

**HERRAMIENTA DE SOFTWARE PARA CONCIENTIZACIÓN DE RIESGOS DE
GROOMING POR MALA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
PERSONAL EN FACEBOOK**
(Trabajo de Grado)

SINDY CATALINA NIEBLES PARRA
NIXON DUVAN PIÑEROS MONTENGRO

Director:

Ing. Juliana Alejandra Arévalo, MSc

Codirector:

Ing. Edgar Camilo Camacho, MSc

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ, 2019

DEDICATORIA

El siguiente trabajo lo dedicamos principalmente a nuestros padres, quienes gracias a su amor y acompañamiento incondicional nos apoyaron durante todo el proceso de nuestra carrera, en segunda instancia a nombre de Nixon Piñeros a la Gobernación de Cundinamarca quienes fueron los impulsores económicamente para el proceso de la matrícula por medio del programa 4*1 opción de vida.

AGRADECIMIENTOS

Nuestros agradecimientos van dirigidos principalmente a nuestros directores de tesis, Juliana Arévalo quien nos guio durante todo el proceso de realización opción grado y quien se comprometió del todo con nuestro proyecto, al igual que el director Camilo Camacho quien nos brindó orientación y soporte con la realización de la herramienta del proyecto. Así mismo agradecemos a la Dirección de Responsabilidad Social Universitaria de la Universidad Santo Tomas que con su ayuda pudimos llegar a los diferentes colegios del proyecto. Por último, agradecemos a las instituciones educativas por recibirnos y permitirnos presentar nuestro proyecto y realizar las diferentes actividades con los estudiantes.

TABLA CONTENIDO

1	MARCO GENERAL DEL PROYECTO.....	12
1.1	OBJETIVOS	12
1.2	ALCANCE	12
1.3	METODOLOGÍA.....	13
2	IDENTIFICACIÓN DE RIESGOS EN REDES SOCIALES PARA ADOLESCENTES	15
2.1	Políticas de facebook.....	16
2.2	Políticas especiales para menores de edad.....	18
2.3	Manejo de las aplicaciones en facebook.....	19
2.4	Grooming en facebook	20
2.5	Herramientas e investigaciones contra el grooming.....	23
3	HÁBITOS DE LOS ESTUDIANTES EN REDES SOCIALES.....	25
3	HERRAMIENTAS DE SOFTWARE PARA EL DESARROLLO	30
3.1	LENGUAJES DE PROGRAMACIÓN Y MARCAS.....	30
3.1.1	Java.....	31
3.1.2	C/C++	33
3.1.3	HTML5.....	33
3.2	PLATAFORMAS ONLINE.....	34
3.2.1	Powtoon	34
3.2.2	APLICACIÓN INFORMATICA	35
3.2.3	Adobe Flash Player	35
3.2.4	Unity	36

3.2.5	Framework de Facebook	37
4	REQUISITOS FUNCIONALES DE LA HERRAMIENTA DE SOFTWARE.....	38
4.1	IDENTIFICACIÓN DE AUTORES.....	38
4.2	FUNCIONES DE LA APLICACIÓN.....	40
5	DESARROLLO DE LA HERRAMIENTA	41
5.1	ESPECIFICACIÓN DE REQUERIMIENTOS	41
5.1.1	API Facebook.....	41
5.1.2	Motor	41
5.1.3	SDK Unity Facebook	42
5.1.4	Unity WebGL	42
5.1.5	Alojamiento <i>web</i>	42
5.1.6	Browser	42
6	DEFINICIÓN GENERAL DE LA HERRAMIENTA	43
6.1	REQUERIMIENTOS DE LA HERRAMIENTA	44
6.1.1	Aplicación web.....	44
6.1.2	Integración web con funcionalidades, permisos de Facebook e impacto generado del proyecto	46
6.1.3	Integración web con funcionalidades	46
6.1.4	Permisos de Facebook.....	49
6.1.5	Revisión De Permisos De La Aplicación	50
6.1.6	Impacto Generado Del Proyecto.....	53
6.1.7	Socialización Y Recomendaciones Generales.....	54
7	INSTALACIÓN Y EJECUCIÓN DE LA HERRAMIENTA	57
7.1	INSTALACIÓN DE LA HERRAMIENTA.....	58
7.2	EJECUCIÓN DE LA HERRAMIENTA.....	59

8	IMPLEMENTACIÓN DEL PROYECTO, USO DE LA HERRAMIENTA Y RESULTADOS OBTENIDOS	61
9	CONCLUSIONES	65
10	TRABAJOS FUTUROS	67
	REFERENCIAS	68
	ANEXOS.....	76
	ANEXO A. CONSENTIMIENTO INFORMADO.....	76
	ANEXO B. ENCUESTA.....	78
	ANEXO C. RESPUESTAS PRUEBA PILOTO.....	81
	ANEXO D. TABULACIÓN DE RESPUESTAS PRUEBA PILOTO	88
	ANEXO E. INFORME DE CONSULTORÍA ESTADÍSTICA	98
	ANEXO F. TABULACIÓN DE RESPUESTAS DE LA MUESTRA ESTABLECIDA.....	102
	ANEXO G. LIENCIA ESTANDAR.....	122
	ANEXO H. GUIÓN PARA EL SOCIALIZADOR DE LA HERRAMIENTA	123
	ANEXO I. GUION PARA EL SOCIALIZADOR DE LA ACTIVIDAD	124
	ANEXO j. PRESENTACIÓN PARA EL SOCIALIZADOR DE LA ACTIVIDAD.....	129
	ANEXO K. TERMINOS Y CONDICIONES DE MONKEY COLLECTOR.....	134
	ANEXO L. ALGUNOS DE LOS CONCENTIMIENTOS INFORMADOS DEBIDAMENTE FIRMADOS POR LOS ACUDIENTES.....	136
	ANEXO M. VIDEO.....	137

Tabla de figuras

Figura 1. Lenguajes de programación principales Fuente:	31
Figura 2. Pacman en java	32
Figura 3. Ajedrez desarrollado en Java.....	32
Figura 4. Triki en java Netbeans	32
Figura 5. Ahorcado en c++.....	33
Figura 6. Mario Bros en C++/Allegro.....	33
Figura 7. Página principal de Powtoon	34
Figura 8. Animación de Personaje en Adobe Flash	36
Figura 9. Imagen de preparación de Unity	36
Figura 10. Interfaz de usuario de Unity	37
Figura 11. Relación entre actores dentro de la herramienta	39
Figura 12. Perfil del juego"Monkey Collector"	45
Figura 13. Daño causado al personaje	46
Figura 14. Proceso de Conexión entre el Api con el Token de Usuario.....	48
Figura 15. . Lista de permisos y funciones para agregar a la solicitud	51
Figura 16. Uso común del permiso "user_friends".....	52
Figura 17. Muestra de las Preguntas que exige Facebook para la Revisión de Funciones	52
Figura 18. Captura del video explicativo de las funciones que se Van a Usar	53
Figura 19. Imagen de Impacto	54
Figura 20. Imagen de socialización y Recomendaciones.....	55
Figura 21. Muestra del Video Tutorial	56
Figura 22. Pantalla de Inicio de "Te Protejo"	57
Figura 23. . Situaciones que se pueden Denunciar en la Aplicación	57
Figura 24. Built Settings WebGL.....	59
Figura 25. Diagrama de Red	60
Figura 26. Resultado de la pregunta #4.	62
Figura 28. Resultado de la pregunta # 10	62
Figura 29. Resultado de la pregunta # 12	63
Figura 30. Relación de algunas de las respuestas de la encuesta realizada.....	63

RESUMEN

El siguiente proyecto pretende beneficiar a estudiantes de dos de los colegios distritales oficiales de Bogotá de la localidad de chapinero, y a estudiantes del Instituto Técnico Olga Santamaría del municipio de Anolaima, entre 12 y 18 años, con el fin de mostrarles la importancia de cuidar sus datos personales en la red. Se realizó una prueba piloto, la cual brindó elementos claves para la creación de una herramienta tecnológica desarrollada sobre la red social Facebook. Dicha aplicación permite obtener datos personales de perfiles de Facebook, cuando el usuario haya iniciado sesión estará aceptando una serie de permisos que la aplicación a requerido antes de ser ejecutada, utilizando el protocolo OAuth. La interfaz gráfica de la aplicación se estudió con el fin de seleccionar una opción adecuada y llamativa para los adolescentes de los lugares escogidos, se desarrolló un juego. Una vez creada la aplicación se pretende generar un impacto social (validado en forma de entrevistas) en los estudiantes a través de la socialización, de tal manera que vean que la información personal puede ser usada para fines diferentes a los que el usuario desea en las redes sociales como Facebook. En este caso se proyectó enfocar la problemática del Grooming.

Palabras clave: Grooming, Red social, Aplicación informática, Adolescentes, Términos y Condiciones

ABSTRACT

The following project targeted students of two official schools in Bogotá, (Chapinero sector) and students of the **Olga Santamaria Technical Institute** in the municipality of Anolaima (Cundinamarca), between ages 12 to 18. A pilot test was carried out which provided key elements for the creation of a software tool developed to be used with the social network Facebook. The application allows you to obtain personal data from Facebook profiles, when the user logs in with OAuth protocol. The graphic interface of the application was studied in order to select the most appropriate and striking option for the adolescents of the chosen places. Once an application was created, a social impact has been generated on the students through socialization (measured using interviews), so that the personal information

can be used for unlegitimed purposes of the social networks, such as Facebook. In this case, it is intended to focus on the problem of grooming.

Keywords: Grooming, Social network, Computer application, Adolescents, Terms and Conditions.

INTRODUCCIÓN

La información que es publicada en redes sociales online (OSN) por sus siglas en inglés (*online social network*) como Facebook, es susceptible a tener un mal uso por personas malintencionadas, que se aprovechan del propósito real de la red, de la vulnerabilidad de algunas funciones, o el desconocimiento de los usuarios de las restricciones de seguridad que pueden implementar. Un ejemplo de esas restricciones es quien puede ver la información: solo amigo, amigos de los amigos o todo el mundo. La OSN es una manera fácil para los delincuentes adquieran la información que necesitan para cometer el delito, pues ahí se encuentra toda clase de personas, como por ejemplo menores de edad, siendo este el blanco para los groomers¹. Además le permite una gran cantidad de ventajas para estos atacantes, como, por ejemplo, la información real de las víctimas, lugares visitados con frecuencia, fotos e imágenes que revelan la personalidad de los jóvenes etc. Aunque muchos de los usuarios de Facebook tengan su información personal o publicaciones bajo restricciones de seguridad, las aplicaciones llamativas como juegos, encuestas u otras en esta red social, tienen acceso a la información ya que este tipo de aplicaciones solicitan los datos registrados en la cuenta de Facebook desde el momento que se aceptó las condiciones y restricciones.

Frente a esta situación planteamos la siguiente pregunta problema ¿Cómo concientizar a los adolescentes de los riesgos de grooming por mala gestión de seguridad de la información personal en Facebook con una herramienta de software?

¹ Groomer, son aquellas personas adultas que engañan a adolescentes para tener una satisfacción sexual ya sea violación u obtención de fotos íntimas.

1 MARCO GENERAL DEL PROYECTO

1.1 OBJETIVOS

Elaborar una herramienta de software de concientización de riesgos de Grooming por mala gestión de seguridad de la información personal de las aplicaciones en Facebook, para estudiantes de secundaria.

- Identificar los riesgos de Grooming por mala gestión de seguridad de la información personal en la red social Facebook, en cuanto al uso de la información utilizada por parte de las aplicaciones montadas en la red social Facebook, en el momento de ser utilizadas por los usuarios estudiantes de colegios de secundaria.
- Realizar un sondeo sobre hábitos en redes sociales de la población objetivo para identificar las generalidades de la percepción de seguridad en Facebook.
- Establecer las diferentes herramientas de software disponibles para la elaboración de la herramienta tecnológica y seleccionar la más adecuada.
- Establecer los requisitos funcionales de una herramienta de software, que permita concientizar a estudiantes de colegios sobre los riesgos de Grooming, por mala gestión de la seguridad de información personal, identificados en la red social Facebook.
- Desarrollar y aplicar la herramienta de software en una población de al menos 100 estudiantes de secundaria.

1.2 ALCANCE

Revisión bibliográfica sobre los peligros de Grooming para los adolescentes en OSN, particularmente a través de la red social Facebook.

Realización de encuestas a forma de sondeo, a través de medios virtuales y/o visitas físicas para identificar las generalidades de la percepción de seguridad en Facebook de la población objetivo.

Desarrollo de la herramienta de software que consiste en una aplicación de Facebook que atraiga la atención de la población objetivo y obtenga información personal al solicitar autorización de acceso a los datos. Una vez obtenida la información se presentará una animación que mostrará todo lo que se puede llegar a hacer con esta información en caso de que cayera en manos de un Groomer. Adicionalmente se mostrará cómo manejar las configuraciones de seguridad de Facebook.

Integración de herramientas y uso de estas para socializar con los adolescentes en grupos, alcanzado al menos 83 jóvenes, por medio de la visita a colegios a través de los centros de proyección social de la universidad y al menos en un colegio departamental del municipio de Cundinamarca.

1.3 METODOLOGÍA

Este es un proyecto enmarcado en la estrategia de Desarrollo Comunitario de la Unidad de proyección social que busca promover conciencia en una población específica, con la ayuda de una herramienta tecnológica o aplicación. Este proyecto tiene como objeto de estudio basado que relaciona el comportamiento de un grupo de personas. Permitiendo examinar por valores numéricos de encuestas, experimentos, entrevistas y estudios estadísticos, para así estudiar el problema social al que están enfrentados los jóvenes con el mal uso de las OSN. Con proposición a dar una solución al problema se realizará y se entregará una herramienta a un grupo social o comunidad.

A continuación, se describen los módulos de trabajo del proyecto:

1. Revisión bibliográfica sobre los riesgos de Grooming por mala gestión de seguridad de la información personal en la red social Facebook, a los que están expuestos estudiantes de colegios de secundaria, además, se revisará el marco normativo, en

cuanto a la utilización de los datos personales de los estudiantes, como objetivo de prueba y concientización.

2. Se identificarán los hábitos por medio de una encuesta piloto, teniendo varios factores críticos como la inseguridad, la poca importancia a proteger las publicaciones en las OSN etc.
3. Se identificarán las estrategias tecnológicas que se pueden usar para llamar la atención de los adolescentes. Se tendrá en cuenta: ¿Qué motiva a la población? y ¿Qué herramienta les llamaría la atención?, así mismo realizar una revisión de término y condiciones sobre las políticas y herramientas de seguridad que usa Facebook.
4. Selección de la tecnología para el desarrollo de la aplicación: Una vez en esta investigación haya identificado los comportamientos de los estudiantes en OSN al igual que las estrategias para dirigirse a la población objetivo, se procede a seleccionar la plataforma o lenguaje de programación donde se realizará una aplicación (herramienta tecnológica) para así poder ejecutada en la red social Facebook.
5. Desarrollo y diseño de la herramienta: Con base a los estudios realizados, se desarrollará y creará la aplicación didáctica, donde los jóvenes puedan visualizar como sus datos personales pueden ser obtenidos fácilmente por los delincuentes.
6. Utilizar la herramienta: Realizar una visita a los colegios seleccionados para socializar la herramienta y validar su impacto a través de entrevistas a estudiantes y docentes. Se pretende, llegar a al menos 83 niños y/o adolescentes los cuales son la muestra total de una población total de los dos colegios.

Nota: No todas las actividades se van a realizar en forma secuencial.

2 IDENTIFICACIÓN DE RIESGOS EN REDES SOCIALES PARA ADOLESCENTES

El objetivo de las OSN está en compartir una serie de elementos que se basa en la información personal dentro de un grupo social usuarios o cuentas vinculadas como amigos, con el fin de establecer comunicación entre sus usuarios y relaciones de interés entre diferentes grupos o comunidades. Sin embargo, también genera una gran brecha en la seguridad de la información personal, pues son elementos informáticos vulnerables al mal uso que le pueden dar los usuarios. Facebook estableció la función de amigos en su plataforma como la manera de que los usuarios pueden relacionarse con otros usuarios, permitiendo tener acceso a cierta información que es publicada entre los usuarios que conforman una conexión de amistad en la red. El vínculo de amistad es creado cuando un usuario envía una solicitud de amistad desde su perfil y el otro usuario la acepta. La información que es publicada en OSN como Facebook entre el vínculo de amistad de los usuarios está relacionada con el nombre real del usuario, direcciones de lugares donde trabaja, estudia y vive; publicaciones de fotos, lugares visitados, sentimientos y emociones.

Sin embargo, nuestro estudio² ha identificado que muchos de los usuarios de las OSN, no conocen en el mundo real a todos sus amigos de la red, es un gran número de contactos o amigos de la red a quienes se les confía muchas de las cosas que se hacen a diario, pues se hacen publicaciones que a veces sin querer se trasmite información que vuelven vulnerable al usuario. Por ejemplo, fotos donde se está compartiendo con toda su familia en algún viaje un fin de semana, dejando ver que sin intención que su casa está sola, o algún miembro de su familia se encuentra allí y este podría correr peligro. Es por eso que como usuario de las OSN se debe tener sospecha de quien se acepta como amigo, de la información que se está publicando, de los ajustes de privacidad que brinda la red, etc. (‘INVERSIA - Stadio Alicante, 2013)

De acuerdo con el artículo (MILENIO - KATIA LEYVA, 2017) la edad apropiada para que un joven adolescente acceda al mundo de la OSN, debe ser a los 14 años, pues algunos

² Ver encuesta del ANEXO B

factores como la comunicación oral tiende a degradarse ya que los jóvenes pierden esta habilidad para expresarse y prefieren hacerlo frente a un aparato electrónico. Además, el estado emocional es otro elemento que entra en juego con los adolescentes que tienden a disminuir su autoestima, debido a que los usuarios de las OSN en sus publicaciones intentan presumir y esto genera sentimientos de frustración en algunos jóvenes, sintiendo que la vida de ellos no tiene nada comparada con los demás o simplemente genera cambios bruscos en su personalidad.

Pasar demasiado tiempo en las OSN tanto para los jóvenes como para los adultos, es una conducta que conlleva, a la adicción, puesto que a la permanencia de estar conectado en línea en las OSN conlleva a un problema social en el que las personas prefieren hablar por medio de dispositivos y no frente a frente con otra persona (ALEJANDRA MONTES SOTELO, 2016). El uso de la tecnología no es el problema, el problema radica en el uso desproporcionado y mal uso de estas herramientas, pues herramientas como Facebook permite a los usuarios un poco de esparcimiento, interactividad, comunicación y entretenimiento en lo usuarios. Según el artículo (Socidrogalcohol (Society) & Corral, 2010) los problemas más graves que enfrentan los usuarios son el acceso a contenidos inapropiados, el acoso o la pérdida de intimidad, debido a que las Facebook y las OSN se pueden crear perfiles falsos, permitiendo la potencialidad de engaño, autoengaño y fantasía. Además, se pierde el consentimiento de lo que es íntimo o de lo que es público; es por ello que los adolescentes juegan un papel de riesgo, así como los padres y los educadores deben formar un papel fundamental en la dirección y acompañamiento de los jóvenes. (p.90)

2.1 POLÍTICAS DE FACEBOOK

Facebook es una red social dedicada a personas mayores de 13 años como lo establece la ley del país de origen de la compañía, puesto que la ley de dicho país no permite el manejo de la información de los estos menores, de acuerdo con la ley COPPA por sus siglas en inglés Children's Online Privacy Protection Act (ley estadounidense de protección de la privacidad infantil en Internet), que se encarga de proteger la privacidad de los niños en internet. (LA COMISIÓN FEDERAL DE COMERCIO, 1998) COPPA prohíbe el almacenamiento de información de los menores de 13 años en las OSN, es por ello que Facebook se dedica a eliminar cuentas, dentro de su plataforma tiene la opción de que los

demás usuarios puedan denunciar cuentas de estos menores, pues Facebook lo considera una falta grave según un artículo de las políticas de Facebook “La creación de una cuenta con información falsa constituye una infracción de nuestras condiciones. Eso incluye las cuentas registradas en nombre de un menor de 13 años”. (Facebook 2018) Además, se estima que hay una población de 5,6 millones de niños infringiendo esta norma por lo que para el año 2012, Facebook eliminó para ese año a 800.000 usuarios menores de 13 años a través de un proceso de selección por niveles, proceso que no se ha destacado según lo describe este artículo. (EXPANSION con alianza CCN, 2012). En la actualidad no se sabe cuál es el reporte de cuentas de niños menores según Mary Aiken's en su libro *The cybert effect* del 2016.

Facebook dentro de sus normas y políticas se preocupa por evitar que algún tipo de contenido infrinja incomodidad para el resto de los usuarios es por eso que ha establecido botones que permitan denunciar y alertar contenido abusivo en sus páginas y publicaciones. Cuando el caso sea denunciado es decir dicha publicación como contenido inapropiado, ya que para el usuario es ofensivo y grosero, el equipo de seguridad de la compañía se encargará de estudiar y revisar para determinar si el contenido debe ser eliminado de su plataforma. (Phillips, Baird, & Bj, n.d.)

Entre las medidas de prevención que toma Facebook frente a casos de bullying, explotación sexual y contenido que anime al suicidio o al daño así mismo, su primera acción a intervenir es con la eliminación de este contenido; Facebook reporta a National Center for Missing and Exploited Children (NCMEC) en colaboración del grupo de expertos y el consejo asesor de seguridad de Facebook cuando el caso es identificado como desnudos de menores de edad en publicaciones de Facebook; cuando el caso es referente al suicidio Facebook cuenta con organizaciones a nivel mundial para tratar estas personas. (facebook 2018)

Facebook también cuenta con otro botón o sección llamada “conectar”, este es el encargado de configurarse de acuerdo con el usuario predetermine quien podrá ver su información publicada, es decir “Todos”, “Amigos de amigos”, “Sólo amigos”, “Recomendada” (que es el ajuste predeterminado) o “Personalizada”. Aplicaciones y sitios web es otra sección de la seguridad que brinda Facebook, pues otras compañías de aplicaciones como juegos y motores de búsqueda como Google, obtiene información de la cuenta de Facebook cuando se está trabajando en conjunto, es decir se obtiene información

de Facebook para hacer procesos más rápidos como el registro en App de juegos. En la sección de aplicaciones se podrá ver sus aplicaciones, eliminar las que no desee usar o desactivar la plataforma por completo para la transferencia de información. Bloqueados en esta sección se puede bloquear a personas de la lista de amigos o personas concretas para que no se interactúen con su información ni se puedan comunicar (Phillips et al., n.d.).

2.2 POLÍTICAS ESPECIALES PARA MENORES DE EDAD

Facebook se encarga de mostrar diversas funciones como mensajes o anuncios que les recuerda con quien se está compartiendo información y limita comunicación e interacción con los desconocidos, además informa de las consecuencias al momento de hacer pública la información. La información relevante como fecha de nacimiento, colegios, sea abstenida y relacionada con las búsquedas por otros usuarios. Los menores de edad no disponen de una búsqueda pública en los motores de búsqueda como Google, caso contrario sucede con los mayores de edad que pueden ser buscados por este método. Cuando los menores de edad establecen dentro de sus configuraciones su perfil “todos” la función de quien puede ver sus publicaciones e información esta es bloqueada y solo “Amigos de amigos” y “Sólo amigos” pueden ver información del menor. (Facebook 2018b)

Los ajustes de compartir la ubicación para menores de edad, está predeterminado en modo desactivado, sin embargo, los menores pueden activar la ubicación y ser pública, pero cuando el menor realiza la acción de activar, Facebook da como alerta que se está compartido la ubicación (Facebook 2018b). Esta función es particularmente peligrosa pues facilita a posibles groomers identificar la ubicación de los niños, niñas o adolescentes.

Facebook brinda la opción de denunciar las cuentas de los menores 13 años mediante el servicio de ayuda de Facebook en él, que se ingresa el link de la cuenta del menor par que Facebook estudie dicha cuenta y pueda ser eliminada. En caso de que los jóvenes menores de edad se vean involucrados en retos o aplicaciones que el menor no quiera hacer uso, Facebook tiene la opción de configurar etiquetas antes de ser expuestas en su muro o perfil. (Facebook 2018a)

2.3 MANEJO DE LAS APLICACIONES EN FACEBOOK

Las OSN se han convertido en grandes bases de datos, que en ocasiones la información recolectada ha sido beneficiosa y necesaria para ser compartida en cuanto a datos de interés como análisis técnicos, claves en sociología moderna, geografía, economía, ciencia de la información entre otros.(Ninggal & Abawajy, 2011)

Facebook es la red social más grande del mundo, pues es la más utilizada con 2.167 millones de usuarios activos según (Ana Martín del Campo, n.d.) blog que describe cuáles son las OSN más utilizadas, de acuerdo con un Estudio Anual de OSN en España de 2018. Esto confirma que es una de las bases de datos más grandes, teniendo información de un usuario de cada cuatro personas en el mundo. Facebook además de ser una plataforma social, es una plataforma de interfaces programables que permite publicar juegos y aplicaciones informáticas (app) para uso de sus propios de usuarios. Sin embargo, muchas de estas aplicaciones pueden acceder a información de quienes se registran o utilizan estas apps como por ejemplo un horóscopo app que necesita de la fecha de nacimiento del usuario. Sin embargo, el problema radica en el acceso a la información por parte de los desarrolladores que pueden manipular la información en grandes masas o personales, aunque Facebook confía en estos desarrolladores y los datos que les brinda, es decir, que este tipo de datos no los usen de manera equivocada, como: enviar spam, fines propios, fines comerciales (facebook, 2019).

Las pasadas elecciones del 2016 de Estados Unidos, Facebook se encontró en un escándalo debido a la gran filtración de datos de votantes por parte de la compañía Cambridge Analytica dedicada al análisis de datos para campañas electorales. Cambridge Analytica con ayuda del señor Aleksandr Kogan, un profesor de la University of Cambridge creador de una app llamada "thisisyourdigitallife" encargada de tomar pruebas de personalidad donde aproximadamente 270 mil personas participaron siendo el blanco para obtener información mediante la aceptación de los términos y condiciones que exigía la app. (BRIAN X. CHEN, 2018)

Cambridge Analytica obtuvo información de más de 50 millones de perfiles de usuarios, para identificar sus cualidades como votantes en las elecciones y así orientar anuncios específicos hacia ellos. El candidato Donald Trump, presidente del Gobierno de los Estados

Unidos al día de escritura de este documento, aprovechó toda la información para poder asistir en zonas específicas para hacer campaña. Los 270 mil perfiles utilizados fueron suficientes para llegar a la información de más de 50 millones de personas, pues las personas que utilizaron la app dieron los permisos suficientes para acceder a los datos de sus amigos vinculados, por ejemplo, si el usuario que hizo uso de la aplicación tenía en su momento 500 amigos, Cambridge Analytica tendría la información del usuario y de sus 500 amigos. (SHERR, 2018). Vale la pena mencionar que después de que estas pruebas vieron la luz en 2018, Facebook reforzó sus políticas de seguridad para el uso de información personal.

2.4 GROOMING EN FACEBOOK

“Sexual Grooming” (se traduce del inglés como preparación en online³) es el proceso que realizan los pedófilos en las OSN con el fin de establecer una relación y un control emocional de los niños o jóvenes menores de edad que lo conllevan a una preparación de acoso sexual online. (Marcelino Madrigal, 2012). Uno de los procesos más comunes en la preparación online de los niños parte desde el momento que los Groomers suplantando su identidad y su edad en la OSN para aparentar una edad igual a la de la víctima con el objetivo de acercarse y hacerse amigo por la OSN. El objetivo de los Groomers es realizar actividades sexuales, empezando con conversaciones que comprometen actos o palabras sexuales, para luego acceder a intercambio de fotos y videos de sus cuerpos desnudos. Finalmente, los pedófilos o Groomers proceden al acto sexual con los niños físicamente.

Los niños y niñas están expuestos desde la misma forma, sin embargo, hay una especial vulnerabilidad en los niños que son homosexuales, su probabilidad de utilizar las OSN para desarrollar y explorar su sexualidad los hace más susceptibles al peligro del Grooming sexual. Otro grupo de niños que se ven afectados como víctimas de Grooming y que sobresalen más al peligro, es aquel grupo de niños que presenta enfermedades psicológicas como psicopatológicos. Así lo revela el artículo (Montiel, Carbonell, & Salom,

³ Preparación online, es el término para referirse al proceso y estructura planeada por el delincuente para acercarse a los niños mediante la red social.

2014) de acuerdo a una serie de estudios citados en su desarrollo, destacando los niños más vulnerables a sexual Grooming.

El siguiente estudio realizado por (Whittle, Hamilton-Giachritsis, & Beech, 2014) identificó algunos de los factores que contribuyen a la vulnerabilidad de una persona joven hacia la preparación en línea, de acuerdo con el estudio realizada en 8 víctimas de Grooming, según el estudio, el papel de la familia juega mucha a favor de los jóvenes, pues 6 de las víctimas no tenían un núcleo familiar estable, sus padres se encontraban separados. La baja autoestima es otro de los factores que se identificó en las víctimas, las víctimas indicaron sentir un punto de bajo en la vida llegándose a sentir solas, factor que las llevó a refugiarse en alguien desconocido. La escuela fue un último factor en este caso a favor, las víctimas aclararon que en algunas ocasiones se había advertido de los peligros que se podían encontrar en internet.

Un estudio realizado a 12 hombres condenados por el delito de sexual Grooming, Los resultados muestran cómo los agresores estudian activamente el entorno cotidiano, las necesidades y vulnerabilidades de los menores. Los agresores se adaptan mediante el uso de las estrategias como la persuasión con argumentos de tal forma que los niños actúen o piensen de un modo determinado, de tal forma que el niño no pueda salir y el agresor pueda mantener al niño bajo presión y chantaje. Los participantes en este estudio fueron 12 hombres condenados en las cárceles españolas, que habían perpetrado contactos sexuales contra menores que tenían menos de 16 años, Los agresores tenían edades entre 21 y 51 años de edad. Los agresores definieron internet como el entorno facilitador para la preparación online de los niños, además aseguraron robar identidades de otros niños para parecer más convincente. Una vez los agresores logran contactarse con los jóvenes o niños menores, retroalimentaron su entorno, tales como los adultos se interesaron en los elementos estructurales de la vida cotidiana de los niños, tales como horarios, actividades o cuidadores disponibles. Los adultos sabían detalles importantes sobre de conflictos de la situación de los niños con la familia. Los perfiles de los adultos se caracterizaban por los cientos de amigos que tenían, en diferentes redes como Facebook, Badoo entre otras. (de Santisteban, del Hoyo, Alcázar-Córcoles, & Gámez-Guadix, 2018)

En un estudio se analizaron cinco series de casos, que comprenden 29 transcripciones de 22 interacciones, utilizando el enfoque cualitativo del análisis temático. Los informes

policiales se revisaron para obtener información descriptiva y específica de cada caso. Los cinco delincuentes eran hombres de entre 27 y 52 años, y el número de niños con los que se comunicaron varió de uno a 12. Las víctimas tenían entre 11 y 15 años, y ambos eran mujeres ($n = 17$) y hombres ($n = 6$), donde n es el número de participantes. Los hallazgos revelaron que los delincuentes emplearon un enfoque indirecto o directo a las conversaciones con las víctimas y el inicio de contacto con ellas. El enfoque de los delincuentes empleados también se reflejó en los tipos de estrategias que utilizaron. Solo se encontró que dos delincuentes participaban en aspectos de Grooming sexual como parte de un enfoque indirecto; la mayoría de las interacciones de los otros tres delincuentes, que carecían por completo de características de deseo sexual, se consideraron de un enfoque directo. Estos hallazgos se discuten en relación con los problemas actuales que rodean la terminología y la definición de Grooming sexual, así como las implicaciones teóricas y prácticas, que concluyen con sugerencias para futuras investigaciones (Kloess, Hamilton-Giachritsis, & Beech, 2017).

El estudio en (Black, Wollis, Woodworth, & Hancock, 2015) consideró las similitudes y diferencias en el proceso de preparación en entornos en línea mediante el análisis del lenguaje utilizado por los delincuentes en línea al comunicarse con sus víctimas. Las transcripciones de 44 delincuentes convictos en línea se analizaron para evaluar una teoría propuesta del proceso de preparación en línea (O'Connell, 2003). Utilizando un enfoque basado en etapas, el análisis de texto computarizado examinó los tipos de lenguaje utilizados en cada etapa de la interacción delincuente-víctima. Las transcripciones también se analizaron en su contenido para examinar la frecuencia de las técnicas específicas que se sabe que son empleadas por delincuentes presenciales y en línea, como la adulación. Los resultados revelan que, si bien hay evidencia de las estrategias utilizadas por los delincuentes a lo largo del proceso de preparación en entornos en línea, el orden y el momento de estas etapas parecen ser diferentes. Los tipos (y el posible patrón subyacente) de las estrategias utilizadas en la preparación en línea respaldan el desarrollo de un modelo revisado para la preparación en entornos en línea.

La organización Pantallas Amigas, en su página publicó un artículo donde describe tres principales elementos para la prevención de un ataque de Grooming hacia los jóvenes de manera que los jóvenes puedan tomar conciencia: 1) Abstención de proporcionar

información comprometedor, 2) Mantener con seguridad elementos informáticos que puedan contener información de los niños, y por último 3) No caer bajo ninguna circunstancia en chantajes, desde luego lo mejor será dar aviso a un adulto mayor o a las autoridades (Flores Fernández, n.d.).

2.5 HERRAMIENTAS E INVESTIGACIONES CONTRA EL GROOMING

A Dark Side of Computing and Information Sciences: Characteristics of Online Groomers, es una investigación que se dedicó a identificar los patrones de comportamiento identificando en tres grupos. El primer tipo de Groomer identificado es el sujeto distorsionado delincuente. Los hombres de este grupo tenían creencias de apoyo ofensivas que implican ver el contacto con el joven como una "relación". El segundo tipo es el Groomer en línea adaptable. Este grupo de hombres tenía creencias de apoyo ofensivas que involucran sus propias necesidades y consideraban que la víctima era madura y capaz. Finalmente, el hiper-sexualizado un grupo de hombres se caracterizó por una extensa colección de imágenes indecentes de niños y un contacto importante en línea con otros delincuentes sexuales o grupos de delincuentes. (Gottschalk, 2011) Pero "Detectar a adultos que pretenden ser niños es un desafío difícil, tanto para los humanos como para las computadoras". (Ashcroft, Kaati, & Meyer, 2015) así lo describe el artículo donde se identifica patrones de escritura que se puede utilizar para detectar si un adulto se hace pasar por un niño en una conversación en la sala de chat. Los participantes se clasifican primero como niños o adultos, y luego se examina a cada niño y se distingue a los niños falsos de los niños genuinos. El enfoque en el que centran es un análisis de texto para distinguir a los adultos que se hacen pasar por niños.

La siguiente investigación propone un sistema de prevención para la preparación online de los Groomers, (Rybníček, Poisel, & Tjoa, 2013) propone que se debe tener un patrón de identificación de los comportamientos y manera de expresarse con los niños, además propone tres áreas a analizar en la OSN, contenido multimedia como fotos e imágenes con contenido pornográfico, contenido textual que se pueda identificar palabras potenciales de obscenidad en una sala de chat y por último, contexto social que hace referencia a información de un perfil en cuanto a la frecuencia de chat/mensaje, frase o mensaje promedio, cantidad de Me gusta recibidos o recibidos, cantidad de imágenes subidas, cantidad de invitaciones a eventos o tiempo de actividad. Las tres áreas a analizar son

propuestas para la funcionalidad de una herramienta en Facebook llamada watchdog. (Rybnicek et al., 2013)

En la actualidad la mejor herramienta para la prevención de ataques de Grooming, es la herramienta de la educación, con esta herramienta se puede crear múltiples políticas y programas de educación sexual, y recalcar sobre la responsabilidad y el uso adecuado de las herramientas de internet. (Iovelle, m.i., Soria, m.a. & García, 2014)

Actualmente en varios países como Argentina hay leyes las cuales sancionan contra este crimen, con el objetivo de proteger los derechos de niños y adolescentes. La ley 27.458 “Día Nacional de la lucha contra el Grooming”, declara como Día Nacional de la Lucha contra el Grooming el 13 de noviembre de cada año, desarrollando distintas actividades de información y concientización sobre este peligro, por parte del gobierno (Medina, 2018). Pero, lamentablemente en Colombia no hay leyes que tan específicas sobre este delito, aunque existen algunas que protegen la infancia en Colombia, por ejemplo: la Ley 1098 de 2006, garantiza a los niños y adolescentes su armonioso desarrollo para crecer en familia y comunidad, en un ambiente sano; la Ley 765 de 2002, busca proteger a los menores frente a los acosos sexuales y pornografía infantil, los cuales se encuentran en el Código de la Infancia y la Adolescencia (ICBF, 2019).

3 HÁBITOS DE LOS ESTUDIANTES EN REDES SOCIALES

Con el fin de identificar algunos hábitos de estudiantes de colegio, se planteó una encuesta inicial. Dicha actividad se realizó considerando que ninguno de esos datos será guardado y se usará para uso académico únicamente. Además, se cuenta con un “consentimiento informado” a los padres de los estudiantes, en donde se explique que se está realizando, la razón por la cual se necesita la información de su respectivo hijo(a) y la autorización que se brinda para adquirir los datos necesarios, el documento se encuentra en el ANEXO A.

Para poder establecer el sondeo de los hábitos de los adolescentes se dividió esta sección en dos partes: la primera, es una prueba piloto y la segunda, es una encuesta y análisis de resultados de la muestra definitiva. A continuación, se explica cada una de las partes:

En la primera parte se realizó una encuesta de forma electrónica (Formularios – Google), una encuesta es la manera más efectiva de obtener información, (Abascal, E., & Esteban, 2005) la llamamos prueba piloto ya que se hizo en adolescentes entre el rango de edades (12 y 18 años) pero no se realizó en los colegios beneficiados (Abascal, E., & Esteban, 2005). Ver ANEXO B.

La facultad de Estadística de la Universidad Santo Tomás de Bogotá cuenta con un Consultorio Estadístico, el cual ofrece asesoría gratuita en temas estadísticos, por parte de los estudiantes que están cursando los últimos semestres de la carrera, los estudiantes de esta facultad Mauricio Alarcón Granados y Oscar Iván Castro Osorio nos dieron unas observaciones y sugerencias con respecto a la prueba piloto, en donde una se tomaron en cuenta y otras no, porque no era significativo para nuestro proyecto.

La investigación que se hizo fue cualitativa, es decir, que se usó un grupo de enfoque y aunque las preguntas de la encuesta son cerradas, las respuestas que se ofrecen son en palabras, con el fin de realizar una exploración de los hábitos que los adolescentes tienen.

Por ejemplo, dentro de esta prueba piloto se identifica ¿Qué edad tiene la persona que está realizando la encuesta? y ¿Que género es la persona?, y así sacar mejores resultados,

también se pudo identificar con qué frecuencia usan Facebook y que personas prevalecen en su cuenta. Ver ANEXO C y ANEXO D.

Se realizó la prueba a 53 jóvenes y como resultado de estas pruebas piloto encontramos que:

- El 67,3% de los encuestados tienen acceso a internet desde el Wifi de su hogar.
- El 69,2% usa más de dos (2) horas del día en redes sociales como Facebook.
- El 50% no conocen a muchos de sus “amigos” de Facebook, en donde el 42.3% corresponde a algunos y el 7.7% a pocos de los que pueden tener acceso a su información.
- El 73,1% de los encuestados declaran conocer los peligros que puede hacer en Facebook, pero ¿Saben cómo proteger su cuenta de estos peligros?

Una de las preguntas propuesta es: ¿A quién le dirías en caso de sentirte en peligro en Facebook? Y con respecto a esta pregunta se encontró que: el 67,3% responde que, a su familia, el 17,3% a autoridades, pero el resto (11.5% y 3.8%) responden que a sus amigos y a ninguno respectivamente. Ese 15,3% declara no estar seguro de que se van a tomar las correspondientes precauciones y el castigo debido a los delincuentes.

Esta pregunta nos causaba intriga, así que se decidió pedir una explicación de esta pregunta y unas respuestas fueron inesperadas, como: “porque mi familia no me creería”, “me da miedo”, “porque nunca me pasará”. Esto evidencia que algunos adolescentes se sienten desprotegidos y piensan que si le llegara a pasar una mala experiencia sentiría desconfianza y temor de expresarle a alguien lo que ha sucedido, especialmente a su familia, según las encuestas.

Para la segunda parte, se definió la población ⁴ a trabajar, en este caso se quiso trabajar con los tres colegios distritales oficiales de la localidad de Chapinero, el Colegio Simón

⁴ Población se define como, un conjunto de personas que cumplen con características similares y de quienes se quiere estudiar algunos datos. (Tomás-Sábado, n.d.)

Rodríguez, el Colegio San Martín de Porres (IED) y el Colegio campestre monte verde (IED), sin embargo, debido a las restricciones de acceso a la información para disponer de un marco muestral ⁵ adecuado para la población estudiada, se trabajó finalmente los dos primeros colegios nombrados, se estableció realizar un tipo de diseño de muestras ⁶ no probabilístico ⁷ que aproveche la información dispuesta por el consultante, por lo que finalmente se decidió trabajar con la siguiente información:

- Colegio Simón Rodríguez (IED) – Sede A

El número de estudiantes que están dentro del rango de edad establecido es: 411

- Colegio San Martín de Porres (IED) – Sede A

El número de estudiantes que están dentro del rango de edad establecido es: 183.

Solo se tomaron esas sedes porque las otras sedes de los colegios no están en el rango de edades que se va a estudiar.

Con ayuda de los estudiantes anteriormente nombrados de la facultada de Estadística, se estableció la muestra. Según el informe de consultoría enviado por los estudiantes, el procedimiento para calcular la muestra fue el siguiente: “Se tomó el total de estudiantes de los colegios Simón Rodríguez y San Martín de Porres de la localidad de chapinero en secundaria como el universo de estudio. Respecto a él, se realizó la cuantificación del tamaño de muestra con distintos niveles de confianza y margen de error para después, de acuerdo a la participación de cada colegio dentro del universo, establecer la cantidad de estudiantes a encuestar por cada subgrupo (colegio)...”, con la respuesta anterior el grupo

⁵ Un marco muestral se define como los elementos que componen lo que se quiere estudiar, de la cual se saca la muestra. Estos elementos pueden ser personas, colegios, o cualquier otro tipo de cosas que puedan ser investigadas. (Carlos Ochoa, 2015)

⁶ Diseño muestral, son los métodos que se usan para extraer las muestras con el fin de obtener sus características promedio. (Vivanco Arancibia, 2006)

⁷ Un diseño muestral no probabilístico, es el cual se selecciona una muestra en donde no tiene una posibilidad conocida de ser seleccionado, además de que no todos los de la población están dentro del estudio. (Vivanco Arancibia, 2006)

de consultorio estadístico ofrece cuatro diseños y optamos por utilizar la muestra con un nivel de confianza del 95% y un margen de error del 10%.

Opción 2:

Tabla 1: Diseño de la muestra estadística

Nivel de confianza	95%		
Margen de Error	10%		
Colegios	Universos	Proporción(%)	Muestra
Colegio Simón Rodríguez	411	69%	57
Colegio San Martín de Porres	183	31%	26
Total Población	594	100%	83

Fuente: Consultorio Estadístico – Universidad Santo Tomás

Para ver el informe completo y el resto de las opciones presentadas, por favor referirse al ANEXO E.

La tabla 1 muestra que, para un total de población de 594 estudiantes entre 12 y 18 años, de dos de los colegios distritales oficiales se obtuvo una muestra de 83, en donde, 57 estudiantes (69%) pertenecen al Colegio Simón Rodríguez y 26 estudiantes (31%) al Colegio San Martín de Porres. A esta muestra se piensa realizar la encuesta anteriormente nombrada y analizar si los resultados fueron similares a los de la prueba piloto.

Después de haber realizado la actividad en los colegios anteriormente nombrados se pudo observar que los resultados fueron muy similares a la prueba piloto, más del 70 % de los encuestados tienen Facebook y según la encuesta realizada, Facebook es la red social más usada por los adolescentes en el rango de edad mencionado.

Otras de las cosas que mostró la encuesta es que, aunque son pocos, todavía hay adolescentes que creen mucho o totalmente lo que la gente publica en internet o en redes sociales y que entrega información personal (Nombre completo, fecha de nacimiento, dirección, etc.) sin medir las consecuencias que esto trae.

Por último, muestra que los encuestados leen los términos y condiciones de los juegos antes de usarlos y conocen los peligros en las redes, pero lo realmente importante es que sepan cómo actuar en el momento que lleguen a ser posibles víctimas de los peligros en las redes sociales. Para ver el informe completo de las respuestas obtenidas, por favor Ver ANEXO F.

3 HERRAMIENTAS DE SOFTWARE PARA EL DESARROLLO

Para poder identificar las estrategias con las cuales se puede llamar la atención de los adolescentes para posteriormente presentarles la problemática, se tuvo en cuenta que motiva a la población y así poder usar una herramienta que sea de fácil uso y llamativa para los jóvenes. Teniendo en cuenta esto se realizó una descripción de cada una de las herramientas planteadas y lenguajes de programación con algunas consideraciones para tener en cuenta.

3.1 LENGUAJES DE PROGRAMACIÓN Y MARCAS

Un lenguaje de programación es un sistema de comunicaciones el cual ayuda a que el usuario pueda realizar lo que desea en el dispositivo o aplicaciones que esté usando, teniendo en cuenta que es un conjunto de instrucciones (código fuente) ordenadas y sucesivas para así llevar a cabo el objetivo deseado. Hay un código fuente para cada lenguaje. (MORALES, 2014)

Existen varios lenguajes de programaciones y estos a su vez se dividen en dos grandes grupos: Lenguajes de programación de bajo nivel y de alto nivel, los primeros también llamados “código máquina” son aquellos que tiene dependen directamente son el hardware y a cumplir tareas únicamente de la máquina. Mientras los lenguajes de programación de alto nivel son aquellos que sirvan para crear diferentes programas y aplicaciones informáticas. (Abel & Ibarra Mercado, 1996)

En este caso se tratará los lenguajes de programación más usados (Java y C/C++) los cuales pertenecen a los lenguajes de programación de alto nivel que se habló anteriormente.

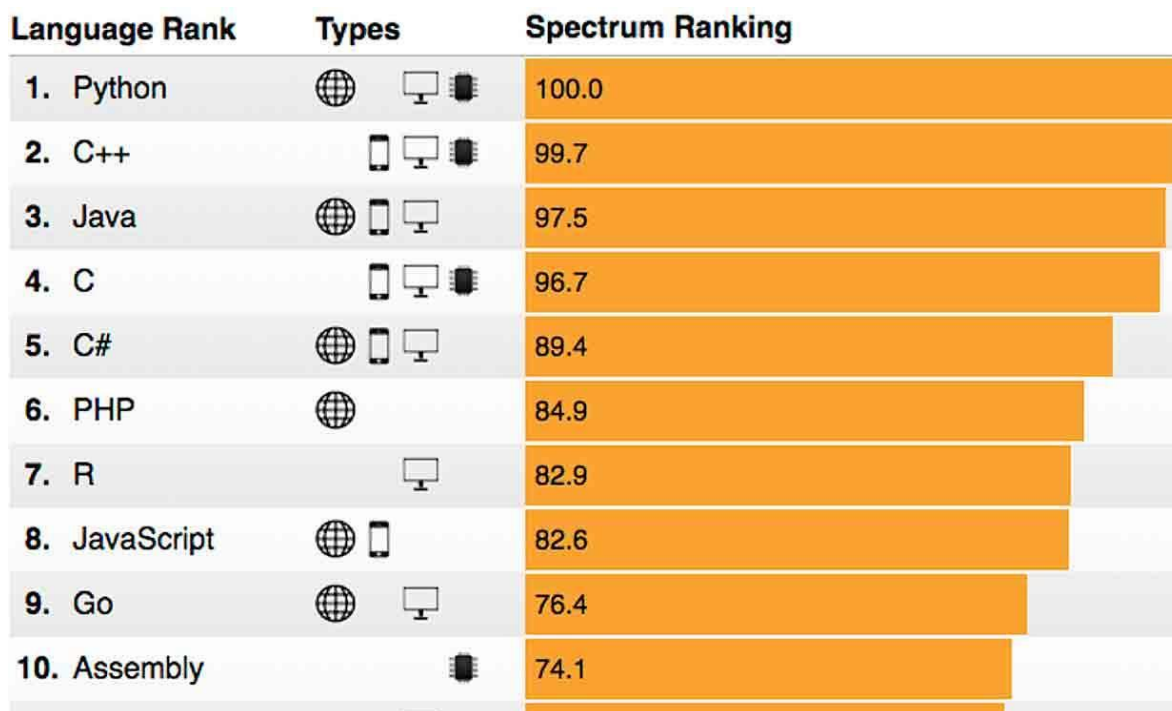


Figura 1. Lenguajes de programación principales

Fuente: IEEE SPECTRUM - (Cass, 2018)

Los lenguajes de marcas son aquellos que utilizan etiquetas, este tipo de etiquetas contienen información adicional para interpretar mejor el texto. A diferencia del lenguaje de programación este no tiene funciones de variables o aritméticas. (AULA FORMATIVA, 2016)

3.1.1 Java

Una de las principales ventajas de este lenguaje de programación orientado a objetos es la independencia de plataforma, lo cual significa que cualquier programa puede funcionar desde un dispositivo diferente sin importar el sistema operativo, esto es llamado "write once, run anywhere" o en español "Escribe una vez, corre a cualquier lugar". Otra ventaja de este lenguaje es que brinda una multiplataforma que lastimosamente a causa de eso su rendimiento bajó notoriamente. Además, permite incluir recursos como sonido y objetos multimedia y la información sobre este lenguaje es abundante. Por último, Java posee un recolector de basura, así como crea objetos fácilmente puede eliminarlos ofreciendo mayor seguridad. (Groussard, 2014)(Paipa, n.d.)(Twago Community, n.d.)

Aunque Java maneja una sintaxis similar a la de c++, es más compleja. Java requiere de un buen intérprete puesto que si no es bien interpretado puede tener inconvenientes, los resultados no serían los deseados y su lentitud podría aumentar. (Paipa, n.d.)

Ejemplos:

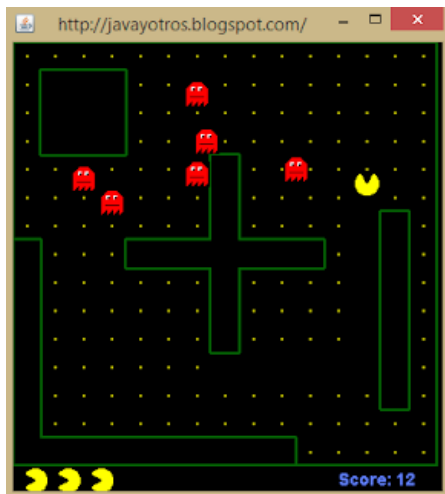


Figura 2. Pacman en java
Fuente: Yedith, Andrés (Yedith, 2015)

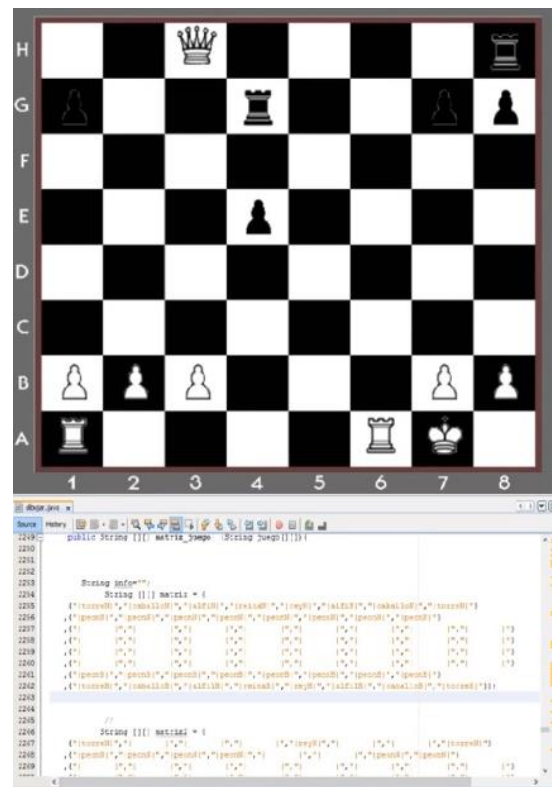


Figura 3. Ajedrez desarrollado en Java
Fuente: Yedith, Andrés (Yedith, 2014)

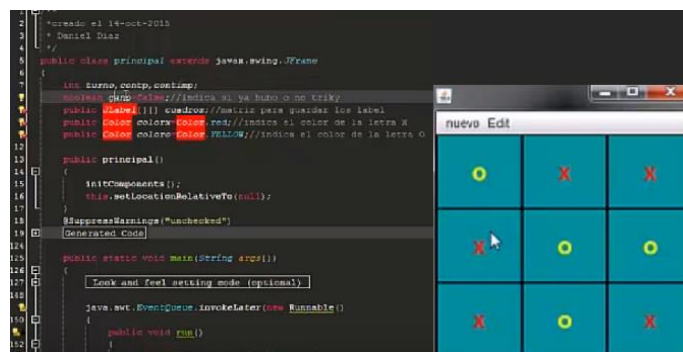


Figura 4. Triki en java Netbeans
Fuente: Daniel Díaz (Díaz, 2015)

3.1.2 C/C++

C++ es un lenguaje de programación que tiene como principal ventaja la eficacia y flexibilidad a la hora de programar al igual que C con la diferencia de que le quitaron algunas limitaciones que este último lenguaje nombrado tiene. Es posible ejecutarlo desde cualquier otro dispositivo y fácil de compilar. C junto a C++ son normalmente usados en la creación de software en diferentes sistemas operativos. Por último, se dispone de gran información y documentación acerca de este lenguaje. (Cárdenas, 2016) (EcuRed, n.d.) (Pascual & Pérez López, n.d.)

No es recomendable para creaciones de páginas web y es necesario liberar memoria correctamente por parte del programador, como efecto contrario el programa se queda con esa parte de la memoria llena y puede afectar su rendimiento. (Cárdenas, 2016)

Ejemplos:

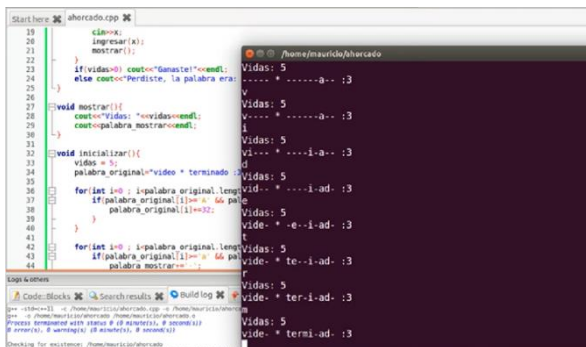


Figura 5. Ahorcado en c++

Fuente: Andrés Rondón (Rondón, 2015)



Figura 6. Mario Bros en C++/Allegro

Fuente: Daniel Díaz (Brunosg2002, 2011)

3.1.3 HTML5

Es la última versión de lenguaje de marcas de hipertexto para crear páginas web, el beneficio adicional que HTML5 brinda es que es posible añadir a la página web audio y video, sin necesidad de utilizar ningún reproductor multimedia, lo cual ayuda a que el archivo de la página web disminuya en tamaño. Usando esta nueva versión de HTML es posible visualizar la ubicación de cada persona que ingrese a la página web. Con HTML5 es posible crear animaciones en 2D y añadirlas a la página web deseada. Es compatible con la mayoría de los navegadores y se puede acceder a la página web o al resultado

deseado desde cualquier dispositivo. HTML5 utiliza librerías de Java las cuales ayuda que es muestre e interprete cada elemento en HTML5. (AULA FORMATIVA, 2016) (HiperText Markup Language, 2013) (Diez, Domínguez, Martínez, Joseba, & De Navarrete, n.d.)

Actualmente Facebook dejó a un lado a Flash en cuanto a sus videos y empezó a usar HTML5 por la velocidad que este les ofrece y otro tipo de beneficios como los ya mencionados anteriormente, además de que poco a poco las aplicaciones que ofrece esta red social serán desarrolladas con HTML5 por el rendimiento que les puede ofrecer. (Leticia Vela, 2010)

Una de las desventajas de HTML5 es que no se ha encontrado un formato de video que sea compatible con todos los navegadores, además de que aún no tiene todos los complementos que muchos reproductores tienen (subtítulos, anuncios o interacciones entre los usuarios). (HiperText Markup Language, 2013)

3.2 PLATAFORMAS ONLINE

Las plataformas online son programas o softwares informáticos que están diseñados para usar únicamente en internet. Cuenta con una interfaz gráfica la cual es sencilla de usar para el usuario. Algunas de ellas no es posible descargar en los dispositivos, sin embargo, pueden guardar el progreso de la actividad en la nube.

3.2.1 Powtoon

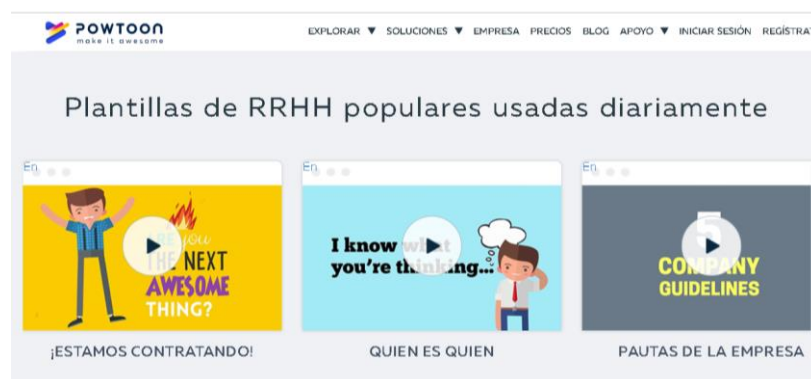


Figura 7. Página principal de Powtoon
Fuente: Powtoon (Powtoon, 2018)

Powtoon es una herramienta educativa, gratuita y didáctica, para su uso solo es necesario registrarse y consta del método de arrastrar el objeto hasta donde se desee lo cual se considera muy sencillo de utilizar, esta herramienta viene con un tutorial explicando y guiando cada paso para realizar el proyecto deseado, es posible añadir música o voz a el proyecto y se puede exportar al formato deseado. (Quiroz, n.d.)(modelo presentaciones, n.d.)(Recursos educativos digitales - Gobierno de Canarias, n.d.)(Blog Luis Villa - INFORMÁTICA, n.d.)

Aunque se guarda en la nube, lamentablemente solo es posible usar esta herramienta online y no es colaborativa. (Blog Luis Villa - INFORMÁTICA, n.d.)

3.2.2 APLICACIÓN INFORMATICA

Una aplicación informática está diseñada como una herramienta para que el usuario pueda realizar diferentes tareas, que se instala en un computador y otro dispositivo con capacidad de conmutación. Una desventaja de estas aplicaciones informáticas es que solo se puede usar en los dispositivos en los que están instalados, sin embargo, hay unas aplicaciones que manejan una plataforma virtual, con el objetivo de que no solo se pueda trabajar con el mismo dispositivo. (SoftwareDoit, n.d.)

3.2.3 Adobe Flash Player

También llamada Flash, es una herramienta informática que tiene como fin crear y manipular gráficos vectoriales en 2 y 3 dimensiones, al usar gráficos vectoriales puede disminuir el ancho de banda para su transmisión y el tiempo de carga de la aplicación. Con el tiempo se ha convertido en la herramienta más usada en aplicaciones web, pues a que se le puede añadir audio y video a cualquier animación y muchos de los navegadores respaldan Flash sin importar el sistema operativo. (HardSoftware, 2010) (Juan Carlos - Blogspot Recursos flash, 2011)(Jenifer - Blogspot, 2011)

Las paginas creadas con flash suelen ser muy pesadas por esta razón la herramienta tiene limitaciones de velocidad y ancho de banda, además al momento de realizar algún cambio sobre la página puede aumentar el tiempo de espera normal de una página. Adobe Flash Player es una herramienta que necesita de pago para realizar creaciones. (HardSoftware, 2010)

Ejemplo:



Figura 8. Animación de Personaje en Adobe Flash
Fuente: Ina Alavedra (Alavedra, 2012)

3.2.4 Unity



Figura 9. Imagen de preparación de Unity

Fuente: Unity (Unity Technologies, 2019)

Unity es un motor de videojuego que funciona como multiplataforma compatible con sistemas operativos como Linux, Microsoft Windows y OS X. Con esta herramienta es posible crear animaciones y juegos en 2 y 3 dimensiones, es fácil de usar con ayuda de la documentación que se puede encontrar, además de que la herramienta cuenta con ayudas y ejemplos para facilitar la creación de diferentes juegos, la sintaxis con la que funciona son los lenguajes que anteriormente de nombraron (Java, C y C++). Otra de las ventajas que se puede nombrar es que Unity puede es posible subir y añadir sonidos, diferentes controles

u otros distintos objetos. (Fenrir - La leyenda de Darwan, 2017) (Mula, n.d.)(Luttecke, n.d.)(Vázquez García, 2017)

Todos los proyectos creados con esta herramienta ocupan un gran espacio y por ende necesita de un buen dispositivo para que este responda a la ejecución de los diferentes programas. (Fenrir - La leyenda de Darwan, 2017)

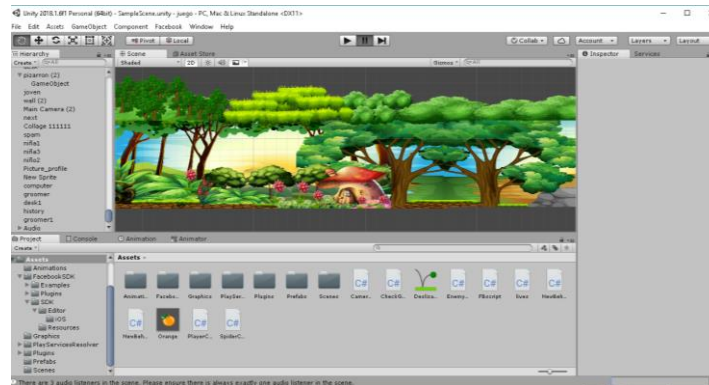


Figura 10. Interfaz de usuario de Unity
Fuente: Autores

Después de revisar las posibles herramientas, se seleccionó la de Unity, por su usabilidad y la posibilidad de generar aplicaciones web.

3.2.5 Framework de Facebook

Framework, traducido como “marco de trabajo” es un entorno el cual desarrolla e implementa software. No están basado en ningún lenguaje específico. Una de sus principales ventajas es que los programadores pueden colaborar entre ellos, además de que existe numerosa documentación sobre este marco de trabajo. (Jordisan, 2006)

Facebook ofrece un framework para el desarrollo de aplicaciones que se publiquen dentro de su plataforma.

4 REQUISITOS FUNCIONALES DE LA HERRAMIENTA DE SOFTWARE

Los requisitos funcionales de una herramienta o sistema, en este caso de una herramienta de software, son los cuales detallan cada función específica de cada elemento que está dentro del sistema y cumplen algunas condiciones.

A continuación, se identifica cada actor que hace parte del sistema y cuál es su función dentro del mismo para que la herramienta cumpla con las funciones establecidas y funcione de manera óptima, las cuales se encuentran en el numeral 5.2.

4.1 IDENTIFICACIÓN DE AUTORES

En seguida, se realiza la identificación de actores dentro del diagrama:

- Usuario: Serán los adolescentes que utilizan la aplicación de Facebook, en donde usaran la herramienta creada.
- Socializador: Será la persona (profesor, padre de familia, o creador de la aplicación), el cual busca mostrar los riesgos (como el Grooming), que puede haber por la mala gestión de seguridad de la información personal en Facebook a través de una herramienta de software.
- Aplicación: La herramienta informática desarrollada en este trabajo con la cual se va a mostrar a los adolescentes el riesgo que existe al tener una mala gestión de seguridad de la información en las redes sociales.
- Facebook: Red social con alrededor de 1.94 mil millones de usuarios activos al mes, a partir del 2006 permitió registrarse y convertirse en usuario de esta red social a cualquier persona que diga tener por lo menos trece (13) años, pero uno de los problemas es la falta de verificación de esta información de las personas que se registran.

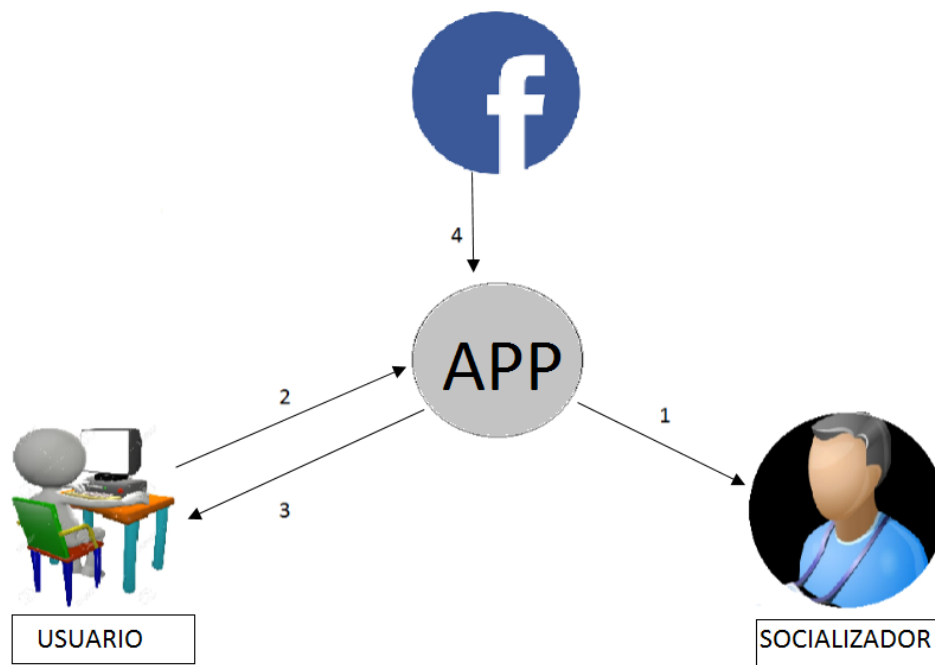


Figura 11. Relación entre actores dentro de la herramienta
Fuente: Autores

Tabla 2. Relación entre actores

ID	Actores	Descripción
1	Aplicación al socializador	El socializador tiene acceso a documentación dentro de la aplicación
2	Usuario a la aplicación	consentimientos de los datos
3	Aplicación al usuario	La aplicación le brinda al usuario el juego desarrollado
4	Facebook a la aplicación	Desde Facebook poder obtener los datos personales de los usuarios

Fuente: Autores

4.2 FUNCIONES DE LA APLICACIÓN

- Presentar un juego al usuario.
- Mostrar una aplicación al usuario.
- Halar la información personal del usuario desde su Facebook.
- Hacer la lectura de la información de Facebook.
- Mostrar cómo cambiar las opciones de seguridad.

5 DESARROLLO DE LA HERRAMIENTA

En esta sección se presenta información acerca de, soporte de implementación, objetivo general y funcionalidad principal del software de la herramienta de generación de concientización de los peligros del Grooming. Así mismo se incluirán detalles técnicos de la herramienta, y por último detalles de la realización de la instalación y pruebas del sistema.

5.1 ESPECIFICACIÓN DE REQUERIMIENTOS

Esta herramienta requirió estudios sociales acerca de cómo los jóvenes adolescentes le están dando uso a su perfil social Facebook. Así mismo se hizo una revisión de literatura acerca de los comportamientos de los Groomers. En cuanto a los requerimientos técnicos se revisó lenguajes y motores que fuesen útiles y de fácil integración con el API de Facebook, para la construcción de la aplicación software que se integrara con funcionalidades de la red social Facebook.

A continuación, se describirán elementos técnicos y herramientas claves para el desarrollo de la aplicación, que se deben tener en cuenta durante la documentación y desarrollo del proyecto, desde el punto de vista técnico.

5.1.1 API Facebook

Interfaz de programación de aplicación, (por sus siglas en inglés Application Programming Interface), es una herramienta que permite a las aplicaciones y juegos informáticos, hacer llamados de funciones o consultar datos mediante programación a la red social de Facebook. Estas funciones de Facebook pueden ser permisos de aplicación para interactuar directamente con la aplicación, tales permisos pueden ser el acceso a información como lista de amigos, fotos públicas, videos públicos, entre otros relacionados con contenido del usuario proporcionado cuenta en su perfil de Facebook (Facebook, 2019).

5.1.2 Motor

Plataforma de software que permite realizar y desarrollar aplicaciones en uno o varios lenguajes de programación, para el desarrollo del software se utilizó el motor de desarrollo

Unity, debido a su fácil integración con el SDK Unity Facebook y a su respuesta con el Api de Facebook. (unity facebook)

5.1.3 SDK Unity Facebook

Herramienta multiplataforma que proporciona una escritura en entornos como plataformas de juegos clave de WebGL, Unity Web Player, Android e iOS, su principal característica se basa en su base de código única, esta plataforma ofrece una gama amplia de funcionalidades de Facebook, como la opción de hacer el registro a x aplicación o juego y compartir contenido con sus amigos de la misma red. Su función principal es hacer los llamados de funciones al API de Facebook para así poder ser gestionados estas funciones o permisos desde la aplicación.

5.1.4 Unity WebGL

Es una API de Java script para la realización de gráficos 3D y el funcionamiento en los navegadores web. Una aplicación WebGL aprovecha los recursos java script fundamentales para la ejecución sobre HTML.

5.1.5 Alojamiento web

Recurso online para el almacenamiento de información como imágenes, videos, recursos HTML entre otros que puedan ser legibles vía web. Para este proyecto se utilizó el servicio de alojamiento web con el proveedor webhosting una plataforma gratuita que permite alojamiento HTML sin publicidad y un 1Gb de almacenamiento necesario para llevar la herramienta a un servidor de alojamiento web.

5.1.6 Browser

Herramienta necesaria visualizar el contenido HTML en el que se ejecutara la herramienta del proyecto. Siendo la interfaz de lectura para la ejecución de la herramienta del proyecto actual.

6 DEFINICIÓN GENERAL DE LA HERRAMIENTA

La siguiente herramienta tecnológica de concientización de los peligros de Grooming es creada con el fin de generar conciencia del mal uso que se está dando en las redes sociales en especial la red social Facebook. Esta herramienta busca socializar la problemática del grooming a una población específica de estudiantes de la ciudad de Bogotá en la localidad de Chapinero, además se socializará este proyecto final con jóvenes de la zona rural, que en este caso aplicara en un colegio departamental correspondiente al municipio de Anolaima Cundinamarca, las dos zonas de aplicación tanto la zona urbana de Bogotá y la zona rural de Anolaima toma lugar en nivel socioeconómico estructurado en Colombia como estrato 1, 2 y 3. De acuerdo con el estudio anteriormente en el documento, de las vulnerabilidades que se exponen los usuarios al no leer los términos y condiciones, necesarios o innecesarios para dicho funcionamiento de la aplicación a la que el usuario de la red social Facebook está ingresando.

La herramienta no es de uso público, por el contrario, se realizó como soporte y ayuda para socializadores del tema y futuras investigación al respecto. Además, que para garantizar la privacidad de los menores ningún dato fue guardado.

La herramienta tecnológica de concientización de los peligros de Grooming es una herramienta basada en software, que se estructura en cuatro funcionalidades descritas como:

- Aplicación web
- Integración web con funcionalidades, permisos de Facebook e impacto del proyecto
- Socialización y recomendaciones

Estas 3 funcionalidades fueron estructuradas con el fin de demostrar una posible forma de capturar información relevante para Groomers, generar conciencia de la información que se permite al brindar al momento de aceptar términos y condiciones, generación de impacto del uso de su información como posible víctima del Grooming, y por último recomendaciones y cuidados que se deben tener en cuenta cuando se usa aplicaciones

que usan de su información personal que usted como usuario brinda a través de la plataforma social Facebook como un ejemplo de demás redes sociales.

6.1 REQUERIMIENTOS DE LA HERRAMIENTA

En esta sección se describe el desarrollo y funcionamiento de la herramienta de concientización de los riesgos del Grooming. Así mismo se describirán sus estructuras planteadas anteriormente en la sección anterior. Las tres (3) estructuras de la aplicación son definidas para cumplir un objetivo específico del desarrollo, todo esto para cumplir el objetivo general del proyecto.

6.1.1 Aplicación web

Es descrita como la primera estructura de la aplicación que tiene como objetivo llamar la atención de los jóvenes como posible ejemplo de señuelo, donde a través de estas aplicaciones los usuarios interactúan con la red social de Facebook. Aplicaciones y juegos de este tipo son montados en la plataforma de Facebook para interactuar con las funciones y permisos que brinda la red social para hacer más divertidas estas aplicaciones.

La aplicación web de este proyecto es un juego basado en WebGL por el motor Unity, este juego actuará como elemento de enganche para llamar la atención de los jóvenes adolescentes, este juego hace parte de la categoría acción y aventura de la plataforma Facebook Developers. El objetivo principal de esta estructura de la herramienta tecnológica para la concientización de los riesgos grooming es crear una aplicación web llamativa que sirva como ejemplo social para generar conciencia de la responsabilidad que se debe tener al permitir acceder a información que como usuario brinda al aceptar permisos.

Monkey Collector es el nombre que se le dio a este juego, donde el protagonista es un mono encargado de recolectar frutas en un bosque, su objetivo es recolectar 100 frutas que deben ser llevadas a casa. En la siguiente imagen se podrá observar el perfil del mono encargado de llamar la atención de los usuarios prueba como proyecto social de grooming.



Figura 12. Perfil del juego "Monkey Collector"
Fuente: Autores

Para cumplir su objetivo Moonkey Collector tiene que afrontar los peligros que se encuentran en el bosque, estos peligros son animales como insectos que al tocarlos causa cierto daño en la salud de Monkey, es por eso que él debe tener precaución al momento de ingresar al bosque, cuando el sube a los árboles el peligro es el mismo que cuando camina por el bosque. Monkey Collector no tiene opción de cuál es su mejor ruta si el suelo o los árboles, es decir, si Monkey decide caminar en el suelo encontrará con un insecto muy peligroso que causa daño en su salud, al mismo tiempo se ve obligado a subir a los árboles pues es allí donde está el alimento que debe recolectar para llevar a casa. Sin embargo, en los árboles también encontrará peligro pues en las ramas de los árboles habitan arañas del mismo peligro de los insectos terrestres, que en ocasiones bajan al suelo y es donde Monkey tiene la oportunidad pasar por algunas ramas y recolectar el alimento. En la siguiente imagen se puede observar el daño que causado en la vida de Monkey al tocar el insecto terrestre.



Figura 13. Daño causado al personaje
Fuente: Autores

Monkey Collector fue desarrollado sobre el motor de Unity con una interfaz 2d en su versión 5.0 y convertido en el entorno de Unity WebGL. Para el uso de sus gráficos y del mismo protagonista los derechos de uso fueron comprados a 123rf de acuerdo con la licencia, Dver ANEXO G). El desarrollo e idea principal están sujetas a los autores del proyecto sin embargo están ligadas a las licencias Creative Commons, permitiendo modificaciones de compañeros con el fin de complementar el trabajo.

6.1.2 Integración web con funcionalidades, permisos de Facebook e impacto generado del proyecto

En esta sección se encontrará la integración web con funcionalidades, es decir, el juego con una serie de funciones que permite extraer cierta información. Una vez se haya integrado estas dos partes es importante tener en cuenta los permisos que se van a solicitar a Facebook y las políticas que esta red social tiene para brindar dichos permisos. Por último, se mostrará en la segunda escena de la aplicación un impacto para los adolescentes.

6.1.3 Integración web con funcionalidades

El objetivo principal de esta sección es extraer información desde el perfil de usuario en Facebook, este procedimiento es posible a través de los componentes como el Api de Facebook y el SDK de Facebook Unity. El Api de Facebook se basa en html que permite dar respuesta desde cualquier navegador, la información que permite halar del perfil está representada como nodos, nodos bordes y campos. Los nodos hacen referencia a el punto central de la información como una página o usuario, los campos son información general de un perfil como fecha de cumple años, fotos amigos de un nodo, los bordes hacen referencia a información más específica como por ejemplo la información detallada de un

campo como “likes” de una foto. Actualmente Facebook cuenta con un protocolo llamado OAuth (por sus siglas en ingles “Open Authorization”), es un estándar abierto, el cual permite que el usuario use cualquier aplicación, se logueé en Facebook, sin que esta aplicación tenga acceso a toda la información de su cuenta de Facebook, incluyendo correo y password. Encargando al servicio que gestiona las cuentas la autenticación de usuario, de tal manera que sea este quien conceda el acceso a las aplicaciones (Obaya, 2015).

Para solicitar permisos al Api es necesario el “acces_token” como parámetro de solicitud, este parámetro debe ser utilizado para acceder mediante inicio de sesión a Facebook desde un aplicativo como por ejemplo un juego, la aplicación obtiene un acces_token que es el encargado de proporcionar seguridad el ingreso al Api de Facebook. Este acces token está limitado por cierto tiempo para la aplicación y debe ser renovado (facebook, 2019).

El AT (por sus siglas en inglés “acces_token”), es un parámetro de identificación de un usuario, página o aplicación para garantizar el uso de llamadas a la Api de Facebook, incluye información acerca de los permisos que se van a solicitar, información de la aplicación que lo genera y fecha de caducidad del AT. AT es solicitado a través del SDK que se encarga de enviar la solicitud al servidor Facebook y este es gestionado en su Api. Además, hay diferentes tipos de AT, para el desarrollo de esta aplicación se utilizó dos tipos AT de aplicación y AT de usuario (facebook, 2019).

AT usuario es utilizado para que la aplicación solicite al Api que lea información del perfil, de quien está solicitando ingresar o registrarse en la aplicación estos son requeridos mediante el inicio de sesión y la aceptación de los términos y condiciones. AT aplicación es necesario para leer la configuración de la aplicación generando una clave secreta entre la aplicación y El siguiente diagrama ilustra el proceso que lleva hacer un llamado al Api con el token de usuario; el AT es generado desde la plataforma del SDK creando una petición de inicio de sesión con Facebook, para luego el usuario estar en condiciones de aceptar los permisos y continuar con los requerimientos de la aplicación de forma que el AT es devuelto al usuario.

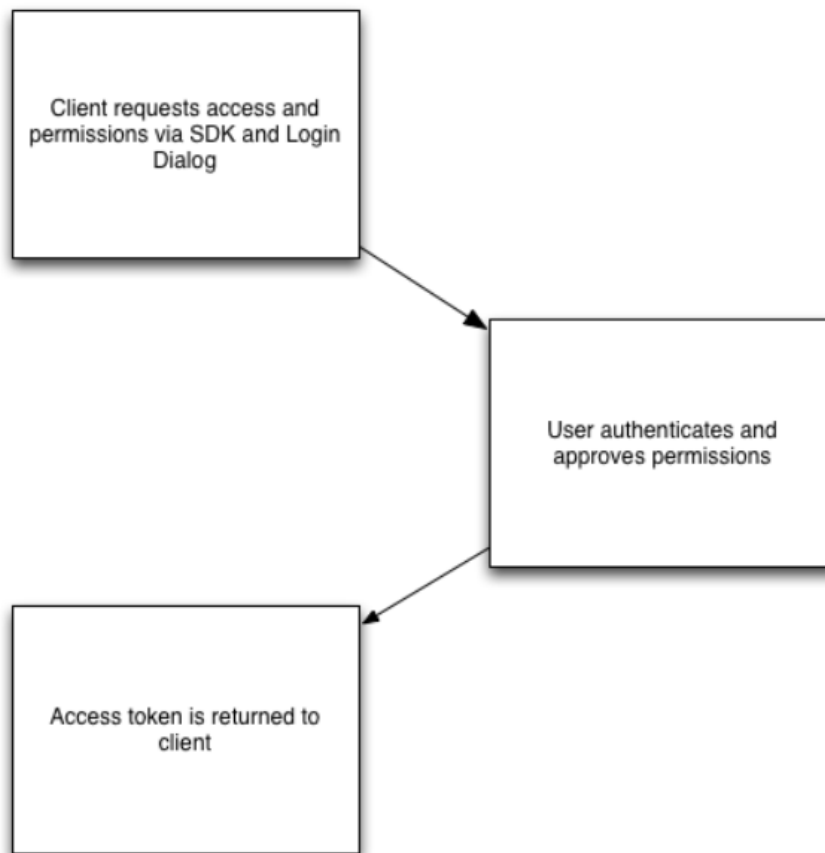


*Figura 14. Proceso de Conexión entre el Api con el Token de Usuario
Fuente: (facebook, 2019)*

Para la herramienta de concientización de los peligros del Grooming, el proceso de inicio de sesión que se realiza a través del AT de usuario fue gestionado desde el SDK de Unity Facebook; el equipo completo de herramientas y funciones que permiten interactuar, crear una aplicación sociable y una interfaz amena entre los usuarios, es gestionada desde el SDK Unity Facebook, las herramientas que entrega SDK Unity Facebook ofrecen un conjunto de funciones programables para que el usuario comparta información y/o contenido entre sus seguidores, esta información puede catalogarse como invitación a amigos a participar de uso de la aplicación o simplemente logros. Para que el usuario utilice y/o comparta información desde su perfil de Facebook, es necesario realizar la petición de permisos en la plataforma de desarrolladores Facebook (developers Facebook) y así podrá ser gestionada en el SDK Unity (facebook, 2019)

6.1.4 Permisos de Facebook

Los permisos de Facebook son un conjunto de restricciones a los datos almacenados en la red social, estas restricciones pueden ser levantadas por la misma OSN y el usuario, en el momento de la creación de las herramientas de software para el entretenimiento y cuando el usuario va a ser usado por primera vez de dicha aplicación. Para ser usado o beneficio de la aplicación, estos permisos deben ser aceptados por el mismo usuario mediante la aceptación de términos y condiciones antes de iniciar la ejecución de cada herramienta o aplicación que los requiera. Facebook permite a los desarrolladores hacer uso de dos permisos previos para el “Inicio de sesión” sin consultar el acceso al usuario, “Email” y “public_profile” son los permisos necesarios para el inicio de sesión con Facebook, estos son requeridos sin previo aviso, pues son elementales para la identificación tanto en la aplicación como en la plataforma de Facebook, una vez son identificados el usuario podrá decidir si desea continuar con los demás requerimientos y permisos que la aplicación solicite a Facebook.

Se debe aclarar que las aplicaciones pueden solicitar permisos adicionales a los que se usaron después de haber solicitado en primera instancia, es decir, después de que el usuario aceptó los permisos en su primer inicio de sesión con la aplicación, de igual forma Facebook le notificará al usuario si desea que la aplicación agregue una función del nombre del usuario los nuevos permisos solicitados. El uso de cada permiso debe cumplir con las políticas de Facebook. La herramienta de concientización de los peligros del Grooming hace uso de los siguientes permisos:

- Default

El permiso de “default” como su nombre lo indica son los permisos que Facebook brinda por defecto, el cual no necesita revisión de parte de Facebook. Dentro de los permisos de default están: id, nombres, apellidos, foto del perfil, nombre de usuario o el alias que tenga la persona (Facebook, 2019).

- Email

Este permiso brinda acceso a la dirección de correo electrónico de la persona. Este permiso se aprueba de manera anticipada, es decir que no requiere enviarlo a revisión por parte de

la red social. Según Facebook, el uso permitido de “email” es para que una persona utilice el correo electrónico el cual tenga en su cuenta de Facebook para iniciar sesión en cualquier aplicación, el uso no permitido es para realizar “Spamming” a los usuarios, este término se refiere a la acción de enviar Spam, correos o mensajes basura de personas desconocidas, no deseadas ni solicitadas, con el fin enviar información de carácter publicitario (Top, 2017) (Facebook, 2019).

- Fotos

Este permiso llamado en Facebook como “user_photos”, proporciona acceso a las fotos que ha subido la persona o en las que ha sido etiquetado. Este permiso necesita de una revisión previa por parte de Facebook para que la red social determine la razón de la solicitud y si es necesario el permiso o no. Según Facebook, los usos comunes de este permiso son: Muestra de fotos o imágenes de manera digital con distintos filtros o diseños, facilidad a los usuarios de exportar imágenes con el fin de imprimirlas (solo para uso personal), usar las fotos solicitadas para mejorar visiblemente una aplicación, ayudar a crear álbumes o collage en nombre del usuario. (Facebook, 2019)

- Amigos

También llamado en Facebook como “user_friends”, este permiso brinda acceder a la lista de amigos del usuario. Es importante saber que para que la lista de amigos aparezca a una persona, las dos personas deber haber compartido y aceptado este permiso. User_friends requiere una revisión previa por parte de Facebook. El uso permitido y común es para crear un uso social en la aplicación (Facebook, 2019).

6.1.5 Revisión De Permisos De La Aplicación

Como se dijo en la sección anterior algunos permisos requieren una revisión previa por parte de Facebook, con el fin de asegurar de que se usan los permisos y datos de manera segura. Este proceso implica detallar el tipo de datos que requiere la aplicación y describir cómo se va a usar, Facebook hace seguimiento a cada paso para culminar la revisión.

En la figura 15, se puede observar la lista de permisos y funciones que Facebook permite usar pero con permisos de ellos, cada función tiene: estado, si el permiso se ha solicitado en qué estado está el proceso; llamadas activas, muestra si un usuario instala la aplicación

con ese permiso; requisitos adicionales, se refiere a los permisos que se necesitan para que el permiso funcione adecuadamente; usos no permitidos, los usos que Facebook no aprueba con el fin de hacer un buen uso a los datos personales del usuario y acción, en esta última sección se muestra si desea solicitar o continuar editando el permiso. En la figura mencionada se muestra que se solicitó los permisos de “user_friends” y “user_photos” los cuales requieren permiso de Facebook, por esta razón se observa la acción que tiene (continuar), pero no se solicitó “user_location” por ende tiene la opción de solicitar este permiso.

Permisos y funciones ↕	Estado ↕	Llam... ↓	Extremos co...	Requisitos adicio...	Usos no permitidos	Acción ↕
user_friends Otorga permiso a una aplicación para acceder a una lista de los amigos que también usan la aplicación. Este permiso está restringido a un conjunto limitado ...	● No solicitado	✓	/user/friends	<div>⊖ Acceso limitado con verificación individual</div> <div>📄 Requiere firma de contrato adicional</div>		Continuar ➡
user_location Otorga permiso a una aplicación para acceder a la ciudad actual de una persona mediante el campo "ubicación" en el objeto del usuario. Las persona...	● No solicitado	✓	/user	<div>⊖ Acceso limitado con verificación individual</div> <div>📄 Requiere firma de contrato adicional</div>		Solicitar
user_photos Otorga permiso a una aplicación para acceder a las fotos que subió una persona.	● No solicitado	✓	/user/photos	<div>⊖ Acceso limitado con verificación individual</div> <div>📄 Requiere firma de contrato adicional</div>		Continuar ➡

Figura 15. . Lista de permisos y funciones para agregar a la solicitud

Fuente: Developers Facebook (Facebook, 2019)

El paso siguiente de haber escogido el permiso se describe como se usará el permiso, en la figura 16 se muestra un ejemplo con el permiso de amigos, allí Facebook explica cada paso que se debe hacer para enviar la solicitud, el uso que este permiso debe tener y realiza unas preguntas a las cuales se respondió:

user_friends

Uso común

- ✓ Utiliza la lista de amigos para crear una experiencia social en tu aplicación.

☒ Acepto las normas de uso de permisos y funciones de Facebook.

Figura 16. Uso común del permiso "user_friends"

Fuente: Developers Facebook (Facebook, 2019)

Primera pregunta:

¿Cómo se usará el permiso o función en la aplicación?

"Monkey Collector acepta todas las normas de uso de permisos de Facebook, con el permiso de obtener la lista de amigos se quiere crear una experiencia social en la aplicación, invitando los amigos del usuario a usar la aplicación y disfrutarla. Además, que el invitar amigos le dará un "bono extra" de vida al personaje."

Segunda pregunta:

Explica de qué modo las plataformas seleccionadas harán uso del permiso o la función

Selecciona las plataformas correspondientes y proporciona instrucciones paso a paso en las que detalles de qué modo el miembro del equipo de revisión puede probar el permiso o la función del mismo modo que lo haría un usuario de la app.

☒ Web [?] ☐ Celular [?] ☐ Otra [?]

Nota: Si tu app no usa ninguna plataforma o no está orientada al usuario, consulta la [documentación sobre apps de servidor a servidor](#) para obtener información sobre los pasos de la revisión.

Web

Figura 17. Muestra de las Preguntas que exige Facebook para la Revisión de Funciones

Fuente: Developers Facebook (Facebook, 2019)

¿Qué plataforma usará su aplicación y cuáles son los pasos para explicar esos permisos en la plataforma usada (web)?

"1. Iniciar sesión con Facebook en "Monkey Collector"

2. Aceptar el permiso "user_friends"

3. Empezar a jugar "Monkey Collector" y cuando se esté quedando sin vida podrá invitar a sus amigos de Facebook a jugar para recuperar vida. Haciendo clic en el botón de amigos, que se encuentra en la parte inferior izquierda de la pantalla. Solo se puede recuperar vida una vez."

Por último, pide mostrar cómo se usa el permiso por medio de un video con instrucciones paso a paso y detalladamente.

Muéstranos cómo usas este permiso o función

Envía un video con instrucciones paso a paso en el que se detalle cómo usará la app el permiso o la función, para que podamos confirmar que se usan correctamente y no infringen nuestras políticas. Más información sobre las capturas de video

Requisitos de la captura de video:

1. Cómo una persona inicia sesión con Facebook.
2. Cómo una persona ve este permiso usado en tu aplicación.

Ver captura de video subida

Arrastra un archivo nuevo aquí para reemplazar la captura de video actual

 Subir archivo

o

Seleccionar de la carga anterior ▼

Figura 18. Captura del video explicativo de las funciones que se Van a Usar

Fuente: Developers Facebook (facebook, 2019)

En la aplicación realizada no se usó los permisos de user_friends y user_photos porque al enviar estos permisos a revisión y cumplir con todos los requisitos aun no respondían ante la solicitud, incluso hasta haber terminado la aplicación sin estos permisos, aun no respondían. Lo anterior puede atribuirse a que después de las revelaciones de mal uso de información de Facebook por parte de la consultora Cambridge Analytics en 2018, se endurecieron algunos accesos.

6.1.6 Impacto Generado Del Proyecto

Para esta parte de la aplicación se quiere mostrar elementos que generen impacto en los adolescentes con el fin de que se concienticen de la problemática. Se usó la figura 18, la cual quiere mostrar al usuario: El hombre misterioso quien es el grommer, el grommer tiene

Recuerda revisar la información que le estas otorgando a las aplicaciones, la información tuya no es para divulgar, cuida mucho de ti, tu integridad y tu salud mental podrian estar en peligro. Estas son algunas posibles actividades que el groomer puede hacer con esta información, sustitución de identidad, cualquier tipo de spam, editor de fotos, y en cualquier de estas actividades se puede llegar al chantaje, teniendo como fin, grooming y/o otros delitos.

unity

Nombre Pepito Grooming

Email: appkgrooming@gmail.com

EL PROXIMO ERES TU

¡¡¡FELICIDADES!!!

Hemos registrado su información en nuestros bases de datos, pero que estos sean eliminados debe seguir los siguientes pasos:

1. Ingrese al siguiente link: www.monjequedador.com/links_2019
2. Allí encontrará un formulario al cual debe completar.
3. Adjunte los archivos indicados para confirmar su identidad.

De no cumplir con la anterior tendremos acceso y control de su computadora

Next

6.1.7 Socialización Y Recomendaciones Generales

Es importante aclarar que las redes sociales en general prestan un buen servicio de comunicación y distracción, siempre y cuando se haga buen uso de ellas. No siempre las personas que usan sitios de internet, como Facebook, tienen buenas intenciones, los groomers algunas veces lo que quieren son fotos y videos con algún contenido sexual que se pueda vender en internet, pero otras veces buscan abusar sexualmente de sus víctimas o arrastrarlas a redes de tráfico de personas y varios adolescentes no son conscientes de esto. La idea no es dejar de usar estas redes sociales, sino entender la problemática y concientizar a las posibles víctimas para que no les pase este tipo de cosas (Magic Markers, 2017).

como víctimas del grooming, estas descripciones son casos de la vida real; la segunda parte de esta escena, se muestra un video que se realizó como recomendaciones tipo tutorial, por medio de la plataforma online (Powtoon). En el cual se dan 6 consejos para proteger su cuenta de Facebook, la manera en que se puede proteger su cuenta (fotos, publicaciones, ubicación, etc), para que todos los usuarios que usen la aplicación conozcan la forma que pueden estar protegidos (Facebook, 2019a). También hay una pequeña descripción de la escena.



Figura 20. Imagen de socialización y Recomendaciones
Fuente: Autores

Todas las caras mostradas en las Figuras 18 y 19 son de personas que no existen y fueron tomadas de un programa "Una arquitectura generadora basada en el estilo para redes adversas generativas" creado por Cornell University (arXiv: 1812.04948, 2019).



Figura 21. Muestra del Video Tutorial

Fuente: Autores

Además, es indispensable conocer las modalidades para denunciar este tipo de crímenes, en Colombia el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) cuenta con una herramienta virtual (Te protejo), la cual ayuda a denunciar de manera virtual a los ciberdelincuentes que hacen daños a menores, además de protegerlos y advertirles sobre esta situación. La policía Nacional estará enterada de todas las denuncias bajo este canal con el fin de que sea más pronta la judicialización (MinTic, 2016). Como parte de recomendaciones a los adolescentes, pero no parte de la herramienta se muestra un video el cual explica cómo funciona esta página web y aplicación que protege la integridad de los niños y adolescentes de Colombia (Vargas Trujillo. E.; Restrepo & Paz, 2015). A continuación, se mostraran unas imágenes de la aplicación y el uso que se le puede dar, recordando que el grooming se puede reportar en situaciones como: Material de abuso sexual, ciberacoso, contenidos inapropiados en medios de comunicación, o en otras situaciones con menores de 18 años



Figura 22. Pantalla de Inicio de “Te Protejo”
Fuente: Te protejo



Figura 23. . Situaciones que se pueden Denunciar en la Aplicación
Fuente: Te protejo

A parte de esta herramienta otorgada por el MINTIC, también existen otras entidades donde se puede acudir en caso de pasar por estas situaciones, como: marcar el 106 (la línea de ayuda nacional), ICBF (Instituto Colombiano de Bienestar Familiar), CAIVAS (Centro de Atención Integral a Víctimas de Abuso Sexual) o también se puede enviar un correo a: denunciamoselabusosexual@fiscalia.gov.co (Vargas Trujillo. E.; Restrepo & Paz, 2015).

7 INSTALACIÓN Y EJECUCIÓN DE LA HERRAMIENTA

Como objetivo principal del proyecto se basa en crear una herramienta de concientización de los peligros del grooming, por lo que se optó por realizar una herramienta que se integrará con funcionalidades de la red social Facebook, lo que permite que usuarios de Facebook pueden acceder con su cuenta y hacer uso de las aplicaciones que son subidas en la plataforma Facebook For Developers.

El uso de la herramienta de concentración de los peligros del grooming es dirigido hacia una población objetivo que involucra a jóvenes estudiantes de colegios distritales de Bogotá y colegios departamentales del municipio de Anolaima Cundinamarca.

7.1 INSTALACIÓN DE LA HERRAMIENTA

Esta herramienta es creada sobre el motor de desarrollo de Unity5, estructurada con el lenguaje programación c, y subida a la plataforma de Facebook Developers sitio oficial para aplicaciones y juegos que requieren de las funcionalidades de Facebook. Facebook For Developers brinda la posibilidad de aprovisionar varias aplicaciones en diferentes sistemas o plataformas de desarrollos de programación, como, por ejemplo, java, webg y sistemas operativos como androide Windows y Mac; lo que permite entregar a los desarrolladores de integración con el API de Facebook.

Si bien el desarrollo de la herramienta del proyecto se estructuro en Unity5 con su respectiva Unity SDK Facebook; la ejecución de la herramienta para el público en general y usuarios de Facebook se basa en un lenguaje Webgl que permite ejecutarse en los browsers Firefox y Google Crome. Debido a que esto es uno de los lenguajes que Facebook permite aprovisionar en su plataforma Facebook For Developers como lo podemos ver en la siguiente (Figura 23), además de que es una manera más fácil de ejecutarse para la población objetivo donde se quiere llegar, pues no dependería de un sistema operativo en específico ni mucho menos de una consola de videojuegos para su ejecución.

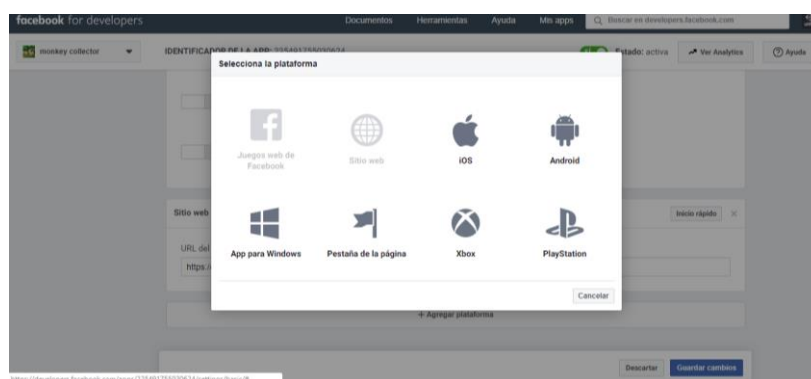


Figura 23. Compatibilidad de plataformas con Facebook.

Fuente: Autores

El motor de desarrollo Unity cuenta con la opción de construcción WebGL que permite la conversión de su mismo contenido de desarrollado que puede ser en c o java a un lenguaje HTML. Para construir y probar su contenido para WebGL, se dirige desde el motor Unity selecciona en el menú > File > Build, en ese momento se ejecuta una ventana de construcción WebGL(figura 24) > Build and run. La conversión WebGL entrega una carpeta con archivo HTML y archivos .json que contiene código de ejecución de reproducción entre el código anterior de Unity y el ahora de HTML, y archivos .data que contiene toda la información de la aplicación como escenas, gráficos, es decir, todos los elementos lógicos programados y que se configuraron en el motor de Unity para que la aplicación corriera de acuerdo a la lógica planteada.

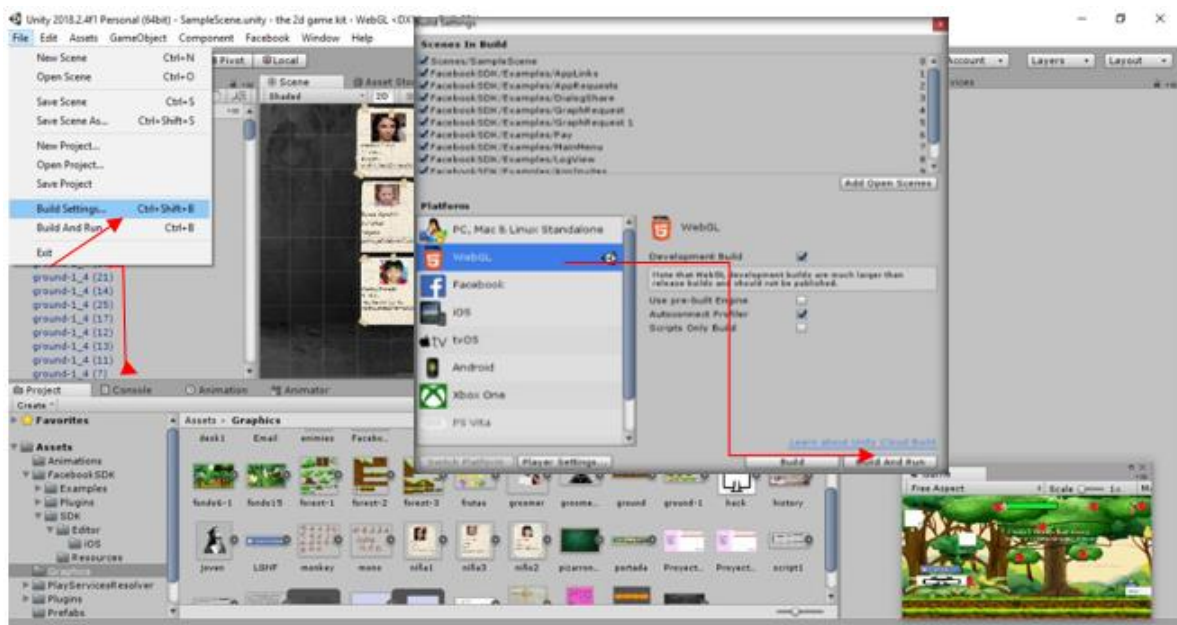


Figura 24. Built Settings WebGL
Fuente: Autores

7.2 EJECUCIÓN DE LA HERRAMIENTA

Los archivos WebGL quedan como un archivo ejecutable desde los navegadores conocidos, pero al ser un archivo que requiere conexión con Facebook, no puede ser ejecutado desde el localhost debido a que Facebook debe verificar los dominios desde donde se aloja la

aplicación para que los usuarios puedan hacer conexión con Facebook, para entonces los archivos Webgl deben ser llevados a un servidor web que con dominio donde Facebook lo pueda monitorear.

La herramienta tecnológica de concientización de los peligros del grooming está instalada desde un servidor web (WEBHOST) en internet que brinda servicios de alojamiento web, los usuarios podrán acceder a esta herramienta desde un enlace web. Para acceder a la herramienta se debe realizar desde un computador con acceso a internet y un navegador web (Google chrome, Firefox). El uso de la herramienta requiere acceder desde su cuenta en Facebook. Para realizar la solicitud de inicio de sesión con Facebook, la herramienta o aplicación debe estar aceptada en la plataforma Facebook For Developers. En la siguiente figura se podrá observa el diagrama de red de la herramienta.

DIGRAMA DE RED

Catalina and Nixon | April 8, 2019

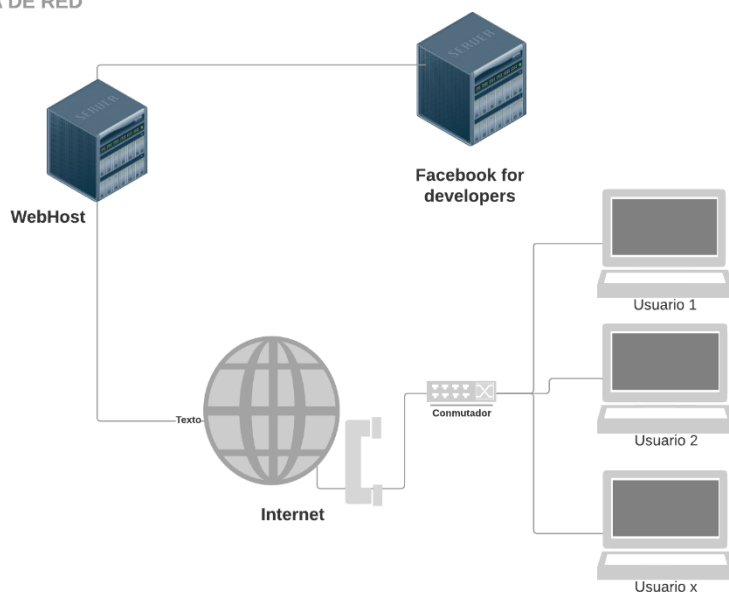


Figura 25. Diagrama de Red
Fuente: Autores

Facebook For Developers es la plataforma que se encarga de realizar a gestión del contenido de las aplicaciones que se sube allí, como las políticas de privacidad, términos y condiciones, (para este proyecto las podremos visualizar en ANEXO I) y dominios que cuentan con las apps, información que debe ser cargada allí para aquellas app que

requieran del inicio de sesión con Facebook; una vez son configurados los anteriores parámetros, Facebook For Developers hace la verificación de las aplicaciones, para aceptar que los usuarios realicen el inicio de sesión con Facebook.

En el siguiente link se podrá encontrar la herramienta de concientización de los peligros del grooming <https://monkeycollector.000webhostapp.com>, además está acompañada de una presentación PowerPoint y guías para el socializador (ver ANEXO I, J, K).

8 IMPLEMENTACIÓN DEL PROYECTO, USO DE LA HERRAMIENTA Y RESULTADOS OBTENIDOS

Para realizar la implementación del proyecto en las instituciones objetivo de Bogotá y del municipio de Anolaima, se envió los consentimientos informados a cada uno de los estudiantes implicados, y así primar la privacidad y derechos de los menores de edad (Ver ANEXO L) donde se informó que ninguno de los datos mostrados de los estudiantes en la herramienta de concientización de los peligros del grooming serían almacenados y usados para el beneficio propio de los autores del proyecto, así mismo los acudientes de los estudiantes autorizaron el uso de su información personal para beneficio del proyecto, es decir el uso de la información personal sólo por el tiempo que duró la actividad, según se puede confirmar en el ANEXO L.

Para la ejecución del proyecto se realizó mediante actividades organizadas en tres partes: la primera, es realizar una encuesta digital (ver ANEXO B), sobre los hábitos de seguridad de los estudiantes al utilizar Facebook, teniendo en cuenta que el proyecto está basado en la seguridad de la información personal en Facebook, la primera pregunta de la encuesta se realizó con el fin hacer un filtro si se utiliza Facebook y así poder continuar con las demás preguntas. La segunda parte, es usar la herramienta propuesta (mencionada en el desarrollo de la herramienta), en donde se ejecuta un acompañamiento en el cual se explica las distintas etapas descritas y la tercera parte, es la explicación del tema y socialización de la actividad.

Antes de empezar la actividad se solicita diligenciamiento de la encuesta que se adecuó a partir de los resultados de la prueba piloto y las sugerencias del Consultorio Estadístico. Un total de 103 estudiantes diligenciaron la encuesta cuyos resultados más importantes se muestran a continuación:

4. ¿Cual es la red social que más usas?

80 respuestas

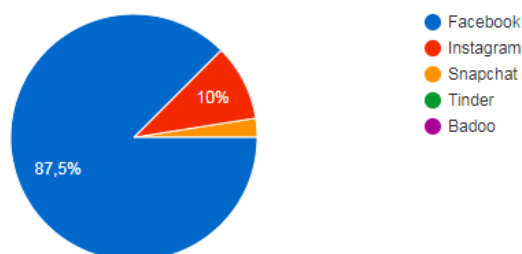


Figura 26. Resultado de la pregunta #4.
Fuente: Autores

10. ¿A quién le dirías en caso de sentirte en peligro en Facebook?

132 respuestas

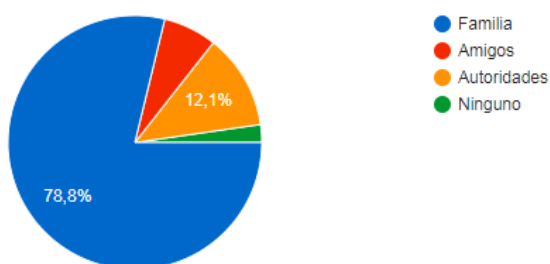


Figura 27. Resultado de la pregunta # 10
Fuente: Autores

12. ¿Crees lo que los demás publican en Facebook?

132 respuestas

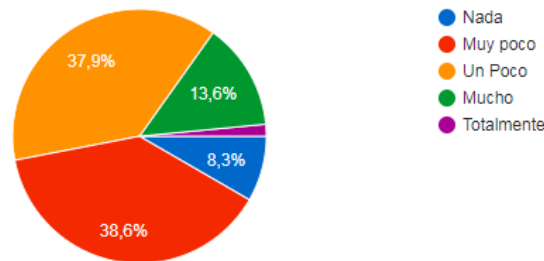


Figura 28. Resultado de la pregunta # 12
Fuente: Autores

Tabla 3. Relación de algunas de las respuestas de la encuesta realizada

¿A quién le dirías en caso de sentirte en peligro en Facebook?	¿Por qué?
Ninguno	porque me podrian hacer bullying mis amigos
Ninguno	porque mi familia no me creería
Ninguno	Me da miedo
Familia	porque me aconsejarían
Familia	los puede denunciar en cambio los amigos no asen nada

Figura 29. Relación de algunas de las respuestas de la encuesta realizada

Fuente: Autores

A continuación, durante la actividad se expone cada una de las partes de la herramienta, Se realizó un guion para el socializador (ver ANEXO H), el cual puede usarse en el momento que se vaya a implementar la herramienta, asimismo, se elaboró una guía (ver ANEXO I), con una presentación (ver ANEXO J), las dos últimas tienen como fin socializar toda la actividad (encuesta, herramienta y explicación del tema), teniendo en cuenta la problemática principal que es el grooming.

Al final de la actividad, se crea un video con una entrevista realizada a cuatro estudiantes y un profesor de las instituciones objetivo, con el fin de hacer una retroalimentación desde la perspectiva estudiantil hacia el grooming u otros peligros en la red, conociendo su opinión precedente al ejercicio y posterior a este. Las respuestas a la entrevista muestra que la

socialización de la problemática permite que los adolescentes logran identificar los peligros y será más posible que tomen acciones para protegerse (Ver ANEXO M).

9 CONCLUSIONES

El grooming es una problemática que en los últimos años se ha conocido con mayor claridad y siendo más frecuente por falta de conciencia de los adolescentes. Es importante tomar las medidas respectivas para que la población cuide sus datos personales en las redes sociales y así evitar que los más vulnerables de la sociedad paguen grandes consecuencias que pueden afectar su futuro.

Según las respuestas obtenidas en la encuesta, se pudo notar que los adolescentes se muestran indiferentes ante la problemática que trae el mal uso de su información en Facebook y lo vulnerables que pueden llegar a ser con cualquier mínimo detalle.

De acuerdo al estudio realizado, las herramientas de software que más se ajustara al desarrollo del proyecto, se pudo concluir que Unity es uno de los motores de desarrollo más completos para el proceso de creación de la herramienta tecnológica, debido a que contiene una gran variedad de elementos que facilitan el proceso de desarrollo. Además, cuenta con la opción de manejar dos lenguajes de programación como lo son C y Java, revisados en el proyecto. Por último, cuenta con la facilidad de conexión entre el API de Facebook con el motor de desarrollo, pues está integrado el SDK Unity Facebook y una herramienta que permite hacer ejecutable la aplicación en distintas plataformas, así como en los sistemas operativos más conocidos.

Acorde con las especificaciones del rol de los actores de la herramienta, todos juegan un papel muy importante, debido a que no es una aplicación específicamente para un solo actor, al contrario, involucra dos partes: el socializador y el público participante. De no haber un socializador, quizás al público participante no le sea claro el objetivo con en que se hizo la herramienta.

Durante el desarrollo de la herramienta se identificó que, solo basta con obtener los permisos que Facebook otorga por defecto a las aplicaciones que requieren el inicio de sesión, para llegar al perfil de la persona y obtener el resto de la información. De acuerdo con esto, se hizo un análisis de la situación y se concluyó que los datos como: nombre

del usuario, imagen de perfil y correo, son elementos claves a la hora de realizar una búsqueda y una selección de posibles víctimas por el groomer.

Ante este escenario, concluimos que elementos importantes para la seguridad de los datos en las redes sociales son: tener el perfil privado, revisar los permisos que se han entregado a las aplicaciones de Facebook y verificar que estas aplicaciones vengan de desarrolladores confiables, pues es de gran ayuda para evitar que groomer u otras personas tengan acceso a la información personal de cada uno.

Se identificó la importancia de dar a conocer a los jóvenes, la verificación de los permisos que se entregan a las aplicaciones, así mismo de leer los términos y condiciones antes de aceptarlos, pues es allí donde se encuentran los permisos que exigen para la interacción con la aplicación. Es necesario recalcar que así el perfil sea privado, al entregar aquellos permisos su información deja de ser privada.

Se pudo demostrar con la socialización de la actividad que al presentar experiencias de jóvenes los cuales fueron víctimas de este peligro en la red, dentro del desarrollo de la herramienta, generó impacto en los adolescentes, al saber que podrían jugar el mismo papel de víctimas, si no hacen un buen manejo de sus datos en las redes sociales.

En el uso de la herramienta en los colegios se observó que los adolescentes aprendieron no solo de los peligros que puede haber en las redes sociales, sino también, cómo evitar ser víctima y a quien acudir en caso de serlo, además, varios de los profesores se muestran interesados para servir como socializadores en su área de trabajo.

10 TRABAJOS FUTUROS

Para la continuación del trabajo se propone adecuar la aplicación para facilitar el acceso a otros permisos de Facebook que permiten obtener más información del usuario, se aconseja tener disponibilidad, debido a la cantidad de tiempo que toma la respuesta por parte de la red social Facebook. Adicionalmente, se propone el estudio de una población más amplia de la que se trabajó en el presente proyecto, con el fin de atraer interesados que cumplan con el rol de socializadores y generar una posible cadena contra peligros en las redes sociales.

Asimismo, se sugiere que se integre la encuesta que se realizó con Google Forms dentro de la herramienta, con el fin visualizar y estudiar los resultados generados cada vez que se use dicha herramienta, optimizando los recursos.

Por último, se propone que la aplicación genere estadísticas anónimas de los usuarios que han hecho uso de ella para conocer la cantidad de población que se ha beneficiado con esta herramienta.

REFERENCIAS

INVERSIA - Stadio Alicante. (2013). Privacidad y seguridad en las Redes Sociales, un problema actual. Retrieved June 19, 2018, from <http://noticias.universia.net.mx/en-portada/noticia/2013/03/01/1008138/privacidad-seguridad-redes-sociales-problema-actual.html>

MILENIO - KATIA LEYVA. (2017). El peligro de tener redes sociales antes que cédula. Retrieved June 19, 2018, from <https://sipse.com/milenio/adiccion-adolescentes-redes-sociales-causas-260583.html>

ALEJANDRA MONTES SOTELO. (2016). BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA. Retrieved from http://eprints.rclis.org/29200/1/Montes_BUAP_2016_redes.pdf

Socidrogalcohol (Society), E., & Corral, P. de. (2010). *Adicciones. Adicciones* (Vol. 22). Socidrogalcohol. Retrieved from

LA COMISIÓN FEDERAL DE COMERCIO. (1998). Facebook, Inc. | Comisión Federal de Comercio. Retrieved July 6, 2018, from <https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc>

facebook. (2018). ¿Cómo reporto a un menor de 13 años? | Servicio de ayuda de Facebook. Retrieved July 6, 2018, from https://www.facebook.com/help/157793540954833?helpref=uf_permalink

EXPANSION con alianza CCN. (2012). El 3.5% de los usuarios en Facebook en EU son niños menores de 13 años | Expansión. Retrieved July 7, 2018, from <https://expansion.mx/tecnologia/2012/09/20/el-35-de-los-usuarios-en-facebook-en-eu-son-ninos-menores-de-13-anos>

facebook. (2018). Menores y privacidad | Servicio de ayuda de Facebook. Retrieved July 6, 2018, from https://www.facebook.com/help/473865172623776?helpref=faq_content

Ninggal, M. I. H., & Abawajy, J. (2011). Privacy Threat Analysis of Social Network Data (pp. 165–174). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-24669-2_16

Ana Martín del Campo. (n.d.). Las Redes Sociales más utilizadas: cifras y estadísticas. Retrieved June 28, 2018, from <https://www.iebschool.com/blog/medios-sociales-mas-utilizadas-redes-sociales/>

BRIAN X. CHEN. (2018). Consejos para protegerte (y a tus amigos) en Facebook – Español. Retrieved June 28, 2018, from <https://www.nytimes.com/es/2018/03/21/facebook-seguridad-privacidad-consejos/>

SHERR, I. (2018). Facebook, Cambridge Analytica y tus datos: Todo lo que debes saber del escándalo y cómo te afecta a ti.

Marcelino Madrigal. (2012). Grooming y sexting en Facebook. Retrieved June 19, 2018, from <https://www.mmadrigal.com/grooming-y-sexting-en-facebook/>

Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). In Their Own Words: Young Peoples' Vulnerabilities to Being Groomed and Sexually Abused Online. *Psychology*, 05(10), 1185–1196. <https://doi.org/10.4236/psych.2014.510131>

de Santisteban, P., del Hoyo, J., Alcázar-Córcoles, M. Á., & Gámez-Guadix, M. (2018). Progression, maintenance, and feedback of online child sexual grooming: A qualitative analysis of online predators. *Child Abuse & Neglect*, 80, 203–215. <https://doi.org/10.1016/j.chiabu.2018.03.026>

Flores Fernández, J. (n.d.). Decálogo para combatir el Grooming en Internet. Retrieved from www.PantallasAmigas.net

Gottschalk, P. (2011). Journal of Computing:: A Dark Side of Computing and Information Sciences: Characteristics of Online Groomers, 2(9). Retrieved from <http://www.cisjournal.org447>

Ashcroft, M., Kaati, L., & Meyer, M. (2015). A Step Towards Detecting Online Grooming -- Identifying Adults Pretending to be Children. In *2015 European Intelligence and Security Informatics Conference* (pp. 98–104). IEEE. <https://doi.org/10.1109/EISIC.2015.41>

Rybnicek, M., Poisel, R., & Tjoa, S. (2013). Facebook Watchdog: A Research Agenda for Detecting Online Grooming and Bullying Activities. In *2013 IEEE International Conference on Systems, Man, and Cybernetics* (pp. 2854–2859). IEEE. <https://doi.org/10.1109/SMC.2013.487>

lovelle, m.i., soria, m.a. & garcía, V. (2014). Agresores en alerta y adolescentes en la “Nube” Grooming on–line. Retrieved from <http://diposit.ub.edu/dspace/bitstream/2445/101995/1/636839.pdf>

Abascal, E., & Esteban, I. G. (2005). *Análisis de encuestas*. Retrieved from [https://books.google.com.co/books?id=qFczoOiwRSgC&lpg=PA9&ots=eBZCiaP5Zd&dq=Abascal%2C E.%2C %26 Esteban%2C I. G. \(2005\). Análisis de encuestas. Esic Editorial&hl=es&pg=PA21#v=onepage&q&f=false](https://books.google.com.co/books?id=qFczoOiwRSgC&lpg=PA9&ots=eBZCiaP5Zd&dq=Abascal%2C%20E.%2C%20%26%20Esteban%2C%20I.%20G.%20(2005).%20Análisis%20de%20encuestas.%20Esic%20Editorial&hl=es&pg=PA21#v=onepage&q&f=false)

Tomás-Sábado, J. (n.d.). *Fundamentos de bioestadística y análisis de datos para enfermería*. Tomás-Sábado, J. (2010). Retrieved from http://www.conductitlan.org.mx/04_Investigacion/Materiales/L_Tomas-Sabado_muestreoparaenfermeria.pdf

Carlos Ochoa. (2015). Muestreo probabilístico o no probabilístico. Retrieved from <https://www.netquest.com/blog/es/blog/es/muestreo-probabilistico-o-no-probabilistico-ii>

Vivanco Arancibia, M. (2006). MUESTREO ESTADISTICO. DISEÑO Y APLICACIONES, 1, 212. Retrieved from <https://books.google.com.co/books?id=->

_gr5l3LbpIC&lpg=PA149&dq=Vivanco%2C M. (2005). Muestreo estadístico. Diseño y aplicaciones. Editorial Universitaria.&pg=PA149#v=onepage&q=Vivanco, M. (2005). Muestreo estadístico. Diseño y aplicaciones. Editorial Universitaria.&f=false

MORALES, R. (2014). Lenguajes de programación: ¿qué son y para qué sirven? Retrieved July 7, 2018, from <https://colombiadigital.net/actualidad/articulos-informativos/item/7669-lenguajes-de-programacion-que-son-y-para-que-sirven.html>

Abel, P., & Ibarra Mercado, V. H. (1996). *Lenguaje ensamblador y programación para PC IBM Y compatibles*. Prentice Hall.

AULA FORMATIVA. (2016). Definición, usos y ventajas del lenguaje HTML5. Retrieved July 10, 2018, from <http://blog.aulaformativa.com/definicion-usos-ventajas-lenguaje-html5/>

Java, O.-. (n.d.). Descarga del software Java. Retrieved from <https://www.java.com/es/download/>

Groussard, T. (2014). *Java 8: los fundamentos del lenguaje Java*. Ediciones ENI. Retrieved from <https://books.google.es/books?hl=es&lr=&id=9zWOQpRm0AoC&oi=fnd&pg=PA11&dq=java+lenguaje+de+programacion&ots=ELPtEtI19-&sig=yafxaPULF49uByqnzjzyMOuzQIQ#v=onepage&q=java+lenguaje+de+programacion&f=false>

Paipa, L. (n.d.). Programación java : VENTAJAS Y DESVENTAJAS DE JAVA. Retrieved June 28, 2018, from <http://programemosenjava.blogspot.com/2014/04/ventajas-y-desventajas-de-java.html>

Twago Community. (n.d.). Java, características y ventajas de uno de los lenguajes de programación más populares. Retrieved June 28, 2018, from

<https://www.twago.es/blog/java-ventajas-caracteristicas-lenguaje-programacion-mas-populares/>

Yedith, A. (2015). Pacman en java codigo tutorial explicado. Retrieved from <https://www.mbajava.com/2015/07/pacman-en-java-codigo-tutorial.html>

Yedith, A. (2014). Ajedrez Desarrollado En Java Utilizando Netbeans Con Tiempos. Retrieved from https://www.youtube.com/watch?v=1I_SpvjvHSs

Díaz, D. (2015). Triki en java netbeans. Retrieved from <https://www.youtube.com/watch?v=9r9wZuOTPtE>

Cárdenas, D.-A. A. C. (2016). Ventajas y desventajas de programar en C++. Retrieved June 28, 2018, from <http://adictoalcodigo.blogspot.com/2016/07/ventajas-y-desventajas-de-programar-en-c.html>

EcuRed. (n.d.). C++. Retrieved June 28, 2018, from <https://www.ecured.cu/C%2B%2B>

Pascual, F. L., & Pérez López, E. (n.d.). C++-OO como lenguaje introductorio a la programación. Retrieved from <http://bioinfo.uib.es/~joemiro/aenui/procJenui/ProcWeb/actas2001/llcoo107.pdf>

Rondón, A. (2015). Como hacer el ahorcado en c++. Retrieved from <https://www.youtube.com/watch?v=wUzzbWTpILo>

Brunosg2002. (2011). Game Mario Bros made in C++/Allegro. Retrieved from <https://www.youtube.com/watch?v=DjbCRfWn5qE>

AULA FORMATIVA. (2016). Definición, usos y ventajas del lenguaje HTML5. Retrieved July 10, 2018, from <http://blog.aulaformativa.com/definicion-usos-ventajas-lenguaje-html5/>

HiperText Markup Language, V. 5. (2013). Ventajas y desventajas. Retrieved July 10, 2018, from <https://unbermenchdotcom.wordpress.com/ventajas-y-desventajas/>

Diez, T., Domínguez, M. J., Martínez, J. J., Joseba, J., & De Navarrete, S. (n.d.). Creación de páginas Web accesibles con HTML5. Retrieved from http://www.esvial.org/wp-content/files/Atica2012_pp120-129.pdf

Leticia Vela. (2010). FACEBOOK SE PASA A HTML5 Y DEJA A UN LADO A ADOBE FLASH. Retrieved from <https://www.tuexperto.com/2010/04/29/facebook-se-pasa-a-html5-y-deja-a-un-lado-a-adobe-flash/>

Powtoon. (2018). Powtoon | Make it awesome. Retrieved from <https://www.powtoon.com/home/?>

Quiroz, N. (n.d.). Powtoon. Retrieved June 28, 2018, from <http://powtoontherramienta.blogspot.com/>

modelo presentaciones. (n.d.). Características de las plantillas Powtoon. Retrieved June 28, 2018, from <https://www.modelopresentacion.com/caracteristicas-de-las-plantillas-powtoon.html>

Recursos educativos digitales - Gobierno de Canarias. (n.d.). Herramienta: Powtoon. Retrieved June 28, 2018, from <http://www3.gobiernodecanarias.org/medusa/ecoescuela/recursosdigitales/2015/09/29/herramienta-powtoon/>

Blog Luis Villa - INFORMÁTICA. (n.d.). Ventajas y desventajas de Powtoon. Retrieved June 19, 2018, from <http://blogluisavilla.blogspot.com/2015/11/ventajas-y-desventajas-de-powtoon.html>

SoftwareDoit. (n.d.). DEFINICIÓN TÉRMINOS DE SOFTWARE. Retrieved from <https://www.softwaredoit.es/definicion/index.html>

HardSoftware. (2010). Ventajas y desventajas de flash. Retrieved June 28, 2018, from <http://hardsoftware.es/innovacion/ventajas-y-desventajas-de-flash>

Juan Carlos - Blogspot Recursos flash. (2011). DEFINICIÓN Y CARACTERÍSTICAS DE ADOBE FLASH CS4. Retrieved June 28, 2018, from <http://recursos-flash.blogspot.com/2011/06/definicion-y-caracteristicas-de-adobe.html>

Jenifer - Blogspot. (2011). FLASH: Concepto de Flash y sus características. Retrieved June 28, 2018, from <http://jenifer-todoflash.blogspot.com/2011/06/concepto-de-flash-y-sus-caracteristicas.html>

HardSoftware. (2010). Ventajas y desventajas de flash. Retrieved June 28, 2018, from <http://hardsoftware.es/innovacion/ventajas-y-desventajas-de-flash>

Alavedra, I. (2012). Animacion de Personaje en Adobe Flash. Retrieved from <https://www.youtube.com/watch?v=IVugCIHr8Ec>

Unity Technologies. (2019). Unity | Home. Retrieved from <https://unity3d.com/es>

Fenrir - La leyenda de Darwan. (2017). Cinco cosas buenas y cinco no tan buenas de Unity 3D. Retrieved June 28, 2018, from <https://laleyendadedarwan.es/2017/12/21/cinco-cosas-buenas-y-cinco-no-tan-buenas-de-unity-3d/>

Mula, J.-D. F. (n.d.). Las principales características de Unity 2017. Retrieved June 28, 2018, from <https://www.deustoformacion.com/blog/programacion-diseno-web/principales-caracteristicas-unity-2017>

Luttecke, C.-Z. (n.d.). ¿Sabes que es UNITY? Retrieved June 28, 2018, from <https://deideaaaapp.org/sabes-que-es-unity-descubrelo-aqui/>

Jordisan. (2006). ¿Qué es un 'framework'? Retrieved from <https://jordisan.net/blog/2006/que-es-un-framework/>

Facebook. (2019). Facebook for developers. Retrieved from <https://developers.facebook.com/docs>

Medina, D. F. (2018). Grooming: El Mayor Riesgo Del Desconocimiento Que Existe Una Ley Es La “No Denuncia.” Retrieved from <http://elcorreografico.com.ar/grooming-el-mayor-riesgo-del-desconocimiento-que-existe-una-ley-es-la-no-denuncia/>

Magic Markers. (2017). ¿Qué es el grooming? Retrieved from <https://www.youtube.com/watch?v=OdixH25nCHk>

MinTic. (2016). MinTIC invita a denunciar los abusos contra menores de edad en Internet. Retrieved from <https://www.mintic.gov.co/portal/604/w3-article-15041.html>

Vargas Trujillo. E.; Restrepo, A. M., & Paz, R. pa. (2015). Kit PaPaz prevención del riesgo y manejo del abuso sexual en línea. Retrieved from <http://redpapaz.org/prasi/index.php/component/k2/item/57-donde-denunciar>

ICBF, I. C. de B. F. (2019). Ley de infancia y adolescencia. Retrieved from <https://www.icbf.gov.co/bienestar/ley-infancia-adolescencia>

arXiv: 1812.04948. (2019). Una arquitectura generadora basada en el estilo para redes adversas generativas.

Facebook. (2019). Privacidad del perfil y la biografía. Retrieved from <https://www.facebook.com/help/www/393920637330807/>

ANEXOS

ANEXO A. CONSENTIMIENTO INFORMADO



UNIVERSIDAD SANTO TOMÁS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA

VIGILADA MINEDUCACIÓN - SNIES: 1704



El semillero de investigación MAGNADATA junto con el grupo INVTEL de la Facultad de Ingeniería de Telecomunicaciones de la Universidad Santo Tomás se han propuesto socializar en la comunidad (Adolescentes, Padres, Profesores) los peligros presentes en las redes sociales. Para esto se presentó el proyecto "HERRAMIENTA DE SOFTWARE PARA CONCIENTIZACIÓN DE RIESGOS DE GROOMING POR MALA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PERSONAL EN FACEBOOK" cuyo objetivo es "Elaborar una herramienta de software de concientización de riesgos de grooming por mala gestión de seguridad de la información personal en Facebook, para estudiantes de secundaria".

El proyecto se basa en presentar una herramienta, la cual los estudiantes principalmente de colegios distritales de Chapinero que cursan grados decimo y once la utilicen, al final muestre los riesgos de compartir información en Facebook y los peligros a los que se pueden enfrentar como el grooming.

La metodología se propone para generar consciencia en la comunidad (adolescentes, padres y/o profesores) de los peligros presentes en las redes sociales. Para lograr esto, es necesario que los adolescentes individualmente realicen un juego en Facebook accediendo a todas las condiciones y términos de privacidad que este juego pide.

Al aceptar estas condiciones el juego tendrá varios permisos para acceder a toda la información del que esté usando el juego. Al final se mostrará una animación que evidencia la captura de datos.

Para el ejercicio anterior existirá un socializador quien este guiando a los adolescentes y pueda sacar estadísticas y conclusiones del ejercicio.

Se busca que la herramienta le muestre a los adolescentes lo que podría hacer un groomer (personas adultas que engañan a adolescentes y/o niños para tener una satisfacción sexual ya sea violación u obtención de fotos íntimas u otro tipo de información) con la información personal publicada en Internet. Al final presenta una forma para cambiar las opciones de privacidad en Facebook. En detalle la clase tendrá las siguientes características:

- Se obtendrá alguna información compartida de red social de Facebook del usuario
- La información se trabajará bajo confidencialidad y responsabilidad
- Toda la información obtenida será borrada y no se almacenará

Luego de conocer la actividad a realizar con los niños y niñas:

1. Como adulto responsable por el niño o la niña: _____, acepto voluntariamente su participación en una jornada en el contexto escolar.
2. Permito que se tomen fotografías o videos del ejercicio, SIEMPRE Y CUANDO ÉSTAS SÓLO SEAN CON FINES ACADÉMICOS Y NO SEAN REPRODUCIDAS CON FINES COMERCIALES.
3. Permito la participación del niño o la niña: _____, siempre y cuando en TODO MOMENTO estén presentes las y los docentes responsables por él o ella en el contexto escolar donde se realizará el ejercicio.
4. Permito la participación del niño o la niña: _____, siempre y cuando me sea informado el resultado de la actividad y pueda tener acceso al material audiovisual o al documento de resultados de la jornada.

NOMBRE DEL PADRE Y/O ACUDIENTE:

FIRMA: _____ C.C. _____

FECHA: /__/__/__/

RUTA DE PUBLICACIÓN: <https://monkeycollector.000webhostapp.com/>

ANEXO B. ENCUESTA

Encuesta de hábitos en redes sociales

***Obligatorio**

¿Tienes cuenta en Facebook? * *Marca solo un óvalo.*

Sí *Pasa a la pregunta 1.*

No *Pasa a "Debes de tener cuenta en Facebook para contestar este formulario, gracias.."*

1. ¿Cuántos años tienes? * *Marca solo un óvalo.*

12 años

13 años

14 años

15 años

16 años

17 años

18 años

2. Género * *Marca solo un óvalo.*

Masculino

Femenino

3. ¿Cómo entras a Internet? * *Marca solo un óvalo.*

Datos móviles/Paquetes de datos

WiFi del colegio

WiFi del hogar

Café Internet

4. ¿Cual es la red social que más usas? * *Marca solo un óvalo.*

Facebook

Instagram

Snapchat

Tinder

Badoo

5. ¿Cuánto tiempo al día usas las redes sociales? * *Marca solo un óvalo.*

Menos de 15 minutos

Entre 15 y 30 minutos

Entre 30 minutos y 1 hora
Entre 1 y 2 horas
Entre 2 y 6 horas
Más de 6 horas

6. ¿Cuántos amigos tienes en Facebook? * *Marca solo un óvalo.*

Menos de 100
Entre 100 y 1200
Entre 200 y 300
Entre 300 y 400
Entre 400 y 500
Entre 500 y 600
Entre 600 y 700
Mas de 700

7. ¿Cuántos amigos de Facebook conoces en la vida real? * *Marca solo un óvalo.*

81% - 100%
61% - 80%
41% - 60%
21% - 40%
0 - 20%

8. La mayoría de tus amigos de Facebook son: * *Marca solo un óvalo.*

Familia
Amigos
Compañeros del colegio
Amigos de amigos
Desconocidos

9. ¿Conoces los peligros que pueden haber en Facebook? * *Marca solo un óvalo.*

Sí
No

10. ¿A quién le dirías en caso de sentirte en peligro en Facebook? * *Marca solo un óvalo.*

Familia
Amigos
Autoridades
Ninguno

11. ¿Por qué? *

12. ¿Crees lo que los demás publican en Facebook? * *Marca solo un óvalo.*

Nada
Muy poco
Un Poco
Mucho
Totalmente

13. ¿Aceptas invitaciones de aplicaciones o juegos en Facebook? * *Marca solo un óvalo.*

Sí
No

14. Si alguna aplicación Facebook pregunta tu información personal (Nombre completo, fecha de nacimiento, dirección, etc.), ¿tu la entregas? * *Marca solo un óvalo.*

Nunca
A menudo
Usualmente
Casi siempre
Siempre

15. ¿Sabes cómo un delincuente puede obtener tu información personal de Facebook? * *Marca solo un óvalo.*

Sí
No

16. ¿Lees los términos y condiciones de los juegos antes de usarlos? * *Marca solo un óvalo.*

Sí
No

Debes de tener cuenta en Facebook para contestar este formulario, gracias.

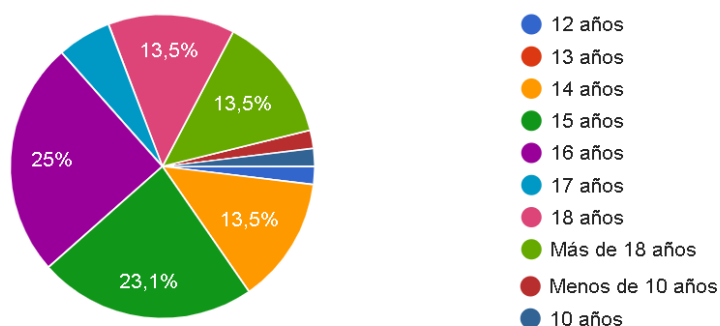
Con la tecnología de



ANEXO C. RESPUESTAS PRUEBA PILOTO

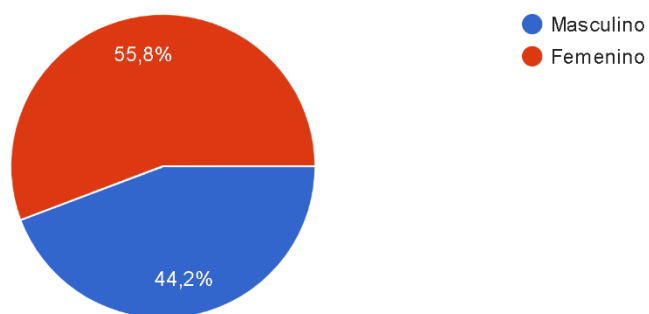
1. ¿Cuántos años tienes?

52 respuestas



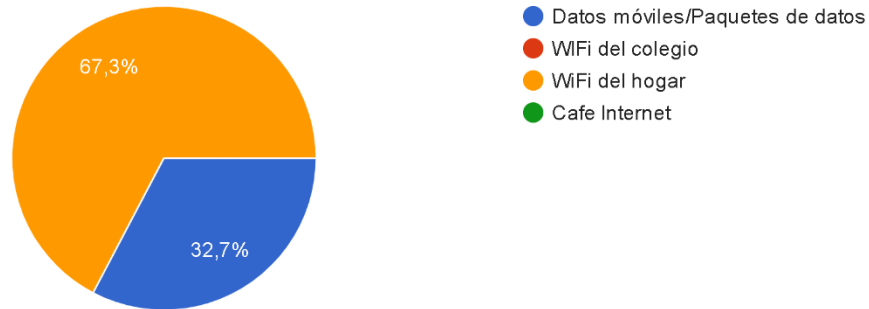
2. Genero

52 respuestas



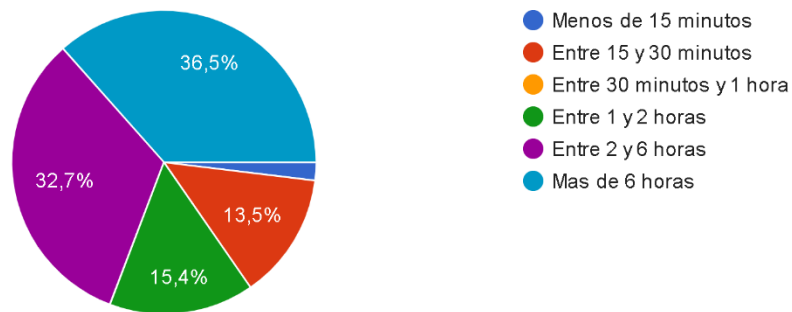
3. ¿Cómo entras a Internet?

52 respuestas



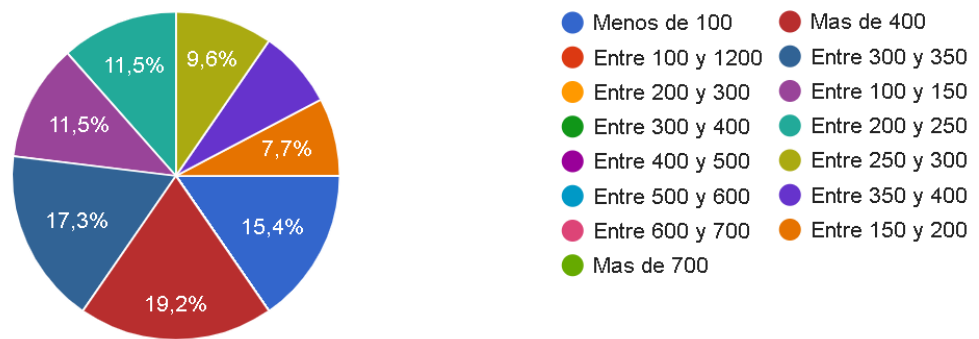
5. ¿Cuánto tiempo al día usas las redes sociales?

52 respuestas



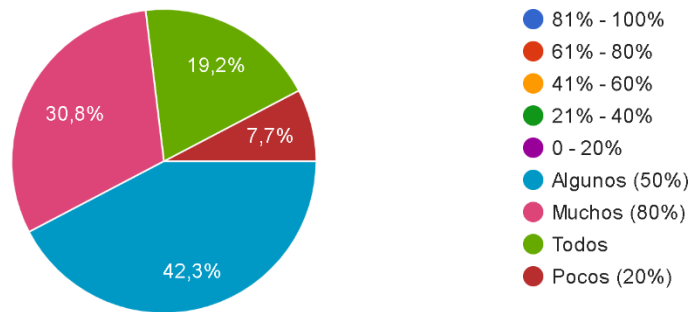
6. ¿Cuántos amigos tienes en Facebook?

52 respuestas



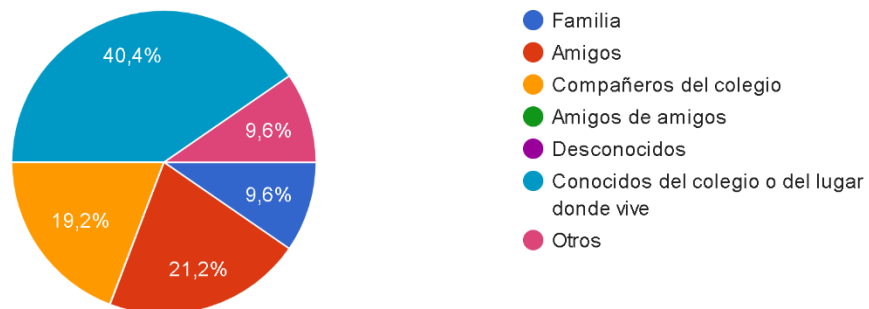
7. ¿Cuántos amigos de Facebook conoces en la vida real?

52 respuestas



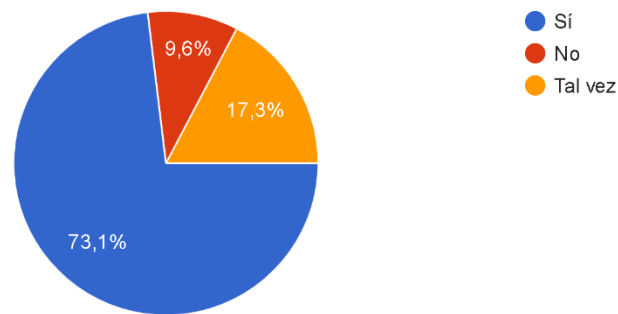
8. La mayoría de tus amigos de Facebook son:

52 respuestas



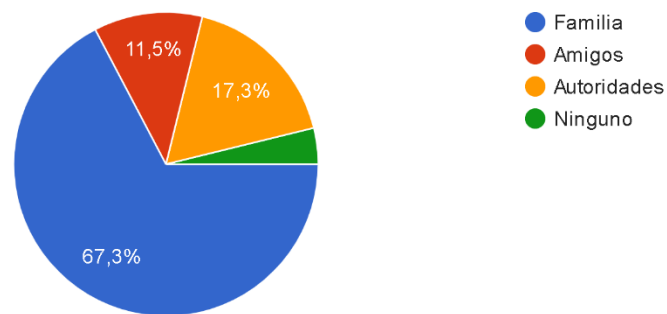
9. ¿Conoces los peligros que pueden haber en Facebook?

52 respuestas



10. ¿A quién le dirías en caso de sentirte en peligro en Facebook?

52 respuestas



11. ¿Por qué?

52 respuestas

Por que es mi apoyo moral y son las personas que tengo confianza
porque me podrian hacer bullyng mis amigos
porque mi familia no me creeria
porque me aconsejarian
Por qué les tengo confianza
Por que dirían que hacer
Son las personas que nos pueden guiar y aconsejar sobre cómo proceder frente a este peligro
Tengo mas confianza en ellos
Para que me aconsejen que hacer
Por qué son los que pueden hacer algo al respecto

Primero hablar con la familia para tomar una solución y medidas necesarias

Por que me pueden ayudar a resolver el caso de peligro que tengo

Para que me guíen

Confianza

Porque me pueden secuestrar o desaparecer

Porque ellos son los expertos en el tema y brindan apoyo a los casos de fraudes y acosos por Internet

Por que se que me pueden ayudar con ese problema si se llegara a presentar

Son los de más confianza

Son los unicos que pueden tener manejo sobre la situación

Porque responden por mi

Peligro

Son las personas en que más confío

les tengo mucha confianza

Ellos siempre me han apoyado, confío en ellos, sabrían que hacer
me da miedo

Por Que Son Base Fundamental Para Ayudarme A Solucionar Mis Problemas.

porque nunca me pasara

Son de confianza

por es lo mas seguro

Porque me puede suceder algo y ellos estarían informados

La Familia es de mayor confianza

Por que ellos deberian saber que accion tomar ante cualquier peligro

Confianza

Porque ellos tienen las capacidades para ayudar a solucionar los problemas

Porque siemore están para mi y quieren mi bienestar

Por q ellos me ayudaran a solucionarlo

Por qué son las personas que les tengo la confianza

Porque es las personas mas cercanas

Por que ellos pueden poner alto al asunto

Porque puede pasarme algo

Porque ellos entienden de estos temas

Porque es lo mejor e iría con ellos a las autoridades

Porque si

Le diría a mi mamá por ella sabría que hacer

Creo que son las primeras personas en saber ya que ellos me Brindan la confianza

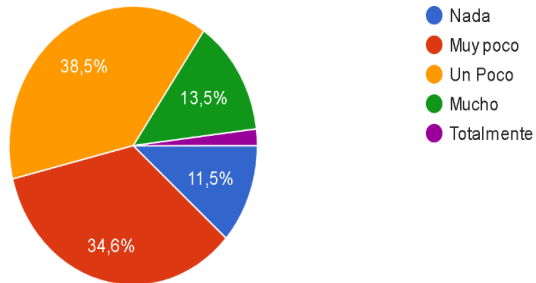
Por qué son la fuente más confiable

Porque me quieren y me darán la solución por mi bien

Porque me siento más segura de hablar del peligro en las redes sociales con mi familia

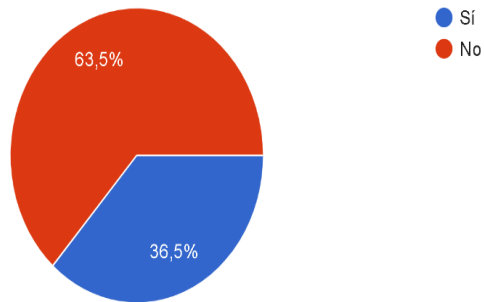
12. ¿Crees lo que los demás publican en Facebook?

52 respuestas



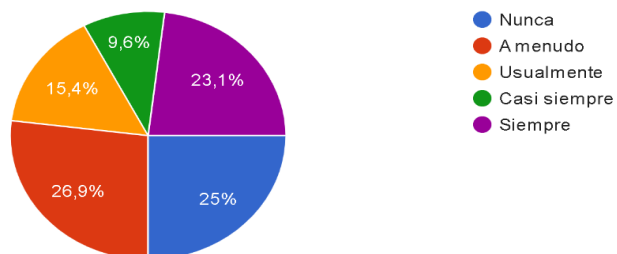
13. ¿Aceptas invitaciones de aplicaciones o juegos en Facebook?

52 respuestas



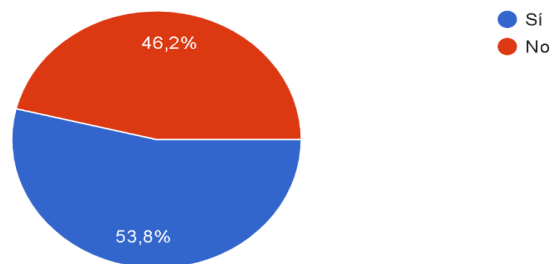
14. Si alguna aplicación Facebook pregunta tu información personal (Nombre completo, fecha de nacimiento, dirección, etc.), ¿tu la entregas?

52 respuestas



15. ¿Sabes cómo un delincuente puede obtener tu información personal de Facebook?

52 respuestas



Dentro de este anexo hace falta las preguntas 4 y 16, porque cuando se hizo la prueba piloto no estaba incluidas, posterior a estos resultados se agregaron estas dos preguntas que se mostrarán a continuación:

4. ¿Cual es la red social que más usas?

0 respuestas

Aún no hay respuestas para esta pregunta.

16. ¿Lees los términos y condiciones de los juegos antes de usarlos?

0 respuestas

Aún no hay respuestas para esta pregunta.

ANEXO D. TABULACIÓN DE RESPUESTAS PRUEBA PILOTO

Preguntas

1. ¿Cuántos años tienes?
2. Género
3. ¿Cómo entras a Internet?
4. ¿Cuánto tiempo al día usas las redes sociales?
5. ¿Cuántos amigos tienes en Facebook?
6. ¿Cuántos amigos de Facebook conoces en la vida real?
7. La mayoría de tus amigos de Facebook son:
8. ¿Conoces los peligros que pueden haber en Facebook?
9. ¿A quién le dirías en caso de sentirte en peligro en Facebook?
10. ¿Por qué?
11. ¿Crees lo que los demás publican en Facebook?
12. ¿Aceptas invitaciones de aplicaciones o juegos en Facebook?
13. Si alguna aplicación Facebook pregunta tu información personal ¿tu la entregas?
14. ¿Sabes cómo un delincuente puede obtener tu información personal de Facebook?

#	Preguntas													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	< 10 años	Masculino	WiFi del hogar	Entre 2 y 6 horas	Menos de 100	Algunos (50%)	Familia	Sí	Familia	Por qué les tengo confianza	Un Poco	No	Casi siempre	Sí
2	10 años	Femenino	WiFi del hogar	Entre 1 y 2 horas	Menos de 100	Todos	Compañeros del colegio	Sí	Familia	Por que dirían que hacer	Mucho	No	Nunca	Sí
3	> 18 años	Femenino	WiFi del hogar	Entre 2 y 6 horas	Entre 350 y 400	Algunos (50%)	Conocidos del colegio o del lugar donde vive	Sí	Familia	Son las personas que nos pueden guiar y aconsejar sobre cómo proceder frente a este peligro	Muy poco	Sí	Nunca	No
4	16 años	Masculino	WiFi del hogar	Mas de 6 horas	Mas de 400	Algunos (50%)	Conocidos del colegio o del lugar donde vive	No	Familia	Tengo mas confianza en ellos	Un Poco	No	Siempre	No
5	16 años	Femenino	WiFi del hogar	Mas de 6 horas	Entre 100 y 150	Todos	Familia	Sí	Familia	Por que es mi apoyo moral y son las personas que tengo confianza	Muy poco	No	Casi siempre	Sí

6	15 años	Femenino	WiFi del hogar	Mas de 6 horas	Menos de 100	Pocos (20%)	Compañeros del colegio	Sí	Familia	Para que me aconsejen que hacer	Muy poco	No	A menudo	Sí
7	18 años	Masculino	WiFi del hogar	Entre 2 y 6 horas	Mas de 400	Algunos (50%)	Conocidos del colegio o del lugar donde vive	Sí	Autoridades	Por qué son los que pueden hacer algo al respecto	Un Poco	Sí	Nunca	Sí
8	14 años	Femenino	WiFi del hogar	Entre 2 y 6 horas	Entre 200 y 250	Algunos (50%)	Conocidos del colegio o del lugar donde vive	Tal vez	Familia	Primero hablar con la familia para tomar una solucion y medidas necesarias	Muy poco	No	A menudo	No
9	16 años	Masculino	WiFi del hogar	Entre 1 y 2 horas	Entre 100 y 150	Algunos (50%)	Amigos	Tal vez	Familia	Por que me pueden ayudar a resolver el caso de peligro que tengo	Un Poco	No	Usualmente	No
10	16 años	Femenino	WiFi del hogar	Mas de 6 horas	Entre 100 y 150	Todos	Familia	Sí	Familia	Por que es mi apoyo moral y son las personas que tengo confianza	Muy poco	No	Casi siempre	Sí
11	15 años	Femenino	WiFi del hogar	Entre 15 y 30 minutos	Entre 100 y 150	Todos	Compañeros del colegio	Sí	Familia	Para que me guíen	Muy poco	No	Usualmente	Sí

12	14 años	Masculino	WiFi del hogar	Entre 2 y 6 horas	Entre 100 y 150	Muchos (80%)	Amigos	Tal vez	Amigos	Confianza	Muy poco	Sí	Siempre	No
13	12 años	Masculino	WiFi del hogar	Entre 15 y 30 minutos	Menos de 100	Todos	Familia	Sí	Familia	Porque me pueden secuestrar o desaparecer	Nada	No	Siempre	Sí
14	> 18 años	Masculino	Datos móviles/Paquetes de datos	Entre 15 y 30 minutos	Entre 100 y 150	Muchos (80%)	Amigos	Sí	Autoridades	Porque ellos son los expertos en el tema y brindan apoyo a los casos de fraudes y acosos por Internet	Un Poco	Sí	Usualmente	Sí
15	16 años	Femenino	WiFi del hogar	Mas de 6 horas	Entre 300 y 350	Algunos (50%)	Conocidos del colegio o del lugar donde vive	Sí	Familia	Por que se que me pueden ayudar con ese problema si se llegara a presentar	Nada	No	Usualmente	Sí
16	18 años	Masculino	WiFi del hogar	Mas de 6 horas	Entre 350 y 400	Muchos (80%)	Compañeros del colegio	Sí	Familia	Son los de más confianza	Mucho	No	Nunca	Sí
17	16 años	Femenino	WiFi del hogar	Mas de 6 horas	Entre 250 y 300	Muchos (80%)	Otros	Sí	Autoridades	Son los unicos que pueden tener	Un Poco	No	Usualmente	Sí

										manejo sobre la situacion				
18	16 años	Masculino	WiFi del hogar	Entre 2 y 6 horas	Menos de 100	Todos	Compañeros del colegio	Sí	Familia	Porque responden por mi	Un Poco	No	A menudo	Sí
19	15 años	Femenino	WiFi del hogar	Entre 2 y 6 horas	Entre 350 y 400	Algunos (50%)	Conocidos del colegio o del lugar donde vive	Sí	Familia	Peligro	Muy poco	No	A menudo	Sí
20	15 años	Masculino	WiFi del hogar	Entre 2 y 6 horas	Entre 300 y 350	Algunos (50%)	Amigos	Tal vez	Familia	porque me podrian hacer bullyng mis amigos	Muy poco	Sí	Siempre	No
21	15 años	Masculino	WiFi del hogar	Entre 2 y 6 horas	Entre 300 y 350	Algunos (50%)	Amigos	Tal vez	Familia	porque me podrian hacer bullyng mis amigos	Muy poco	Sí	Siempre	No
22	15 años	Femenino	WiFi del hogar	Mas de 6 horas	Entre 150 y 200	Todos	Amigos	Sí	Familia	Son las personas en que más confío	Mucho	No	A menudo	No
23	17 años	Femenino	WiFi del hogar	Mas de 6 horas	Entre 150 y 200	Pocos (20%)	Conocidos del colegio o del lugar donde vive	Tal vez	Amigos	les tengo mucha confianza	Un Poco	Sí	Casi siempre	No

24	16 años	Femenino	Datos móviles/Paquetes de datos	Mas de 6 horas	Entre 250 y 300	Algunos (50%)	Compañeros del colegio	No	Autoridades	porque mi familia no me creeria	Nada	Sí	Siempre	No
25	16 años	Femenino	Datos móviles/Paquetes de datos	Mas de 6 horas	Entre 250 y 300	Algunos (50%)	Compañeros del colegio	No	Autoridades	porque mi familia no me creeria	Nada	Sí	Siempre	No
26	16 años	Femenino	Datos móviles/Paquetes de datos	Mas de 6 horas	Entre 200 y 250	Muchos (80%)	Conocidos del colegio o del lugar donde vive	Tal vez	Amigos	porque me aconsejarían	Muy poco	Sí	Siempre	No
27	16 años	Femenino	Datos móviles/Paquetes de datos	Mas de 6 horas	Entre 200 y 250	Muchos (80%)	Conocidos del colegio o del lugar donde vive	Tal vez	Amigos	porque me aconsejarían	Muy poco	Sí	Siempre	No
28	15 años	Femenino	WiFi del hogar	Entre 2 y 6 horas	Entre 150 y 200	Todos	Compañeros del colegio	Sí	Familia	Ellos siempre me han apoyado, confío en ellos, sabrían que hacer	Un Poco	No	Nunca	Sí
29	14 años	Masculino	Datos móviles/Paquetes de datos	Entre 2 y 6 horas	Entre 150 y 200	Muchos (80%)	Conocidos del colegio o del lugar donde vive	Tal vez	Ninguno	me da miedo	Mucho	Sí	Siempre	No

30	18 años	Masculino	Datos móviles/Paquetes de datos	Entre 2 y 6 horas	Mas de 400	Algunos (50%)	Conocidos del colegio o del lugar donde vive	Sí	Familia	Por Que Son Base Fundamental Para Ayudarme A Solucionar Mis Problemas.	Un Poco	No	A menudo	Sí
31	18 años	Femenino	Datos móviles/Paquetes de datos	Mas de 6 horas	Mas de 400	Algunos (50%)	Otros	Sí	Ninguno	porque nunca me pasara	Nada	Sí	Siempre	No
32	16 años	Femenino	Datos móviles/Paquetes de datos	Entre 1 y 2 horas	Entre 300 y 350	Algunos (50%)	Conocidos del colegio o del lugar donde vive	Sí	Familia	Son de confianza	Nada	No	A menudo	No
33	15 años	Masculino	WiFi del hogar	Entre 2 y 6 horas	Entre 200 y 250	Muchos (80%)	Conocidos del colegio o del lugar donde vive	Sí	Autoridades	por es lo mas seguro	Muy poco	No	A menudo	Sí
34	> 18 años	Femenino	WiFi del hogar	Mas de 6 horas	Entre 250 y 300	Pocos (20%)	Otros	Sí	Familia	Porque me puede suceder algo y ellos estarían informados	Un Poco	Sí	Nunca	No
35	> 18 años	Femenino	WiFi del hogar	Mas de 6 horas	Entre 300 y 350	Muchos (80%)	Amigos	Sí	Familia	La Familia es de mayor confianza	Un Poco	No	Usualmente	Sí

36	> 18 años	Femenino	Datos móviles/Paquetes de datos	Entre 15 y 30 minutos	Entre 250 y 300	Todos	Amigos	Sí	Autoridades	Por que ellos deberian saber que accion tomar ante cualquier peligro	Un Poco	No	Nunca	Sí
37	> 18 años	Masculino	Datos móviles/Paquetes de datos	Mas de 6 horas	Entre 350 y 400	Muchos (80%)	Otros	No	Familia	Confianza	Muy poco	No	Nunca	No
38	14 años	Femenino	WiFi del hogar	Mas de 6 horas	Mas de 400	Muchos (80%)	Compañeros del colegio	Sí	Autoridades	Porque ellos tienen las capacidades para ayudar a solucionar los problemas	Muy poco	Sí	A menudo	Sí
39	15 años	Masculino	Datos móviles/Paquetes de datos	Entre 2 y 6 horas	Mas de 400	Algunos (50%)	Conocidos del colegio o del lugar donde vive	No	Familia	Porque siemore están para mi y quieren mi bienestar	Muy poco	No	Nunca	Sí
40	15 años	Masculino	WiFi del hogar	Entre 15 y 30 minutos	Menos de 100	Muchos (80%)	Conocidos del colegio o del lugar donde vive	Sí	Amigos	Por q ellos me ayudaran a solucionarlo	Mucho	Sí	A menudo	Sí

41	14 años	Femenino	WiFi del hogar	Entre 2 y 6 horas	Entre 200 y 250	Algunos (50%)	Conocidos del colegio o del lugar donde vive	Sí	Familia	Por qué son las personas que les tengo las confianza	Un Poco	No	Nunca	No
42	16 años	Masculino	Datos móviles/Paquetes de datos	Entre 15 y 30 minutos	Entre 300 y 350	Algunos (50%)	Conocidos del colegio o del lugar donde vive	Sí	Familia	Porque es las personas mas sercanas	Un Poco	Sí	A menudo	Sí
43	14 años	Femenino	Datos móviles/Paquetes de datos	Entre 15 y 30 minutos	Entre 300 y 350	Muchos (80%)	Conocidos del colegio o del lugar donde vive	Sí	Autoridades	Por que ellos pueden poner alto al asunto	Un Poco	No	Nunca	Sí
44	17 años	Masculino	WiFi del hogar	Entre 1 y 2 horas	Entre 300 y 350	Muchos (80%)	Compañeros del colegio	Sí	Familia	Porque puede pasarme algo	Totalmente	No	Usualmente	No
45	15 años	Masculino	WiFi del hogar	Menos de 15 minutos	Menos de 100	Algunos (50%)	Amigos	Sí	Amigos	Porque ellos entienden de estos temas	Muy poco	Sí	Nunca	Sí
46	17 años	Masculino	WiFi del hogar	Entre 1 y 2 horas	Mas de 400	Muchos (80%)	Otros	Sí	Familia	Porque es lo mejor e iría con ellos a las autoridades	Mucho	Sí	A menudo	No

47	18 años	Femenino	WiFi del hogar	Entre 2 y 6 horas	Mas de 400	Pocos (20%)	Conocidos del colegio o del lugar donde vive	Sí	Familia	Porque si	Un Poco	No	Nunca	Sí
48	14 años	Masculino	WiFi del hogar	Entre 1 y 2 horas	Entre 200 y 250	Algunos (50%)	Conocidos del colegio o del lugar donde vive	Sí	Familia	Le diría a mi mamá por ella sabría que hacer	Un Poco	No	Siempre	No
49	> 18 años	Masculino	Datos móviles/Paquetes de datos	Entre 1 y 2 horas	Mas de 400	Muchos (80%)	Amigos	Sí	Familia	Creo que son las primeras personas en saber ya que ellos me Brindan la confianza	Un Poco	No	A menudo	Sí
50	18 años	Femenino	Datos móviles/Paquetes de datos	Mas de 6 horas	Entre 300 y 350	Algunos (50%)	Amigos	Sí	Familia	Por qué son la fuente más confiable	Mucho	No	A menudo	Sí
51	18 años	Femenino	Datos móviles/Paquetes de datos	Entre 2 y 6 horas	Mas de 400	Algunos (50%)	Conocidos del colegio o del lugar donde vive	Sí	Familia	Porque me quieren y me darán la solución por mi bien	Un Poco	No	Casi siempre	No
52	15 años	Femenino	WiFi del hogar	Entre 1 y 2 horas	Menos de 100	Todos	Familia	Sí	Familia	Porque me siento más segura de hablar del peligro en las redes so	Muy poco	No	Usualmente	No

ANEXO E. INFORME DE CONSULTORÍA ESTADÍSTICA

Consultorio Estadístico



Mauricio Alarcón Granados

Oscar Iván Castro Osorio

HERRAMIENTA DE SOFTWARE PARA CONCIENTIZACIÓN DE RIESGOS DE GROOMING POR MALA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Objetivo

Elaborar una herramienta de software de concientización de riesgos de grooming por mala gestión de seguridad de la información personal en Facebook, para estudiantes de secundaria.

Contexto

La metodología se propone para generar conciencia en los adolescentes, entre 12 y 18 años, de colegios públicos en la localidad de Chapinero de los peligros presentes en las redes sociales. Para esto, se requiere que los adolescentes individualmente realicen un juego en Facebook accediendo a todas las condiciones y términos de privacidad que este juego pide. Al aceptar estas condiciones el juego tendrá varios permisos para acceder a toda la información del que esté usando el juego. Al final se mostrará una animación que evidencia la captura de datos. Para lograr esto, es necesario saber los hábitos de los estudiantes.

Propuesta y desarrollo de la Consultoría

El objetivo de la consultoría es identificar un tipo de muestreo adecuado que permita conocer los hábitos de los estudiantes de la localidad de Chapinero entre los 12 y 18 años frente a la red social Facebook.

Inicialmente se hacen algunas observaciones y sugerencias respecto a la estructura de la encuesta que se desea aplicar, tales como:

1. Incluir la variable Estrato Socio-económico
2. Incluir la variable Grado de Escolaridad
3. Para facilitar el análisis de los datos, se sugiere reducir el número de categorías de la pregunta ¿Cuántos amigos (contactos) tienes en Facebook? y dejarlo en una escala de 100.
4. Enumerar las preguntas
5. Respecto a la pregunta ¿Cuántos años tienes? Limitar el rango de edades de acuerdo a la población objetivo de estudio. (12 a 18 años)
6. Respecto a la pregunta ¿Cuántas veces al día usas las redes sociales? Incluir el rango de 30 minutos a 1 hora y redefinir la pregunta ya que no hace referencia a tiempo de uso de las redes sociales sino a cantidad de veces.
7. Revisar ortografía y redacción
8. Para la pregunta ¿A cuántas de tus amigos de Facebook conoces en la vida real?, se sugiere manejar las opciones por rangos expresados en porcentajes (0 - 20%, 21% - 40%...)
9. Agregar la pregunta ¿Tiene cuenta en Facebook? como filtro
10. Para la pregunta, "La mayoría de tus amigos de Facebook son:", excluir las categorías (Conocidos del colegio o del lugar donde vive y Otros) e incluir las categorías (Amigos de amigos y desconocidos)
11. Para la pregunta ¿Conoces los peligros que pueden haber en Facebook?, quitar la categoría "Tal vez".

Calculo de la Muestra

Para el cálculo de la muestra, inicialmente se tenía planeado incluir como población objetivo a los estudiantes de los tres colegios públicos de la localidad de Chapinero entre los 12 y 18 años de edad, sin embargo, debido a las restricciones de acceso a la información para disponer de un marco muestral adecuado para la población estudiada, se estableció realizar un tipo de diseño de muestras no probabilístico que aproveche la información dispuesta por el consultante, por lo que finalmente se decidió trabajar con la siguiente información:

Colegio Simón Rodríguez (IED) – Sede A

Número de estudiantes: 411

Colegio San Martín de Porres (IED) – Sede A

Número de estudiantes: 183

Muestreo no probabilístico:

A diferencia del muestro probabilístico donde todos los sujetos de la población tienen una posibilidad cuantificada y conocida de ser seleccionados, en el muestreo no probabilístico, el investigador selecciona a juicio propio los individuos, lo cual agrega un componente subjetivo a la elección de la muestra. Por tanto, no todos los individuos tienen la oportunidad de ser seleccionados en el estudio.

Muestreo por cuotas:

Esta técnica de muestreo asegura una representación equitativa y proporcionada de los individuos de una población, pues los sujetos son escogidos de acuerdo a las características deseadas para el estudio y no de una manera aleatoria.

Procedimiento

Se tomó el total de estudiantes de los colegios Simón Rodríguez y San Martín de Porres de la localidad de Chapinero en secundaria como el universo de estudio. Respecto a él, se realizó la cuantificación del tamaño de muestra con distintos niveles de confianza y margen de error para después, de acuerdo a la participación de cada colegio dentro del universo, establecer la cantidad de estudiantes a encuestar por cada subgrupo (colegio).

Es de esta manera que se presenta al consultante las cuotas por realizar, de acuerdo con los cuatro diseños propuestos. Como recomendación, se sugiere utilizar la muestra con un nivel de confianza del 95% y un margen de error del 5%.

Opción 1:

Nivel de confianza	95%		
Margen de Error	5%		
Colegios	Universos	Proporción (%)	Muestra
Colegio Simón Rodríguez	411	69%	162
Colegio San Martin de Porres	183	31%	72
Total Población	594	100%	234

Opción 2:

Nivel de confianza	95%		
Margen de Error	10%		
Colegios	Universos	Proporción (%)	Muestra
Colegio Simón Rodríguez	411	69%	57
Colegio San Martin de Porres	183	31%	26
Total Población	594	100%	83

Opción 3:

Nivel de confianza	90%		
Margen de Error	5%		
Colegios	Universos	Proporción (%)	Muestra
Colegio Simón Rodríguez	411	69%	129
Colegio San Martin de Porres	183	31%	57
Total Población	594	100%	186

Opción 4:

Nivel de confianza	90%		
Margen de Error	10%		
Colegios	Universos	Proporción (%)	Muestra
Colegio Simón Rodríguez	411	69%	42
Colegio San Martin de Porres	183	31%	19
Total Población	594	100%	61

Bibliografía Recomendada:

- Cochran, W. G., & Booklier, A. S. (1980). *Técnicas de muestreo* (No. 04; HA31. 2, C6 1980.). México: Compañía Editorial Continental.
- Gutiérrez, H. A. (2009). *Estrategias de muestreo diseño de encuestas y estimacion de parametros*. Universidad Santo Tomas, Bogota (Colombia).
- Survey Monkey. https://www.surveymonkey.com/mp/sample-size-calculator/?utm_expid=.cOMQLyyUQhqbVct5bsJIAA.0&utm_referrer=https%3A%2F%2Fwww.google.com.co%2F

ANEXO F. TABULACIÓN DE RESPUESTAS DE LA MUESTRA ESTABLECIDA

Preguntas

1. ¿Cuántos años tienes?
2. Genero
3. ¿Cómo entras a Internet?
4. ¿Cuánto tiempo al día usas las redes sociales?
5. ¿Cuántos amigos tienes en Facebook?
6. ¿Cuántos amigos de Facebook conoces en la vida real?
7. La mayoría de tus amigos de Facebook son:
8. ¿Conoces los peligros que pueden haber en Facebook?
9. ¿A quién le dirías en caso de sentirte en peligro en Facebook?
10. ¿Por qué?
11. ¿Crees lo que los demás publican en Facebook?
12. ¿Aceptas invitaciones de aplicaciones o juegos en Facebook?
13. Si alguna aplicación Facebook pregunta tu información personal ¿tú la entrega?
14. ¿Sabes cómo un delincuente puede obtener tu información personal de Facebook?

Marca temporal	¿Tienes cuenta en Facebook?	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
4/3/2019 11:26	No																
4/9/2019 9:11	Sí	16 años	Femenino	WiFi del hogar	Facebook	Entre 1 y 2 horas	Entre 100 y 1200	81% - 100%	Amigos	Sí	Familia	Son las personas en las que mas confió.	Un Poco	No	A menudo	No	No
4/9/2019 9:17	Sí	17 años	Femenino	WiFi del colegio	Facebook	Mas de 6 horas	Mas de 700	81% - 100%	Amigos	Sí	Autoridades	POR QUE SI	Un Poco	No	Nunca	Sí	Sí
4/9/2019 9:17	Sí	15 años	Masculino	Cafe Internet	Facebook	Menos de 15 minutos	Mas de 700	81% - 100%	Amigos	Sí	Familia	porque es en la que puedo confiar	Un Poco	No	Nunca	Sí	No
4/9/2019 9:18	Sí	15 años	Femenino	WiFi del hogar	Facebook	Entre 1 y 2 horas	Entre 400 y 500	81% - 100%	Amigos	Sí	Familia	porque se que me ayudaran enseguida a salir del peligro	Muy poco	No	Nunca	No	No
4/9/2019 9:18	Sí	14 años	Femenino	Datos móviles/Paquetes de datos	Facebook	Entre 15 y 30 minutos	Mas de 700	61% - 80%	Amigos	Sí	Familia	por que siempre están hay y pues si me da pena les digo y yo lo de mandan aun sabiendo que yo tengo que decirlas a las autoridades	Muy poco	No	A menudo	No	No

												pero q hago con decirles a las autoridades primero y mi familia es primero					
4/9/2019 9:20	Sí	15 años	Masculino	WiFi del hogar	Facebook	Menos de 15 minutos	Entre 100 y 1200	61% - 80%	Amigos	Sí	Amigos	Por que se ;;v	Muy poco	No	Usualme nte	Sí	Sí
4/9/2019 9:21	Sí	16 años	Femenino	WiFi del hogar	Facebook	Entre 15 y 30 minutos	Entre 200 y 300	81% - 100%	Amigos	Sí	Familia	Por que son la fuente de confianza mas cercana que tengo	Muy poco	No	Nunca	Sí	No
4/9/2019 9:22	Sí	14 años	Masculino	WiFi del colegio	Facebook	Menos de 15 minutos	Menos de 100	21% - 40%	Amigos	Sí	Autoridades	porque es lo normal	Mucho	No	Nunca	Sí	Sí
4/9/2019 9:23	Sí	18 años	Masculino	Cafe Internet	Facebook	Menos de 15 minutos	Entre 100 y 1200	81% - 100%	Amigos de amigos	Sí	Familia	MI FAMILA ES UNA BASE DE SEGURIDAD PARA MI U OTRAS PERSONAS	Nada	No	Nunca	No	No
4/9/2019 9:24	Sí	18 años	Masculino	WiFi del hogar	Instagram	Entre 15 y 30 minutos	Menos de 100	81% - 100%	Amigos	Sí	Familia	porque el ellos tengo más confianza y me pueden ayudar	Mucho	No	A menudo	No	Sí

4/9/2019 9:24	Sí	17 años	Masculino	WiFi del hogar	Facebook	Menos de 15 minutos	Menos de 100	41% - 60%	Comp añeros del colegi o	Sí	Amigos	porque puede dar un gran problema	Mucho	Sí	A menudo	Sí	Sí
4/9/2019 9:25	Sí	17 años	Masculino	WiFi del colegio	Facebook	Entre 1 y 2 horas	Entre 500 y 600	81% - 100%	Familia	No	Familia	por que es quien mas con parto la mayoria de tiempo	Un Poco	Sí	Casi siempre	No	Sí

4/9/2019 9:27	Sí	17 años	Femenino	WiFi del hogar	Facebook	Entre 2 y 6 horas	Entre 300 y 400	81% - 100%	Amigos	Sí	Familia	por que me brindan la confianza y son mas responsables	Muy poco	No	Nunca	No	Sí
4/9/2019 9:28	Sí	17 años	Femenino	WiFi del hogar	Facebook	Mas de 6 horas	Mas de 700	81% - 100%	Amigos de amigos	Sí	Familia	Mi familia es en los que confio	Muy poco	No	Nunca	Sí	Sí
4/9/2019 9:30	Sí	15 años	Femenino	WiFi del hogar	Facebook	Entre 1 y 2 horas	Mas de 700	81% - 100%	Amigos	Sí	Familia	Por Que En Ellos Puedo Confiar Y Me Dicen Que Debo Hacer	Un Poco	No	Nunca	Sí	Sí
4/9/2019 9:30	Sí	16 años	Femenino	WiFi del colegio	Facebook	Entre 1 y 2 horas	Entre 200 y 300	61% - 80%	Amigos	Sí	Familia	por mas confianza	Un Poco	No	A menudo	Sí	Sí
4/9/2019 9:31	Sí	15 años	Masculino	WiFi del hogar	Facebook	Mas de 6 horas	Menos de 100	81% - 100%	Amigos	Sí	Familia	por que confió en ella	Muy poco	Sí	Nunca	Sí	No
4/9/2019 9:32	Sí	15 años	Femenino	WiFi del hogar	Facebook	Entre 2 y 6 horas	Entre 300 y 400	61% - 80%	Amigos	Sí	Familia	Confió en mi familia y se que podrían ayudarme	Un Poco	Sí	A menudo	Sí	Sí
4/9/2019 10:02	No																
5/7/2019 10:31	Sí	13 años	Femenino	WiFi del hogar	Facebook	Entre 2 y 6 horas	Entre 200 y 300	81% - 100%	Amigos	Sí	Familia	porque tengo mas confianza	Un Poco	No	Usualme nte	No	Sí

5/7/2019 10:32	Sí	16 años	Femenino	Datos móviles/P aquetes de datos	Facebook	Mas de 6 horas	Entre 600 y 700	61% - 80%	Comp añeros del colegi o	Sí	Autoridades	Para que me ayuden a solucionar el problema y no se haga mas grande	Muy poco	No	Nunca	No	Sí
5/7/2019 10:32	Sí	15 años	Masculino	WiFi del colegio	Facebook	Entre 1 y 2 horas	Entre 500 y 600	61% - 80%	Amigos	Sí	Familia	por que yo confio en ellos	Muy poco	No	Nunca	No	No
5/7/2019 10:32	Sí	16 años	Masculino	Datos móviles/P aquetes de datos	Facebook	Entre 15 y 30 minutos	Mas de 700	81% - 100%	Comp añeros del colegi o	Sí	Familia	para que me ayuden	Un Poco	No	Nunca	No	Sí
5/7/2019 10:32	Sí	16 años	Masculino	WiFi del hogar	Instagram	Entre 1 y 2 horas	Entre 200 y 300	81% - 100%	Amigos	Sí	Familia	por que tengo confianza en ellos	Muy poco	No	Nunca	Sí	Sí
5/7/2019 10:32	Sí	13 años	Femenino	WiFi del colegio	Facebook	Menos de 15 minutos	Entre 400 y 500	81% - 100%	Amigos	Sí	Autoridades	porque ellos pueden ayudarnos a resolver el problema	Un Poco	No	Nunca	Sí	Sí
5/7/2019 10:33	Sí	14 años	Masculino	Datos móviles/P aquetes de datos	Facebook	Entre 30 minutos y 1 hora	Entre 300 y 400	81% - 100%	Familia	Sí	Familia	por que mi familia me puede ayudar en mi problema	Un Poco	No	Nunca	No	Sí

5/7/2019 10:33	Sí	13 años	Femenino	WiFi del hogar	Facebook	Entre 1 y 2 horas	Entre 400 y 500	61% - 80%	Comp añeros del colegi o	Sí	Familia	Porque son las personas mas cercanas a mi y las que llevarían mejor la situación	Un Poco	No	A menudo	No	Sí
-------------------	----	------------	----------	-------------------	----------	----------------------	-----------------------	-----------------	--------------------------------------	----	---------	---	---------	----	-------------	----	----

5/7/2019 10:33	Sí	13 años	Femenino	WiFi del hogar	Facebook	Mas de 6 horas	Entre 200 y 300	81% - 100%	Amigos	Sí	Familia	por que me sentiría mas apoyanda con mis familiares y por que tengo mucho mas confianza con ellos	Un Poco	Sí	Nunca	Sí	No
5/7/2019 10:33	Sí	13 años	Femenino	WiFi del hogar	Facebook	Entre 1 y 2 horas	Menos de 100	81% - 100%	Amigos	Sí	Familia	porq me sentiria cn mas apoyos	Un Poco	Sí	Nunca	Sí	No
5/7/2019 10:33	Sí	14 años	Femenino	WiFi del hogar	Facebook	Entre 30 minutos y 1 hora	Menos de 100	81% - 100%	Familia	Sí	Familia	por que confio mucho en ellos	Muy poco	No	Siempre	Sí	No
5/7/2019 10:33	Sí	13 años	Femenino	Datos móviles/P aquetes de datos	Snapchat	Entre 1 y 2 horas	Entre 200 y 300	21% - 40%	Familia	Sí	Familia	porque es lo correcto habisar a nuestros padres	Un Poco	No	A menudo	No	Sí
5/7/2019 10:33	Sí	16 años	Femenino	WiFi del hogar	Facebook	Mas de 6 horas	Mas de 700	81% - 100%	Amigos	Sí	Familia	para recibir una ayuda y salir de eso	Muy poco	No	A menudo	Sí	Sí
5/7/2019 10:33	Sí	17 años	Masculino	WiFi del colegio	Facebook	Entre 1 y 2 horas	Menos de 100	0 - 20%	Amigos	Sí	Familia	me pegan sino les dijo	Nada	No	Nunca	No	Sí

5/7/2019 10:33	Sí	15 años	Masculino	Datos móviles/P aquetes de datos	Facebook	Entre 15 y 30 minutos	Entre 100 y 1200	81% - 100%	Amigos	Sí	Familia	por que es con las personas que entienden mazo menos eso y que todo tiempo lo veo	Un Poco	No	Nunca	No	Sí
5/7/2019 10:33	Sí	16 años	Femenino	WiFi del hogar	Facebook	Entre 30 minutos y 1 hora	Mas de 700	81% - 100%	Amigos	No	Autoridades	porque ellos me dirian que hacer en caso de algo muy serio	Nada	No	Nunca	No	Sí
5/7/2019 10:33	Sí	14 años	Femenino	Cafe Internet	Facebook	Entre 2 y 6 horas	Entre 500 y 600	81% - 100%	Amigos	Sí	Familia	porque le tengo la confianza a ellos casi amigos no	Muy poco	Sí	Nunca	Sí	Sí
5/7/2019 10:34	Sí	14 años	Masculino	WiFi del hogar	Facebook	Entre 1 y 2 horas	Entre 400 y 500	81% - 100%	Comp añeros del colegi o	Sí	Autoridades	por que ellos me pueden ayudar con ese caso	Muy poco	No	Nunca	Sí	Sí
5/7/2019 10:34	Sí	13 años	Femenino	WiFi del colegio	Facebook	Entre 1 y 2 horas	Entre 100 y 1200	61% - 80%	Amigos	Sí	Amigos	puedo confiar en ellos	Muy poco	No	Nunca	Sí	Sí

5/7/2019 10:34	Sí	13 años	Masculino	WiFi del hogar	Facebook	Entre 30 minutos y 1 hora	Entre 100 y 1200	81% - 100%	Comp añeros del colegi o	Sí	Familia	por que ellos me ayudarían y me darían consejos y que hacer	Un Poco	No	Nunca	No	Sí
5/7/2019 10:34	Sí	16 años	Masculino	Datos móviles/P aquetes de datos	Facebook	Entre 1 y 2 horas	Entre 100 y 1200	0 - 20%	Amigos	No	Familia	porque si, confianza	Muy poco	No	Nunca	No	No
5/7/2019 10:35	Sí	12 años	Femenino	WiFi del hogar	Facebook	Menos de 15 minutos	Entre 200 y 300	81% - 100%	Amigos	Sí	Familia	por que confio en ellos y me ayudaran	Muy poco	Sí	Nunca	Sí	Sí

[illegible]

[illegible]

5/7/2019 11:46	Sí	14 años	Femenino	WiFi del hogar	Facebook	Entre 30 minutos y 1 hora	Mas de 700	21% - 40%	Amigos	Sí	Familia	Por Q Ellos Podrian Ayudarme A Encontrar La Solucion	Muy poco	No	Nunca	Sí	No
5/7/2019 11:47	No																
5/7/2019 11:47	Sí	14 años	Femenino	WiFi del hogar	Facebook	Entre 1 y 2 horas	Entre 400 y 500	81% - 100%	Amigos	Sí	Familia	ps por q ellos me pueden ayudar e ir con migo alas autoridades	Muy poco	Sí	Nunca	Sí	Sí
5/7/2019 11:48	Sí	12 años	Masculino	Datos móviles/P aquetes de datos	Facebook	Entre 2 y 6 horas	Mas de 700	81% - 100%	Amigos de amigos	Sí	Familia	por que me pueden orientar y ayudar en mi caso	Un Poco	Sí	Nunca	Sí	Sí

5/7/2019 11:48	Sí	13 años	Femenino	WiFi del hogar	Facebook	Entre 1 y 2 horas	Entre 100 y 1200	41% - 60%	Amigos	No	Familia	a mi papa y mama	Muy poco	No	Nunca	No	No
5/7/2019 11:48	Sí	12 años	Femenino	Cafe Internet	Facebook	Entre 30 minutos y 1 hora	Menos de 100	81% - 100%	Amigos	Sí	Familia	porque haci ellos podrían ayudarme a hablar con las autoridades	Muy poco	No	Nunca	Sí	Sí
5/7/2019 11:49	Sí	14 años	Femenino	WiFi del hogar	Facebook	Mas de 6 horas	Entre 500 y 600	61% - 80%	Amigos	Sí	Familia	Mi mama sabria que hacer	Muy poco	No	Nunca	Sí	No
5/7/2019 11:49	Sí	13 años	Femenino	WiFi del hogar	Facebook	Mas de 6 horas	Menos de 100	81% - 100%	Amigos	Sí	Familia	porque ellos me pueden apoyar	Muy poco	No	Nunca	Sí	Sí
5/7/2019 11:50	Sí	12 años	Femenino	WiFi del hogar	Instagram	Entre 1 y 2 horas	Menos de 100	41% - 60%	Amigos	No	Familia	porque ellos tienen mi mayor confiansa	Muy poco	No	Nunca	Sí	Sí
5/7/2019 11:50	No																
5/7/2019 11:51	Sí	13 años	Femenino	WiFi del hogar	Facebook	Entre 15 y 30 minutos	Menos de 100	0 - 20%	Amigos	Sí	Familia	por cuidarlos del peligro	Muy poco	No	A menudo	No	No
5/7/2019 11:52	Sí	12 años	Femenino	WiFi del hogar	Facebook	Entre 30 minutos y 1 hora	Entre 200 y 300	81% - 100%	Amigos	Sí	Familia	porque me siento mas segura diciendole a mi familia	Mucho	Sí	Nunca	Sí	Sí

[illegible]

6/7/2019 11:45	Sí	18 años	Masculino	WiFi del hogar	Facebook	Entre 2 y 6 horas	Mas de 700	61% - 80%	Amigos	Sí	Familia	Confio mucho en ellos, y se que me apoyarian	Un Poco	No	A menudo	Sí	No
6/7/2019 11:45	No																
6/7/2019 11:45	No																
6/7/2019 11:45	No																
6/7/2019 11:45	Sí	15 años	Masculino	WiFi del hogar	Instagram	Mas de 6 horas	Entre 100 y 1200	81% - 100%	Amigos	Sí	Familia	Porque confio mas en ellos	Un Poco	No	Casi siempre	Sí	No

6/7/2019 11:45	Sí	14 años	Masculino	WiFi del hogar	Facebook	Entre 1 y 2 horas	Entre 300 y 400	81% - 100%	Amigos	Sí	Familia	Por que tengo confianza en ellos	Un Poco	No	Usualme nte	No	No
6/7/2019 11:46	Sí	15 años	Femenino	WiFi del colegio	Facebook	Entre 15 y 30 minutos	Entre 100 y 1200	21% - 40%	Amigos	Sí	Familia	por que son los que me protegen	Muy poco	Sí	A menudo	Sí	Sí
6/7/2019 11:46	Sí	16 años	Masculino	Datos móviles/P aquetes de datos	Facebook	Menos de 15 minutos	Menos de 100	61% - 80%	Familia	Sí	Familia	por que son las personas mas confiables	Mucho	No	Nunca	No	No
6/7/2019 11:46	Sí	15 años	Masculino	Datos móviles/P aquetes de datos	Facebook	Mas de 6 horas	Entre 200 y 300	21% - 40%	Amigos de amigos	Sí	Familia	porque seria a los primeros que recurriria	Mucho	Sí	Nunca	Sí	No
6/7/2019 11:46	Sí	15 años	Masculino	WiFi del colegio	Facebook	Entre 15 y 30 minutos	Menos de 100	81% - 100%	Amigos	Sí	Familia	en total porque los padres nos pueden ayudar en momentos dificiles	Un Poco	No	Nunca	Sí	Sí
6/7/2019 11:47	Sí	16 años	Femenino	WiFi del hogar	Facebook	Entre 2 y 6 horas	Entre 300 y 400	81% - 100%	Amigos	Sí	Familia	Porque son los mas cercanos	Un Poco	No	Nunca	Sí	No
6/7/2019 11:47	Sí	16 años	Masculino	WiFi del hogar	Facebook	Entre 2 y 6 horas	Entre 400 y 500	61% - 80%	Amigos	Sí	Familia	Confio bastante ellos	Un Poco	No	A menudo	Sí	No

6/7/2019 11:47	Sí	15 años	Femenino	Datos móviles/P aquetes de datos	Facebook	Entre 30 minutos y 1 hora	Entre 600 y 700	81% - 100%	Amigos	Sí	Familia	porque les tengo mas confianza y se que ellos me darían el mejor consejo	Muy poco	No	Nunca	Sí	Sí
6/7/2019 11:47	Sí	15 años	Femenino	WiFi del hogar	Snapchat	Entre 1 y 2 horas	Menos de 100	41% - 60%	Comp añeros del colegi o	Sí	Familia	Porque confío mas en ellos que en alguien más	Mucho	No	Nunca	Sí	Sí
6/7/2019 11:48	Sí	15 años	Masculino	WiFi del hogar	Facebook	Entre 30 minutos y 1 hora	Entre 100 y 1200	61% - 80%	Amigos	Sí	Familia	porque existe una conexiõn mas profunda	Mucho	Sí	Nunca	No	No
6/7/2019 11:48	Sí	18 años	Masculino	WiFi del hogar	Instagram	Entre 2 y 6 horas	Entre 200 y 300	0 - 20%	Amigos de amigos	Sí	Familia	porque son las personas en las que confío si llega a pasar este tipo de situaciones, ademas de que se que me van a ayudar	Muy poco	No	Nunca	No	No
6/7/2019 11:48	Sí	14 años	Masculino	Datos móviles/P aquetes de datos	Facebook	Mas de 6 horas	Mas de 700	61% - 80%	Amigos de amigos	Sí	Familia	Por Que Son Las Personas En Las Primeras Que Confíaria	Un Poco	No	Nunca	Sí	No

6/7/2019 11:48	Sí	14 años	Masculino	WiFi del hogar	Facebook	Entre 15 y 30 minutos	Mas de 700	21% - 40%	Descon ocidos	Sí	Familia	Porque es en las unicas personas que puedo confiar	Muy poco	No	Nunca	Sí	No
-------------------	----	------------	-----------	-------------------	----------	--------------------------	---------------	-----------------	------------------	----	---------	---	-------------	----	-------	----	----

6/7/2019 11:49	Sí	16 años	Masculino	WiFi del colegio	Facebook	Menos de 15 minutos	Mas de 700	41% - 60%	Amigos	Sí	Familia	por que son los primeros que creo que deben saber	Un Poco	Sí	A menudo	No	No
6/7/2019 11:49	Sí	15 años	Femenino	Datos móviles/P aquetes de datos	Facebook	Entre 15 y 30 minutos	Menos de 100	41% - 60%	Familia	Sí	Familia	son mi apoyo personal	Mucho	No	Nunca	Sí	Sí
6/7/2019 11:50	Sí	16 años	Femenino	WiFi del hogar	Instagram	Entre 1 y 2 horas	Entre 100 y 1200	41% - 60%	Comp añeros del colegi o	Sí	Familia	porque ellos sabrían que hacer	Nada	No	Nunca	No	No
6/7/2019 11:50	Sí	15 años	Masculino	Datos móviles/P aquetes de datos	Facebook	Entre 2 y 6 horas	Entre 400 y 500	81% - 100%	Amigos	Sí	Familia	Son con los que tengo más confianza	Un Poco	No	Nunca	Sí	Sí
6/7/2019 11:50	Sí	15 años	Femenino	Datos móviles/P aquetes de datos	Facebook	Entre 1 y 2 horas	Entre 100 y 1200	41% - 60%	Amigos	Sí	Familia	porque ellos me van a ayudar a solucionarlos	Nada	No	Nunca	Sí	Sí
6/7/2019 11:52	Sí	15 años	Masculino	WiFi del hogar	Facebook	Entre 15 y 30 minutos	Entre 100 y 1200	41% - 60%	Amigos de amigos	Sí	Ninguno	porque mi cuenta esta perfectamente protegida	Totalmen te	No	Nunca	Sí	No

ANEXO G. LIENCIA ESTANDAR

USOS	EJEMPLOS DE TRABAJOS BAJO LICENCIA
Publicidad / Marketing / Promoción (Fines Empresariales y Comerciales)	<ul style="list-style-type: none"> Anuncios elaborados por diseñadores gráficos/agencias para clientes en revistas, periódicos, diarios, informes y otros medios impresos tradicionales Anuncios impresos, anuncios publicitarios, folletos, flyers, carteles, catálogos, envases o materiales promocionales que EXCLUYE el embalaje de mercancías (por ejemplo, donde el embalaje forme parte del producto, como una caja de un juguete) y el embalaje como producto (por ejemplo, papel de regalo como producto)
Impresión / Publicaciones / Educación	<ul style="list-style-type: none"> Impresiones sobre portadas de libros (delantera y trasera), hasta 500.000 impresiones de forma colectiva para cada Contenido. Tarjetas de visita, membretes, catálogos, folletos y panfletos
Presentaciones	<ul style="list-style-type: none"> Uso de Contenido para presentaciones multimedia como Powerpoint, <i>provided</i> siempre y cuando el siguiente aviso de copyright aparezca junto al archivo: "[Nombre del colaborador]© 123RF.com"
"Editorial Use Only" "Sólo para Uso Editorial" Contenidos & Contexto Editorial	<ul style="list-style-type: none"> Importante – El Contenido marcado como " Sólo para Uso Editorial " <i>sólo</i> podrá ser utilizado para fines editoriales y <i>no</i> podrá ser utilizado para fines publicitarios, comerciales o promocionales. El Contenido utilizado para uso editorial (por ejemplo, revistas, periódicos, libros de texto, libros, libros electrónicos, directorios en línea o CDs multimedia) deberá mostrar el siguiente aviso de copyright junto al archivo: "[Nombre del colaborador] © 123RF.com" Para evitar cualquier duda, todo el Contenido (incluyendo el contenido no marcado como "Sólo para Uso Editorial") también podrá ser utilizado en un contexto editorial, ya sea en formato impreso tradicional o electrónico, sitios web, blogs, televisión, vídeos en línea, siempre y cuando se muestre el aviso citado anteriormente sobre los derechos de autor. Publicación editorial sólo hasta 500.000 impresiones colectivas para cada Contenido
Elementos de Diseño & Arte	<ul style="list-style-type: none"> En una página Web, videojuego, dispositivo de almacenamiento de datos o programas informáticos, para su distribución o uso por terceros (pero <i>no</i> en relación con cualquier plantilla de página Web o producto de software para distribución, reventa o uso por terceros) Como fondo o Contenido de pantalla en software o aplicaciones móviles, siempre que el Contenido <i>no</i> juegue un Papel Vital en la Obra bajo Licencia. Reproducido sustancialmente en obras de arte originales En vídeo, cine, emisiones de televisión e internet para vídeos domésticos, documentales, largometrajes o uso comercial <i>siempre</i> y cuando el siguiente aviso de copyright aparezca junto al archivo: "[Nombre del colaborador]© 123RF.com" y el Contenido <i>no</i> juegue un Papel Vital en la Obra bajo Licencia. La emisión en forma destacada de los créditos podría incluir, por ejemplo, créditos al principio o al final de un programa de televisión, o citarlo razonablemente cerca del Contenido utilizado, o como anexo o anotación de forma clara.
Redes Sociales & Aplicaciones	<ul style="list-style-type: none"> Publicar y/o subir Contenido en redes sociales y aplicaciones (como Facebook, Instagram y Twitter), siempre que (1) dichas redes sociales y aplicaciones no asuman o consideren la propiedad o derechos (incluidos los Derechos de Autor) en el Contenido (ya sea como imagen independiente, en una forma derivada o como una Obra bajo Licencia), salvo que Usted, como titular de la Licencia del Contenido, lo permita para que el Contenido y/o Obra bajo Licencia se muestre según los términos de la presente Licencia o (2) cumpla con los siguientes puntos: <ul style="list-style-type: none"> ii. el tamaño del contenido subido no debe superar los 800 píxeles jj. Deberá incluir el logotipo de la organización en cualquier esquina del contenido con un tamaño mínimo de 125 píxeles de ancho o de largo, (el que sea el más grade) y/o el Contenido deberá incorporarse en una Obra bajo Licencia.
Uso Personal	<ul style="list-style-type: none"> Diseño de interiores, murales, arte, discos, grabados, bienes personales y el uso de artículos realizados por usted y otras impresiones personales Blogs personales y otras publicaciones personales (tradicional o en línea), siempre que las publicaciones personales no impliquen que usted o cualquier proveedor de servicios de publicaciones de terceros (por ejemplo, proveedores de servicios de blog) asuman o consideren la propiedad o derechos (incluidos los derechos de autor) en el Contenido (ya sea como imagen independiente, en una forma derivada o como una Obra bajo Licencia) Como decoración en una oficina, vestíbulo, área pública, restaurante o tienda al por menor.

ANEXO H. GUIÓN PARA EL SOCIALIZADOR DE LA HERRAMIENTA

V1.0

GUIA PARA EL SOCIALIZADOR DE LA HERRAMIENTA

Socializador

Esta actividad consta de tres partes o escenas, la primera es un juego online en la red social de Facebook; la segunda, es generar impacto; la tercera y última, lleva a unas recomendaciones. Es importante que después de usar la herramienta haya una socialización sobre el tema.

Socializador

La herramienta inicia con un juego, para acceder a él primero es necesario iniciar sesión en la red social Facebook en el navegador de Mozilla Firefox, una vez hayan iniciado sesión empezarán con el juego de "Monkey Collector".

Socializador

Escena 1
La idea en la primera escena es ayudar a Monkey a llegar a casa y recolectar su meta diaria de 100 frutas, juega con las flechas del teclado para caminar hacia adelante, para caminar hacia atrás y para saltar. Al perder todas las vidas o ganar, dale "clic" al botón que se encuentra en la parte izquierda de la pantalla para poder ir a la siguiente escena.

Socializador

Escena 2

En esta escena encontraras algunos de tus datos personales de tu perfil de Facebook y un hombre misterioso.
Recuerda revisar la información que le estas otorgando a las aplicaciones, la información tuya no es para divulgar, cuida mucho de ti, tu integridad y de tu salud mental, podrían estar en peligro. Estas son algunas posibles actividades que el groomer puede hacer con esta información: sustitución de identidad, cualquier tipo de spam, editor de fotos, y en cualquiera de estas actividades se puede llegar al chantaje, teniendo como fin, grooming y/o otros peligros. Al lado derecho de la pantalla encontraras un botón que dice "Next", dale clic para ir a la siguiente escena.

Socializador

Escena 3

En esta escena podrás visualizar casos reales que ocurrieron al brindar cierta información e interactuar con personas desconocidas en la red social Facebook. Así mismo, podrás ver un video de cómo administrar herramientas de privacidad que Facebook brinda y recomendaciones a tener en cuenta para proteger su cuenta de Facebook.

Socializador

Disponemos de dos minutos para ver y tener en cuenta el video con las recomendaciones brindadas en total silencio

Socializador

Por último, se preparado una explicación y socialización para ustedes.

ANEXO I. GUION PARA EL SOCIALIZADOR DE LA ACTIVIDAD

V1.0

GUIA PARA EL SOCIALIZADOR DE LA ACTIVIDAD

Socializador

Esta actividad se va a realizar en tres partes, la primera es realizar una encuesta digital que se encuentra en Google, la segunda es usar la herramienta propuesta y a medida que vayan avanzando se explicara cada parte de la herramienta y por último la explicación del tema y socialización de la actividad.

Socializador

La encuesta cuenta con 16 preguntas, las cuales 15 de ellas son preguntas cerradas con opción múltiple y una restante de justificación, esta última es una explicación muy corta donde respondan exactamente lo que se está preguntando.

Socializador

La herramienta inicia con un juego, para acceder a él primero es necesario iniciar sesión en la red social Facebook en el navegador de Mozilla Firefox, una vez hayan iniciado sesión empezarán con el juego de "Monkey Collector".

Socializador

Escena 1

La idea en la primera escena es ayudar a Monkey a llegar a casa y recolectar su meta diaria de 100 frutas, juega con las flechas del teclado para caminar hacia adelante, para caminar hacia atrás y para saltar. Al perder todas las vidas o ganar, dale "clic" al botón que se encuentra en la parte izquierda de la pantalla para poder ir a la siguiente escena.

Socializador

Escena 2

En esta escena encontraras algunos de tus datos personales de tu perfil de Facebook y un hombre misterioso.

Recuerda revisar la información que le estas otorgando a las aplicaciones, la información tuya no es para divulgar, cuida mucho de ti, tu integridad y de tu salud mental, podrían estar en peligro. Estas son algunas posibles actividades que el grommer puede hacer con esta información: sustitución de identidad, cualquier tipo de spam, editor de fotos, y en cualquiera de estas actividades se puede llegar al chantaje, teniendo como fin, grooming y/o otros peligros.

Al lado derecho de la pantalla encontraras un boton que dice "Next", dale clic para ir a la siguiente escena.

Socializador

Escena 3

En esta escena podrás visualizar casos reales que ocurrieron al brindar cierta información e interactuar con personas desconocidas en la red social Facebook. Así mismo, podrás ver un video de cómo administrar herramientas de privacidad que Facebook brinda y recomendaciones a tener en cuenta para proteger su cuenta de Facebook.

Socializador

Disponemos de dos minutos para ver y tener en cuenta el video con las recomendaciones brindadas en total silencio

Socializador

Por último, hemos preparado una explicación y socialización para ustedes.

Socializador

Alguno de ustedes sabe...

¿Cuáles son los peligros a los que se están expuestos en las redes sociales?

¿Qué es grooming?

¿Qué se debe hacer si llegan a ser víctimas de cualquier tipo de peligro?

Socializador

Diapositiva 2

El Grooming es una forma de acoso sexual que ocurre generalmente en medios como: redes sociales o chats. El acosador es llamado "grommer", este se hace pasar por otra persona comúnmente por gente de tu edad para ganar tu confianza, creando perfiles falsos, con el fin de obtener una satisfacción sexual mediante fotos y videos eróticos, pornografía infantil u otro tipo de propuestas y llegar al ciberchantaje.

El grooming actualmente es el peligro más popular en las redes sociales.

Socializador

Diapositiva 3

El grommer lo que quiere algunas veces son fotos y videos con algún contenido sexual, algo que pueda vender en el mercado negro, pero la mayoría de las veces buscan abusar sexualmente de sus víctimas.

Se basa en dos tácticas: La primera es el engaño, que es cuando el groomer se disfraza y se hace pasar por otra persona de mayor interés, y la segunda es el chantaje, se trata de conseguir algún tipo de información para amenazar a la víctima.

Socializador

Diapositiva 4

¿Qué debe hacer en estos casos?

Por el lado del engaño, hay que identificar ciertas conductas o señales que permitan ver si es un perfil falso, como: hay pocas fotos o hay muchas personas, tiene pocos amigos, dice cosas que no pueden comprobar, no aparece en eventos en los que hay personas conocidas o no prende su cámara.

Socializador

Diapositiva 5

Algunos de los tipos de peligros en la red son los siguientes:

Grooming

Abuso infantil: Pornografía, explotación y turismo sexual a menores

El phishing: Método más utilizado por cibercriminales para estafar y obtener información confidencial de forma fraudulenta.

Sexting: Es el intercambio de fotos propias de contenido sexual, las cuales se envían a otras personas vía teléfono celular o Internet.

Cyberbullying: Acto agresivo e intencionado que se lleva a cabo de manera repetida y constante a lo largo del tiempo mediante contacto electrónico, por parte de un grupo o de un individuo contra una víctima que no puede defenderse fácilmente.

Sextorción: Forma de chantaje sexual en la cual los criminales cuentan con contenido privado de los usuarios (normalmente fotos o videos) y les amenazan con hacerlo público en Internet, a menos que las víctimas paguen con algún favor, en ocasiones sexual.

¿Alguno de estos peligros no conocen?

Socializador

Diapositiva 6

¿Qué hacer para no ser víctima de estos peligros?

Evita usar tu nombre y/o tu año de nacimiento en los correos o usuarios de las redes sociales, como: 'jorge2004@mail.com' o '@estrella2006'. Esto ayuda a que los abusadores conozcan tu nombre completo y tu edad.

Bloquee a los contactos de redes sociales que no conozca personalmente, que le realicen propuestas indecentes o comiencen conversaciones inapropiadas.

Nunca envíes foto o videos en que estés sin ropa o que se preste a malentendidos. Estos archivos pueden ser usados en chantajes.

Socializador

Diapositiva 7

No acudas sin compañía y a lugares cerrados a citas con gente que conociste por internet.

Darle tu información personal o la de tus familiares, fotos o videos comprometedores, secretos, es darles poder. No brindes ese tipo de información.

Guarda cualquier tipo de información que sirva como evidencia para hacer una denuncia: pantallazos, mensajes de WhatsApp o correos enviados, entre otros.

Cuida tu privacidad e información personal, no te fíes de quien no conoces.

Socializador

Diapositiva 8

Si eres víctima de algunos de los peligros mencionados anteriormente de la red es importante denunciarlos.

No te des pena, pocas cosas son tan graves como un abusador de menores. Cuéntales a tus padres, si por algún motivo no lo quieres hacer, existen entidades que te puedes ayudar: Te Protejo, Centro Cibernético Policial y la Fiscalía general de la nación.

Socializador

Diapositiva 9

A continuación, verán un video por parte de “Te protejo”

Socializador

Diapositiva 10

Te protejo es una herramienta del programa “en TIC confío” del Min TIC

¿Alguien Sabe que es “en TIC confío”?

En TIC confío es la estrategia para un uso responsable de internet y de las nuevas tecnologías del Ministerio de las Tecnologías de la Información y las Comunicaciones.

Te protejo, sirve como canal para denuncias virtuales en tiempo real, de contenido ilegal o abusos que afecten a los menores.

Es muy fácil de usar esta herramienta:

Primero: Identifica la situación que está poniendo en riesgo a los menores

Segundo: Descargar la aplicación “Te protejo” en los celulares o acceder a teprotejo.org. Tanto en la aplicación como en la página debes escoger la situación que desea reportar y llenar el formulario de denuncia.

Tercero: La herramienta verifica la información y determina si es legal o ilegal, es decir, si es contenido para adultos es legal, al ser legal pero inapropiado interviene “Red papaz”, el cual es una entidad que tiene como fin abogar por la protección de los derechos de los menores en Colombia. Pero si por otro lado contenido sexual con menores, es ilegal, te protejo canalizará a las autoridades competentes dependiendo de la situación.

En todo este proceso te protejo hace seguimiento en cada uno de los casos.

Socializador

Diapositiva 11

Estos son los resultados de las denuncias de los últimos 5 meses:

8.446 páginas web bloqueadas por contener imágenes de abuso sexual infantil, en donde 10.500 imágenes de abuso sexual infantil cuyo desmonte se solicitó a la red INHOPE (el cual es una red de colaboración en 40 países, que se ocupa del contenido ilegal en línea y se compromete a eliminar el abuso sexual infantil)

También hubo 16 procesos de judicialización

Sanciones desde \$399 millones de pesos a 81 ISP (son los proveedores de servicios de internet) por no cumplir este parámetro.

Por último, hubo 27.056 descargas de la aplicación de Te protejo en los dispositivos móviles

Del 23 al 29 de marzo del 2019, la Dirección de investigación criminal e interpol (DIJIN) dio orden de bloqueo a 78 sitios con material de abuso sexual infantil.

Socializador

Diapositiva 12

En varios países como argentina hay leyes específicamente para el Grooming, Colombia no posee una en específico pero varias leyes y artículos de la constitución política de Colombia los protegen para este peligro social u otros ya mencionados.
Ejemplo:

Constitución política de Colombia

Art. 44. Los derechos de los niños prevalecen sobre los derechos de los demás.

Art. 45. El adolescente tiene derecho a la protección y a la formación integral.

Ley 679 de 2001

Prevenir y contrarrestar la explotación, pornografía y turismo sexual con menores

Socializador

Diapositiva 13

Ley 1098 de 2006

Código de infancia y adolescencia

Ley 1581 de 2012

Dicta disposiciones generales para la protección de datos personales

Ley 1620 de 2013

Crea el sistema Nacional de convivencia escolar

Socializador

Diapositiva 14

Estas son algunas noticias actuales en Colombia...

ANEXO J. PRESENTACIÓN PARA EL SOCIALIZADOR DE LA ACTIVIDAD

GROOMING

Catalina Niebles Parra
Nixon Piñeros Montenegro

¿QUÉ ES EL GROOMING?

“Se llama grooming al acoso sexual virtual que se realiza a un menor de edad. Se trata de acciones intencionales desarrolladas por un adulto para establecer un vínculo con un menor con una intención sexual.”



Fuente: Definición <https://definicion.de/grooming/> - 2018
EducarChile www.educarchile.cl

¿QUÉ BUSCA EL GROOMER?



Fotos para
vender



Amiguit@s

TÁCTICAS

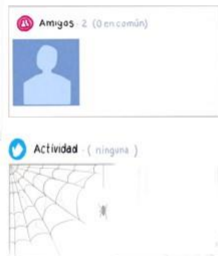
1) Engaño:

Disfraz de otra persona

1) Chantaje:

Intenta conseguir cualquier tipo de información para amenazar a la víctima

UN PERFIL FALSO TAMBIÉN ESTÁ LLENO DE SEÑALES QUE LO DELATAN



Fuente: Magic Markers (<https://www.youtube.com/watch?v=OdixH2SnCHK>) - 2017



TIPOS DE PELIGROS EN LA RED

- Grooming
- El phishing
- Ciberbullying
- Abuso infantil
- Sexting
- Sextorsión

¿QUÉ HACER SI ERES VÍCTIMA DE LOS PELIGROS EN LA RED?

- Te Protejo
- Centro Cibernético Policial
- Fiscalía general de la nación



Fuente: Te Protejo/<http://www.teprotejo.org/index.php/es/>



Fuente: Te Protejo/<http://www.teprotejo.org/index.php/es/>

RESULTADOS DE LAS DENUNCIAS



Fuente: Te Protejo/<http://www.teprotejo.org/index.php/es/>

¿QUÉ DICE LA LEY?

Constitución política de Colombia

- Art. 44. Los derechos de los niños prevalecen sobre los derechos de los demás.
- Art. 45. El adolescente tiene derecho a la protección y a la formación integral.

Ley 679 de 2001

- Prevenir y contrarrestar la explotación, pornografía y turismo sexual con menores

Fuente: Te Protejo/<http://www.teprotejo.org/index.php/es/>

¿QUÉ DICE LA LEY?

Ley 1098 de 2006

- Código de infancia y adolescencia

Ley 1581 de 2012

- Dicta disposiciones generales para la protección de datos personales

Ley 1620 de 2013

- Crea el sistema Nacional de convivencia escolar

Fuente: Te Protejo/<http://www.teprotejo.org/index.php/es/>

NOTICIAS ACTUALES

NOTICIAS RCN

Agosto
2017

Menor fue manipulada por adultos para compartir contenido sexual en redes sociales

La Unidad Investigativa de Noticias RCN logró hacer el seguimiento a un caso aterrador en el que una menor de 14 años era asediada por dos hombres que triplican su edad y la inducían a compartir contenido sexual explícito en redes sociales.

De acuerdo a lo que pudo establecer la Unidad Investigativa de Noticias RCN los hombres aprovecharon el uso de redes sociales por parte de la menor, especialmente el de mensajería instantánea, para enredarla y pedirle imágenes y videos suyos.

Unidad Investigativa
Fecha: Agosto 28 de 2017, 7:58 am

Ante los largos y continuos encierros de la menor, los padres optaron por decomisarle el teléfono celular y lograron quitarle la clave, allí descubrieron el misterio y se encontraron con que la menor compartía fotos íntimas con dos hombres, uno de 39 años y otro de 44.

Según los padres de la niña, la menor vivía absorta en conversaciones de abierto contenido sexual con un hombre de 39 años, quien resultó ser un conocido y, además, se percataron de que un profesor de la adolescente también le pedía fotos y videos íntimos a la niña.

'Grooming', la nueva modalidad de abuso sexual a través de internet

Mayo de 2018

Sebastián Bedoya - Sistema Informativo del Canal 1

En alerta se encuentran las autoridades luego de capturar a un hombre de 32 años por abuso sexual de menores de edad a través de la modalidad conocida como "grooming".

La denuncia de un menor de 14 años permitió la captura del sujeto que se hacía pasar por un infante para ganarse su confianza, luego de engañarlo con falsos perfiles y testimonios lo citó en una residencia para abusarlo sexualmente.

El coronel Fabián Ospina, subcomandante de la Policía Metropolitana de Cali, indicó que "esta persona le pasaba unas imágenes al menor de 14 años incentivándolo con regalos y dinero en efectivo, donde ya después los citaba y luego accedía sexualmente de esta persona. El hombre fue capturado en el barrio Alfonso Bonilla Aragón".

Fran Alexander Ramírez, secretario de TIC del Valle, dijo que en esta modalidad los "adultos se hacen pasar por niños, ponen un perfil falso de un artista o un famoso y empiezan a entablar una conversación con los niños para poco a poco ganarse la confianza del menor hasta pedirle compartir una foto".

REFERENCIAS

<https://noticias.canalrcn.com/nacional-unidad-investigativa/unidad-investigativa-menor-fue-manipulada-adultos-compartir-contenido>

<https://canal1.com.co/noticias/nacional/grooming-la-nueva-modalidad-de-abuso-sexual-a-traves-de-internet/>

<http://www.teprotejo.org/index.php/es>

<https://www.enticconfio.gov.co/Como-evitar-ser-victima-de-grooming>

<https://www.youtube.com/watch?v=OdixH25nCHK>

<https://definicion.de/grooming/>

<https://www.educarchile.cl>



Categoría	Entidad	Tiempo (Días)
 Material de Abuso Sexual Infantil (Pornografía Infantil)	DIJIN - CCP	5
 Explotación Sexual (ESCNA)	DIPRO	18
 Intimidación Escolar	Institución Educativa ICBF	17
 Ciberacoso	DIJIN/DIPRO	19
 Contenidos Inapropiados	Red PaPaz	12
 Venta de Alcohol y Drogas	DIPRO	18
 Maltrato, trabajo y abuso infantil	ICBF	45
 Otros	Te Protejo	14

Esta última es para el socializador, debe tener en cuenta cual entidad le puede ayudar a los adolescentes dependiendo de la situación y cuánto tiempo dura en tener respuesta.

ANEXO K. TERMINOS Y CONDICIONES DE MONKEY COLLECTOR

Incluye la URL de la política de privacidad en el panel de aplicaciones.

TERMINOS Y CONDICIONES

DESCRIPCIÓN DEL SERVICIO

Monkey collector provee a los usuarios diversión, mediante las aventuras de un mico llamado “Pepito”, el cual tiene que recoger frutas y ganar muchos puntos antes de que cualquier enemigo lo mate, al matarlo va perdiendo vidas y al perderlas todas las vidas se reiniciará el juego desde el principio.

POLITICAS DE PRIVACIDAD Y PROTECCIÓN DE DATOS

Tus amigos, conexiones y las personas con las cuales juegan “Monkey collector” podrán ver tu actividad en el juego.

El juego tendrá acceso a la información de tu perfil, las personas (amigos) que conoces y a tus fotos con el fin de saber que personas usan el juego y realizar una estadística sobre el uso de la aplicación.

Se usará para fines académicos, no almacenará ningún tipo de tu información, al igual que no hará uso inapropiado de ella, ni se brindará a otros usuarios y así proteger los datos brindados por Facebook, brindando confidencialidad y seguridad.

No se publicará contenido en tu nombre y sin tu autorización.

No se usarán los datos obtenidos de Facebook para tomar decisiones sobre requisitos de participación,

Monkey collector no confundirá, defraudará, engañará, sorprenderá ni enviará spam a ninguna persona que use la aplicación. No se transmitirá, solicitará ni recopilará nombres de usuarios ni contraseñas de Facebook.

No nos hacemos responsables del mal uso de la aplicación por parte de los usuarios.

Todas nuestras políticas de privacidad están sujetas a las políticas de Facebook.

III. CENTRO DE AYUDA

Monkey collector hace lo posible por proteger los datos del usuario. Si tiene alguna queja o preguntas sobre nuestras Políticas de privacidad o sobre el uso de datos del usuario, comuníquese con nuestro Centro de ayuda

[Centro de ayuda]

- Correo electrónico: appkgrooming@gmail.com

<https://developers.facebook.com/policy>

ANEXO L. ALGUNOS DE LOS CONCENTIMIENTOS INFORMADOS DEBIDAMENTE FIRMADOS POR LOS ACUDIENTES

UNIVERSIDAD SANTO TOMAS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
VEREDAS RENOVACIÓN 1902-1704

Se busca que la herramienta le muestre a los adolescentes lo que podría hacer un groomer (personas adultas que engañan a adolescentes y/o niños para tener una satisfacción sexual ya sea violación u obtención de fotos íntimas u otro tipo de información) con la información personal publicada en Internet. Al final presenta una forma para cambiar las opciones de privacidad en Facebook. En detalle la clase tendrá las siguientes características:

- Se obtendrá alguna información compartida de red social de Facebook del usuario
- La información se trabajará bajo confidencialidad y responsabilidad
- Toda la información obtenida será borrada y no se almacenará

Luego de conocer la actividad a realizar con los niños y niñas:

- Como adulto responsable por el niño o la niña: Daniel Alejandro Perini acepto voluntariamente su participación en una jornada en el contexto escolar.
- Permiso que se tomen fotografías o videos del ejercicio, SIEMPRE Y CUANDO ÉSTAS SÓLO SEAN CON FINES ACADÉMICOS Y NO SEAN REPRODUCIDAS CON FINES COMERCIALES.
- Permiso la participación del niño o la niña: Daniel Alejandro Perini siempre y cuando en TODO MOMENTO estén presentes las y los docentes responsables por él o ella en el contexto escolar donde se realizará el ejercicio.

CS Scanned with CamScanner

UNIVERSIDAD SANTO TOMAS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
VEREDAS RENOVACIÓN 1902-1704

4. Permiso la participación del niño o la niña: Daniel Alejandro Perini siempre y cuando me sea informado el resultado de la actividad y pueda tener acceso al material audiovisual o al documento de resultados de la jornada.

NOMBRE DEL PADRE Y/O ACUDIENTE:
Flor Alba Montoya Ortiz

FIRMA: Flor Montoya c.c. 20 330 129

FECHA: 02/06/21

RUTA DE PUBLICACIÓN:
<https://apps.facebook.com/225491755030624> Ruta de Facebook
<http://monkeycollector.00webhostapp.com/>

CS Scanned with CamScanner

UNIVERSIDAD SANTO TOMAS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
VEREDAS RENOVACIÓN 1902-1704

Se busca que la herramienta le muestre a los adolescentes lo que podría hacer un groomer (personas adultas que engañan a adolescentes y/o niños para tener una satisfacción sexual ya sea violación u obtención de fotos íntimas u otro tipo de información) con la información personal publicada en Internet. Al final presenta una forma para cambiar las opciones de privacidad en Facebook. En detalle la clase tendrá las siguientes características:

- Se obtendrá alguna información compartida de red social de Facebook del usuario
- La información se trabajará bajo confidencialidad y responsabilidad
- Toda la información obtenida será borrada y no se almacenará

Luego de conocer la actividad a realizar con los niños y niñas:

- Como adulto responsable por el niño o la niña: Adrian Javier Gula R acepto voluntariamente su participación en una jornada en el contexto escolar.
- Permiso que se tomen fotografías o videos del ejercicio, SIEMPRE Y CUANDO ÉSTAS SÓLO SEAN CON FINES ACADÉMICOS Y NO SEAN REPRODUCIDAS CON FINES COMERCIALES.
- Permiso la participación del niño o la niña: Adrian Javier Gula R siempre y cuando en TODO MOMENTO estén presentes las y los docentes responsables por él o ella en el contexto escolar donde se realizará el ejercicio.

CS Scanned with CamScanner

UNIVERSIDAD SANTO TOMAS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
VEREDAS RENOVACIÓN 1902-1704

4. Permiso la participación del niño o la niña: Adrian Javier Gula R siempre y cuando me sea informado el resultado de la actividad y pueda tener acceso al material audiovisual o al documento de resultados de la jornada.

NOMBRE DEL PADRE Y/O ACUDIENTE:
William R. Gula R

FIRMA: William R. Gula R c.c. 80 310 237

FECHA: / /

RUTA DE PUBLICACIÓN:
<https://apps.facebook.com/225491755030624> Ruta de Facebook
<http://monkeycollector.00webhostapp.com/>

CS Scanned with CamScanner

ANEXO M. VIDEO



Segunda pregunta...

**¿Qué cambios harás en un Facebook
de ahora en adelante?**

Por último...

**Opinión de
un docente**

—◆—
**Estas fueron algunas de las opiniones
de los estudiantes y docentes de los
colegios a los cuales asistimos**
—◆—