que aporta

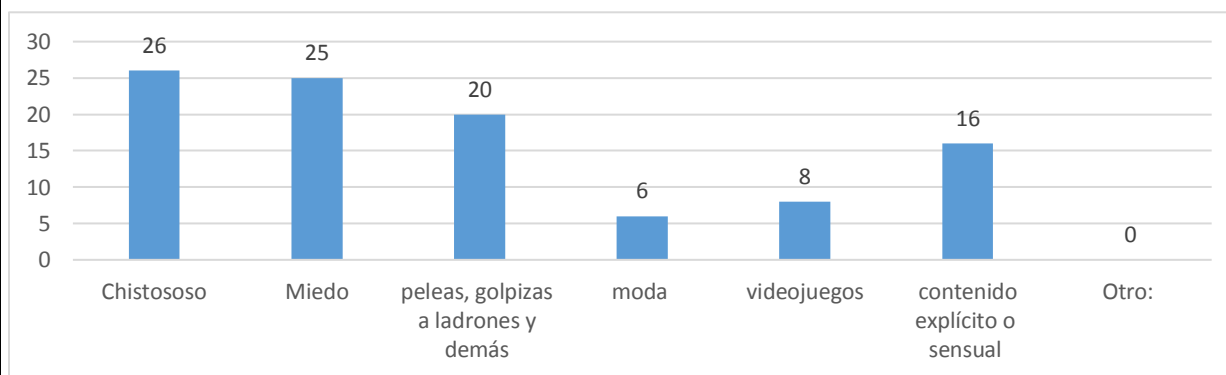
Identificar peligros de internet

Tipo de respuesta

Opción múltiple donde el estudiantes puede seleccionar mas de una respuesta

Según el contenido de un vídeo ¿qué tipos de vídeos ves?

Respuestas obtenidas



Pregunta 22

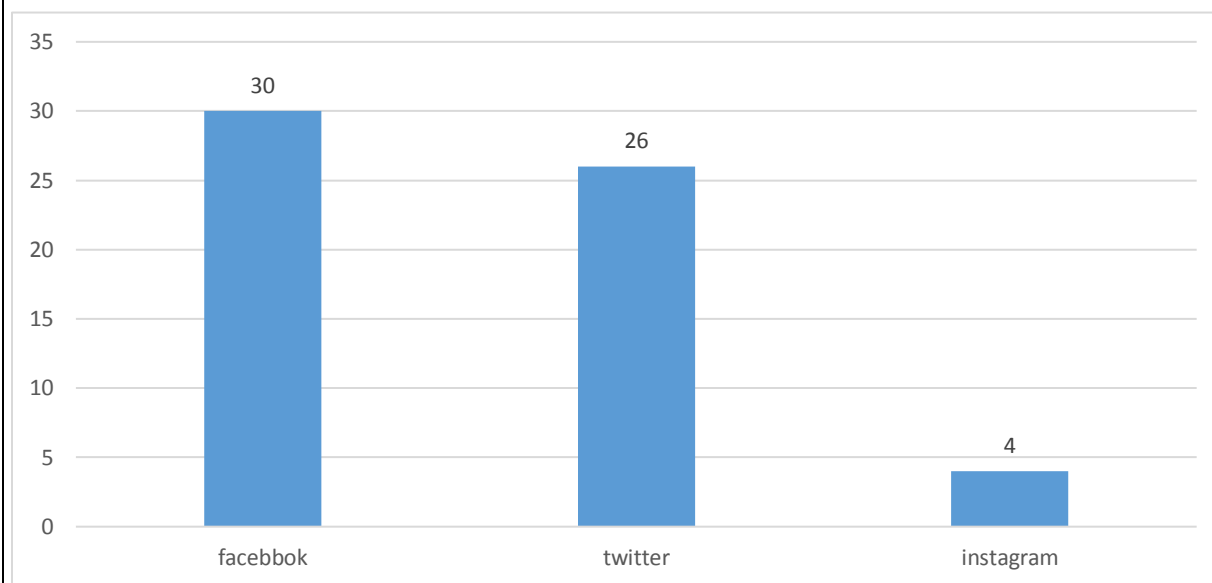
Categoría a la que aporta

Informativa

Tipo de respuesta

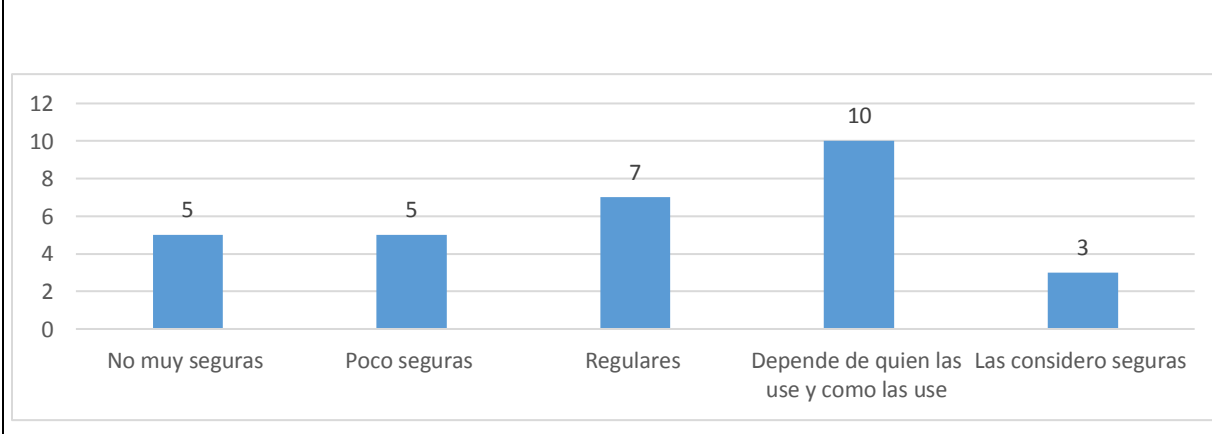
Opción múltiple el estudiante puede seleccionar varias respuestas

que redes sociales manejas

Respuestas obtenidas**Pregunta 23**

Categoría a la que aporta	informativa
Tipo de respuesta	Respuesta abierta

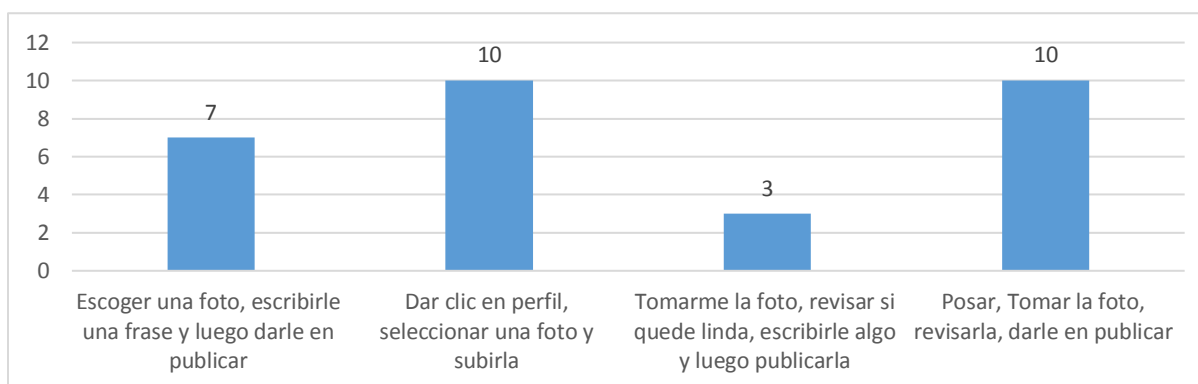
que tan seguras considera las redes sociales

Respuestas obtenidas**Pregunta 24**

Categoría a la que aporta	Acciones en internet
Tipo de respuesta	Respuesta abierta

Describe cuales son los pasos que realiza para subir una foto a una red social. (pregunta de respuesta abierta)

Respuestas obtenidas



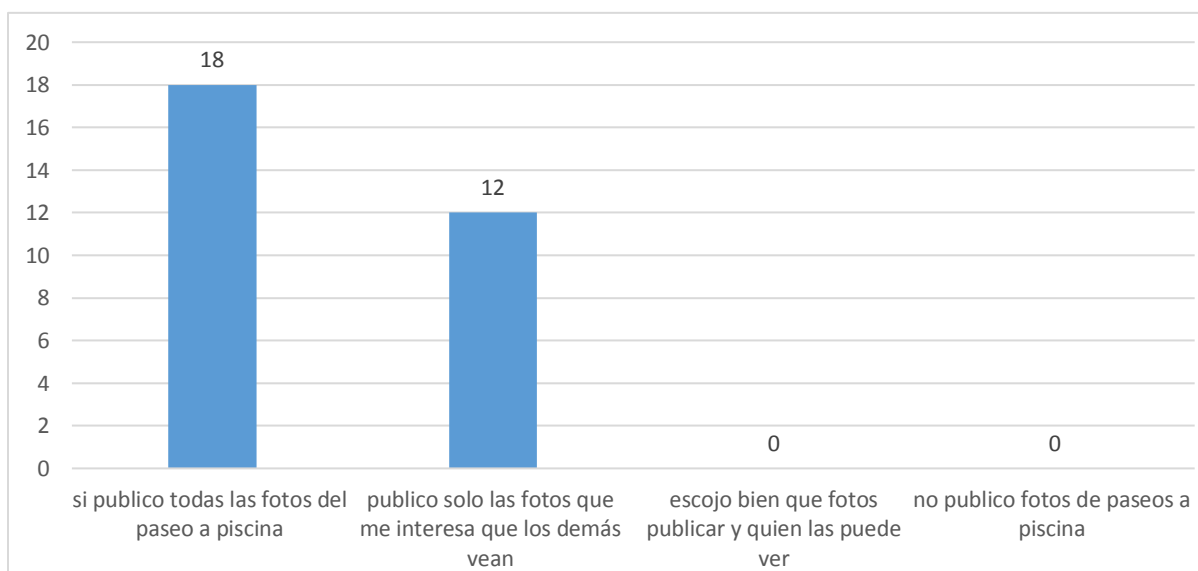
Pregunta 25


Categoría a la que aporta	Identificar peligros de internet
----------------------------------	----------------------------------

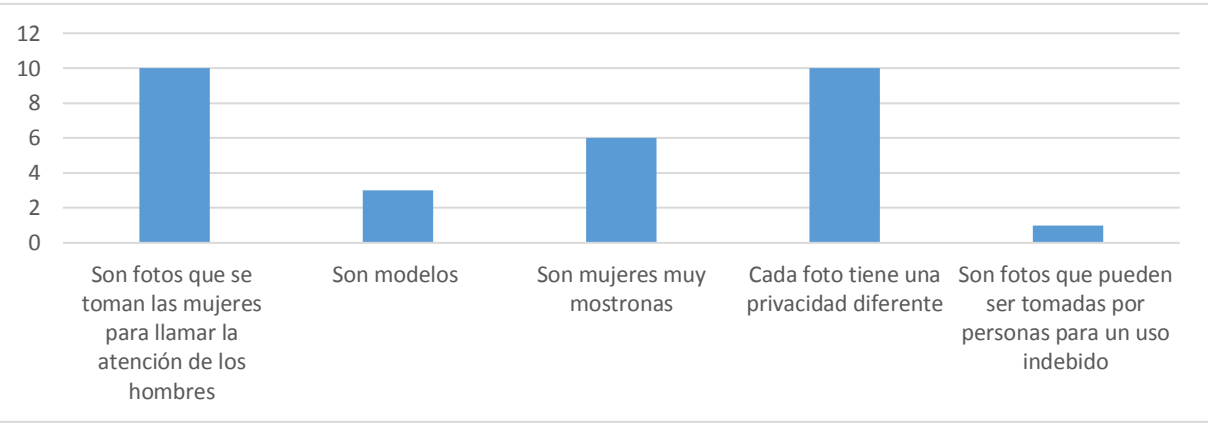
Tipo de respuesta	Opción múltiple
--------------------------	-----------------

Cuando vas de paseo a un sitio de clima caliente es probable que vaya a la piscina o al rio y se tomen fotos, ¿publica usted este tipo de fotos, o se fija en cuales publicar?

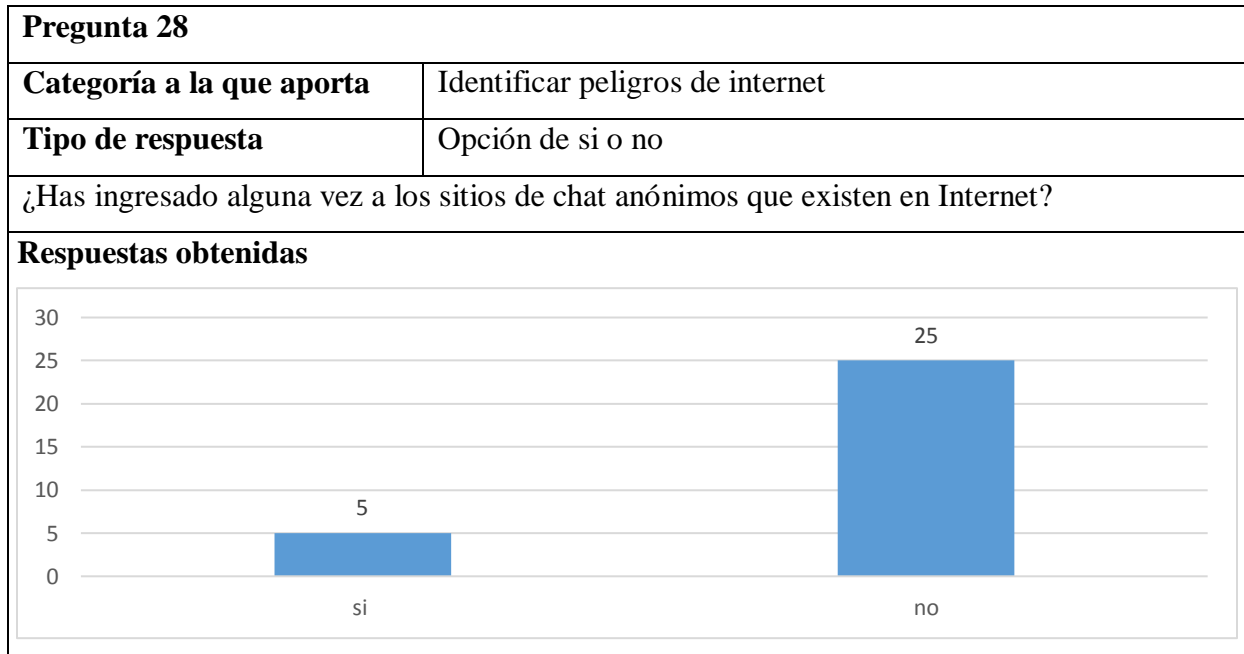
Respuestas obtenidas



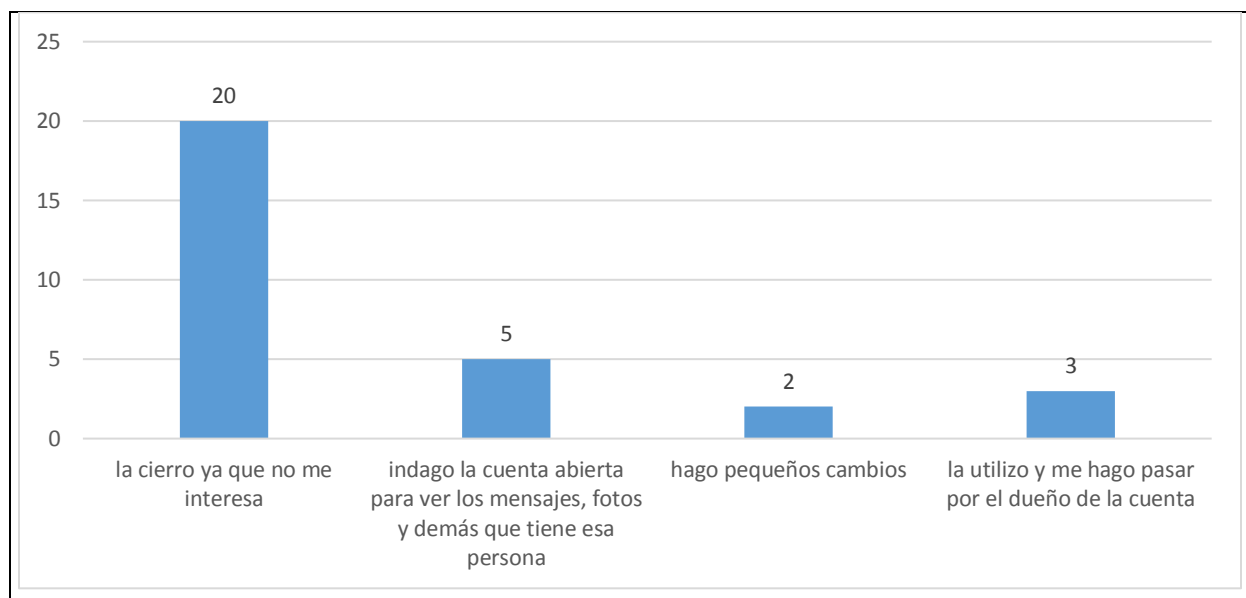
Pregunta 26	
Categoría a la que aporta	Identificar peligros de internet
Tipo de respuesta	Respuesta abierta
<p>Observe la siguiente imagen y escribe lo que piensas al respecto, es necesario que observes todos los detalles presentes en la imagen.</p>	
	

Respuestas obtenidas													
 <table border="1"> <thead> <tr> <th>Categoría</th> <th>Respuestas</th> </tr> </thead> <tbody> <tr> <td>Son fotos que se toman las mujeres para llamar la atención de los hombres</td> <td>10</td> </tr> <tr> <td>Son modelos</td> <td>3</td> </tr> <tr> <td>Son mujeres muy mostronas</td> <td>6</td> </tr> <tr> <td>Cada foto tiene una privacidad diferente</td> <td>10</td> </tr> <tr> <td>Son fotos que pueden ser tomadas por personas para un uso indebido</td> <td>1</td> </tr> </tbody> </table>		Categoría	Respuestas	Son fotos que se toman las mujeres para llamar la atención de los hombres	10	Son modelos	3	Son mujeres muy mostronas	6	Cada foto tiene una privacidad diferente	10	Son fotos que pueden ser tomadas por personas para un uso indebido	1
Categoría	Respuestas												
Son fotos que se toman las mujeres para llamar la atención de los hombres	10												
Son modelos	3												
Son mujeres muy mostronas	6												
Cada foto tiene una privacidad diferente	10												
Son fotos que pueden ser tomadas por personas para un uso indebido	1												

Pregunta 27	
Categoría a la que aporta	Pregunta informativa
Tipo de respuesta	Respuesta abierta
<p>Cuantos "amigos" tiene usted en sus diferentes redes sociales, y de esos amigos ¿cuantos conoce en la vida real? (pregunta de respuesta abierta)</p>	
<p>Respuestas obtenidas</p> <p>Para esta pregunta cada persona respondió la cantidad de amigos que tenía y los que conocían, pero como cada persona respondió diferente a partir de los resultados se puede ver que según las respuestas estas personas no conocen en la vida real ni más de la mitad de los amigos virtuales que dicen tener.</p>	



Pregunta 29	
Categoría a la que aporta	Acciones en internet
Tipo de respuesta	Opción múltiple
Si llegas a una sala de Internet y en el computador que vas a utilizar hay una cuenta de correo o red social abierta ¿qué harías tú?	
Respuestas obtenidas	



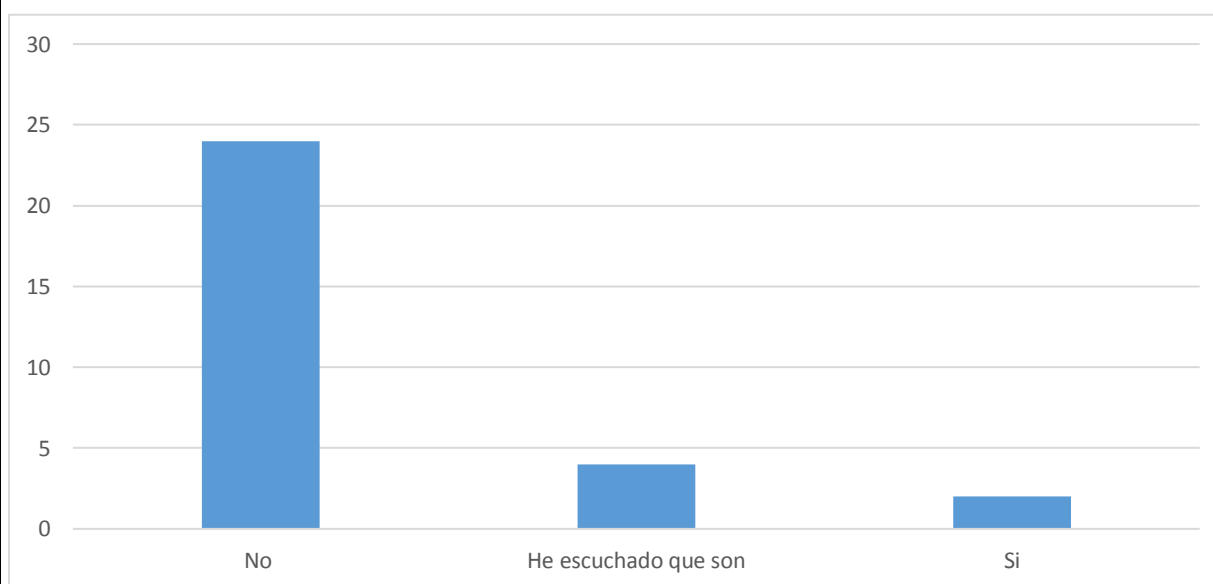
Pregunta 30

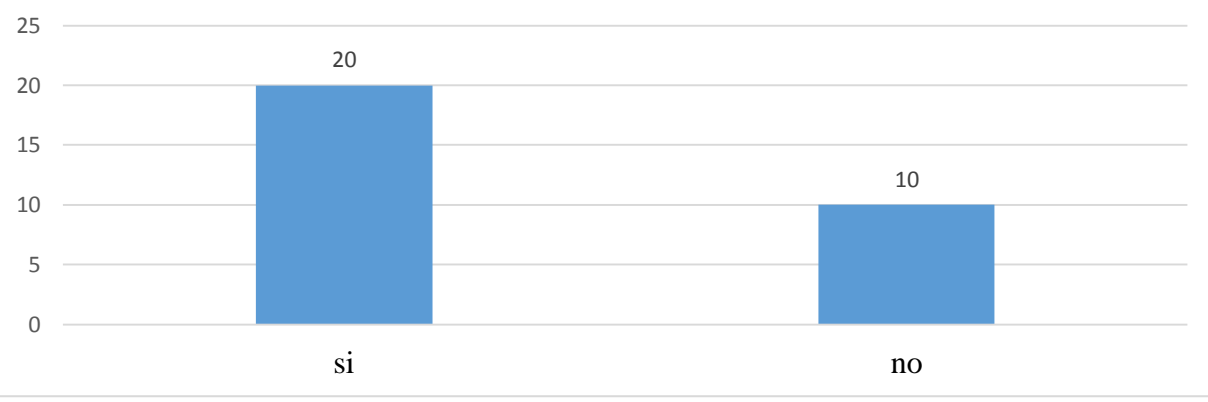
Categoría a la que aporta	Identificar peligros de internet
----------------------------------	----------------------------------


Tipo de respuesta	Respuesta abierta
--------------------------	-------------------

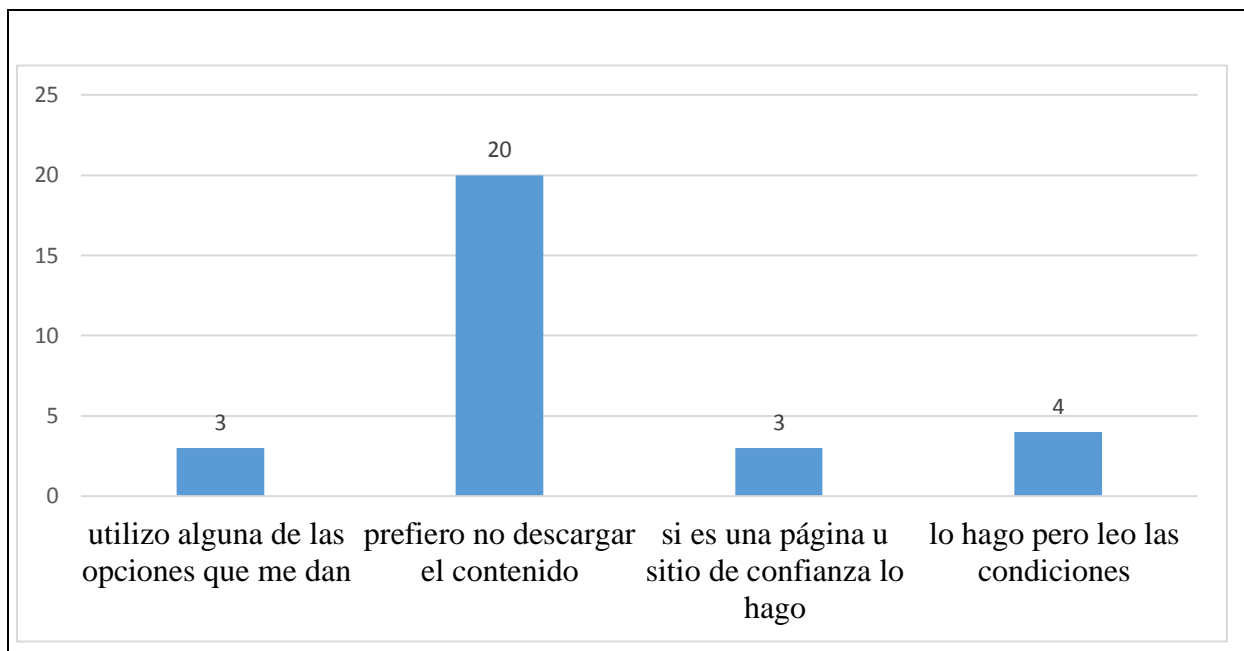
conoces que son los capturadores de teclado o también llamados keyloggers

Respuestas obtenidas



Pregunta 31							
Categoría a la que aporta	Pregunta informativa						
Tipo de respuesta	Respuesta abierta						
maneja la misma contraseña para uno o varios sitios de Internet a los que usted tenga acceso, por ejemplo la misma contraseña del Facebook la utiliza en twitter o en drive o algún otro sitio (pregunta de respuesta abierta)							
Respuestas obtenidas							
 <table border="1"> <caption>Data for Bar Chart: Respuestas obtenidas</caption> <thead> <tr> <th>Respuesta</th> <th>Cantidad</th> </tr> </thead> <tbody> <tr> <td>si</td> <td>20</td> </tr> <tr> <td>no</td> <td>10</td> </tr> </tbody> </table>		Respuesta	Cantidad	si	20	no	10
Respuesta	Cantidad						
si	20						
no	10						

Pregunta 32	
Categoría a la que aporta	Acciones en internet
Tipo de respuesta	Respuesta abierta
Supongamos que deseas descargar algún contenido de Internet, pero el sitio de donde desea descargarlo le pide hacer alguna de las condiciones que aparece en la imagen siguiente. ¿Qué harías?	
	
Respuestas obtenidas	

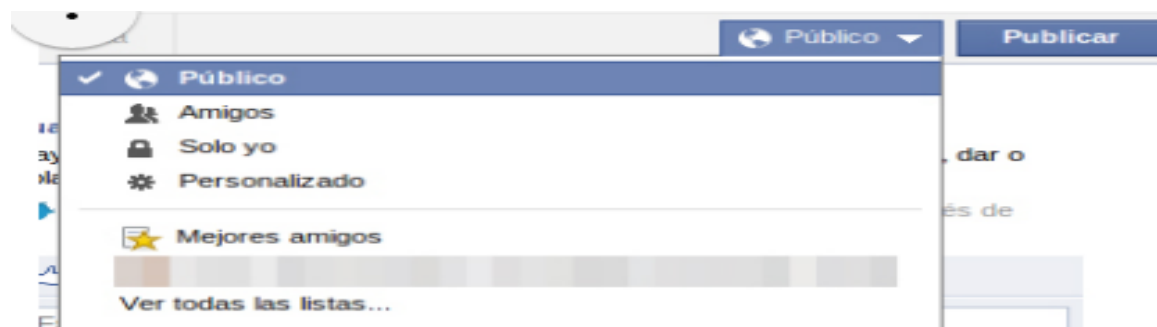


Pregunta 33

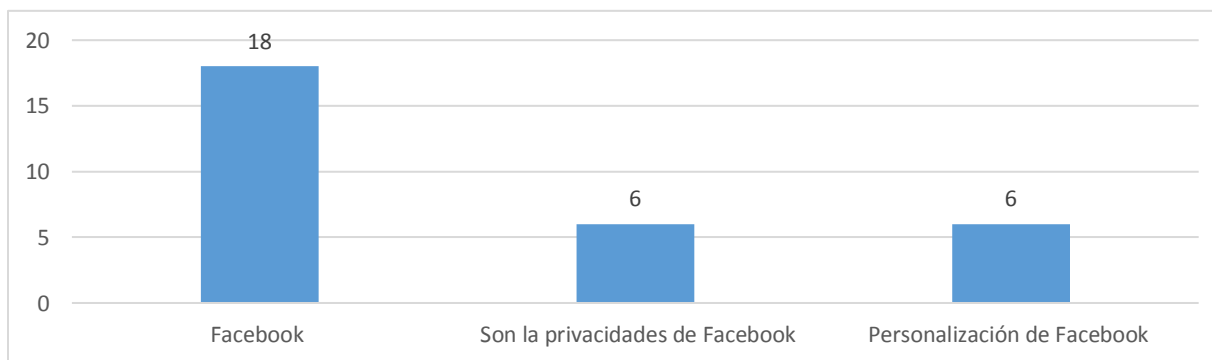
Categoría a la que aporta Acciones en internet

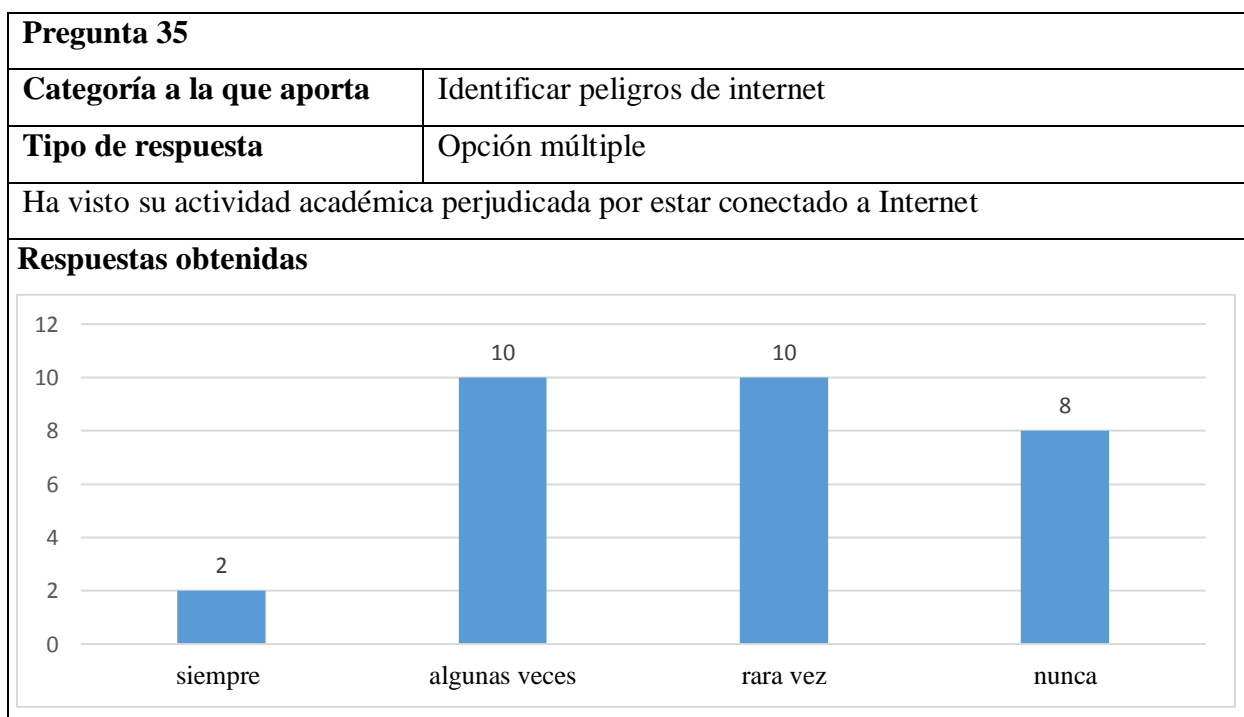
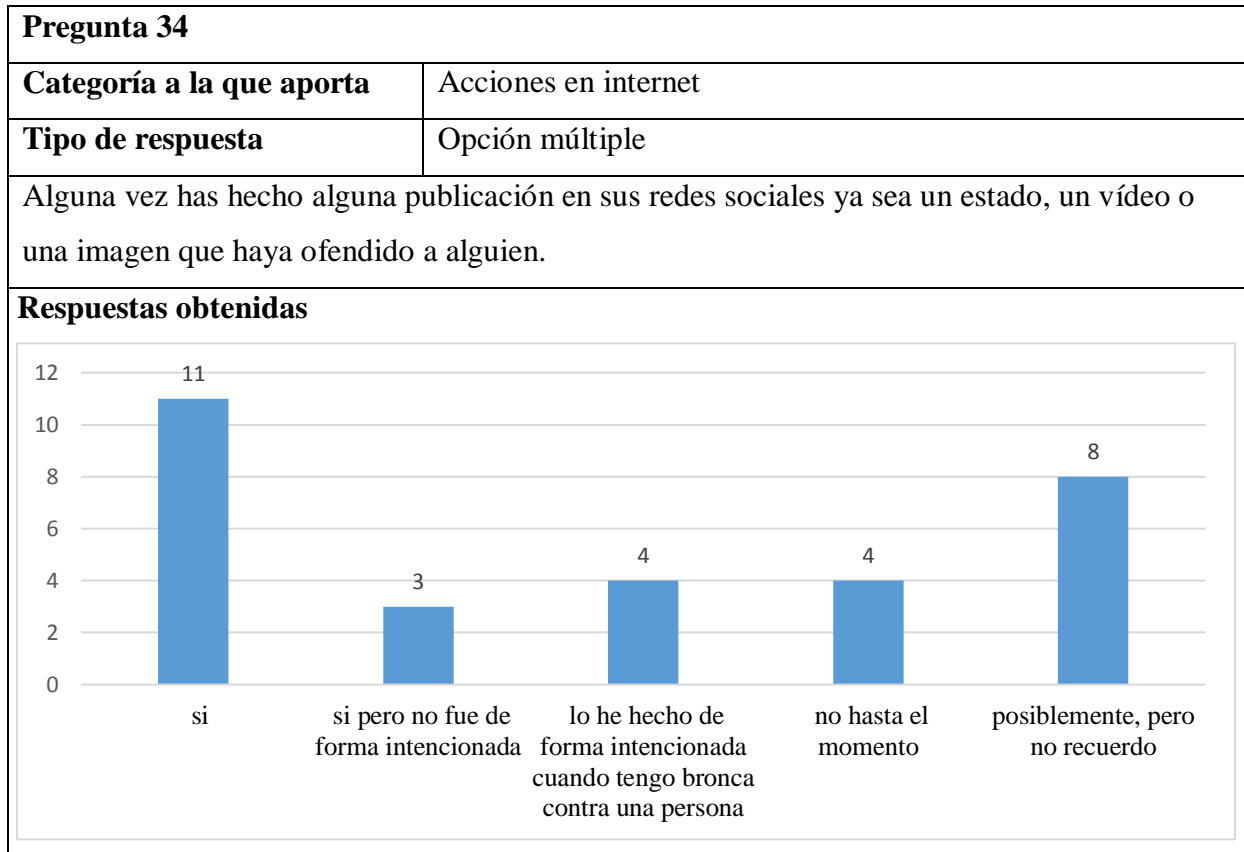
Tipo de respuesta Respuesta abierta

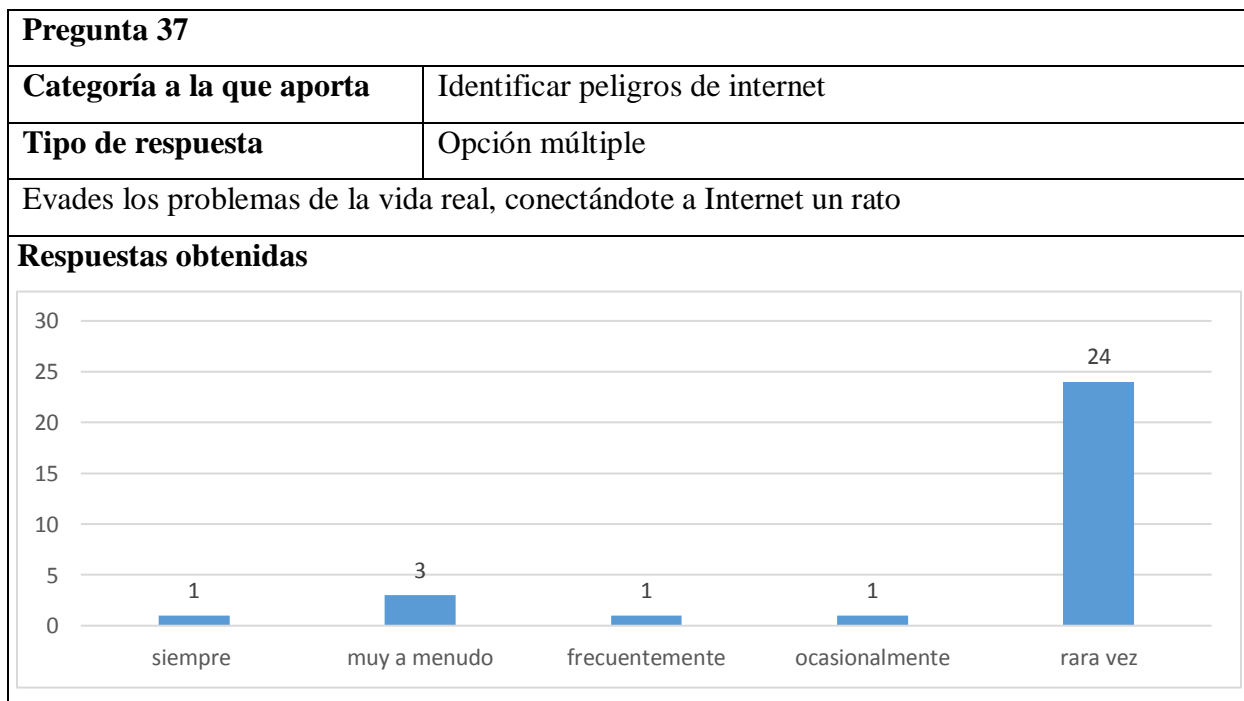
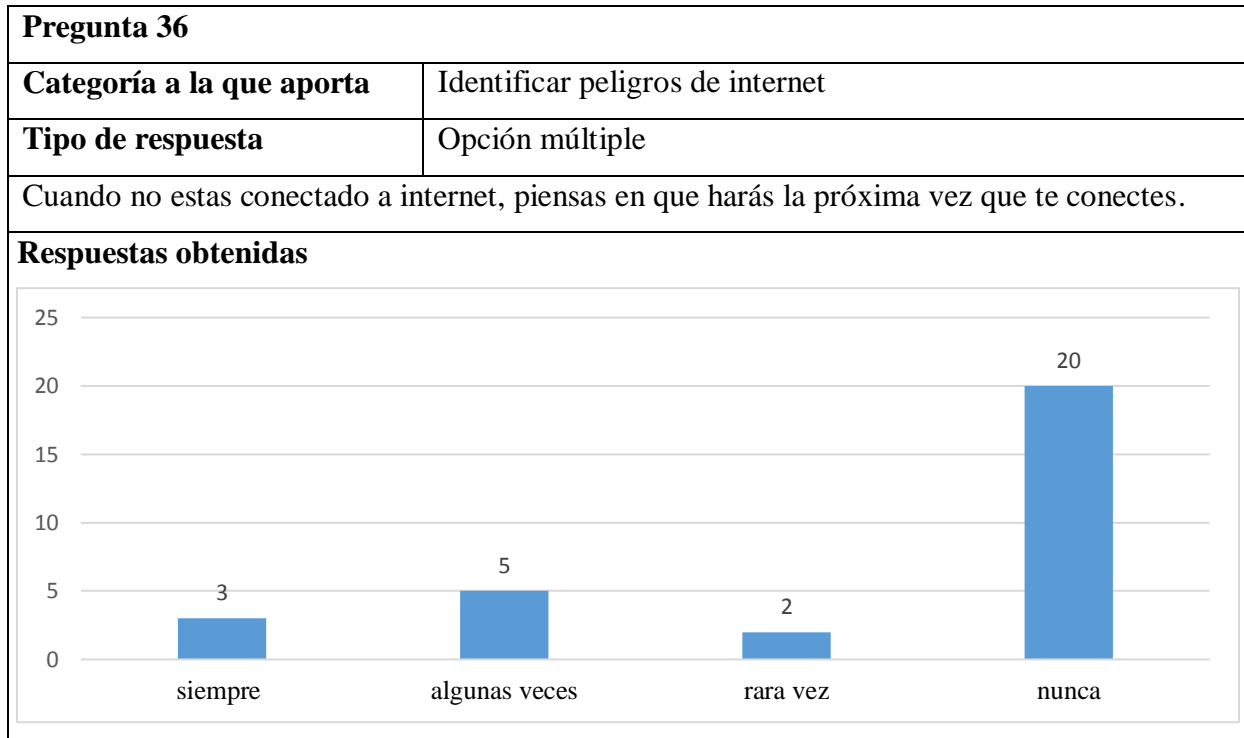
Con que asocias la siguiente imagen:



Respuestas obtenidas





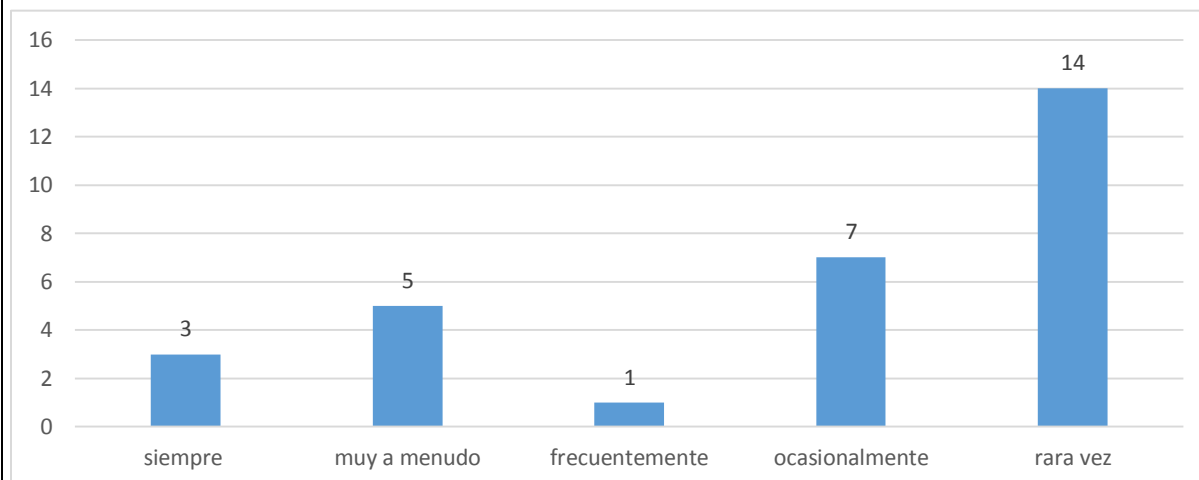


Pregunta 38

Categoría a la que aporta	Identificar peligros de internet
----------------------------------	----------------------------------

Tipo de respuesta	Opción múltiple
--------------------------	-----------------

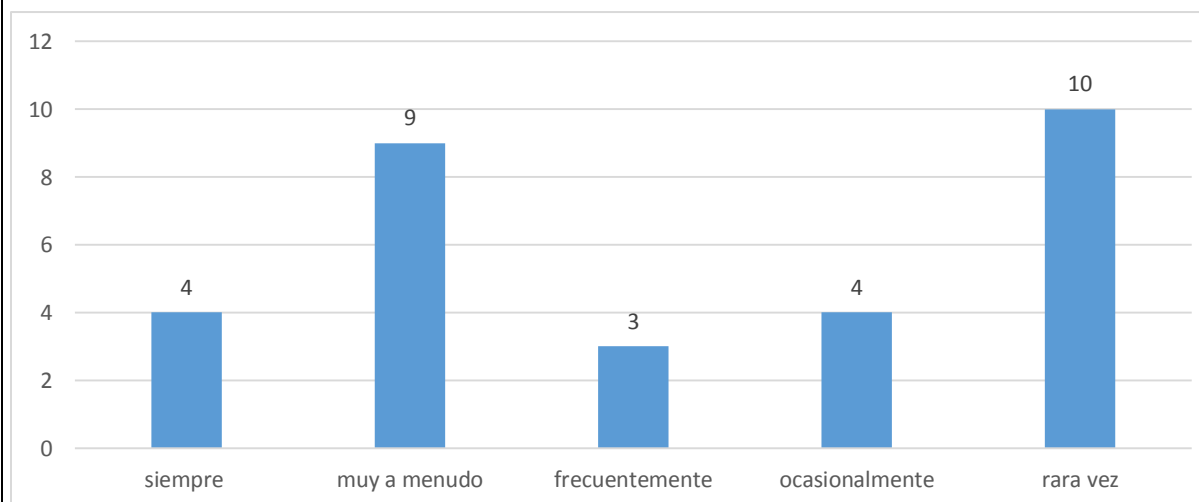
Teme que su vida sin internet sea aburrida y vacía

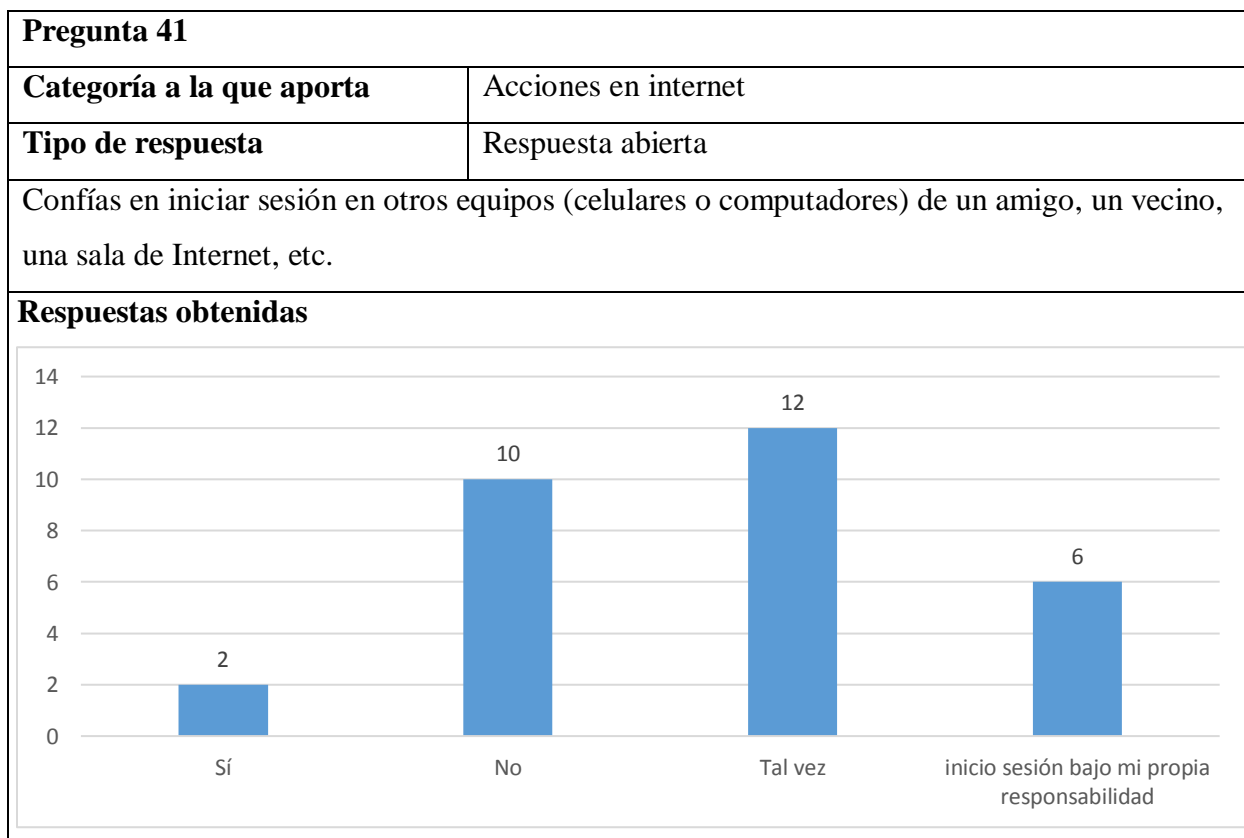
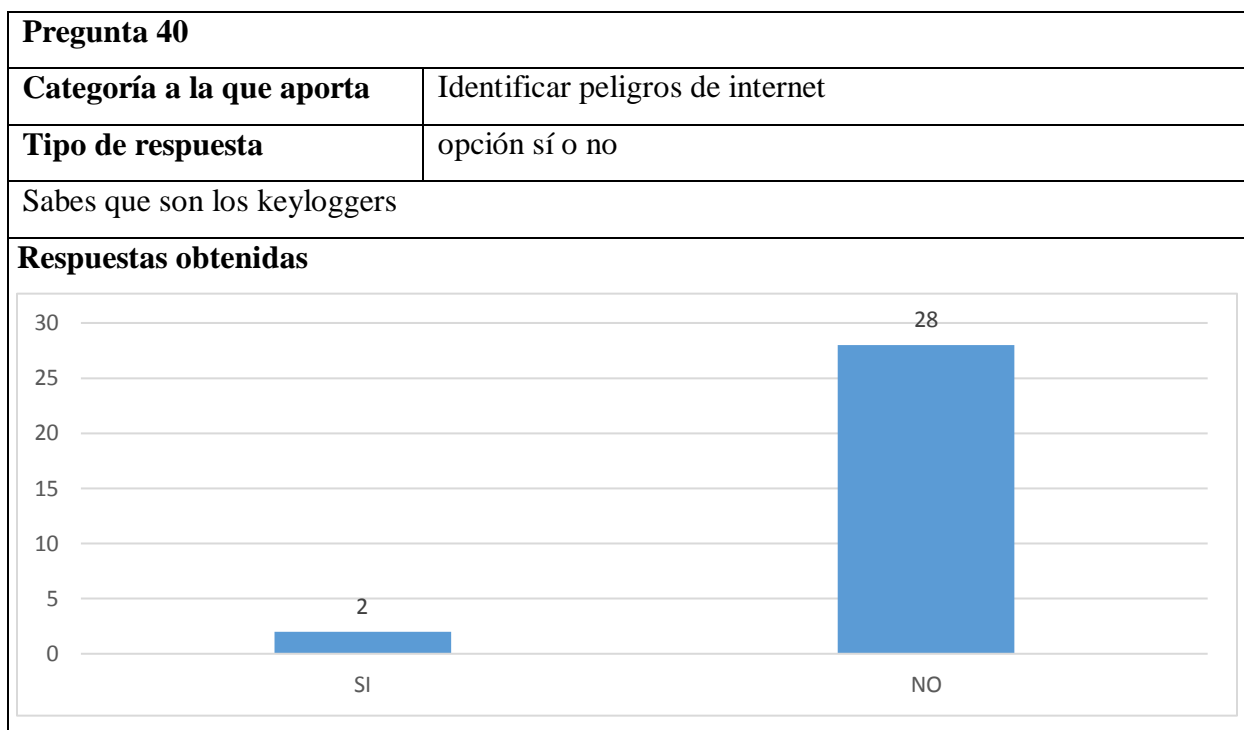
Respuestas obtenidas**Pregunta 39**

Categoría a la que aporta	Identificar peligros de internet
----------------------------------	----------------------------------

Tipo de respuesta	Opción múltiple
--------------------------	-----------------

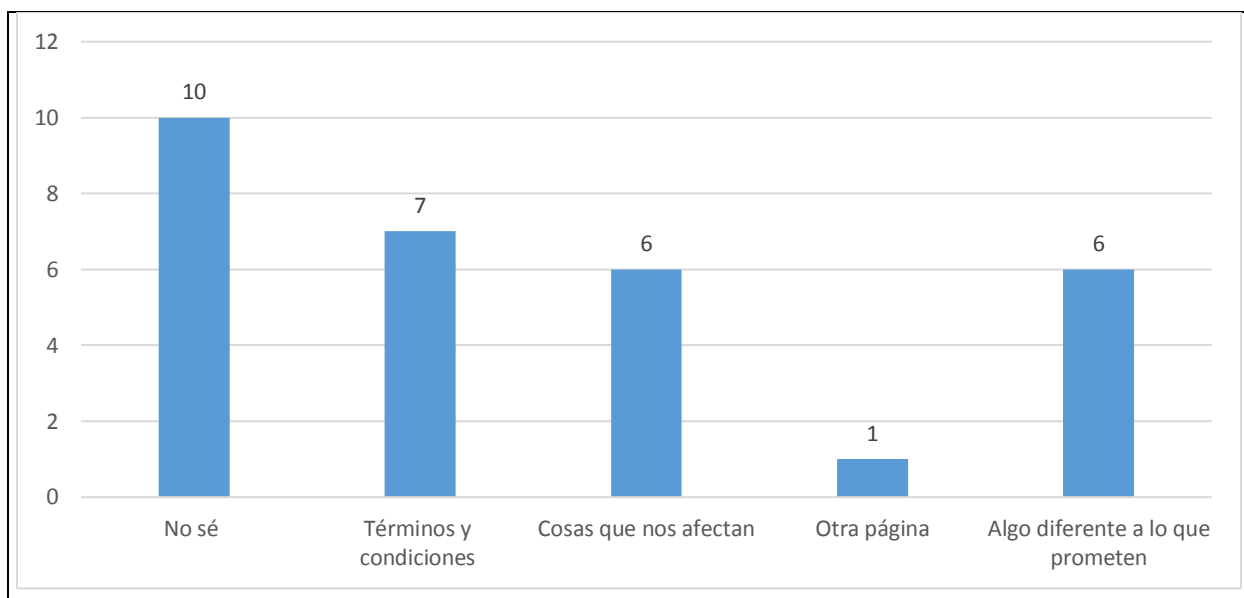
¿Con que frecuencia pierde horas de sueño pasándolas conectado a Internet?

Respuestas obtenidas



Pregunta 42									
Categoría a la que aporta	Acciones en internet								
Tipo de respuesta	Opción múltiple								
Alguna vez mientras navega por Internet le ha aparecido una imagen como esta. ¿Qué has hecho?									
									
Respuestas obtenidas									
 <table border="1"> <thead> <tr> <th>Respuesta</th> <th>Número de respuestas</th> </tr> </thead> <tbody> <tr> <td>Si pero la cierro</td> <td>9</td> </tr> <tr> <td>Si y he ingresado mi número de teléfono</td> <td>0</td> </tr> <tr> <td>No nunca me ha aparecido esta imagen</td> <td>21</td> </tr> </tbody> </table>		Respuesta	Número de respuestas	Si pero la cierro	9	Si y he ingresado mi número de teléfono	0	No nunca me ha aparecido esta imagen	21
Respuesta	Número de respuestas								
Si pero la cierro	9								
Si y he ingresado mi número de teléfono	0								
No nunca me ha aparecido esta imagen	21								

Pregunta 43	
Categoría a la que aporta	Pregunta informativa
Tipo de respuesta	Respuesta abierta
en la imagen anterior se puede observar que hay unos enunciados en letra más pequeña, que cree que diga en esos anuncios	
Respuestas obtenidas	



Pregunta 44

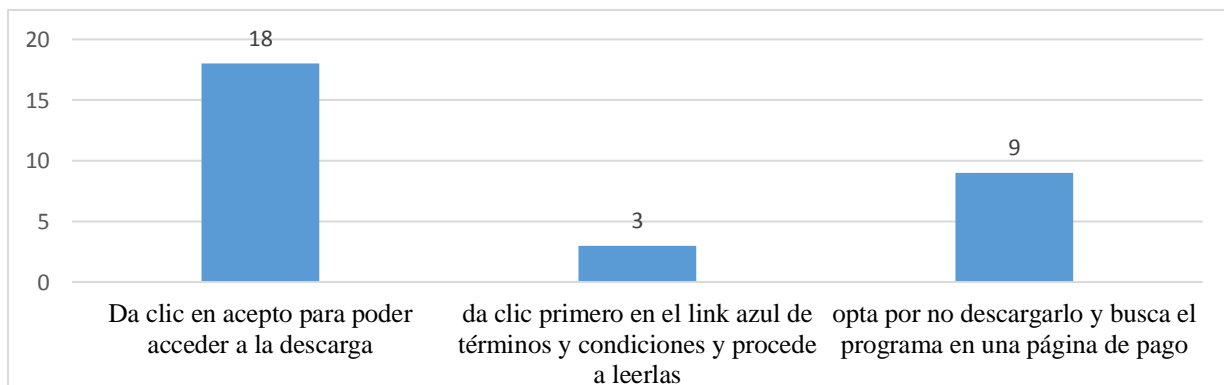
Categoría a la que aporta	Acciones en internet
----------------------------------	----------------------

Tipo de respuesta	Opción múltiple
--------------------------	-----------------

Muchas veces cuando se intenta descargar algo, es posible que salga en alguna parte una imagen como la siguiente, que haces frente a este tipo de enunciados.



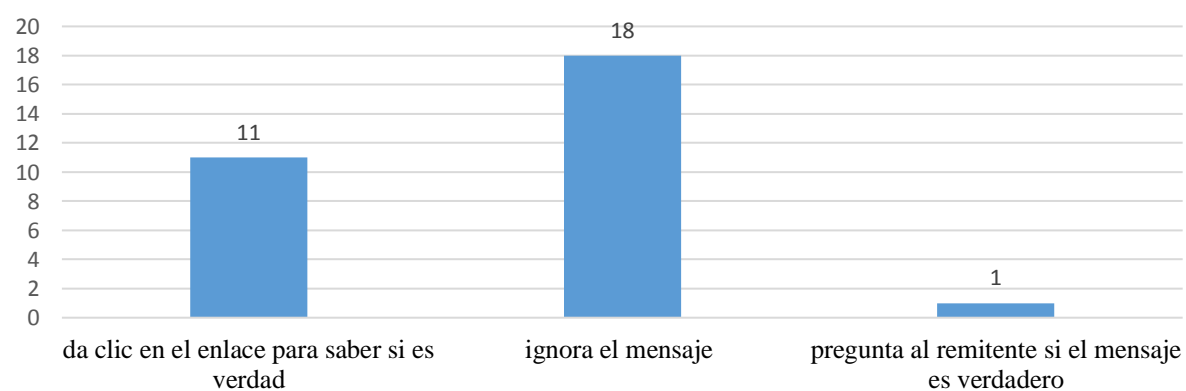
Respuestas obtenidas

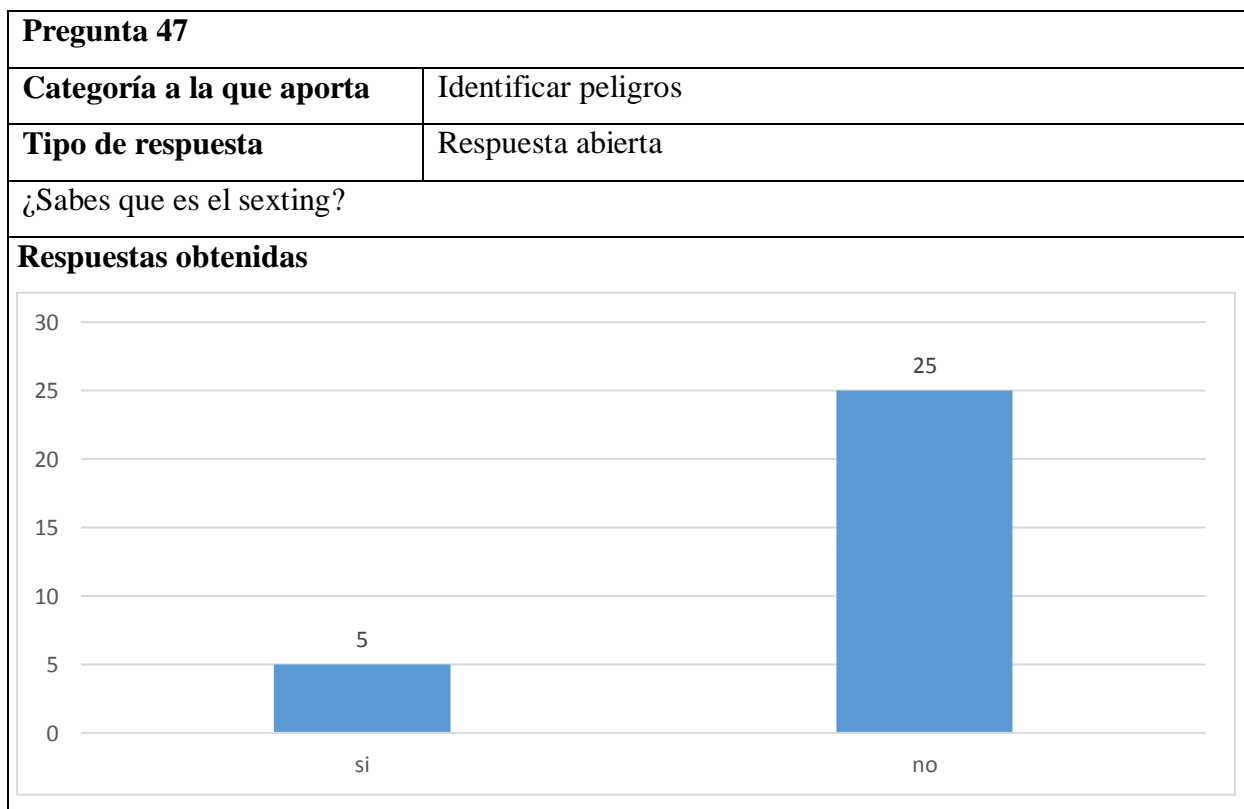
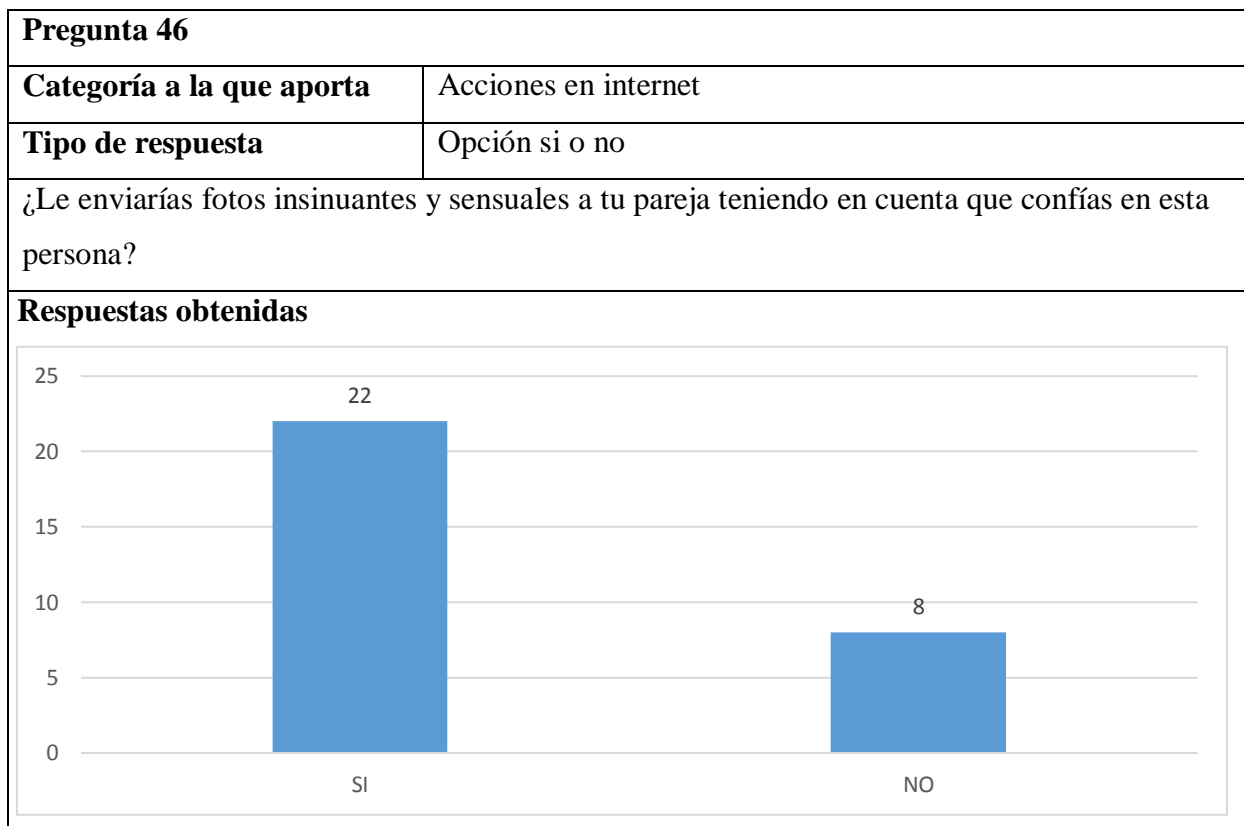


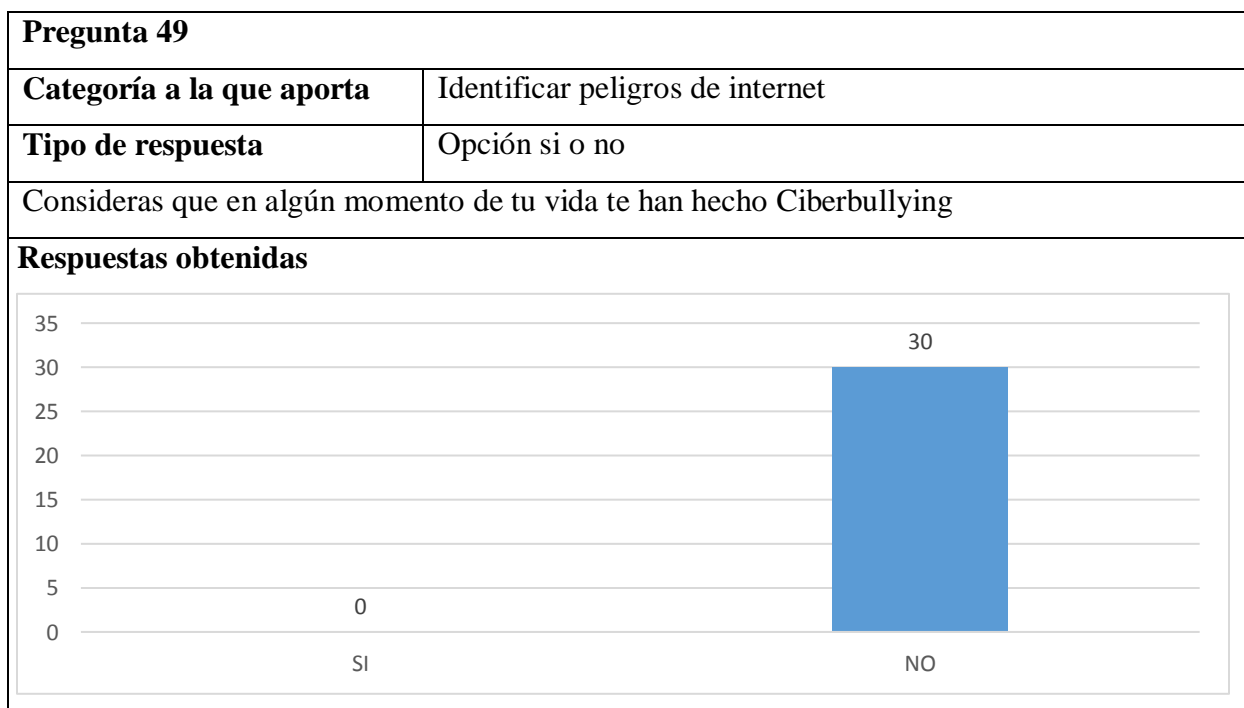
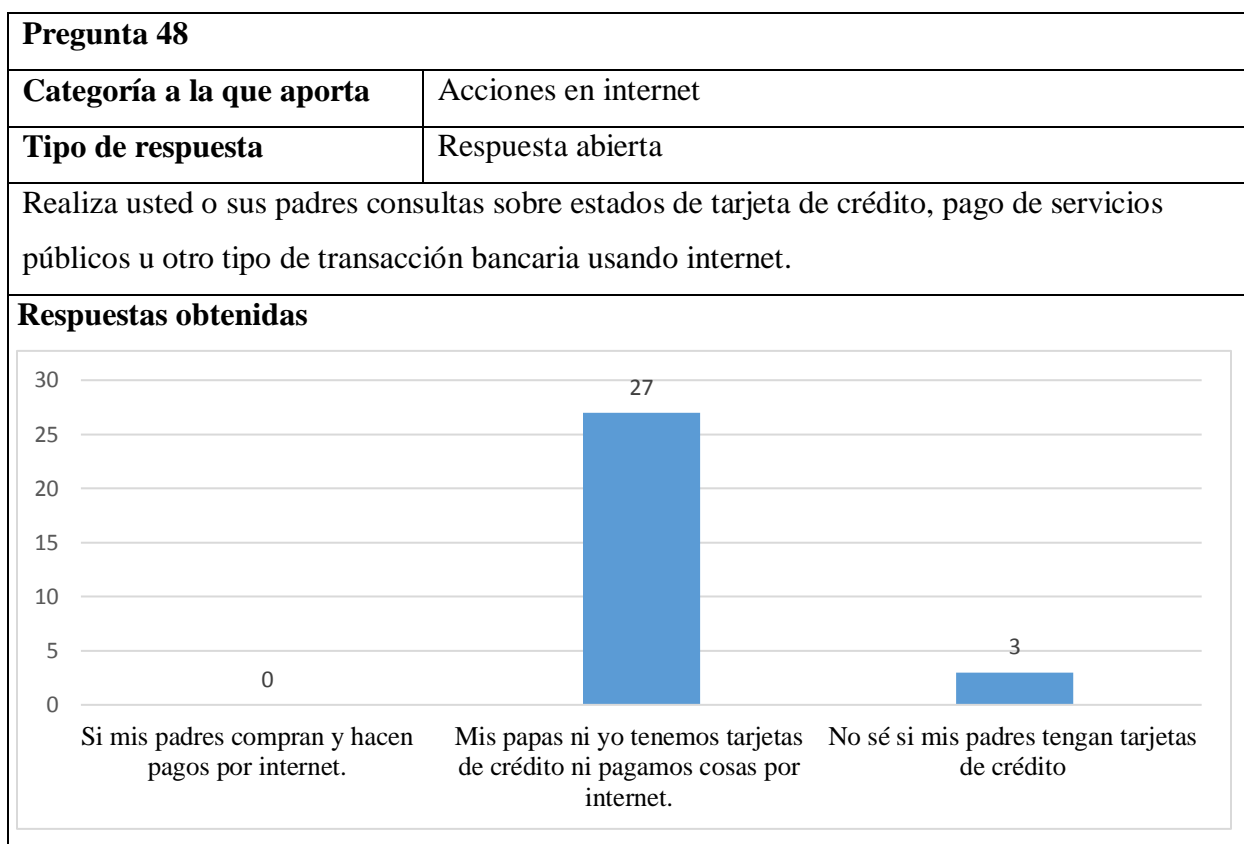
Pregunta 45

Categoría a la que aporta	Acciones en internet
Tipo de respuesta	Opción múltiple

si está chateando en alguna de sus redes sociales y por casualidad alguien le envía un mensaje como este, usted

**Respuestas obtenidas**





Anexo 2 pantallazos del material educativo computacional.

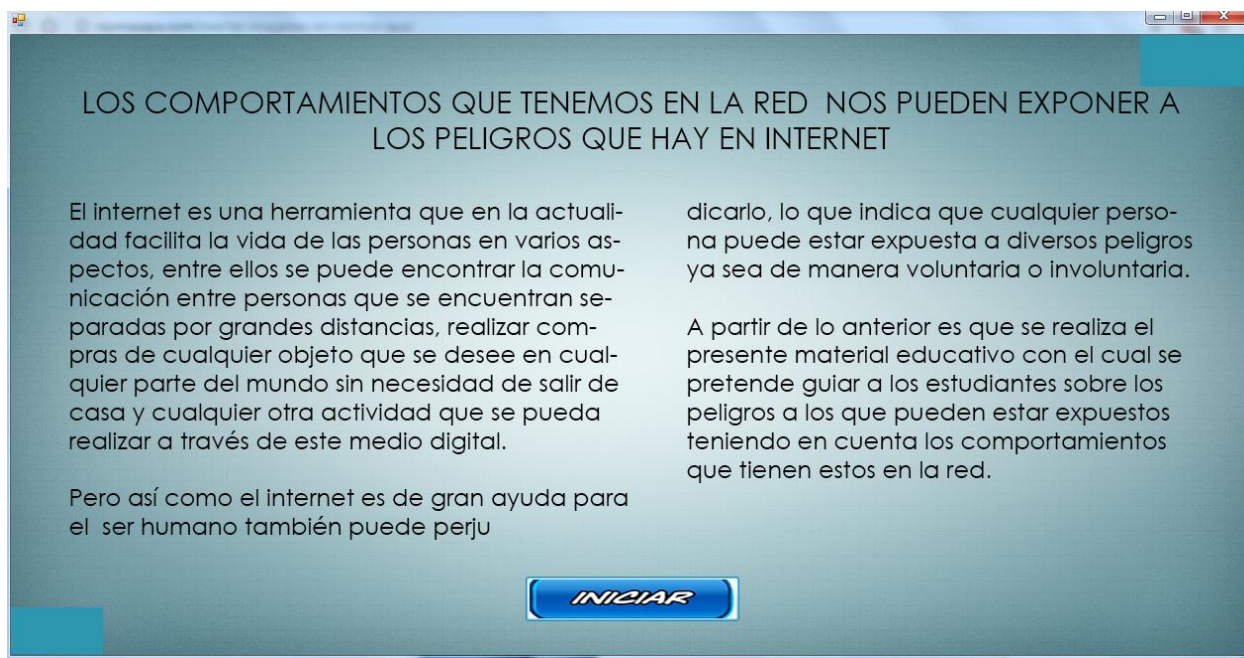


Imagen 1. Ventana 1 del material educativo computacional, en esta se encuentra una breve introducción del material.

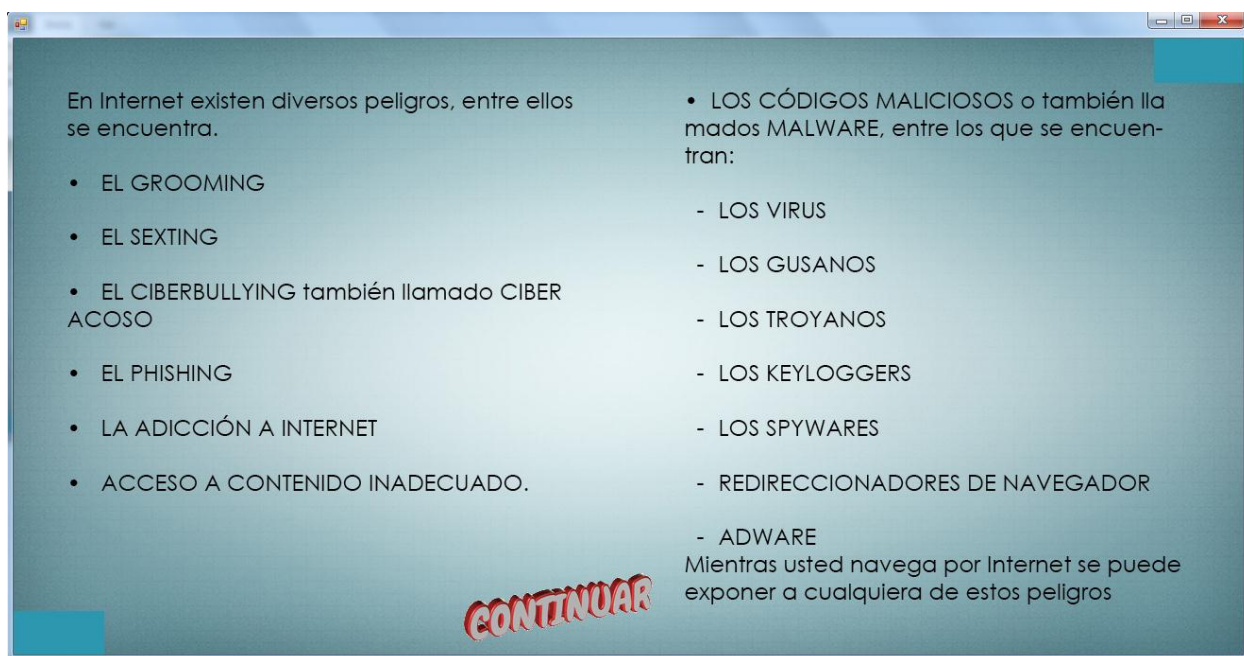


Imagen 2. Ventana 2 del material educativo computacional, en esta se encuentra una lista de todos los peligros existentes en internet.

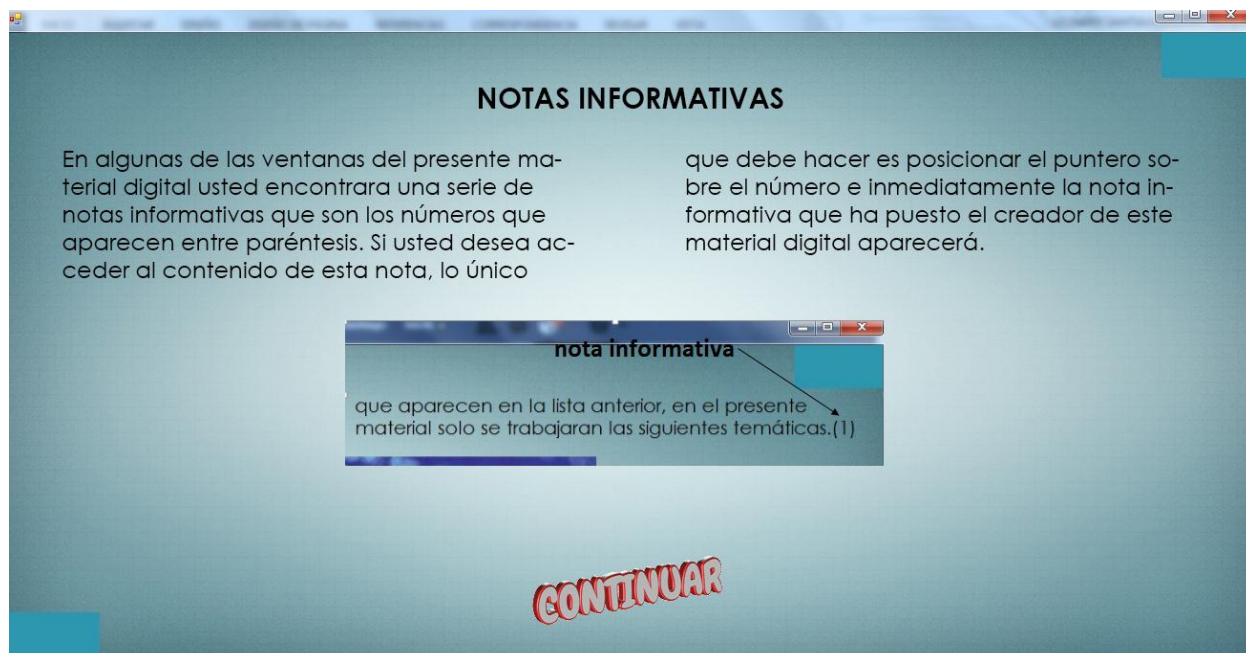


Imagen 3. Ventana 3 del material educativo computacional aquí se informa como observar notas aclaratorias que contiene el material en ciertas ventanas.

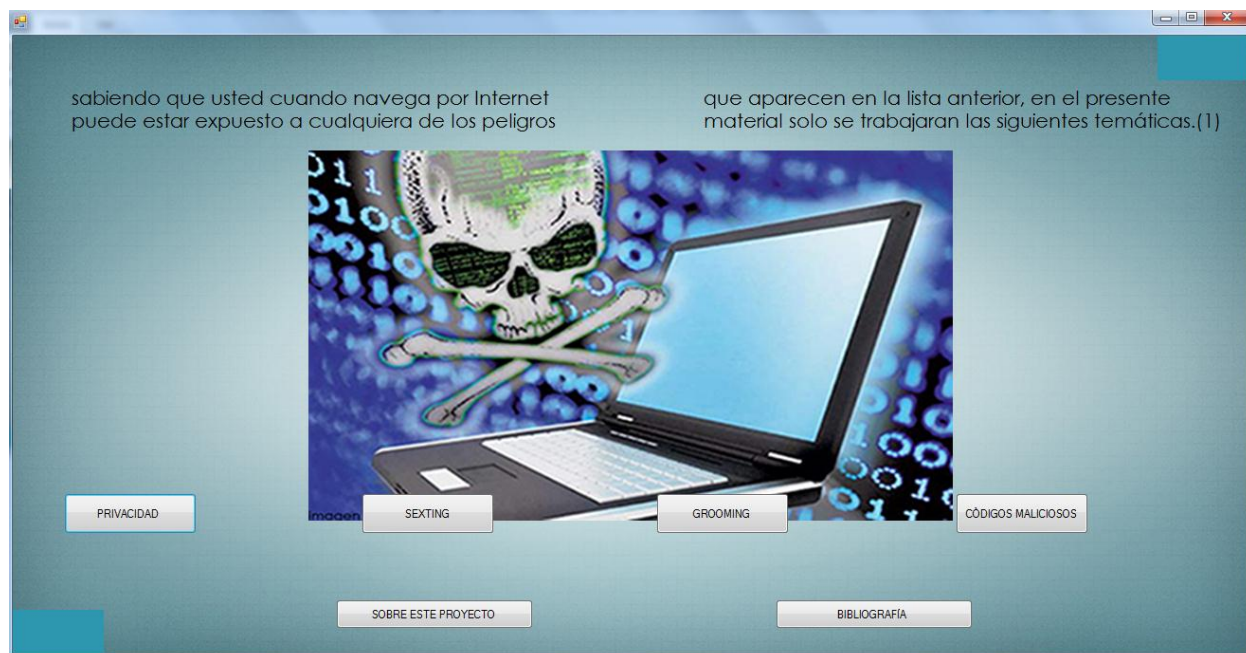


Imagen 4. Ventana 4 del material educativo computacional este es el menú principal del material

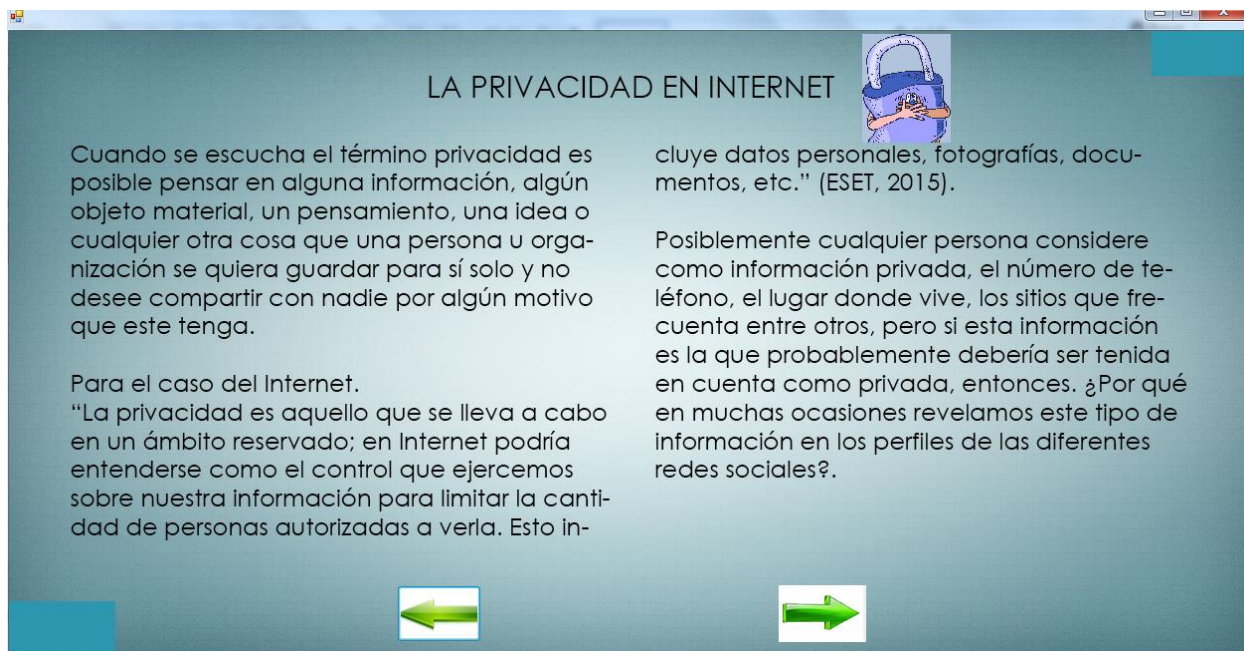


Imagen 5. Ventana 1 del material educativo computacional de la temática privacidad en internet

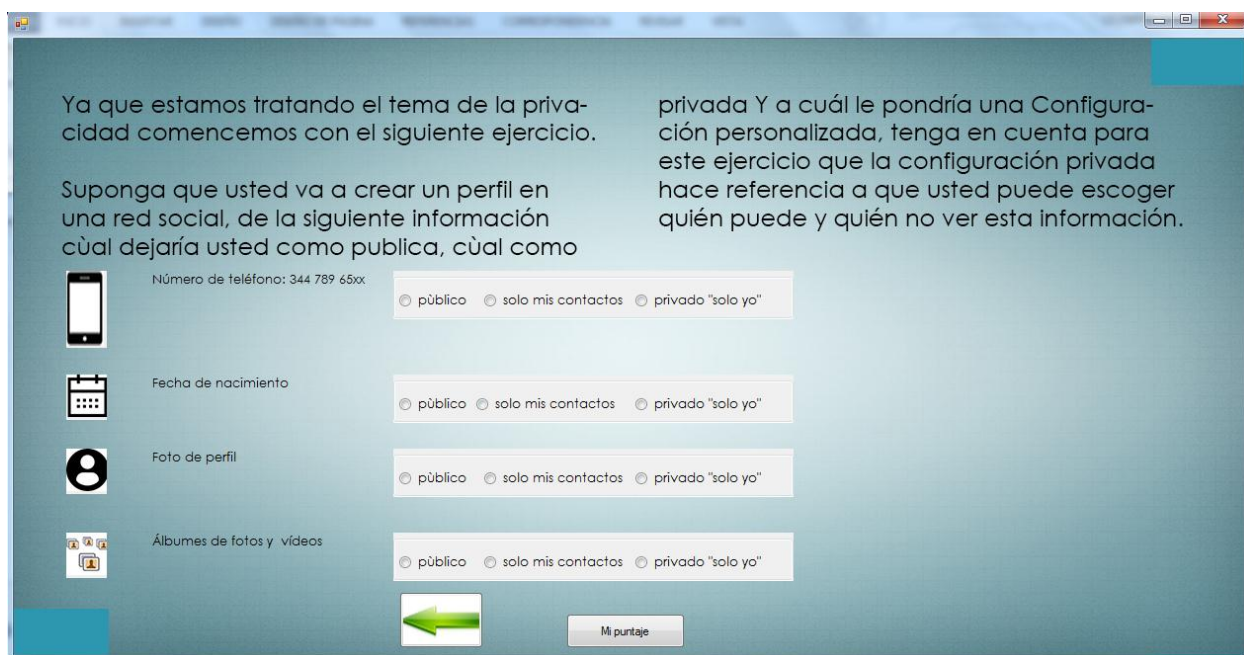


Imagen 6. Ventana 2 del material educativo computacional de la temática privacidad en internet

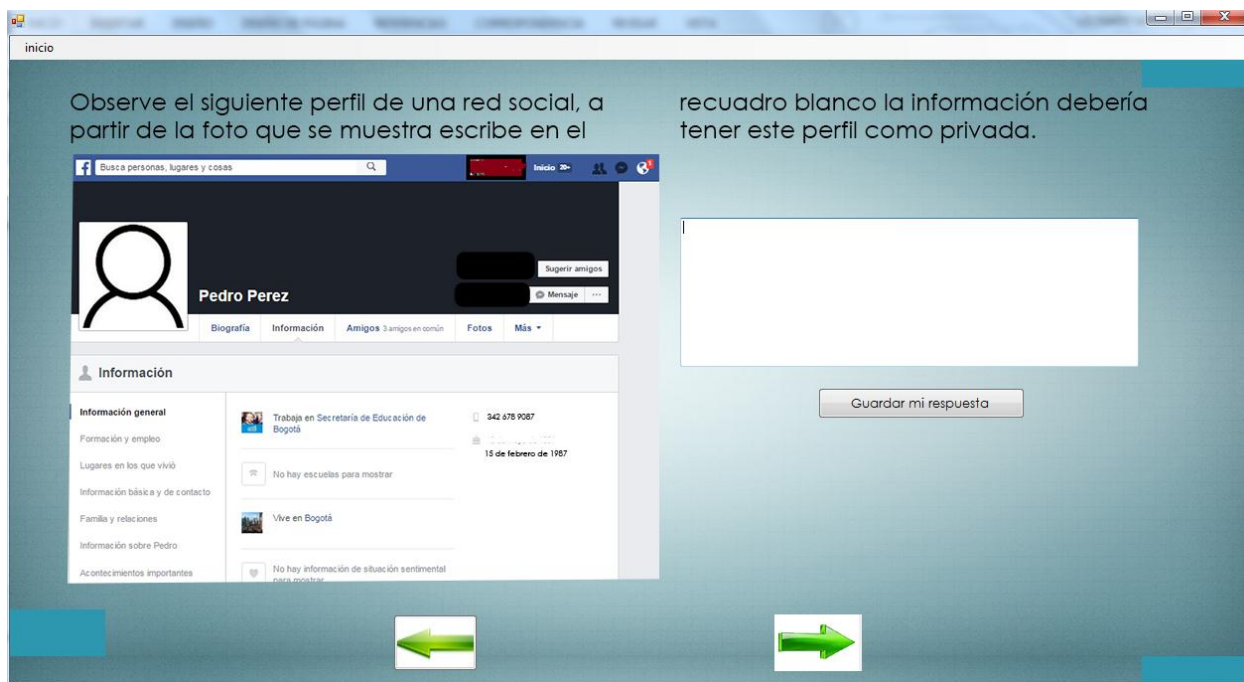


Imagen 7. Ventana 3 del material educativo computacional de la temática privacidad en internet

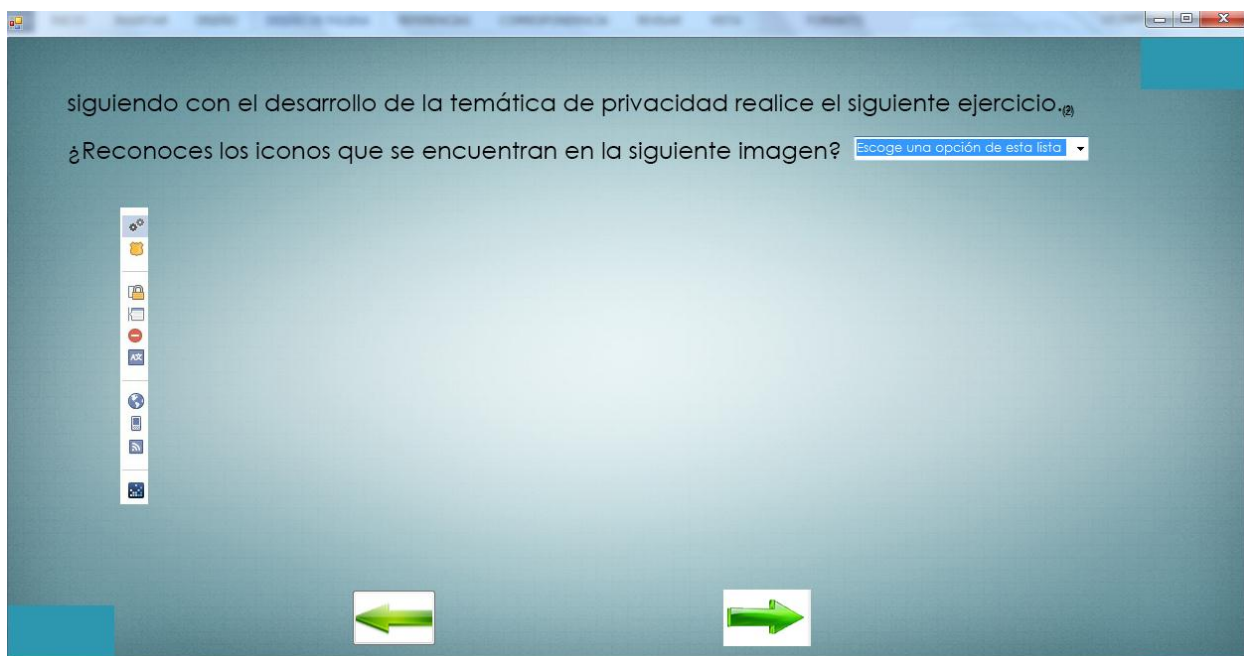


Imagen 8. Ventana 4 del material educativo computacional de la temática privacidad en internet

Entre las diversas configuraciones de seguridad que se pueden realizar en Facebook, se encuentra la configuración de privacidad.

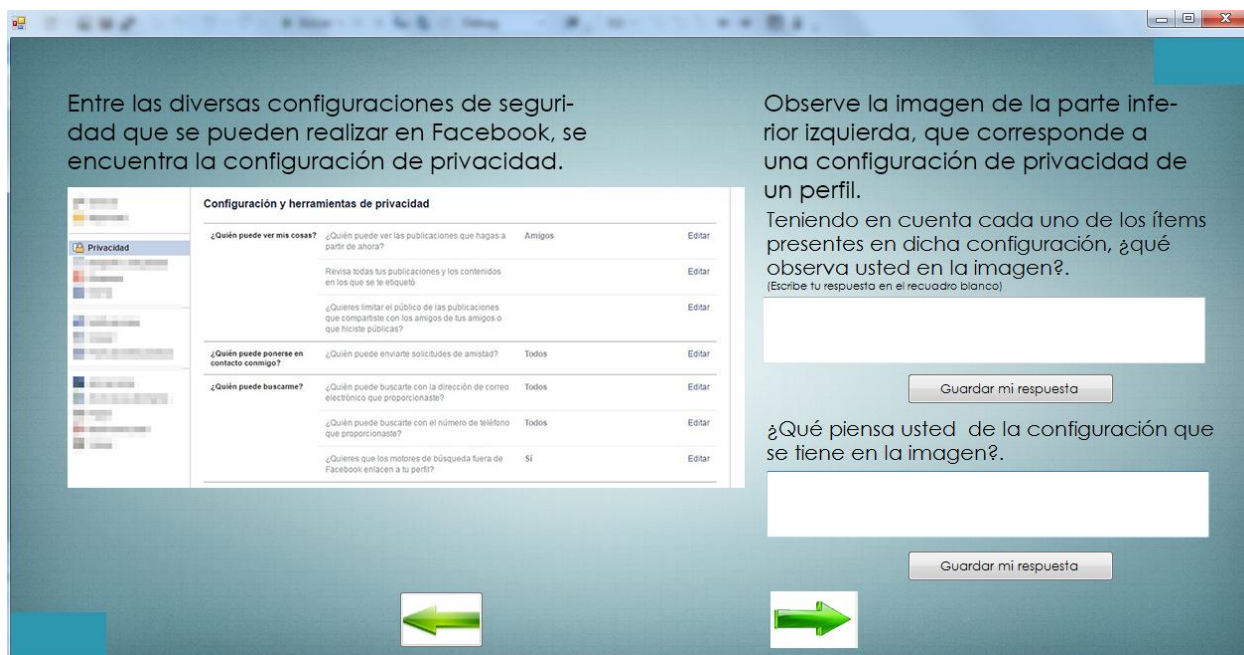
Observe la imagen de la parte inferior izquierda, que corresponde a una configuración de privacidad de un perfil.

Teniendo en cuenta cada uno de los ítems presentes en dicha configuración, ¿qué observa usted en la imagen?
(Escribe tu respuesta en el recuadro blanco)

Guardar mi respuesta

¿Qué piensa usted de la configuración que se tiene en la imagen?
(Escribe tu respuesta en el recuadro blanco)

Guardar mi respuesta



The image shows a screenshot of a Facebook privacy settings window. On the left, there is a sidebar with 'Privacidad' selected. The main content area is titled 'Configuración y herramientas de privacidad' and contains several settings with 'Editar' buttons. Below the settings, there are two green arrows pointing left and right. On the right side of the window, there is instructional text in Spanish, a question about the configuration, a white text input box, a 'Guardar mi respuesta' button, another question about the configuration, another white text input box, and another 'Guardar mi respuesta' button.

Configuración y herramientas de privacidad		
¿Quién puede ver mis cosas?	¿Quién puede ver las publicaciones que hagas a partir de ahora?	Amigos Editar
	Revisa todas tus publicaciones y los contenidos en los que se te etiquetó	Editar
	¿Quieres limitar el público de las publicaciones que compartiste con los amigos o que hiciste públicas?	Editar
¿Quién puede ponerse en contacto conmigo?	¿Quién puede enviarte solicitudes de amistad?	Todos Editar
¿Quién puede buscarme?	¿Quién puede buscarte con la dirección de correo electrónico que proporcionaste?	Todos Editar
	¿Quién puede buscarte con el número de teléfono que proporcionaste?	Todos Editar
	¿Quieres que los motores de búsqueda fuera de Facebook enlacen a tu perfil?	Si Editar

Imagen 9. Ventana 5 del material educativo computacional de la temática privacidad en internet