

PROTOTIPO DE APLICACIÓN MÓVIL DE ASESORÍA EN PRIVACIDAD EN LÍNEA

JESÚS ALEJANDRO LORA TOVAR

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

**FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y
COMUNICACIÓN**

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLÍN

2018

PROTOTIPO DE APLICACIÓN MÓVIL DE ASESORÍA EN PRIVACIDAD EN LÍNEA

JESÚS ALEJANDRO LORA TOVAR

**Trabajo de grado para optar al título de maestría en tecnologías de información y
comunicación**

Asesor

Ferney Orlando Amaya Fernández

Ingeniero Electrónico

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

**FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y
COMUNICACIÓN**

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLÍN

2018

DECLARACIÓN ORIGINALIDAD

“Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad”. Art. 82 Régimen Discente de Formación Avanzada, Universidad Pontificia Bolivariana.

A handwritten signature in black ink, enclosed within a large, hand-drawn oval. The signature appears to read "Alejandro Roura".

FIRMA AUTOR (ES) _____

Medellín febrero 2019

A la memoria de mi Abuelito Landulfo Aureliano Tovar Bolaños, de quien aprendí que la recompensa viene después del trabajo duro. Fue, es y será mi modelo de padre a seguir, inspiración de responsabilidad, honradez y amor por la familia.

AGRADECIMIENTOS

Primeramente agradezco y dedico este trabajo de grado a mi padre Dios quien es el principal artífice y patrocinador de este sueño, quien me trajo a esta hermosa ciudad y me regalo la oportunidad de seguir mi camino académico y profesional, a Él sea la honra y el honor por siempre; en segundo lugar a mi familia mi madre Myriam Tovar, mi hermano Luis Felipe Lora, mis abuelitos Landulfo Tovar, Clemencia Coral y Teresa Revelo, especialmente a mi madre mujer virtuosa e incansable, nunca se dio por rendida y nunca escatimo en darle lo mejor a sus hijos, a ella le debo todo lo que soy como persona; agradezco a mi tía Lucia quien con corazón generoso me recibió y acogió en esta ciudad, agradezco a mis profesores, Leonardo Betancur quien me dio la oportunidad de vincularme como estudiante a esta gran universidad, a mi asesor y director de Tesis Ferney Amaya, por su excelente trabajo y compromiso en este trabajo de grado, a mis jefes Juan Manuel Parra y Carolina Jaramillo quienes me dieron la oportunidad de poder trabajar mientras terminaba mi maestría.

CONTENIDO

<u>1</u>	<u>INTRODUCCIÓN</u>	<u>10</u>
<u>2</u>	<u>PLANTEAMIENTO DEL PROBLEMA</u>	<u>11</u>
2.1	PROBLEMA	11
2.2	JUSTIFICACIÓN	12
<u>3</u>	<u>OBJETIVOS</u>	<u>15</u>
3.1	OBJETIVO GENERAL	15
3.2	OBJETIVOS ESPECÍFICOS	15
<u>4</u>	<u>MARCO REFERENCIAL</u>	<u>16</u>
4.1	MARCO CONTEXTUAL	16
4.2	MARCO CONCEPTUAL	16
4.3	MARCO LEGAL	21
4.4	ESTADO DEL ARTE	22
<u>5</u>	<u>METODOLOGÍA</u>	<u>36</u>
<u>6</u>	<u>PRESENTACIÓN Y ANÁLISIS DE RESULTADOS</u>	<u>38</u>
6.1	DISEÑO DEL MODELO DE APLICACIÓN MÓVIL	38
6.2	CONSTRUCCIÓN DEL PROTOTIPO DE APLICACIÓN MÓVIL	56
6.3	DESPLEGAR EL PROTOTIPO DE APLICACIÓN MÓVIL	74
<u>7</u>	<u>CONCLUSIONES</u>	<u>107</u>
<u>8</u>	<u>TRABAJOS FUTUROS</u>	<u>110</u>
<u>9</u>	<u>REFERENCIAS</u>	<u>111</u>
<u>10</u>	<u>ANEXOS</u>	<u>120</u>

LISTA DE FIGURAS

Figura 1. Conexiones de banda ancha por tipo de acceso. (MINTIC, 2017).....	16
Figura 2. Casos de uso.....	47
Figura 3. Diagrama de proceso.	48
Figura 4. Diagrama de calificación interna.	49
Figura 5 Mockup de recomendaciones.....	52
Figura 6 Mockup de estadísticas	53
Figura 7 Mockup de encuesta (autoevaluación).....	54
Figura 8 Mockup de perfil.....	55
Figura 9. Diseño y estructura.	63
Figura 10. Elementos de aplicación.	64
Figura 11. Pantalla inicial.....	65
Figura 12. Evalúate.	66
Figura 13. Estadísticas.....	67
Figura 14. Recomendaciones.	67
Figura 15. Página recomendaciones.....	68
Figura 16. Términos y condiciones.....	69
Figura 17. Políticas de privacidad.	69
Figura 18. Crear formulario.	71
Figura 19. Compartir.	72
Figura 20. Función Resultados.....	73
Figura 21. Google Play Developer Console (Antevenio, 2018).	75
Figura 22. Añadir aplicación (Antevenio, 2018).....	76
Figura 23. Pantalla principal Google Console.	77
Figura 24. Vista Previa Privatus.....	78
Figura 25. Información general del uso de la aplicación.	80
Figura 26. Ubicaciones por ciudad.....	81
Figura 27. Ubicaciones por departamento.....	81
Figura 28. Información general de dispositivos y red.....	83
Figura 29. Versiones del SO.	84
Figura 30. Datos por dispositivo.	85
Figura 31. Datos por red.....	86
Figura 32. Duración de la sesión.....	87
Figura 33. Datos de pantallas de usuarios.	88
Figura 34. Usuarios semana 1.	89
Figura 35. Usuarios semana 4.	90
Figura 36. Instalaciones en dispositivos activos por versión de Android.	91
Figura 37. Usuarios que instalaron la Aplicación por primera vez gráfica.....	92
Figura 38. Usuarios que instalaron la Aplicación por primera vez tabla.	92
Figura 39. Instalaciones totales por usuarios.	93
Figura 40. Desinstalaciones totales por usuarios.	93
Figura 41. Calificaciones a lo largo del tiempo.	94
Figura 42. Appy Pie Analytics.	95

Figura 43. Métricas de Type Form.....	96
Figura 44. Datos de instalación.	97
Figura 45 Edad de los encuestados.	98
Figura 46 Género de los encuestados.	98
Figura 47 Estrato socioeconómico de los encuestados.	99
Figura 48 Último nivel educativo de los encuestados.....	99
Figura 49 ¿Cuánto tiempo lleva usando internet?	100
Figura 50 ¿Cuánto tiempo lleva haciendo compras en línea?	100
Figura 51 ¿Cuáles de las siguientes actividades realiza con más frecuencia al acceder a Internet?	101
Figura 52 ¿Hace cuánto tiene cuenta en redes sociales?	101
Figura 53 ¿Cuáles de las siguientes aplicaciones y/o redes sociales utiliza?.....	102
Figura 54 ¿Cuándo está o ha estado en una relación afectiva, comparte alguna de la siguiente información con la otra persona?	103
Figura 55 Clasificación de usuarios encuestados.	103
Figura 56. Plataforma MobApp Creator (MobApp Creator, 2018).	144
Figura 57. App Makr (Makr, 2018).....	145
Figura 58. Appyourself (Appyourself, 2018).....	146
Figura 59. Good Barber (Appyourself, 2018).	147
Figura 60. Appy Pie (Appypie, 2018)	148
Figura 61. Wufoo (Wufoo, 2018).....	149
Figura 62. JotForm (Jotform, 2018).	150
Figura 63. Survey Monkey (Surveymonkey, 2018).	151
Figura 64. Type Form (Type Form, 2018).	152
Figura 65 Términos y condiciones	168

LISTA DE TABLAS

Tabla 1 Tipos de usuarios según el estudio de Brandtzæg. (Brandtzæg & Heim, Social network sites - A typology of users, 2010)	33
Tabla 2. Tabla con los rangos de clasificación de los usuarios.....	40
Tabla 3. Plataformas de desarrollo de aplicaciones móviles.....	58
Tabla 4. Plataformas de gestión de encuestas.	61

RESUMEN

En este documento se presenta el proceso de diseño e implementación de un prototipo de aplicación móvil que permite determinar el nivel de exposición de los datos privados en Internet además de asesorar en cómo proteger la privacidad de los datos personales. Con el desarrollo de esta aplicación se pretende mitigar los riesgos de privacidad, aportando así a la seguridad de los datos privados en Internet y a la comunidad que interactúa día a día a través de los dispositivos móviles.

PALABRAS CLAVE

Privacidad en línea, aplicación móvil, autoeficacia de privacidad, autoprotección en línea, protección de datos.

ABSTRACT

This document presents the design and implementation process of a mobile application prototype that allows determining the level of exposure of private data on the Internet, as well as advising on how to protect the privacy of personal data. The development of this application aims to mitigate privacy risks, thus contributing to the security of private data on the Internet and to the community that interacts day by day through mobile devices.

KEY WORDS:

Online Privacy, mobile app, privacy self-efficacy, self-protection online, data protection

1 INTRODUCCIÓN

Este trabajo de grado nace como parte del del proyecto de Investigación de Privacidad UPB Innova 2016 “Privacidad siglo XXI”, ¿reliquia o necesidad? (Aguirre Jaramillo & Amaya Fernández, 2016) que tiene como propósito principal estudiar la privacidad en línea, la autoeficacia y el nivel de preocupación que tienen las personas en cuanto a su privacidad. Centra su interés en la privacidad de la información en línea, destacando la importancia del conocimiento y análisis de las situaciones y comportamientos que ponen en riesgo la seguridad de los datos privados de los usuarios de Internet. Partiendo desde la pregunta de investigación planteada ¿Cómo asesorar al usuario de Internet para que adopte medidas de autoprotección de sus datos privados?, el objetivo general de la presente investigación consiste en desarrollar un prototipo de aplicación móvil que asesore al usuario de Internet para que adopte medidas de protección de sus datos privados. En este documento se presenta el proceso de construcción de la aplicación desde su diseño, análisis, definición de la arquitectura y pruebas, hasta la liberación de la aplicación y seguimiento de esta para comprobar su funcionalidad y obtener datos de uso de distintos usuarios en varias ciudades de Colombia.

El planteamiento del problema presenta una introducción a la problemática general sobre como el usuario de Internet muestra preocupación por cuidar sus datos personales en línea, pero desconoce buenas prácticas de seguridad en línea para la protección de estos. Por tal motivo se propone construir una aplicación que determine el nivel de exposición de los datos privados en internet y asesore de manera personal a cada usuario sobre métodos de proteger su dispositivo móvil.

Los resultados presentan el proceso de diseño, desarrollo, implementación y liberación de la aplicación móvil. Se presenta el proceso de diseño del instrumento de medición o encuesta utilizado para medir la exposición de datos de los usuarios que acceden a la aplicación. Se presentan los requerimientos funcionales de la aplicación y se especifica la estructura de esta. Además, se presentan las plataformas que se utilizaron para desarrollar la aplicación y el proceso utilizado, la implementación y el seguimiento que se realizó a la aplicación durante un mes para recopilar datos de uso, utilizando herramientas de análisis de datos como Google Analytics.

2 PLANTEAMIENTO DEL PROBLEMA

2.1 Problema

Con el avance de la tecnología el mundo ha experimentado un cambio que se refleja en nuevas formas de acceder a la información y de interactuar, en un espacio virtual en el que los internautas hacen parte de una cultura diferente y novedosa, atractiva por la facilidad al momento de acceder a la información y que, de alguna manera, ha logrado permear los diferentes ámbitos de la vida. Adultos, niños y adolescentes son usuarios permanentes de las redes e Internet. Sin embargo, frente a esta oleada de aplicaciones y de acceso a través de dispositivos móviles, surge una voz de alerta donde padres de familia, asociaciones de prensa y académicos se preguntan sobre los efectos del anonimato y la sobre exposición de los individuos en la Red.

De ahí, que entre las situaciones más comunes que preocupan a los usuarios en línea son las relacionadas con la privacidad y el manejo reservado de la información. Por ejemplo, existen algunas compañías que usan de forma inapropiada la información de sus usuarios poniéndolos en riesgo al emplear datos personales que suministran, Como es el caso de Facebook, la red social que fue acusada de vender datos de 87 millones de usuarios a terceros (Picchi, CBS news, 2018). A raíz de este escándalo 3 estados en los Estados Unidos abrieron investigaciones a Cambridge Analytica y Facebook en el que están involucrados los CEO de las respectivas compañías. (Picchi & Carissimo, CBS news, 2018). Otro gigante tecnológico como lo es Google recopila miles de gigabytes de información de sus usuarios a través de servicios como Gmail, YouTube, Google Drive, Google Maps y las Búsquedas de Google. Estas compañías recopilan datos sobre sus usuarios y utiliza esta información para vender publicidad altamente personalizada (Popken, 2018). Un estudio realizado en 2017 en los Estados Unidos dirigido a adultos sobre las situaciones que más preocupan a los usuarios mientras navega en línea, revela que alrededor del 59% de los usuarios de Internet indicaron que estaban preocupados por delitos cibernéticos como el robo de su dinero o información personal en línea (Statista, 2017). De acuerdo a este estudio, el 49% de los usuarios de Internet estaban preocupados por ataques cibernéticos a través de Internet para perturbar usuarios en los EE. UU. (Por ejemplo, robo en línea y de información clasificada o la interrupción de servicios). Cerca del 30% indicaron estar preocupados ya que empresas recopilan y comparten sus datos personales en línea con otras organizaciones (Statista, 2017). El 26% de los usuarios de Internet estaban preocupados por vigilancia en línea de ciudadanos estadounidenses por parte del gobierno de EE. UU (Statista, 2017). Según un reporte de la compañía ESET realizado en 2016 (ESET, 2016), el 69% de los usuarios no protege su dispositivo móvil, es decir, no adoptan estrategias como las que propone la empresa Samsung para proteger su información, realizar copias de seguridad periódicamente, descargar aplicaciones únicamente desde las tiendas oficiales, configurar contraseñas y actualizar las aplicaciones (Samsung, 2016).

Es indudable que el avance de la tecnología no solo proporciona a los individuos facilidad y acceso rápido a la Internet, puesto que también exige de ellos mayor precaución y discreción al

hacerlo. En conclusión, hay un desconocimiento del nivel de exposición de los datos privados de los usuarios cuando acceden a diferentes sitios en Internet (Byer, 2018)., usan servicios o aplicaciones en línea a través de dispositivos (móviles o fijos), también hay desconocimiento de medidas de autoprotección, lo que está llevando a estos usuarios a preocuparse por su privacidad. Al mismo tiempo, estos usuarios incurren en comportamientos que no ayudan para nada a mitigar este problema, sino que por el contrario lo agravan, adoptando comportamientos que los llevan a ser vulnerables ante situaciones que amenazan su seguridad y privacidad (Byer, 2018). En una encuesta reciente realizada por el gigante tecnológico Mozilla (Mozilla Corp., 2017), una abrumadora mayoría de usuarios de Internet admitieron que no están informados sobre cómo protegerse en línea. La encuesta se realizó a más de 30,000 participantes de todo el mundo, entre ellos Francia, Alemania, Australia, Canadá, los EE. UU. Y el Reino Unido. En general, más del 90 por ciento de los encuestados carecen de confianza en su capacidad para mantenerse seguros en línea, y el 11.5 por ciento admite que no sabe nada y necesita ayuda. (Mozilla Corp., 2017). Es por estas razones que el presente estudio propone la pregunta de investigación: ¿Cómo asesorar al usuario de Internet independientemente del tipo de dispositivo que utilice para conectarse a la red, para que adopte medidas de protección de sus datos privados?

2.2 Justificación

En Colombia el uso de teléfonos inteligentes va en aumento, cada vez son más los usuarios que acceden a Internet utilizando su dispositivo móvil a través de aplicaciones móviles, como lo demuestra el boletín trimestral de las TIC (MINTIC, 2017), donde se indica que el número total de accesos por suscripción a Internet móvil fue de 9.916.552 durante el cuarto semestre de 2016, en comparación con el número total de suscriptores, al término del cuarto trimestre de 2014 que fue de 5.565.663 según el informe trimestral de (MINTIC, 2015). Estos datos evidencian que en los últimos años los accesos por suscripción a internet móvil han ido en aumento en la población colombiana, otras cifras de estudios realizados por Infometrika para el ministerio TIC revela que por cada 100 habitantes en Colombia hay 34,43 habitantes con teléfonos inteligentes (MINTIC; Infométrika S.A.S, consultores, 2016).

Fuentes revelan que en los últimos años no solo el uso de internet ha crecido en Colombia sino también el uso de las redes sociales y sus suscriptores. Colombia ocupa el puesto número 15 en el mundo de suscriptores de Facebook, con 26 millones de suscriptores a junio del 2016, según cifras de internet World Stats (Internet World Stats, 2016). También se registran 5.2 millones de usuarios en Twitter según estadísticas (Abad, 2015). En conclusión, los usuarios de internet en Colombia utilizan en gran cantidad los servicios de redes sociales. Durante el “Facebook Day” llevado a cabo en la ciudad de Bogotá en octubre del 2014 (Alvarado, 2014), la directora general de Facebook para Colombia, Sandra Quintero, señaló que alrededor del 60% de los usuarios colombianos acceden a la red por medio de dispositivos móviles. Alberto Arébalos (Alvarado, 2014) director de comunicaciones de Facebook para Latinoamérica indica que a través de la red social se alcanzan a contabilizar 5.2 millones de mensajes instantáneos a través de su plataforma Messenger, 345 millones de comentarios y 225 millones de fotos subidas. Para el caso de Colombia se aclaró que se alcanza mensualmente 1.6 millones de “Me gusta” o “Likes” en los usuarios del país.

Al finalizar el cuarto trimestre del 2016, el número total de conexiones a Internet de Banda Ancha alcanzó los 15.306.066 accesos en el país, las conexiones a Internet de Banda Ancha se componían principalmente por accesos móviles a Internet con un total de 9.414.186, siendo las redes de cuarta generación 4G, con un total de 4.886.391 de los usuarios de internet móvil (MINTIC, 2017).

El abundante tráfico de datos móviles que el uso de las redes sociales produce son consecuencia de que cada día son más los usuarios que navegan en Internet a través de sus dispositivos móviles, naciendo la necesidad de crear estrategias que le permitan al usuario proteger su privacidad y sus datos personales, debido a que en contraprestación a esta situación, puede desarrollarse ciertos comportamientos por parte de los usuarios de internet que los pongan en riesgo y puedan ser víctimas de eventos que vulneren la privacidad y seguridad de su información; la situación problema del presente estudio expone que los usuarios de internet desconocen el nivel de exposición de sus datos privados en internet como de medidas para proteger su privacidad y seguridad en línea, es decir no tienen los conocimientos y estrategias para hacer frente a eventos que pongan en riesgo su privacidad, aun por el contrario los usuarios de internet revelan tener autoeficacia.

Según (Rifon, LaRose, & Lewis, 2007) autoeficacia es la creencia de una persona en su capacidad de tener éxito en una situación particular. Esta autoeficacia de privacidad que aparentemente poseen los internautas se da por la sobreestimación en las capacidades para proteger su propia privacidad en línea. Esta situación ha desencadenado una creciente preocupación por la privacidad en los usuarios de Internet.

Un estudio realizado en estados unidos a jóvenes y adultos, revela en primera instancia que, el nivel de la preocupación de privacidad en línea llevó a los usuarios más jóvenes de internet, a adoptar varios comportamientos para proteger su privacidad de las estrategias de e-marketing (mercadeo electrónico), debido a su comportamiento en cuanto a estrategias de abordaje, los jóvenes buscaron apoyo interpersonal de los padres o maestros, lo que indica que dependen de la orientación proporcionada por los adultos para evitar los riesgos potenciales asociados con la divulgación de información (Youn, 2009), otras situaciones que pueden preocupar a los usuarios adultos de internet es el spam, Un estudio revela que el correo electrónico no deseado genera inquietudes sobre la privacidad y a su vez, estas preocupaciones sobre la privacidad influyen en la forma en que los usuarios manejan el correo no deseado, los resultados muestran que: las experiencias de spam de los usuarios de correo electrónico tienen una relación profunda con sus preocupaciones de privacidad; la preocupación por la privacidad ayuda a mediar la relación entre el comportamiento protector de los usuarios de la experiencia de spam; y (3) cuando están preocupados por la privacidad como resultado del correo no deseado, los usuarios de correo electrónico tienden a mostrar comportamientos tanto pasivos como proactivos (Park, Sharman, Raghav Rao, & Upadhyaya, 2016).

El problema de la presente investigación expone que el desconocimiento del nivel de exposición de los datos privados y de métodos de autoprotección en línea por parte de los usuarios de internet, conllevan a la vulnerabilidad de la privacidad de sus datos. Cabe destacar la importancia de este proyecto, para quienes acceden a Internet a través de su dispositivo móvil,

ya que necesitan conocer cuan expuestos están sus datos en la red para así poder fortalecer sus habilidades de percepción de privacidad para protegerse en la línea, adoptando comportamientos y estrategias de autoprotección que les permita reducir el riesgo de ser víctimas de las múltiples situaciones que violan su privacidad y seguridad. La presente propuesta pretende aprovechar las tecnologías actuales, teléfonos inteligentes y aplicaciones móviles, como medio de la solución al problema, al desarrollar una aplicación que determine el nivel de exposición de los datos privados en internet y asesore de manera personal a cada usuario sobre métodos de proteger su dispositivo móvil, para minimizar los riesgos de convertirse en víctima de situaciones que atenten o vulneren sus datos privados y seguridad en línea.

3 OBJETIVOS

3.1 Objetivo General.

Desarrollar un prototipo de aplicación móvil que asesore al usuario de Internet para que adopte medidas de autoprotección de sus datos privados

3.2 Objetivos Específicos

- 1.** Diseñar un modelo de aplicación móvil que determine el nivel de exposición de los datos privados en Internet y asesore al usuario de internet de manera personalizada, métodos de protección de sus datos privados.
- 2.** Construir el prototipo de aplicación móvil empleando una plataforma de construcción de aplicaciones móviles
- 3.** Liberar el prototipo de aplicación móvil.

4 MARCO REFERENCIAL

4.1 Marco contextual

Al finalizar el cuarto trimestre del 2016 el número total de conexiones a Internet de Banda Ancha alcanzó los 15.306.066 accesos en el país, que se componen principalmente por accesos móviles con 9.414.186 conexiones, las redes de cuarta generación 4G con 4.886.391 conexiones, las cuales aumentaron su participación del 29,36% en el tercer trimestre del 2016 al 31,92% en el cuarto trimestre del mismo año. Los accesos a redes de tercera generación 3G móvil alcanzaron un total de 4.527.795 de conexiones y una participación del 29,58%, disminuyendo esta última cifra 1,08 puntos porcentuales en relación con el tercer trimestre del 2016. Por su parte, las conexiones a Internet fijo dedicado alcanzaron un total de 5.891.880 accesos y una participación del 38,49%. Esta información se muestra en la **Figura 1**. (MINTIC, 2017). Partiendo de estos datos se define el contexto general el cual abarca el presente proyecto es la población colombiana con 15.306.066 de usuarios que acceden a Internet.

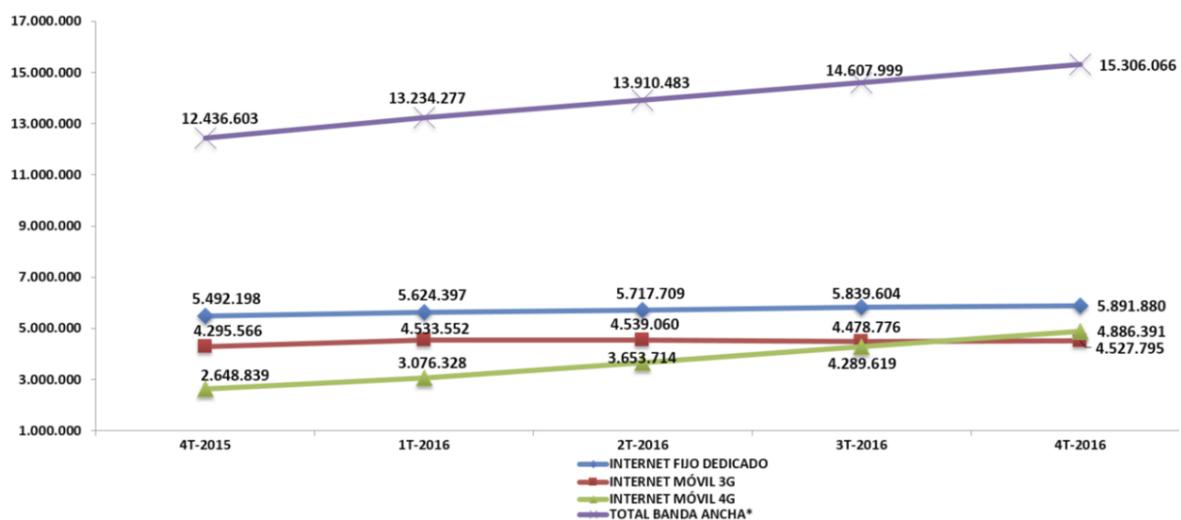


Figura 1. Conexiones de banda ancha por tipo de acceso. (MINTIC, 2017)

Para ubicarnos en un contexto más específico, el proyecto de Investigación de Privacidad UPB Innova 2016 “Privacidad siglo XXI”, ¿reliquia o necesidad? (Aguirre Jaramillo & Amaya Fernández, 2016) del cual hace parte este trabajo de investigación, tiene como propósito principal estudiar la privacidad en línea, la autoeficacia y el nivel de preocupación que tienen las personas en cuanto a su privacidad, en una población específica como es la comunidad de la Universidad Pontificia Bolivariana (UPB) sede Medellín.

El marco poblacional con el que se trabajó durante la etapa de ejecución del presente trabajo y en el que se basan los resultados la constituye una población heterogénea, de diferentes edades y profesiones, ubicados en distintos lugares del área geográfica de Colombia, en ciudades principales como Medellín, Cali, Bogotá, Pasto, Manizales, Ibagué, Popayán.

4.2 Marco conceptual

La Ley de Protección de Datos Personales reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar la información que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada. En este sentido datos personales se refiere a toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos (Mincomercio & Presidente de la república, 2013).

Para hablar de datos personales en Colombia se hace necesario conocer qué medidas de protección existen para estos en el país. Es de conocimiento general que la información es el activo más importante en el mundo actual, es por lo que el 17 de octubre de 2012 el Gobierno Nacional expidió la Ley Estatutaria 1581 de 2012, mediante la cual se dictan disposiciones generales para la protección de datos personales. En ella se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento de este, tal como lo corrobora la Sentencia de la Corte Constitucional C – 748 de 2011 donde, se estableció el control de constitucionalidad de la Ley en mención. La nueva ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión (en adelante tratamiento) por parte de entidades de naturaleza pública y privada. (Congreso de Colombia, 2012)

Existe un término clave utilizado en muchos contextos para referirse a la capacidad y conocimiento de las personas en cierta área laboral o académica, este concepto que será de gran relevancia conocido como **autoeficacia**, que se refiere a la creencia de un individuo de que él o ella tienen la capacidad de realizar un comportamiento deseado (Rifon, LaRose, & Lewis, 2007). Esta creencia o capacidad no siempre va ligada con que el individuo tenga los conocimientos necesarios, para enfrentar el comportamiento deseado. Este término adopta un significado más específico cuando hablamos de "**La autoeficacia de la privacidad**". En este trabajo de investigación se hace referencia a la confianza de los individuos en sus habilidades para proteger su privacidad, de las actividades de recolección y distribución de información de los vendedores electrónicos, centros de datos, entidades financieras, y demás individuos que quieran recopilar datos personales. (Rifon, LaRose, & Lewis, 2007)

El término de la autoeficacia puede ser entendido de muchas maneras dependiendo del contexto en el que sea utilizado y de los intereses implícitos en los individuos que lo emplean. Por lo tanto, para efectos de este proyecto se contempla la necesidad de explorar y desglosar el término de una manera más profunda. Por eso se trabaja con el concepto de la autoeficacia percibida, que es la creencia de una persona en sus capacidades y recursos cognitivos, necesarios para hacer frente a los eventos dados (Bandura A. , 1989). En comparación a un concepto de autoeficacia más moderno planteado por el mismo autor, el cual ha adaptado el término a tiempos más recientes, refiriéndose a la autoeficacia percibida como la creencia que afectan la calidad del funcionamiento humano a través de procesos cognitivos, motivacionales, afectivos

y de decisión. Específicamente influye en si piensan de manera pesimista u optimista, de manera auto-habilitante o auto-debilitante. La creencia de autoeficacia influye en la forma en que las personas se motivan frente a las dificultades a través de los objetivos que se fijan, las expectativas de resultados causales de sus éxitos y fracasos. La creencia de las personas en sus capacidades de afrontamiento desempeña un papel fundamental en su autorregulación de los estados emocionales. Esto afecta la calidad de su vida emocional, su vulnerabilidad al estrés y la depresión. La última forma en que la creencia propia de la autoeficacia contribuye al autodesarrollo personal y las elecciones que las personas toman en puntos decisivos e importantes que marcan el rumbo de su vida y en qué se convierten. (Bandura A. , 2012).

La autoeficacia percibida refleja una autoconfianza optimista de que se pueden realizar tareas nuevas o difíciles en diversos dominios del funcionamiento humano (Schwarzer, 1992). Siguiendo este orden de ideas la autoeficacia percibida es la seguridad en sí mismo que tiene un individuo ligado con sus propias capacidades para hacer frente a una situación en particular y poder resolverla.

El concepto de autoeficacia percibida ha sido actualizado para adaptarse al uso de las tecnologías actuales, como propone el estudio realizado por (Romero Landeros, González Suárez, & Anabalón, 2016), en el que evalúa como las personas que trabajan en las empresas modernas utilizando las nuevas tecnologías como: internet, dispositivos móviles, aplicaciones móviles, siguen percibiendo que la autoeficacia está presente y se define como la sensación de capacidad frente a la realización de una tarea que bajo ciertas condiciones influye en el producto final del trabajo y en cómo se va a experimentar y solventar los problemas que puedan surgir o relacionarse a la implementación de nuevas herramientas. (Romero Landeros, González Suárez, & Anabalón, 2016)

Para los trabajadores en la actualidad, la autoeficacia actuaría como un amortiguador de los posibles estresores que pudieran surgir. De este modo, el malestar de los trabajadores se relaciona no directamente sobre sus capacidades, ni por la falta de conocimiento tecnológico, sino con el servicio que entrega la tecnología en los momentos que falla. Por tanto, esta dependencia tecnológica, el no poseer otras herramientas, los limitaría a continuar con su trabajo normal. Pero la presencia de alta autoeficacia los ayudaría a adoptar estrategias de afrontamiento en tales casos impidiendo así que caigan en la desesperación, cuando deben enfrentar problemas relacionados con la tecnología (Romero Landeros, González Suárez, & Anabalón, 2016)

Es importante establecer el concepto de **Privacidad**, en este sentido el concepto proviene del latín, en el verbo *privare*, que significa “privar”, que a su vez dio lugar a la aparición de la palabra **privatus**, que se puede definir como “aquello que no es público”, por lo cual se define que la privacidad es aquello que una persona lleva a cabo en un ámbito reservado (Pérez Porto & Merino, 2010). Un sujeto, por lo tanto, tiene derecho a mantener su privacidad fuera del alcance de otras personas, asegurándose la confidencialidad de sus cosas privadas. El derecho a la privacidad forma parte de la Declaración Universal de los Derechos Humanos. Esto quiere decir que es un derecho inherente a cada ser humano, que tiene independencia frente a otros

factores, no puede transferirse, ni se puede renunciar a él. Como el resto de los derechos humanos, el derecho a la privacidad busca garantizar la dignidad del individuo.

La naturaleza contextual de la privacidad es evidente en definiciones más recientes. El autor Schoeman (Schoeman F. , 1984) propone la privacidad como un estado o condición de acceso limitado a los individuos. Los individuos tienen privacidad en la medida en que otros tienen acceso limitado a la información sobre ellos, a las intimidades de sus vidas, a sus pensamientos o a sus cuerpos. En otras palabras, la privacidad protege a los individuos de cualquier control excesivo de los demás (Schoeman F. , 1992). La naturaleza contextual de la privacidad es evidente ya que sus significados pueden cambiar de acuerdo con factores ambientales y personales, de modo que el deseo de privacidad de las personas es innatamente dinámico. Los individuos están continuamente involucrados en un proceso de ajuste en el que los deseos de privacidad se miden en contra de los deseos de revelación y comunicación personal con otros (Kimmel, 1996). El ajuste ocurre en el contexto de diversas fuerzas situacionales, como las presiones de otros, las normas sociales y los procesos de vigilancia utilizados para hacerlas cumplir (Kimmel, 1996). Esta definición, entonces, reconoce que la privacidad no existe en el vacío de la sociedad. En cambio, la privacidad influye y puede ser influenciada por las fuerzas sociales. Estas definiciones de privacidad se referencian para contextualizar el concepto de forma general, que será abordado de forma técnica al relacionarse con el contexto del proyecto.

Se hace necesario entrar más en profundidad respecto al término de privacidad, contextualizando este mismo, introduciéndolo con el término de **Privacidad de información**, que es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros (Rouse, 2017). Para términos del presente estudio la privacidad de información es la capacidad del usuario de Internet, para determinar cuáles de sus datos privados comparte con terceros.

Hoffman definió la privacidad de la información en términos de tres derechos distintos: el derecho de los individuos a determinar qué información acerca de sí mismos para compartir con otros, el derecho de las personas a saber lo que se está recogiendo sobre ellos, y el derecho de los individuos a acceder a los datos con el fin de mantener la sociedad y regular el gobierno. Estos tres derechos implican grados de control sobre la información sobre uno mismo y sobre el ambiente, sugiriendo de nuevo la naturaleza contextual de la privacidad (Regan, 1995).

Las anteriores afirmaciones sin duda siguen teniendo validez en la época actual en decir como concepto, que la privacidad es aquel espacio que una persona legítimamente quiere mantener alejado del conocimiento del resto (Ugarte Cataldo, 2013). Este concepto se apoya en dos derechos que son fundamentales y van ligados a la privacidad, el primero de ellos es: la intimidad que se define como el espacio de los pensamientos de cada cual, de la formación de las decisiones, de las dudas que escapan a una clara formulación, de lo reprimido, de lo aún no expresado, el segundo concepto es el de lo privado definido como el ámbito de los deseos y las preferencias individuales (Ugarte Cataldo, 2013). El primero está protegido por la discreción y su velo corresponde develarlo sólo a su titular, el segundo está sujeto a las reglas de convivencia que el contexto cultural y social impongan.

Una posibilidad es entender como privacidad el derecho a un espacio vital cuyo acceso queda vedado para los otros, eso que se ha denominado derecho al secreto que define que: El derecho del individuo de tener una esfera secreta de vida, de la que tenga poder de alejar a los demás (Ugarte Cataldo, 2013). En algunas tradiciones legales, el contenido de la privacidad como secreto es complejo y abarca todos los aspectos de la vida privada bajo un solo derecho como por ejemplo Estados Unidos y en otros países como en Chile, España o Perú los distintos aspectos de la privacidad han dado lugar a diversos derechos, aunque todos interrelacionados: a la vida privada, la imagen, la intimidad, la inviolabilidad de las comunicaciones (Ugarte Cataldo, 2013).

La privacidad debe definirse como el derecho a controlar la información y el acceso a sí mismo. Esta definición plantea que la privacidad se ve como una función del interés y la elección individuales. El autor (Regan, 1995) afirmó que la privacidad como valor debe ser equilibrada con otros valores que los individuos consideran importantes, incluyendo la libertad de prensa, la ley y el orden, y la seguridad nacional. La naturaleza contextual de la privacidad se hace evidente: dado que los individuos parecen no preocuparse por la privacidad hasta que esta se ve amenazada o invadida. La definición de privacidad depende o deriva de la naturaleza de la amenaza a la privacidad (Regan, 1995). La definición de Regan combina tanto el aspecto de control sugerido por Hoffman (Hoffman, 1980), como el concepto de estado limitado sugerido por Schoeman (Schoeman F. , 1984). La naturaleza contextual de la privacidad como se sugiere proporciona la oportunidad de ver la privacidad como un continuo (McLean, 1993).

El desarrollo del instrumento de medición utiliza la escala Likert que se ubica dentro de los diversos tipos de instrumento de medición en la investigación cuantitativa. Es un tipo de escala aditiva que corresponde a un nivel de medición ordinal. Se compone por una serie de ítems o perfiles a modo de afirmación, ante los cuales se solicita el juicio del sujeto. Los perfiles o ítems representan la propiedad que el investigador está interesado en medir. Las respuestas son solicitadas en grado de acuerdo o desacuerdo que el sujeto tenga con la afirmación en particular (Bedoya Laguna & Reyes Roncancio, 2017). Para el caso particular de esta investigación consiste en medir el nivel de preocupación o despreocupación del usuario de Internet frente a la exposición de sus datos en línea. A cada categoría de respuestas se le asigna un valor numérico que llevará al sujeto a una puntuación total. La puntuación final indica la posición del sujeto en la escala, lo ordena acorde con el grado con el cual presenta la actitud o la variable a medir.

4.3 Marco legal

En Colombia el artículo 15 de la Constitución Nacional define que todas las personas tienen derecho a su intimidad personal y familiar. En el mismo artículo se establecen otros dos derechos como el de Protección de Datos privados (Habeas Data) y el del Buen Nombre. (Consejo Superior de la Judicatura, 1991)

En Colombia se han creado leyes para proteger los datos personales de sus ciudadanos, es por ello que el 17 de octubre de 2012 el Gobierno Nacional expidió la Ley Estatutaria 1581 de 2012 (Congreso de Colombia, 2012) mediante la cual se dictan disposiciones generales para la protección de datos personales, en ella se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento del mismo, tal como lo corrobora la Sentencia de la Corte Constitucional C – 748 de 2011 (Corte Constitucional, 2011), donde se estableció el control de constitucionalidad de la Ley en mención. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada.

El Decreto 1377 del 27 de junio de 2013 (Mincomercio & Presidente de la república, 2013) tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, entre otros.

A nivel internacional también se mencionan referentes claves que aportan a la construcción del marco legal de la presente investigación. En los Estados Unidos la afirmación de privacidad de (Brandeis & Warren, 1890) uno de los ensayos más influyentes en la historia del derecho estadounidense, es ampliamente considerado como la primera publicación en los Estados Unidos en abogar por un derecho a la privacidad, articulando ese derecho principalmente como un "derecho a estar solo". Esto ha sido la base de la legislación sobre privacidad durante la mayor parte de este siglo. La ley de privacidad para los individuos en la sociedad se desarrolló con la preocupación de equilibrar las necesidades gubernamentales y las políticas contra las necesidades de los individuos (Moceyunas, 1996). En 1965, la Corte Suprema de los Estados Unidos describió la privacidad como un derecho fundamental, que tenía dos componentes: el primero era el interés de los individuos en evitar la divulgación de asuntos personales, y el segundo era el interés de los individuos en la independencia en tomar ciertos tipos de decisiones personales (Griswoldv. Connecticut. , 1965). La ley siguió desarrollándose en respuesta a la mayor capacidad del gobierno para recopilar, clasificar y divulgar datos sobre personas que usan bases de datos informáticas. En 1977 la Corte Suprema, describió la privacidad como "incluyendo el derecho del individuo a ser libre en sus asuntos privados de la vigilancia e intrusión del gobierno y el derecho de un individuo a no hacer públicos sus asuntos privados por el gobierno". (Whalen v. Roe , 1977). Las referencias mencionadas anteriormente se sustentan en la actualidad, debido a que forman la base de las actuales leyes que protegen los

datos de los usuarios de Internet y el derecho fundamental a la privacidad en cualquier ámbito, incluido la protección de los datos personales en línea.

En el mes de mayo del año 2018 empezó a regir a nivel mundial el reglamento general de protección de datos (RGPD). El RGPD es la norma que afecta por igual a las grandes corporaciones y a las pequeñas y medianas empresas (pymes) en su mayoría muy activas en el uso de datos. El nuevo reglamento general de protección de datos entró en vigor en mayo de 2016 y se convirtió de aplicación obligatoria para todas las empresas de la Unión Europea a partir del 25 de mayo de 2018, y otorga un mayor control y seguridad a los ciudadanos sobre su información personal en el mundo 2.0. El RGPD amplía sus derechos a decidir cómo desean que sus datos sean tratados y a cómo quieren recibir información de las empresas. Aprobando 3 principios a cumplir por parte de las empresas (Diario oficial Unión Europea, 2016) que se describen a continuación:

Principio de responsabilidad (accountability). Habrá que implementar mecanismos que permitan acreditar que se han adoptado todas las medidas necesarias para tratar los datos personales como exige la norma. Es una responsabilidad proactiva. Las organizaciones deben ser capaces de demostrar que cumplen dichas exigencias, lo cual obligará a desarrollar políticas, procedimientos y controles entre otros.

Principios de protección de datos por defecto y desde el diseño. Se deberán adoptar medidas que garanticen el cumplimiento de la norma desde el mismo momento en que se diseñe una empresa, producto, servicio o actividad que implique tratamiento de datos, como regla y desde el origen.

Principio de transparencia. Los avisos legales y políticas de privacidad deberán ser más simples e inteligibles, facilitando su comprensión, además de más completos. Incluso se prevé que, con el fin de informar sobre el tratamiento de los datos, puedan utilizarse iconos normalizados. (Diario oficial Unión Europea, 2016)

4.4 Estado del arte

En esta sección se presentan estudios y artículos que sirvieron de base de referencia el desarrollo de la aplicación, desde la etapa de diseño hasta la construcción y liberación de esta. También se presentan estudios que se utilizaron de referencia para construir y adaptar la encuesta o instrumento de medición los usuarios de internet.

Los estudios mencionados a continuación son investigaciones de los últimos avances realizados en las áreas del actual proyecto en el mundo y como se relacionan, en cuanto a temática, metodologías, aportes y tecnologías utilizadas.

En el artículo “Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences” (Bernhard Debatin, Ann-Kathrin Horn, & Hughes, 2009) se investiga sobre el nivel de conciencia de los usuarios de Facebook sobre los problemas de privacidad y los

beneficios y riesgos percibidos de utilizar Facebook. La investigación encontró que Facebook está profundamente integrado en la vida diaria de los usuarios a través de rutinas y rituales específicos. Los usuarios afirmaron entender las cuestiones de privacidad, pero informaron que subían grandes cantidades de información personal. Los riesgos para la invasión de la privacidad se atribuían más a los demás que a como cada usuario protege su información personal. Esto permite reforzar la falta de autorregulación de los usuarios, que, asociado a su sobreestimación de capacidades y habilidades, los transforman en potenciales víctimas. Este estudio utiliza técnicas cuantitativas y cualitativas para explorar la intersección oportuna, entre el uso de redes sociales en línea y las preocupaciones de privacidad. Muestra que las gratificaciones de usar Facebook tienden a sobrepasar las amenazas percibidas a la privacidad. La estrategia más común para la protección de la privacidad es la disminución de la visibilidad del perfil a través de la restricción del acceso a los amigos, este es también un mecanismo muy débil, una solución rápida en lugar de un enfoque sistemático para proteger la privacidad.

La correlación del estudio mencionado se presenta por que trabaja los comportamientos de los usuarios de Facebook, con respecto a su privacidad y muestra como los usuarios en muchas ocasiones, toman riesgos en los cuales su privacidad puede salir vulnerada, a cambio de recibir ciertos beneficios como conseguir más amigos o ganar más “me gusta” en sus publicaciones.

El estudio de la universidad de Queensland, Australia “Predicting Facebook users’ online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior” (Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014) adopta una teoría del modelo de comportamiento planificado que incluye normas descriptivas, riesgos y confianza para investigar la protección de la privacidad en línea en los usuarios de Facebook. Los resultados de esta investigación muestran que en general los participantes informaron actitudes positivas, un alto control del comportamiento percibido y altas intenciones de proteger su privacidad en Facebook. Relacionaron aproximadamente la mitad de las palabras con el riesgo y, en general, se correlacionaban positivamente con las intenciones de proteger la privacidad en línea, También se descubrió que las intenciones no generalizan el comportamiento en este contexto, que es una advertencia importante para la literatura sobre protección de la privacidad, y es consistente con las advertencias de algunos expertos en seguridad de que las personas a menudo no actualizan y cambian sus configuraciones de seguridad. (Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014).

En el estudio realizado en Estados Unidos denominado “A multinational study on online privacy: global concerns and local responses” (Cho, Rivera-Sánchez, & Lim, 2009) se revela que los comportamientos de protección de la privacidad pueden ser representados principalmente por tres factores subyacentes: la autoprotección proactiva (“proactive protection”), el evitar (“avoidance”) y a exclusión voluntaria (“opt-out”). Los resultados del análisis, después de haber realizado un estudio donde se encuesta a usuarios de internet de diferentes partes del mundo, indican la presencia de tres factores distintivos:

El factor de evitar consiste en elementos tales como "uso de medios no relacionados con Internet para comunicarse, comprar o recopilar información".

El factor de exclusión tiene que ver con la opción activa de no recibir solicitudes de correo electrónico.

El factor de protección proactiva se dirige a la protección más activa de la información personal, utilizando tecnologías que mejoran la privacidad, el borrado de cookies, el control de marcas de confianza, etc.

De acuerdo con la teoría de la motivación de la protección (Rogers R. , A Protection Motivation Theory of Fear Appeals and Attitude Change, 1975), (Rogers R. , Cognitive and Physiological Processes in Fear Appeals and Attitude Change:, 1983) y el Modelo de Proceso Paralelo Extendido (Witte, 1992), la preocupación y la autoeficacia son las variables más críticas que afectan el comportamiento de los individuos frente al riesgo.

La **preocupación** influye en la adopción individual de los comportamientos de afrontamiento, ya que aquellos con altos niveles de preocupación están más motivados para pensar y actuar sobre un problema para reducir la vulnerabilidad a la amenaza.

La autoeficacia, definida como la capacidad percibida para ejercer control personal en el cambio de **comportamientos** (Bandura A. , 1989), es otra variable central que afecta la adopción o el uso de conductas preventivas por parte de los individuos (Rimal, 2000).

Las variables de **preocupación** por la privacidad y autoeficacia serán claves para diagnosticar los **comportamientos** y usos en internet de un usuario, y poder analizar dichos datos para obtener conclusiones, a fin de lograr asesorar al usuario de internet para corregir sus comportamientos en internet.

El artículo titulado “Development of Measures of Online Privacy Concern and Protection for Use on the Internet” (Buchanan, Paine, Joinson, & Reips, 2007) aconseja que es importante contar con métodos para identificar y cuantificar las preocupaciones de la gente sobre la privacidad, herramienta para investigar cómo se comportan las personas tanto dentro, como fuera de Internet. En este estudio se divide a los encuestados en una de tres categorías dependiendo de sus respuestas a tres declaraciones:

- los fundamentalistas de la privacidad, que ven la privacidad como un valor especialmente alto que ellos sienten muy fuertemente vinculados,
- los pragmáticos de la privacidad, que también tienen fuertes sentimientos acerca de la privacidad, pero también pueden ver los beneficios de entregar cierta privacidad en situaciones donde creen que se toman precauciones para evitar que usen esta información y
- los despreocupados por la privacidad, aquellos que no tienen preocupaciones reales sobre la privacidad o sobre cómo otras personas y organizaciones están utilizando información sobre ellos.

Otros estudios también proponen variables para clasificar a los usuarios de Internet. Esto se encuentra en el artículo titulado “Privacy, Trust And Self-Disclosure Online” (Joinson, Reips,

Buchanan, & Schofield, 2008) el cual realizó durante dos períodos de tiempo. Durante el primer periodo se indagó entre los usuarios por las medidas de **preocupación** por la privacidad (actitud y comportamiento previo donde se miden las preguntas de **comportamientos** en línea). Durante el segundo periodo se indagó sobre las medidas de auto-revelación y percepción de privacidad y confianza percibida. A partir de los resultados se puede clasificar el **comportamiento** en línea de los usuarios respecto a la Confianza y Privacidad percibida.

Los artículos a los cuales se hace referencia a continuación son referidos a las nuevas tecnologías empleadas a nivel mundial para controlar la información de los usuarios de internet y el uso de aplicaciones que protegen la privacidad del usuario de Internet.

El artículo publicado por la IEEE titulado “Mobile Crowdsensing: Current State and Future Challenges” (Ganti, Ye, & Lei, 2011) expone que una categoría emergente de dispositivos en el margen de la Internet son sensores móviles y dispositivos de computación centrados en el consumidor, como teléfonos inteligentes, reproductores de música y sensores en el vehículo. Estos dispositivos son la evolución de Internet de las Cosas, ya que alimentan los datos de los sensores a Internet a escala social. Este artículo examina una categoría de aplicaciones que se denomina crowdsensing móvil, en la que individuos con dispositivos de computación y censado, comparten datos y extraen información para medir y mapear fenómenos de interés común. La integración de la detección empleando dispositivos informáticos cotidianos, en el margen de la Internet, dará lugar a la evolución de Internet de las cosas (IoT, Internet of the Things). Los dispositivos IoT típicos incluyen objetos con sensores (por ejemplo, contenedores químicos con sensores de temperatura, medidores inteligentes para el monitoreo remoto del consumo de energía). Una categoría emergente de dispositivos que resultará en la evolución de IoT son sensores móviles y dispositivos de computación centrados en el consumidor, que están conectados a Internet.

La masificación de los dispositivos móviles permite recolectar gran cantidad de información de los usuarios de internet, utilizando sensores del dispositivo (teléfono inteligente) como acelerómetro, micrófono, GPS, entre otros, se pueden saber datos como ubicación, nivel de ruido, rutas y lugares visitados por el usuario, toda esta información almacenada en servidores de empresas particulares. Por estas razones es de suma importancia que el usuario de internet aprenda que su teléfono inteligente es un dispositivo que constantemente está obteniendo información, y es debido que aprenda a proteger la privacidad de sus datos.

Los teléfonos inteligentes se han vuelto omnipresentes y los usuarios móviles confían cada vez más en ellos para almacenar y manejar información personal. Sin embargo, estudios recientes también revelan el hecho preocupante de que la información personal de los usuarios se pone en riesgo por las aplicaciones de teléfonos inteligentes. Las soluciones existentes presentan limitaciones en sus capacidades para domar estas aplicaciones de teléfonos inteligentes que violan la privacidad. El artículo titulado “Taming Information-Stealing Smartphone Applications (on Android)” (Zhou, Zhang, Jiang, & Freeh, 2011) defiende la necesidad de un nuevo modo de privacidad en los teléfonos inteligentes. El modo de privacidad puede habilitar a los usuarios para controlar de manera flexible y sencilla qué tipo de información personal será accesible a una aplicación. Además, el acceso concedido se puede ajustar dinámicamente en

tiempo de ejecución de una manera graneada para adaptarse mejor a las necesidades de un usuario en varios escenarios (por ejemplo, en un momento o lugar diferente). Ellos desarrollaron un sistema llamado TISSA (Zhou, Zhang, Jiang, & Freeh, 2011) que implementa este modo de privacidad en Android. La evaluación con más de una docena de aplicaciones de Android que se sabe filtra información demuestran su efectividad y practicidad.

Este sistema TISSA que implementa un modo de privacidad personalizable es un componente tecnológico que ayuda al usuario de Internet a controlar la información personal que comparte y suministra a las diferentes aplicaciones que instala en su teléfono inteligente, permitiéndole así poder ejercer un control sobre la privacidad de sus datos, porque es un sistema que le permite al usuario decidir sobre su privacidad, y que información hace pública o no, pero también difiere del mismo al no proponer medidas de asesoramiento en privacidad, suponiendo que el usuario tiene la autoeficacia para realizar las configuraciones pertinentes de forma autónoma sin partir de un diagnóstico inicial.

Medir el riesgo de privacidad en las redes sociales es una tarea difícil. Una de las dificultades fundamentales es la cuantificación de la cantidad de información revelada de forma no intencional. Por tal razón (Becker & Chen, 2009) presentan PrivAware, una herramienta para detectar y reportar pérdidas no deseadas de información en redes sociales en línea, cuyo objetivo es proporcionar un marco rudimentario para identificar el riesgo de privacidad y proporcionar soluciones para reducir la pérdida de información. La primera instancia del software se centra en la pérdida de información atribuida a los círculos sociales. En los próximos lanzamientos pretenden incorporar capacidades adicionales para capturar modelos de amenazas auxiliares. A partir de sus resultados iniciales, cuantificando el riesgo de privacidad atribuido a las relaciones de amigos en Facebook. Algunos de sus resultados han demostrado que para cada usuario la mayoría de sus atributos personales pueden derivarse de contactos sociales. Además, presentaron resultados que indican el número de amigos que contribuyen a un atributo correctamente inferido. También proporcionan resultados similares para los diferentes datos demográficos de los usuarios. La intención de PrivAware no es sólo informar la pérdida de información, sino recomendar las acciones del usuario para mitigar el riesgo de privacidad. Las acciones proporcionan a los usuarios los pasos necesarios para mejorar su medición general de la privacidad. Una solución obvia, pero no ideal, es eliminar amigos de alto riesgo, Otro enfoque es agrupar a los amigos de alto riesgo y aplicar controles de acceso al grupo para limitar la visibilidad.

En conclusión, el objetivo de PrivAware es proporcionar una herramienta única para cuantificar la pérdida de información y proporcionar características para reducir el riesgo de privacidad, porque pretende hacer un diagnóstico en cuanto a la privacidad del usuario en Facebook, y generar recomendaciones para que el usuario sea quien las aplique o no dado que solo se limita a las redes sociales, en específico Facebook, dejando por un lado demás aplicaciones y software que se instalan en los dispositivos que no tienen ningún tipo de control de privacidad por parte del usuario de internet.

Los desarrolladores e investigadores (Gilbert, Chun, Cox, & Jung, 2011) presentan AppInspector¹, un sistema de validación de seguridad automatizado que analiza aplicaciones y genera informes de posibles violaciones de seguridad y privacidad. Su visión es hacer aplicaciones de teléfonos inteligentes más seguras mediante la validación automatizada y describir los retos clave como la detección y análisis de violaciones de seguridad y privacidad, asegurando una cobertura de pruebas a fondo, y escalar a un gran número de aplicaciones.

AppInspector analiza las aplicaciones instaladas en los dispositivos móviles y genera informes de seguridad siguiendo 3 pasos: primero evalúa, segundo hace un diagnóstico y tercero genera informes que son presentados al usuario de internet. Sin embargo, no evalúa el comportamiento de los usuarios de internet frente a la privacidad o autoeficacia.

Un mayor uso de teléfonos inteligentes y de APPs está aumentando la preocupación de los usuarios sobre cómo aplicaciones de terceros pueden hacer mal uso o mal manejo de datos sensibles a la privacidad de sus usuarios. Para el caso del sistema operativo Android se encontraron en 2017 cerca de 700 mil aplicaciones maliciosas (Ahn, 2018). Afortunadamente, al contrario que en el mundo del PC, se tiene una oportunidad única para mejorar la seguridad de las aplicaciones móviles, gracias a la naturaleza centralizada de la distribución de aplicaciones, a través de mercados de aplicaciones populares. Google anuncio durante el primer semestre de 2018 realizar validación exhaustiva de aplicaciones como parte del proceso de admisión (ABC Aplicaciones, 2018). También presentó una nueva política de Distribución para Desarrolladores de Google Play (Google LLC , 2018). El mercado de las aplicaciones tiene el potencial de mejorar significativamente la seguridad del dispositivo móvil gracias a mejoras significativas en la capacidad para detectar abusos, suplantación de identidad, contenido inapropiado o programa maligno, a través de nuevos modelos y técnicas de aprendizaje automático. Google también ha desarrollado nuevos modelos y técnicas de detección que pueden identificar infractores reincidentes y redes de desarrolladores abusivas a escala. (Ahn, 2018).

A continuación, se presentan los estudios y artículos utilizados para la construcción de la encuesta o instrumento de medición utilizado el cual se conforma de tres partes.

La primera parte se basa en el estudio titulado “**un estudio multinacional sobre privacidad en línea: preocupaciones globales y respuestas locales**” (Cho, Rivera-Sánchez, & Lim, 2009). Este estudio examinó 1261 usuarios de Internet de cinco ciudades (Bangalore, Seúl, Singapur, Sydney y Nueva York) para examinar las percepciones de los usuarios de Internet de diferentes nacionalidades y las respuestas de comportamiento en relación con la privacidad en línea.

Este estudio uso 3 variables: La primera es: **preocupación por la privacidad en línea** la cual se midió mediante una escala Likert de cinco ítems. Los ítems dados permitieron medir las dimensiones clave de las preocupaciones de privacidad identificadas en estudios anteriores, tales como preocupaciones generales sobre privacidad en línea, recolección y control sobre privacidad en línea. La segunda variable es datos **demográficos y experiencias relacionadas**

¹ https://play.google.com/store/apps/details?id=bg.projectoria.appinspector&hl=es_CO

con Internet. La encuesta midió variables demográficas como género, edad, educación entre otras. La experiencia relacionada con Internet se midió por la duración y la frecuencia del uso de Internet y la experiencia con compras por Internet. Dado que la Internet se utiliza para fines tales como la comunicación, la recopilación de información y transacciones, la experiencia de compra en línea se distingue de la experiencia general de Internet. La tercera variable es **Autoeficacia de la privacidad.** La confianza en la autoeficacia de los usuarios de Internet se midió con respecto a la protección de la privacidad, y esta variable se usó para verificar la medición del comportamiento de protección de la privacidad.

La segunda parte del **instrumento** de medición se basa en el estudio “**hacia una tipología de usuarios de internet y preocupaciones de privacidad en línea 2002**” (Kim Bartel, 2002). En el que participaron 3724 personas, dentro de las cuales hubo 889 encuestas completadas que constituyen una tasa de respuesta del 24% y proporcionan una muestra nacionalmente representativa de usuarios en línea. Para realizar el muestreo se utilizó el buscador en línea Fourl 1 es un directorio de bases de datos de nombres, direcciones, números de teléfono y direcciones de correo electrónico de individuos de todo el mundo, y contiene más de 15 millones de direcciones de correo electrónico. Este estudio utilizó las siguientes medidas para realizar la encuesta: La **preocupación** por la privacidad se evaluó utilizando 15 declaraciones que reflejaban escenarios que representaban 5 influencias de privacidad diferentes que han sido identificadas por la literatura. La primera influencia es el conocimiento de la recopilación de datos. Esto sugiere que los usuarios en línea están menos preocupados por la privacidad cuando son conscientes de que los datos se recopilan que cuando los datos se recogen en secreto (Nowak & Phelps, 1995). La segunda influencia, el uso de la información, sugiere que los consumidores están menos preocupados por su privacidad cuando los datos se utilizan sólo con el propósito de una sola transacción y la preocupación aumenta a medida que los datos se utilizan más allá de esa transacción. Lo que sugiere que los usuarios en línea están menos preocupados por su privacidad en línea cuando están familiarizados con la entidad que recolecta información, y la preocupación por la privacidad aumenta cuando las entidades desconocidas recopilan información (Rogers J. L., 1996). En este estudio se presentaron tres situaciones diferentes, una reflejando una situación que en promedio provocaría un bajo grado de preocupación por la privacidad, una segunda que en promedio causaría un grado moderado de preocupación por la privacidad y una tercera que en promedio causaría un grado alto de preocupación por la privacidad.

La tercera parte del instrumento de medición se basa en el estudio llamado “**desarrollo de medidas de preocupación de privacidad en línea y protección para uso en internet**” (Buchanan, Paine, Joinson, & Reips, 2007). Este estudio se compone **de 3 componentes**, las cuales se mencionan a continuación:

- En el **primer componente** hubo un total de 685 miembros del panel de investigación que fueron invitados por correo electrónico para completar el cuestionario basado en Internet de los cuales 515 lo hicieron (75%). De los 515 encuestados, 220 (43%) eran hombres y 286 (57%) eran mujeres (los datos demográficos no estaban disponibles para nueve participantes). La edad de la muestra fue de 43,9 años. Todos los miembros del panel de investigación recibieron una invitación por correo electrónico para completar

un cuestionario basado en la Web. Se informó a los miembros de que el cuestionario consistía en una serie de preguntas sobre su uso de Internet y, en particular, sobre cualquier preocupación de privacidad que pudieran tener y sobre las medidas que adoptarían para abordar estas preocupaciones. Sobre la base de este estudio, se ha desarrollado un conjunto de tres escalas cortas, internamente consistentes e interpretables. Dos abordan diferentes aspectos de las cosas que las personas hacen para proteger su privacidad (**comportamientos**): el ejercicio de la **precaución general** y la **protección técnica**. La tercera escala, **preocupación por la privacidad**, es actitudinal en lugar de comportamiento, y refleja las preocupaciones generales sobre la privacidad en Internet.

- En el **segundo componente**. Los participantes fueron reclutados a través de dos conjuntos de tableros de anuncios en línea. Los boletines para estudiantes orientados a la tecnología se asociaron con un tablero de anuncios más general para estudiantes de tecnología. Para este estudio se realizó el siguiente procedimiento: Se publicó un mensaje en cada tablero de anuncios en línea pidiendo a los participantes un cuestionario de privacidad de Internet. El mensaje incluyó detalles sobre la importancia de desarrollar nuevas escalas de **preocupación** y **comportamiento** de privacidad. Al acceder a la encuesta, se informó a los participantes que toda la información proporcionada seguiría siendo confidencial. El sitio de la encuesta se mantuvo abierto durante 3 semanas. Los participantes tomaron, en promedio, 5 minutos para completar el cuestionario.
- En el **tercer componente** la medida requirió que los participantes respondan a tres declaraciones en una escala de 4 puntos. Los fundamentalistas de la privacidad, los pragmáticos de la privacidad o los despreocupados por la privacidad. En su lugar, se obtuvo una puntuación total de preocupación por la privacidad sumando las puntuaciones a través de los tres ítems. Las participantes en este estudio son los miembros del panel estudian una variedad de temas en el ambiente universitario. De los 1.122 encuestados (58%), 449 (40%) eran hombres y 672 (60%) eran mujeres. La edad media de la muestra fue de 42,3 años.

Los estudios e investigaciones que se mencionaran a continuación utilizan diferentes metodologías para la clasificación de los usuarios en internet. Estas metodologías de clasificación de usuario se han ido adaptando conforme surgen nuevas tecnologías como dispositivos móviles e internet móvil.

Uno de los primeros estudios que comenzó a considerar y mapear a los usuarios de Internet por patrones de uso es (Howard, Rainie, & Jones, 2001). El estudio se basa en la teoría de la difusión de Roger. Agrupó a los usuarios en cuatro tipos: los internautas que son usuarios experimentados y usan Internet todos los días; los utilitaristas que también son usuarios experimentados, pero tienen un uso menos intensivo; los experimentadores que tienen entre 1 y 3 años de experiencia en Internet, y los recién llegados que tienen menos de un año de experiencia. El estudio utilizó una encuesta por cuestionario y un análisis de frecuencia simple para agrupar a los usuarios.

El siguiente estudio, es de (Shah, Kwak, & Holbert, 2001). El estudio se basa en la teoría de los usos y gratificaciones y la teoría sobre el uso de los medios. Se utilizó una encuesta por cuestionario y fue uno de los primeros estudios en utilizar el análisis factorial para agrupar a los usuarios. Sobre la base de las dos teorías utilizadas, los autores pudieron agrupar a los usuarios en cuatro grupos denominados: **recreativos** (social recreation), **consumidores** (product consumption), **financieros** (financial management) y **negociadores de información** (information Exchange).

Otro estudio fue realizado por (Sheehan, 2010), quien utilizó la teoría de las tipologías de privacidad y las tipologías de consumidores. El estudio fue cuantitativo y utilizó análisis de conglomerados para agrupar usuarios. El autor encontró cuatro tipos de usuarios, a saber, usuarios de Internet **despreocupados**, usuarios **prudentes**, usuarios de Internet **cautelosos** y usuarios de Internet **alarmados**.

Un estudio realizado por (DeYoung & Spence, 2004) se basó en la teoría de la personalidad y la actitud ante el computador. Se utilizó encuesta de cuestionario y análisis factorial para categorizar a los usuarios. El estudio encontró siete tipos de usuarios: El estudio encontró siete tipos de usuarios: **curioso** (interest), **ansioso** (anxiety), **creyente** (approval), **confiado** (confidence), **comprador en internet** (Internet transactions), **recreativo** (entertainment) y **el que prefiere un diseño complejo** (complex design preference).

Otro estudio realizado por (Shih & Venkatesh, 2004), también siguió la teoría de la difusión de Roger (Shih & Venkatesh, 2004) y utilizó la encuesta por cuestionario y el análisis de regresión para agrupar a los usuarios. Encontraron cuatro grupos de usuarios, que son **usuarios de Internet**, usuarios **especializados**, usuarios **no especializados** y usuarios **limitados**.

El framework de Kozinets para segmentar la participación en una comunidad virtual fue utilizado por (Jepsen, 2006) para identificar grupos de usuarios. El estudio utilizó cuestionarios y usuarios segmentados según las puntuaciones de medianas y medias. Jepsen encontró cuatro grupos de usuarios. Son **personas con información privilegiada**, que tienen fuertes lazos con otros miembros de la comunidad; **devotos**, que mantienen un gran interés en el consumo, pero tienen pocos vínculos sociales; **los mezquinos**, que mantienen fuertes lazos sociales y poco interesados en la actividad de consumo; y **turistas**, que no tienen lazos y solo pasan por la comunidad de vez en cuando.

Otro estudio basado en una teoría diferente es la investigación de (Johnson & Kulpa, 2007). Basaron su estudio en la teoría de la personalidad (tipología del comportamiento) y la sociabilidad. El estudio utilizó análisis cuantitativo mediante análisis factorial. Las muestras se limitan a estudiantes universitarios. Basados en esta teoría, los autores clasificaron a los usuarios en tres grupos, denominados, **sociables**, los cuales son los usuarios de Internet cuyos comportamientos en línea se caracterizan por la orientación social; **útiles**, caracterizados por la orientación a la eficiencia; y **recíprocos**. Se caracteriza por la estimulación cognitiva y la participación. Los hallazgos de este estudio se limitan a las teorías en las que se basan el estudio de (Ortega Egea, Menéndez, & González, 2007).

Otro estudio realizado por (Barnes, Bauer, Neumann, & Huber, 2007) se basó en la teoría de tipologías de consumo y construcciones de personalidad en psicología, extraversión y neocriticismo. El estudio encuestó a 1,011 compradores en línea y utilizó el análisis de conglomerados para agruparlos. Los resultados del estudio están, nuevamente. Los autores encontraron personas que **dudan de los riesgos, compradores abiertos y buscadores de información reservados**, que suelen ser cuidadosos y reservados y tienen un alto riesgo percibido cuando compran.

Las investigaciones posteriores en este campo son en su mayoría exploratorias. Uno de los primeros en este grupo es un informe de Forrester (Li, Bernoff, Fiorentino, & Glass, 2007). El estudio realizó un mapeo de tecnología social con participación en diferentes actividades. El estudio no analizó los tipos de usuarios de Internet en particular, pero fue un punto de partida para agrupar usuarios según sus actividades. Agrupó a los usuarios en seis tipos, a saber, **creadores, críticos, coleccionistas, carpinteros, espectadores e inactivos**. El estudio no se basó en ninguna teoría específica y utilizó el análisis de conglomerados para agrupar usuarios.

Otro estudio fue realizado por (Horrigan, 2007). Utilizó técnicas de análisis de conglomerados sin base teórica. Encontró seis grupos de usuarios. Son los **omnívoros**, quienes son los participantes más activos en la sociedad de la información; los **conectores**, aquellos que participan activamente y usan Internet para conectarse con personas; los **mediocres veteranos**, quienes no sienten pasión por las tecnologías de la información y la comunicación (TIC); los **potenciadores** de la productividad, aquellos que hacen muchas cosas mediante el uso de las TIC; **call center**, aquellos que están conectados a sus teléfonos móviles y aplicaciones; y los **conectados pero molestos**, aquellos que invierten en mucha tecnología pero encuentran la conexión como una molestia.

Un estudio realizado por la Oficina de Comunicación de Gran Bretaña (OFCOM, V., 2008) examinó a 39 usuarios de redes sociales y 13 no usuarios. Utilizó entrevistas y un análisis cualitativo en profundidad para agrupar a los usuarios de Internet y encontró que los usuarios se pueden separar en cinco tipos, a saber, los **socializadores alfa**, que son usuarios regulares pero con ráfagas cortas; los **buscadores de atención**, que buscan atención y comentarios de los demás; los **seguidores**, que están en Internet para mantenerse al día con los demás; Los **fieles**, que buscan viejos amigos en internet; y los **funcionarios**, que usan Internet para un propósito particular. Este estudio es un estudio exploratorio y agrupa a los usuarios según sus comportamientos.

Otro estudio realizado por (Brandtzæg & Heim, Social network sites - A typology of users, 2010) agruparon a los usuarios según sus patrones de uso. Las muestras son adolescentes en Noruega. Los autores encontraron que, en función de sus patrones de uso, los usuarios de Internet pueden agruparse de forma diferente a (Brandtzæg P. B., y otros, 2005). Clasificaron a los usuarios en **esporádicos**, que no se involucran demasiado con Internet; Los **acechadores**, que están en Internet para matar el tiempo; **socializadores**, que son activos en comunidades en línea; **polemistas**, que son activos en entrar en las discusiones; y **usuarios activos**, que realizan todo tipo de actividades. Su estudio es cuantitativo y utiliza análisis de conglomerados para agrupar usuarios.

De un gran cuerpo de investigación, uno de los trabajos más completos y más citados es un estudio realizado por (Brandtzæg & Heim, Social network sites - A typology of users, 2010), que realizó una revisión exhaustiva de todos los estudios relevantes durante el período 2001-2010. En total, 22 estudios y 5 teorías relevantes fueron revisados en detalle. Después de esta revisión exhaustiva, Brandtzæg organizó todos los grupos de usuarios de la investigación anterior, independientemente de cómo se llamaron en cada estudio, en varios grupos de las mismas características y los cambió de nombre según sus propios términos (Krairit, 2018). Por ejemplo, agrupó los tipos de usuarios polémicos, contribuyentes y creadores etiquetados en estudios anteriores bajo su término, polémicos.

En la reagrupación de tipos de usuarios encontrados en estudios anteriores, Brandtzæg definió ocho grupos de usuarios. Los ocho grupos se describen en la **Tabla 1** a continuación.

Tipos de usuarios definidos	Justificación
No usuarios	No usuarios de los medios investigados y el más común de todos los tipos de usuarios en estudios representativos.
Esporádicos	Identificado en 20 estudios. Uno de los tipos de usuario más evidentes. Los usuarios que son nuevos y que son usuarios de bajo nivel o esporádicos de los medios particulares estudiados.
Polémicos	Bloggers y debatientes en redes sociales. Este tipo de usuario es un tipo de usuario nuevo y venidero debido a las nuevas redes sociales y las herramientas más sencillas para bloguear, debatir y debatir.
Usuarios recreativos	Este tipo de usuario se identifica en diez estudios. Probablemente sea un tipo de usuario prometedor debido al alto aumento en los juegos.
Socializadores/Sociables	Identificado en nueve estudios. Un tipo de usuario cada vez mayor debido a la llegada de las aplicaciones de medios sociales.
Acechadores	Solo se identifica en cinco estudios, pero representa el tipo de usuario más grande en las redes sociales. Utilizan los medios principalmente para burlarse, acechar, matar el tiempo o comprar escaparates.

Usuarios instrumentales	Identificado en 16 estudios. Este es un tipo de usuario común relacionado con los medios en general y con Internet en particular. Los usuarios que utilizan los medios de comunicación como utilidad y como herramienta de información, tanto en el trabajo como en privado. No es tan obvio en las redes sociales.
Usuarios avanzados	Identificado en 20 estudios. Junto con los esporádicos, este es el tipo de usuario más común. Este tipo representa usuarios que utilizan una amplia gama de medios con frecuencia, utilizando las instalaciones más avanzadas en comparación con el resto de la población de usuarios.

Tabla 1 Tipos de usuarios según el estudio de Brandtzæg. (Brandtzæg & Heim, Social network sites - A typology of users, 2010)

Un estudio más reciente estudio realizado en Tailandia por (Krairit, 2018) se centra en la tipología del usuario de Internet, que es un área que no se ha examinado recientemente. La investigación explora si la tipología de usuario de Internet especificada en la literatura anterior todavía es aplicable en el presente y, si no, qué ha cambiado. Los resultados revelan que la forma anterior de categorizar a los usuarios en varios tipos basándose solo en sus actividades ya no es aplicable. En consecuencia, el investigador propuso una nueva metodología para agrupar usuarios en función de las aplicaciones y la frecuencia de acceso a ellas, junto con el uso de datos demográficos. El análisis de clústeres basado en encuestas muestra cuatro tipos de usuarios de Internet en Tailandia. El hallazgo más interesante e inesperado es el nuevo tipo de usuario que el investigador llama el grupo auto satisfactorio.

Este estudio utiliza una de las técnicas más robustas disponibles, conocida como el enfoque de tres frentes que consiste en una revisión extensa de la literatura para determinar un tema de investigación y el problema de la investigación, posterior se propone el marco conceptual de la investigación y se realiza una revisión detallada de la literatura relacionada. El segundo frente son las entrevistas a expertos para obtener conocimientos e ideas adicionales. Estos dos frentes se combinan para confirmar el marco propuesto, y se pueda redactar el cuestionario de la encuesta. El tercer frente es la encuesta. Contar con datos cuantitativos que pueden fundamentar o contrastar con la literatura previa y las entrevistas con expertos. En consecuencia, la encuesta del cuestionario es una parte importante de la investigación. (Krairit, 2018)

Los usuarios tailandeses actuales utilizan varias aplicaciones y realizan una variedad de actividades en diferentes niveles de frecuencia. Los usuarios tailandeses son una mezcla de lo que la literatura anterior llamó socializadores, acechadores, artistas y usuarios instrumentales.

(Krairit, 2018). Por lo tanto, el uso de los tipos para agrupar los tipos de usuarios de Internet como en el pasado ya no es aplicable en la situación actual.

El primer grupo es el grupo más pequeño. Los rezagados o los no usuarios. Las personas en este grupo no tienen acceso a Internet, o si tienen acceso, no están interesadas en usar dicha conectividad. En este estudio, representaron el 10% de la muestra (Krairit, 2018).

El segundo grupo, tercero y cuarto se toman en conjunto y se denominan grupo auto satisfactorio en el que hay tres subgrupos. Los usuarios Tailandeses que muestran una mezcla de diferentes tipos de usuarios, los tres subgrupos de usuarios representan un grupo auto satisfactorio. (Krairit, 2018).

- El primer clúster llamado el grupo siempre en línea y enfocado es el grupo más grande, que representa el 43.89% de la muestra de usuarios. Este grupo usa 2-5 aplicaciones muy a menudo, más de una vez por día. Las edades de los usuarios oscilan entre los 31 y los 50 años.
- El segundo clúster llamado el grupo a menudo en línea y extenso es el segundo grupo más grande, que representa el 30.56% de la muestra de usuarios. Este grupo usa 6-8 aplicaciones al menos 4-6 veces a la semana (casi todos los días) hasta todos los días. Tienen entre 21 y 35 años
- El último clúster llamado el grupo que rara vez está en representa el 25.55% de la muestra de usuarios. Este grupo utiliza las nueve aplicaciones, pero con la frecuencia más baja de todos los grupos, de 1 a 3 veces por semana. No hay un patrón en sus edades. (Krairit, 2018).

En esta sección se presentan artículos, estudios, que referencian las nuevas tecnologías de construcción de aplicaciones móviles a través de plataformas CMS, estas plataformas le permiten al usuario construir aplicaciones móviles profesionales, y ofrecen diferentes servicios y características que hacen que construir aplicaciones móviles esté al alcance de cualquier persona.

El avance de las tecnologías móviles está superando a la conectividad tradicional desde ordenadores y portátiles. Esto requiere adaptar canales y contenidos a este entorno. Una solución son las apps para móviles. Básicamente nos encontramos dos plataformas en el mercado, iOS y Android. Entre las dos acaparan más del 99% de la cuota del mercado mundial (Stat Counter Global Stats, 2017). No es tarea fácil hacer una aplicación para iOS o para Android. La compatibilidad entre las dos plataformas es nula. Esto obliga a que, si quieres programar una app para los dos sistemas, tengas que hacer dos apps. Sin embargo, existe una posibilidad para no repetir el trabajo, crear una aplicación híbrida. Esta tecnología se basa en los estándares web HTML5, CSS3 y JavaScript para crear aplicaciones multiplataforma (Del Valle, 2016).

Las tecnologías web se están convirtiendo en un estándar para muchas áreas. Ya no solo el desarrollo de apps, tecnologías como el IoT (Internet of Things o Internet de las Cosas) también se nutren de ellas. Es muy sencillo, se instala un pequeño servidor web en el dispositivo que

permite ejecutar la app híbrida. Se llama así porque no son apps nativas, ni web. Es un híbrido entre las dos. El gran inconveniente son las limitaciones con respecto al acceso a los recursos del sistema. Por lo tanto, hacer una app para móviles dependerá de a qué plataforma vaya dirigida, las funcionalidades y el presupuesto. Una plataforma App es un framework web cuya finalidad es la creación y desarrollo de la estructura de aplicaciones de forma completa a través de sus múltiples opciones de diseño y desarrollo que permiten centrarse también en aspectos concretos de la misma, dependiendo de cada servicio. También se conocen como generadores de aplicaciones, creador de aplicaciones, publicadores de aplicaciones o portales web de desarrollo App. (Del Valle, 2016)

Las aplicaciones nativas tienen la capacidad de usar hardware y software específicos del dispositivo y pueden proporcionar calidad con tasas de rendimiento enormes. Las ventajas de las aplicaciones móviles nativas incluyen: alto rendimiento, experiencia de usuario superior y mayor visibilidad de la tienda de aplicaciones (Jagtap & Hanchate, 2017)

Una aplicación multiplataforma es una aplicación móvil que es compatible con múltiples sistemas operativos y, por lo tanto, puede ejecutarse en cualquier teléfono inteligente o tableta. Las ventajas de la aplicación móvil multiplataforma incluyen (Verma, Kansal, & Malvi, 2018):

- Soporte para múltiples sistemas operativos
- Interfaz de usuario de media a alta calidad
- El coste de la aplicación es Medio
- mantenimiento de la aplicación Medio
- Lenguaje de desarrollo Java, HTML, CSS, JavaScript

La propuesta desarrollada por (Ferreira, y otros, 2018) presentan herramientas de desarrollo móvil multiplataforma que permiten a los desarrolladores escribir un código base único y crear la misma aplicación para varias plataformas móviles (por ejemplo, Android y iOS). Se ha propuesto una variedad de marcos para apoyar el desarrollo de aplicaciones móviles multiplataforma. PhoneGap, Sencha Touch y Titanium son marcos bien conocidos diseñados para este propósito. El objetivo principal de esta investigación es analizar su estado actual de madurez. En esa dirección, se desarrolló una aplicación en PhoneGap, Titanium y Sencha, y se implementaron versiones nativas para Android y iOS. Dicha aplicación móvil obtiene información de los sensores, usa la cámara para tomar fotos, aplica filtros de imagen y establece la conexión a un servicio web remoto. Analizamos la viabilidad de construir este tipo de aplicación móvil, el rendimiento de cada versión y el esfuerzo de desarrollo. Con nuestros resultados, tenemos la intención de proporcionar una visión general de las cualidades y limitaciones de estos marcos

La patente de invención (US Patente nº US20180181378A1, 2014) presentada por Eshagh y otros, proporciona un ecosistema de aplicaciones móviles que comprende un kit de desarrollo de aplicaciones móviles y una tienda, los cuales se implementan como servicios basados en la web, de modo que la creación, prueba y distribución de aplicaciones móviles, así como el descubrimiento, investigación y entrega de las mismas aplicaciones. , todo se puede realizar utilizando un navegador web estándar. El kit de desarrollo de aplicaciones móviles ofrece

capacidades comunes en todas las marcas de dispositivos móviles y grupos de marcas, lo que permite que la misma construcción de la aplicación funcione sin modificaciones en todos, al tiempo que crea la aplicación de forma nativa para cada uno, evitando así cualquier requisito de incrustar un dispositivo separado. Tiempo de ejecución común o máquina virtual en cada dispositivo móvil.

5 METODOLOGÍA

En esta sección se define el procedimiento seguido para desarrollar el prototipo de la aplicación móvil que asesora y enseña al usuario de Internet sobre medidas de autoprotección de sus datos privados.

La actual investigación se clasifica como descriptiva, el objetivo de la investigación descriptiva consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos sino a la predicción e identificación de las relaciones que existen entre dos o más variables (Meyer., 2006).

El proyecto de investigación es de tipo descriptivo dado que su fin es desarrollar una aplicación que asesore y enseñe al usuario de Internet a partir de la identificación de relaciones entre variables de estos usuarios. La aplicación desarrollada no se limita únicamente a la recolección y análisis de datos, si no a la identificación de la relación de las variables para posteriormente realizar un diagnóstico del nivel de privacidad, emitir resultados y sugerencias.

La metodología presentada para esta investigación es de tipo mixta porque combina elementos de análisis cuantitativo y cualitativo para la recolección de datos previa a la construcción de la aplicación

El desarrollo de la aplicación que se realizó por fases. En primera fase se crea un **modelo de medición**, para lo cual se genera una encuesta con el fin de definir el perfil del usuario en cuanto al nivel de exposición de sus datos privados en Internet. Dicha encuesta es desarrollada mediante una revisión documental de los estudios definidos en el estado del arte, los cuales han realizado encuestas a nivel internacional a usuarios de internet aplicando técnicas de análisis estadístico. El desarrollo de esta encuesta hace parte del proyecto de investigación “Privacidad siglo XXI”, ¿reliquia o necesidad? (Aguirre Jaramillo & Amaya Fernández, 2016).

Para el desarrollo de la encuesta se usa el paradigma cuantitativo puesto que se hace necesaria la recolección y análisis de datos con el fin de definir un perfil de nivel de exposición de datos del usuario, confiando en las mediciones numéricas y estadísticas para establecer los comportamientos que permitan definir un modelo de medición.

A partir de los resultados obtenidos del modelo de medición, se procede a realizar la construcción de la aplicación la cual se compone de **3 fases**.

La primera fase es el diseño de la aplicación móvil la cual tiene **tres actividades** que se componen de análisis de requerimientos, especificación y arquitectura. En el **análisis** de requerimientos se definen las funcionalidades que tendrá la aplicación móvil a través de la revisión documental de aplicaciones similares, de informes en asesorar al usuario de internet en crear medidas de protección de la privacidad de sus datos personales. La **especificación** se realiza después de definir los requerimientos funcionales de la aplicación móvil y definir las especificaciones, los requerimientos, los alcances y las funcionalidades esperadas del prototipo de aplicación móvil. La **arquitectura** define el proceso de diseño que determina cómo funcionará la aplicación móvil. Se propone la estructura de la aplicación móvil en cuanto a la interfaz gráfica e interfaz de usuario. Se pretende que sea una interfaz amigable y fácil de usar para el usuario final.

La segunda fase es la construcción del prototipo de la aplicación móvil que asesora al usuario de internet en crear medidas de protección de la privacidad de sus datos personales. Esta fase se compone de **dos actividades**: implementación y pruebas. La **implementación** es el proceso en donde el diseño construido anteriormente se traduce a código y se convierte en el prototipo de la aplicación móvil propuesto. Para la implementación se utilizará una plataforma de construcción de aplicaciones móviles, la cual facilita que la aplicación final construida pueda ser utilizada en distintos tipos de dispositivos y sistemas operativos móviles. Las **pruebas** de la aplicación se realizan para comprobar que el software realice correctamente las funciones planeadas desde la etapa de diseño y de ser necesario realizar correcciones, con el propósito de que la aplicación quede totalmente funcional, según lo planeado en la especificación.

La tercera fase es el despliegue del prototipo de aplicación móvil que ha sido desarrollado a través de una plataforma de construcción de aplicaciones móviles. Después de haber terminado las pruebas de aplicación y comprobar que las funcionalidades sean las propuestas, se libera la aplicación para ser descargada y utilizada por los usuarios finales. Esta fase se compone de **tres actividades**: liberación, documentación, y mantenimiento. La **liberación** de la aplicación móvil se realiza cuando se sube a la red la aplicación para poder ser accedida y descargada por los usuarios de internet, podrá ser accedida desde un portal web o descargada desde la tienda de apps como Play Store de Google, para ser utilizada directamente en dispositivos móviles Android. La **documentación** es la realización de un manual de mantenimiento que explica las funcionalidades de la aplicación y su estructura para poder realizar mantenimiento de manera correcta. El **mantenimiento** de la aplicación se realiza para garantizar la correcta funcionalidad de la aplicación y su permanencia en línea para que esté disponible para ser accedida y descargada por los usuarios durante el tiempo que dure la investigación o de ser posible un tiempo mayor a esta investigación si se requiere.

6 PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

En este capítulo se presenta la implementación del prototipo de aplicación móvil que determina el nivel de exposición de los datos privados del usuario de Internet y lo asesora en forma personalizada cómo proteger sus datos privados. En la primera sección se presenta el diseño de la aplicación, luego se presenta la forma como se construyó el prototipo y finalmente se presenta un análisis de la etapa de despliegue del prototipo. Estas secciones corresponden con los tres objetivos específicos planteados durante la formulación de la propuesta del trabajo de grado: 1) diseñar un modelo de aplicación móvil, 2) construir el prototipo de aplicación móvil y 3) desplegar el prototipo.

6.1 Diseño del modelo de aplicación móvil

Para el diseño del modelo de la aplicación móvil se realizaron 3 actividades que se describen en cada una de las siguientes subsecciones:

- Generación del instrumento de medición del nivel de exposición de los datos privados en Internet.
- Análisis de requerimientos para definir la funcionalidad de la aplicación.
- Definición de la arquitectura de la aplicación.

6.1.1 Instrumento de medición

El instrumento de medición desarrollado responde al problema planteado en esta investigación el cual propone medir el nivel de preocupación del usuario por la exposición de los datos privados en Internet. Esta investigación se abordó en un contexto específico donde se tomó como población la comunidad UPB Medellín.

Como se indicó en la Metodología, dentro del proyecto “Privacidad siglo XXI”, ¿reliquia o necesidad? (Aguirre Jaramillo & Amaya Fernández, 2016), se generó una encuesta para medir la privacidad en línea, encuesta que fue adaptada para el desarrollo de la aplicación que es objeto de estudio de este trabajo de grado.

El instrumento de medición desarrollado en este trabajo de grado obtiene tres indicadores para cada usuario que responde la encuesta:

- nivel de preocupación,
- comportamiento frente a la privacidad en línea y
- nivel de exposición total.

El instrumento de medición utilizado se compone de 3 segmentos o partes. La primera parte indaga por datos demográficos y personales, la segunda permite calcular el nivel de preocupación y la tercera parte permite determinar el comportamiento frente a la privacidad en línea. A continuación, se explica detalladamente cada parte de la encuesta. La encuesta diseñada se presenta en el *Anexo 1*.

Es importante aclarar que antes de responder la encuesta los usuarios aceptaron los términos y condiciones así como las políticas de seguridad de la aplicación, en donde se aclara que la encuesta y la aplicación son parte de un proyecto de investigación y de un trabajo de grado, que los datos recolectados únicamente se utilizaran con fines académicos, a los cuales solo tendrán acceso las personas relacionadas con el proyecto, las políticas de seguridad y privacidad, así como los términos y condiciones se presentan en el **Anexo 6**.

En la primera parte del instrumento se preguntan aspectos demográficos, como: edad, sexo, estrato, estado civil, nivel educativo. En cuanto a uso de Internet se pregunta sobre el uso de aplicaciones como redes sociales y compras en línea. Esta primera parte del instrumento se basó en el estudio de Cho y otros. (Cho, Rivera-Sánchez, & Lim, 2009)

En la segunda y tercera parte se analiza la respuesta del usuario frente a situaciones cotidianas en Internet. Para la segunda parte se analizan 17 situaciones y para la tercera parte se analizan 23 situaciones para un total de 40 situaciones. Para la medición de los resultados se utiliza la escala de Likert. (Bedoya Laguna & Reyes Roncancio, 2017)

En la segunda parte se utilizan 17 situaciones diseñadas para medir el nivel de preocupación del usuario por el riesgo de exposición de sus datos en Internet. Esta parte del instrumento (preguntas) se basó en el estudio de Kim (Kim Bartel, 2002); la variable **nivel de preocupación** se mide a través de la escala de Likert (Bedoya Laguna & Reyes Roncancio, 2017). Cada situación se mide en una escala de 1 a 5 de la siguiente forma:

- 1: no me preocupa para nada y es el valor más bajo,
- 2, 3 y 4, son escalas intermedias
- 5: me preocupa mucho y es el valor de preocupación más alto.

La tercera parte de la encuesta analiza el comportamiento de los usuarios ante 23 situaciones cotidianas en internet. Esta parte del instrumento (preguntas) se basó en el estudio de Buchanan y otros (Buchanan, Paine, Joinson, & Reips, 2007); la variable **comportamiento** se mide utilizando la escala de Likert al igual que en la parte dos. Cada situación se mide de la siguiente forma:

- 1: nunca lo he hecho, entendiendo que el usuario nunca ha realizado la acción mencionada,
- 2, 3 y 4, son escalas intermedias
- 5: siempre lo hago, entendiendo que el usuario siempre realiza la acción.

En total se presentaron 40 situaciones medibles (ver Anexo 1). Utilizando la escala Likert se obtiene un puntaje mínimo de 40 y un puntaje máximo de 200. Este resultado se emplea para medir la exposición total del usuario de acuerdo con la tipología definida por Alan Westin (Kim Bartel, 2002). Para realizar la clasificación de los usuarios de Internet que propone Westin se realiza una asignación de puntuaciones donde la puntuación total de un individuo (nivel de exposición total) en la escala es la suma de sus puntuaciones de cada ítem. La intensidad de actitud y su valoración depende del número de ítems y de los puntajes asignados (Alaminos Chica & Castejón Costa, 2006).

El puntaje total en el rango de 40 a 200 puntos se emplea para medir **el nivel de exposición total** del usuario de acuerdo con la tipología definida por Alan Westin (Kim Bartel, 2002). Westin desarrolló una tipología para clasificar a los consumidores a partir de sus preocupaciones con la privacidad en el mercado "tradicional" (es decir, no en línea). Westin sugiere que los consumidores pueden clasificarse en tres grupos en función de su preocupación por la privacidad: aquellos que están interesados en todo tipo de prácticas que afectan su privacidad, aquellos que no se preocupan por su privacidad, y aquellos que son pragmáticos en su preocupación.

Smith utilizó una versión anterior de la tipología de Westin (Equifax & Harris Louis, 1991) para clasificar un grupo de individuos que participaban en un grupo focal sobre privacidad. Esta escala de clasificación es la que se empleó en este trabajo. En el estudio de Smith encontró que el 15% de los usuarios eran fundamentalistas y que el 85% restante lo componían usuarios despreocupados y pragmáticos. Partiendo de estos resultados se construye la **Tabla 2** que presenta los rangos para la clasificación de los usuarios. Se conoce que la amplitud total de la variable **nivel de exposición total** es 160 (máximo 200 y mínimo 40). Se calcula el 15% de esta variable correspondiente a los usuarios alarmados o fundamentalistas obteniendo una amplitud de 24 puntos. El 85% restante se divide en partes iguales para clasificar a los usuarios despreocupados y pragmáticos, obteniendo una amplitud de la variable de **exposición total** de 67 correspondiente al 42% para cada grupo como se presenta en la **Tabla 2**.

	Amplitud total	Amplitud para Despreocupados	Amplitud Indiferentes (Pragmáticos)	Amplitud Alarmados (Fundamentalistas)
Puntaje	160	67	67	24
Porcentaje	100%	42%	42%	15%
Rangos	40-200	40-107	108-175	176-200

Tabla 2. Tabla con los rangos de clasificación de los usuarios.

Un puntaje de 40 representaría a un individuo para el cual ninguna de las 40 situaciones causó preocupación a la privacidad y un puntaje de 200 representaría a un individuo para el cual cada situación causó extrema preocupación por la privacidad. De acuerdo con el resultado, aplicando la tipología de Westin, cada usuario se clasificaría en uno de los siguientes grupos:

- **Despreocupados:** grupo de encuestados cuyo nivel de exposición total está en el rango entre 40 y 107. Esta calificación se da a los encuestados en el presente estudio a los que las 40 situaciones parecieron causar un nivel mínimo de preocupación.
- **Pragmáticos:** grupo de encuestados cuyo nivel de exposición total está en el rango entre 108 y 175. Para efectos de una mejor comprensión del lenguaje para el usuario final en la aplicación y del presente estudio se denominó al grupo como **Indiferentes**. Este grupo se dividió en dos grupos:
 - ❖ Los que comprendían un puntaje entre 108 y 142 llamados usuarios **prudentes**. Las personas de este grupo sentían un nivel bajo o moderado de preocupación en la mayoría de las situaciones.

- ❖ Los que tenían una preocupación total de 143 a 175 llamados usuarios **cautelosos**. Este grupo sentía un nivel moderado de preocupación en la mayoría de las situaciones.
 - **Fundamentalistas**: grupo de encuestados cuyo nivel de exposición total está en el rango de 176 o más. Este grupo está muy preocupado por la privacidad en todas las situaciones. Para efectos de una mejor comprensión del lenguaje para el usuario final en la aplicación y del presente estudio se denominó al grupo como Alarmados.
- En el **Anexo 1** se presenta la encuesta diseñada.

6.1.2 Análisis de requerimientos de la aplicación

Después de definir el instrumento de medición de la privacidad en línea, como se presentó en la sección anterior, se realizó el análisis de requerimientos para definir la funcionalidad de la aplicación.

El análisis de requerimientos hace parte de la **estructura** aplicada al desarrollo de un producto de software denominada **ciclo de vida del desarrollo de software**, el cual define las funcionalidades que tendrá la aplicación móvil y describe la interacción entre el sistema y su ambiente. El ambiente incluye al usuario y cualquier otro sistema externo que interactúa con el sistema desarrollado. El análisis de requerimientos se realizó a partir de una revisión documental de aplicaciones similares, de informes y documentos referentes a asesorar al usuario de internet en crear medidas de protección de la privacidad de sus datos personales.

En **análisis de requerimientos** se compone de dos principales tipos de requerimientos, los requerimientos funcionales y los no funcionales. Los requerimientos funcionales son declaraciones de los servicios que prestará el sistema y define la forma en que reaccionará a determinadas acciones. Pueden ser interacciones con otros sistemas, respuestas automáticas o procesos predefinidos. Los requerimientos no funcionales son aquellos requerimientos que no se refieren directamente a las funciones específicas que entrega el sistema, sino a las propiedades emergentes de éste como la fiabilidad, la respuesta en el tiempo y la capacidad de almacenamiento. (Sommerville, 2005)

6.1.2.1 Requerimientos funcionales

Requerimientos funcionales de proceso

- El sistema deberá contar con una base de datos que sea actualizada la cual almacene y procese los datos para su posterior uso.
- El usuario deberá registrarse en el sistema para poder acceder a sus funcionalidades.
- El sistema enviará un correo electrónico cuando se registre alguna de las siguientes acciones: creación de cuenta, terminación de la encuesta de privacidad.
- Se permitirá el registro de personas que accedan con su cuenta de Google para poder guardar los datos en la base de datos general.
- Al completar la encuesta, la aplicación presentará los resultados de la evaluación además de recomendaciones para mejorar la privacidad en línea.

- El sistema permitirá a los usuarios registrados ingresar a sus resultados personales y poder observar los resultados generales para hacerse una idea de su estado de exposición de privacidad en línea en comparación con el promedio de las demás personas que han utilizado la aplicación.
- El sistema permitirá cambiar o actualizar la puntuación del usuario a medida que el nivel de privacidad del usuario cambie cada vez que responda la encuesta.
- La aplicación tendrá una pantalla de perfil en la cual el usuario podrá consultar sus datos y calificaciones a nivel personal.
- La aplicación debe poder emitir los siguientes resultados: resultados individuales, y recomendaciones generadas al usuario.
- La aplicación contará con una pantalla de recomendaciones donde el usuario podrá consultar información útil que puede utilizar para mejorar su experiencia en línea y aumentar su privacidad.

Requerimientos de rendimiento

- La aplicación debe tener un diseño y entorno claro y entendible.
- Definir en el diseño una correcta integración entre la base de datos y la aplicación para garantizar el óptimo rendimiento del sistema.

Requerimientos funcionales de interfaz gráfica

- La aplicación validará automáticamente el usuario asociado con su correo electrónico de Google.
- El campo de edad, estrato, acepta únicamente valores numéricos.
- La aplicación contará con pantalla de perfil de usuario.
- La aplicación contará con pantalla de realización de encuesta.
- La aplicación contará con pantalla de consulta de resultados generales.
- La aplicación contará con pantalla de recomendaciones.
- El campo nombre acepta caracteres alfabéticos únicamente.

Requerimientos funcionales legales o regulatorios

- El sistema controlará el acceso y permitirá acceder únicamente a usuarios autorizados.
- Únicamente las personas que hacen parte del trabajo de grado tendrán acceso a observar la totalidad de los resultados.
- La base de datos será guardada de manera anónima y solo se permitirá el acceso a personal que hace parte del trabajo de grado

Requerimientos de seguridad

- El sistema controlará el acceso y lo permitirá solamente a usuarios autorizados.
- Los usuarios deben ingresar al sistema con un nombre de usuario y contraseña.
- El sistema enviará un correo al administrador del sistema cuando ocurra alguno de los siguientes eventos: registro de nueva cuenta, ingreso al sistema por parte del usuario,

cuando un usuario tenga dos o más intentos fallidos en el ingreso de la contraseña de usuario y cambio de contraseña de usuario.

Requerimientos de interfaces externas (Hardware y Software)

- La aplicación podrá ser utilizada en los sistemas operativos Android, se elige usar el sistema operativo Android debido a que es el más utilizado en Colombia y el mundo. (Stat Counter Global Stats, 2017)
- La aplicación debe poder utilizarse sin necesidad de instalar ningún software adicional.
- La aplicación se debe poder descargar a través de la Google Play Store plataforma de distribución digital de aplicaciones móviles desarrollada y operada por Google, acatando las regulaciones emitidas por la misma plataforma.
- La aplicación requiere utilizar conexión a internet debido a que las funciones como la encuesta y resultados se actualizan de manera síncrona

6.1.2.2 Requerimientos NO funcionales

Confiabilidad

- La aplicación móvil será desarrollada para las plataformas Android.
- La aplicación deberá consumir menos de 500 Mb de memoria RAM.
- La aplicación no podrá ocupar más de 500 Mb de espacio en disco.
- La nueva aplicación debe manejar fuentes del alfabeto en español

Requerimientos no funcionales organizacionales

- El proceso de desarrollo se gestionará por medio de una determinada herramienta web para gestionar el proceso de desarrollo de software, una plataforma web para la construcción de aplicaciones móviles.
- Deberán producirse reportes en los cuales se evidencie el alcance de la aplicación y los resultados generales de usuarios por el tiempo que dure la investigación.
- Las pruebas de software se gestionarán por parte de usuarios finales y personal técnico calificado.

Requerimientos no funcionales externos

- El nuevo sistema y sus procedimientos de mantenimiento de datos deben cumplir con las leyes y reglamentos de protección de datos de la ley colombiana incluida en el Decreto 1317 de 2013 Sobre la protección de datos personales. (Mincomercio & Presidente de la republica, 2013)
- El sistema no revelara a sus usuarios otros datos personales de los usuarios distintos al registrado en la aplicación móvil.

6.1.3 Arquitectura de la aplicación

La arquitectura define como funcionará la aplicación móvil y determina la estructura de la aplicación en cuanto a la interfaz gráfica e interfaz de usuario, siendo amigable y fácil de usar para el usuario final.

Los elementos de información (pantallas) que se manipulan en la aplicación son:

- **Perfil del usuario:** información y datos personales de cada usuario como: nombre, cuenta de correo electrónico y contraseña.
- **Encuesta o instrumento de medición:** encuesta diligenciada por los usuarios para medir el nivel de privacidad en línea.
- **Estadísticas generales:** resultados generales de las encuestas realizadas por los diferentes usuarios.
- **Recomendaciones:** conjunto de recomendaciones que se sugieren a los usuarios según los resultados de su última evaluación.
- **Términos y condiciones:** información con los términos y condiciones de la aplicación.
- **Políticas de privacidad:** información con los términos en garantías de seguridad para el usuario.

En la aplicación se tienen dos tipos de usuario: usuario administrador y usuario normal (el que realiza la encuesta). Dependiendo del tipo de usuario, este puede realizar diferentes acciones sobre los elementos de información (pantallas) de la aplicación: crear, modificar, eliminar, consultar y diligenciar la encuesta.

A continuación, se presenta mayor detalle sobre la arquitectura de la aplicación.

6.1.3.1 Ámbito del sistema

La aplicación desarrollada y presentada en este documento es una aplicación para dispositivos móviles que asesora al usuario a proteger su privacidad y sus datos en Internet, la cual se construyó utilizando una plataforma de construcción de aplicaciones móviles llamada **Appy Pie**, apoyada en la plataforma web para el manejo y gestión de encuestas en línea llamada **Type Formen**, las cuales se describen más adelante.

La aplicación se basa en un sistema de bajo consumo, basada en web, que garantiza que la información en la base de datos siempre este actualizada.

Se diseñó un Instrumento de medición que se presentó en la sección 6.1.1 que es diligenciado por el usuario y la aplicación analiza esta información y clasificará al usuario de acuerdo a las respuestas seleccionadas. Los datos de la encuesta son procesados y almacenados en forma segura y solo pueden ser accedidos por los autores de la investigación asociada a este trabajo.

6.1.3.2 Casos de uso

Los casos de uso presentan los métodos funcionales de la aplicación, los requerimientos de la aplicación y su funcionamiento. Las funciones principales de la aplicación son seis y se presentan en la *Figura 2*. Estas funciones son:

- **Diligenciar la encuesta (realizar autoevaluación)**

Mediante esta función se diligencia la encuesta y se envían las respuestas a correo electrónico (el cual envía las respuestas del usuario a su correo electrónico personal), a este método tiene acceso los dos usuarios: administrador y usuario normal.

- **Crear**

Este método permite crear el formato de evaluación que contiene las preguntas de la encuesta y las recomendaciones para cada grupo de usuarios, a esta función solo tiene acceso el usuario administrador.

- **Modificar**

Este método permite modificar el formato de evaluación que contiene las preguntas de la encuesta y las recomendaciones para cada grupo de usuarios, a esta función solo tiene acceso el usuario administrador.

- **Eliminar**

Este método permite eliminar el formato de evaluación que contiene las preguntas de la encuesta y las recomendaciones para cada grupo de usuarios, a esta función solo tiene acceso el usuario administrador.

- **Consultar**

Este método es diseñado para los usuarios normales, extiende a las funciones a las que un usuario normal de la aplicación puede acceder: la pantalla de estadísticas generales, recomendaciones, página inicial, términos y condiciones y políticas de privacidad.

- **Consultar todo**

Consultar todo es una función de consulta solo para administradores, incluye todas las funciones del método consultar, pero además extiende a las funciones de Estadísticas de aplicación, estadísticas detalladas, resultados individuales y formulario de aplicación.

El usuario normal tiene acceso solo a dos de las funcionalidades principales de la aplicación que son: la función Consultar y la función Realizar la Autoevaluación. La función consultar se extiende (contiene) a otras funciones en las que el usuario puede consultar información como, Estadísticas generales, Recomendaciones, Pagina inicial, Términos y condiciones y Políticas de privacidad.

La función Realizar autoevaluación, extiende al método Enviar respuestas a correo electrónico, este es el segundo método al que tiene acceso el usuario normal.

El Usuario Administrador tiene acceso a todas las funcionalidades de la aplicación. Las funciones Crear y Modificar se extienden a los elementos de información recomendaciones y encuesta o instrumento de medición. La función Eliminar se extiende a los elementos de información recomendaciones, encuesta y a los resultados individuales de la encuesta. También tiene acceso a la función Realizar autoevaluación que se extiende a la función Enviar respuestas al correo electrónico. También puede Consultar todo accediendo a toda la información de la aplicación que extiende a los elementos de información: Estadísticas de la aplicación, Formulario de evaluación, Estadísticas detalladas, Resultados individuales, además esta función también extiende a la Función padre Consultar, que extiende a los elementos de información Estadísticas generales, Recomendaciones, Pagina inicial, Términos y condiciones y Políticas de privacidad. Es necesario aclarar que el usuario Administrador accede a todas estas funciones de administrador a través del **CMS (Content Management System)** o **administrador de contenido** en español de la aplicación, que la componen la plataforma de gestión de encuestas **TypeForm** y la plataforma de creación de aplicaciones **AppyPie**.

6.1.3.3 Interfaz gráfica

La aplicación cuenta con 6 pantallas en la parte gráfica, cada una presenta a los usuarios diferentes elementos de información de la siguiente forma:

- **Pantalla de perfil de usuario:** pantalla en la que el usuario puede modificar y consultar el **perfil del usuario**.
- **Pantalla de aplicación de encuesta:** pantalla interactiva en la que el usuario puede realizar la **encuesta o instrumento de medición** cuando lo requiera.
- **Pantalla de estadísticas:** pantalla interactiva se actualiza de manera síncrona en la que el usuario puede consultar sus resultados y compararlos con las **estadísticas generales** de otros usuarios que utilicen la aplicación.
- **Recomendaciones:** es una pantalla en la que el usuario encuentra las **recomendaciones** que según los resultados de su última evaluación le sugiere la aplicación, contiene un instructivo para que el usuario aprenda a aplicar y usar las recomendaciones.
- **Pantalla de políticas de privacidad:** pantalla informativa donde se explican al usuario normal los términos en garantías de seguridad para sus datos personales.
- **Pantalla de términos y condiciones:** Pantalla informativa donde se explican al usuario normal los términos y condiciones de la aplicación.

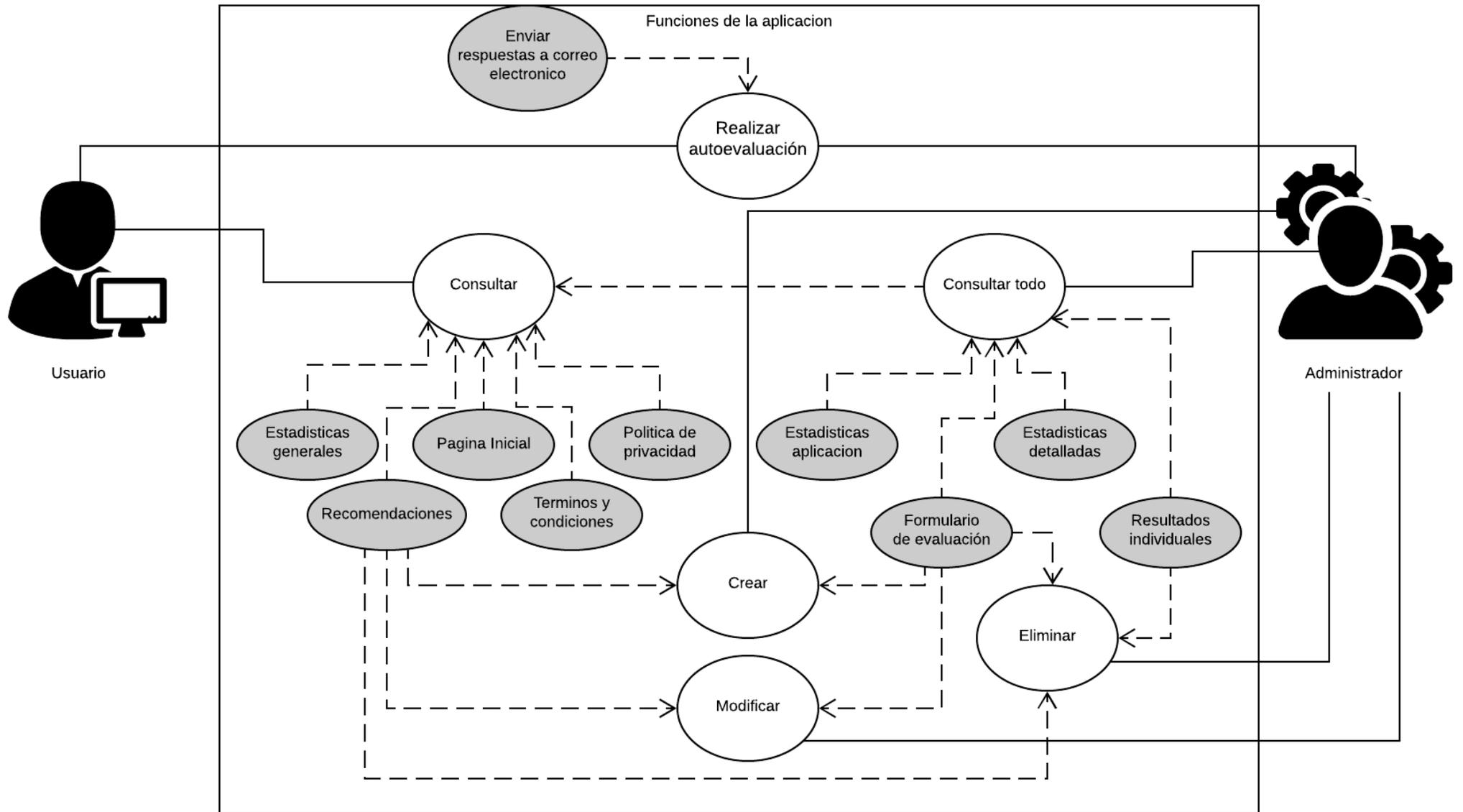


Figura 2. Casos de uso.

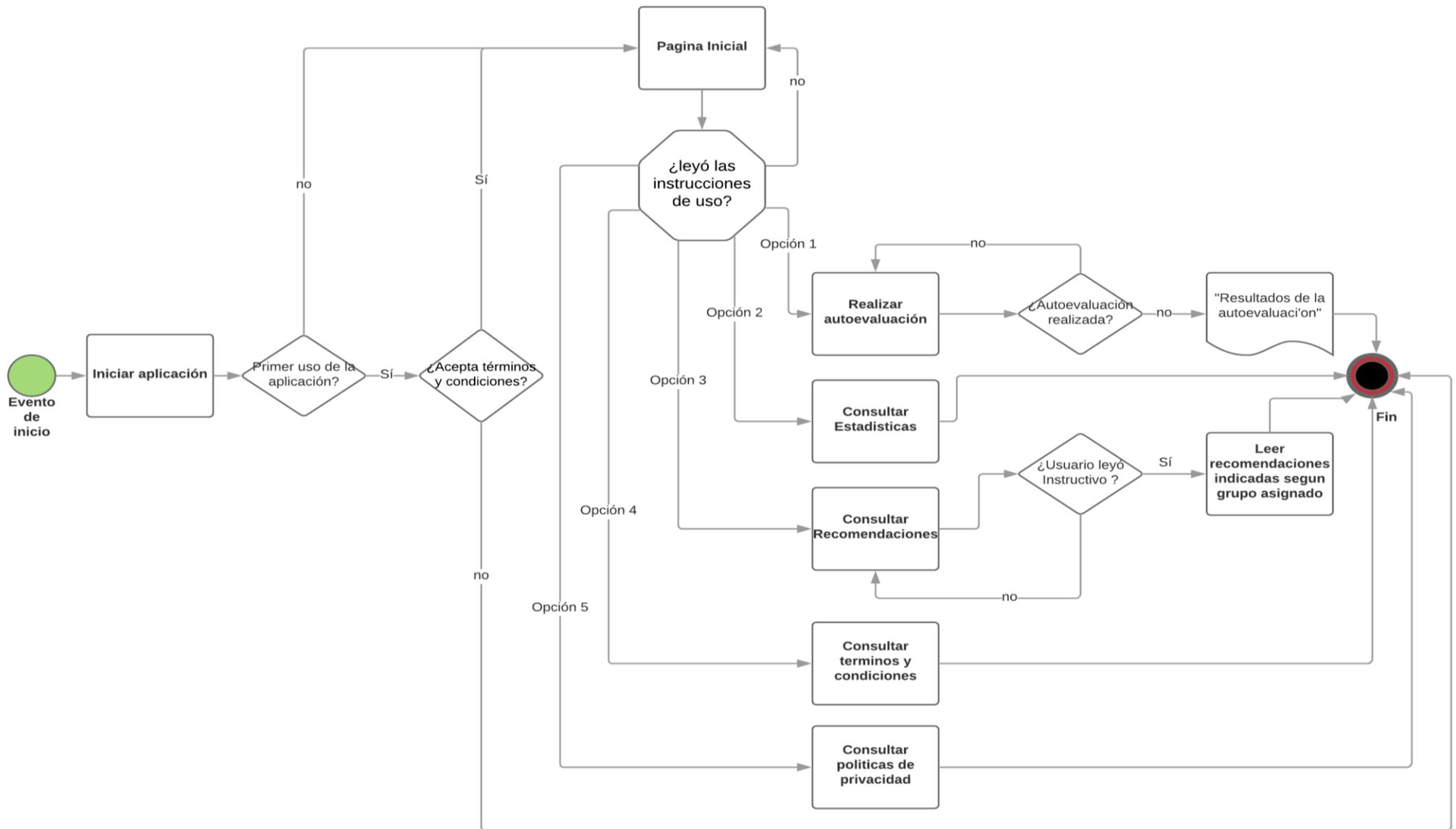


Figura 3. Diagrama de proceso.

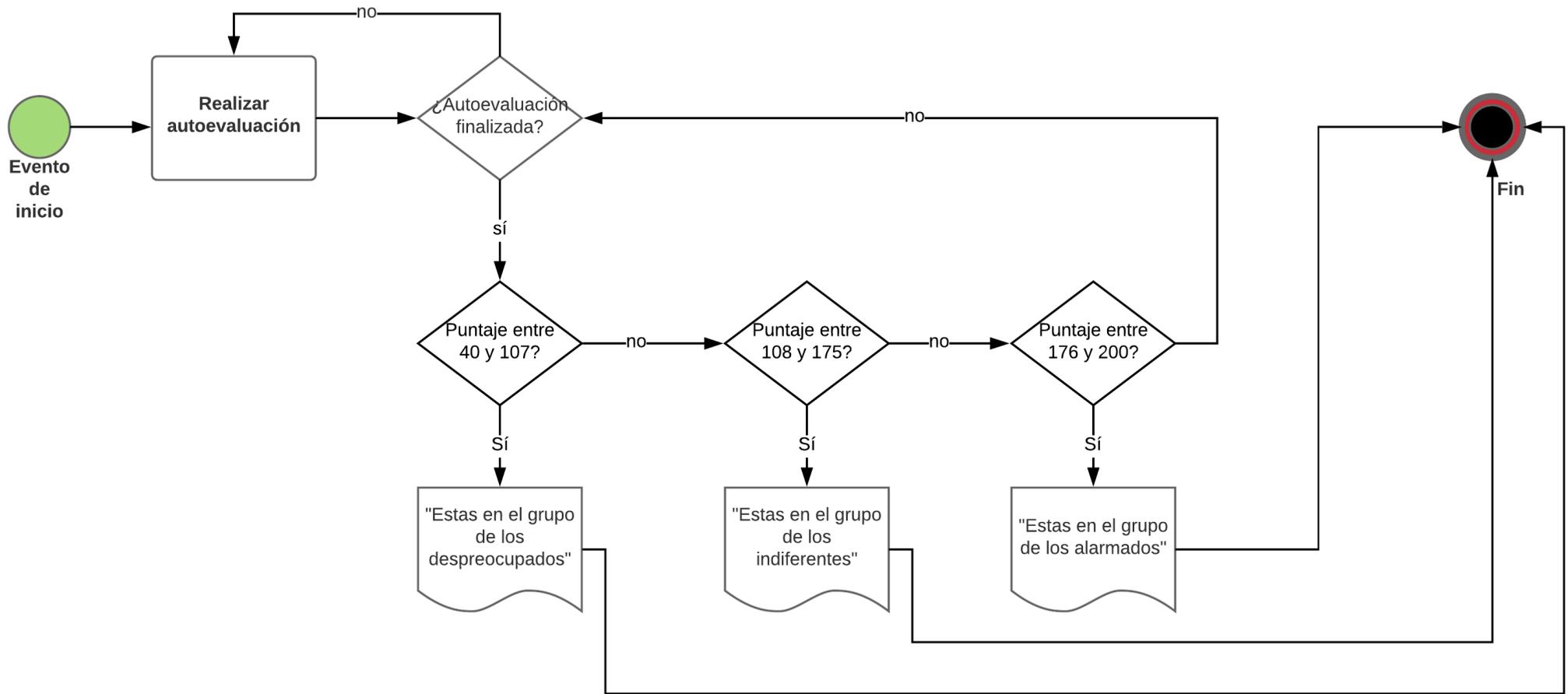


Figura 4. Diagrama de calificación interna.

6.1.3.4 Diagrama de proceso

El **diagrama de proceso** indica cómo se lleva a cabo la interacción entre el usuario normal y la aplicación desde el momento que accede a la aplicación. Este diagrama se presenta en la **Figura 3**.

El evento de inicio se da cuando el usuario normal accede a la aplicación. Si el usuario no está registrado, es decir, accede por primera vez, se le pedirá que lea y acepte los términos y condiciones de uso de la aplicación. Si no acepta los términos accede directamente al menú principal de la aplicación. Después de leer las instrucciones el usuario puede elegir a cuál de las funciones desea acceder entre ellas están:

- Realizar Autoevaluación,
- Consultar estadísticas generales,
- Consultar recomendaciones,
- Consultar términos y condiciones y
- Consultar políticas de privacidad.

Si el usuario elige la opción realizar autoevaluación, se abre el formulario de la encuesta, donde el usuario la diligencia. Al terminar la encuesta la aplicación verifica si la encuesta está completa y finalmente publica los resultados para que el usuario los pueda conocer.

Si el usuario escoge la opción de consultar recomendaciones se abre la página de recomendaciones, donde se presenta el instructivo. Después de leer el instructivo el usuario accede a las recomendaciones indicadas según los resultados de su evaluación.

6.1.3.5 Diagrama de calificación interna

El diagrama de calificación que se observa en la **Figura 4** y presenta cómo se realiza el proceso de calificación de la encuesta y de la clasificación al usuario según el resultado de esta. El evento de inicio se produce cuando el usuario acciona realizar autoevaluación. Al terminar la aplicación calcula y presenta el puntaje obtenido y los resultados (ver sección 6.1.1):

- si el puntaje obtenido esta entre 40 y 107 la aplicación clasifica al usuario dentro del grupo de los despreocupados,
- si el puntaje obtenido por el usuario esta entre 108 y 175 la aplicación clasifica al usuario dentro del grupo de los indiferentes,
- si el puntaje obtenido por el usuario esta entre 176 y 200 la aplicación clasifica al usuario dentro del grupo de los alarmados.

6.1.3.6 Mockups

Para una mayor comprensión de los requerimientos y funcionalidades del alcance del sistema, se han desarrollado Mockups, que es un modelo del diseño de cada pantalla del sistema, a través de los cuales se constituyen en la base para la construcción de la interfaz gráfica real de la aplicación, los Mockups se describen a continuación:

Mockup 1. Se observa en la *Figura 5* el diseño en Mockups (diseño en borrador) para la página de recomendaciones. Como sería la posible distribución de las recomendaciones (información recolectada para cada grupo de usuarios) y las apps recomendadas.

Mockup 2. Se observa en la *Figura 6* el diseño en Mockups (diseño en borrador) para la página de estadísticas. Página que muestra las estadísticas generales de los resultados de las encuestas.

Mockup 3. Se observa en la *Figura 7* el diseño en Mockups (diseño en borrador) para la página de autoevaluación (la encuesta). Página a la cual el usuario accede y diligencia la encuesta.

Mockup 4. Se observa en la *Figura 8* el diseño en Mockups (diseño en borrador) para la página de perfil. El usuario accede a su perfil para modificar sus datos.

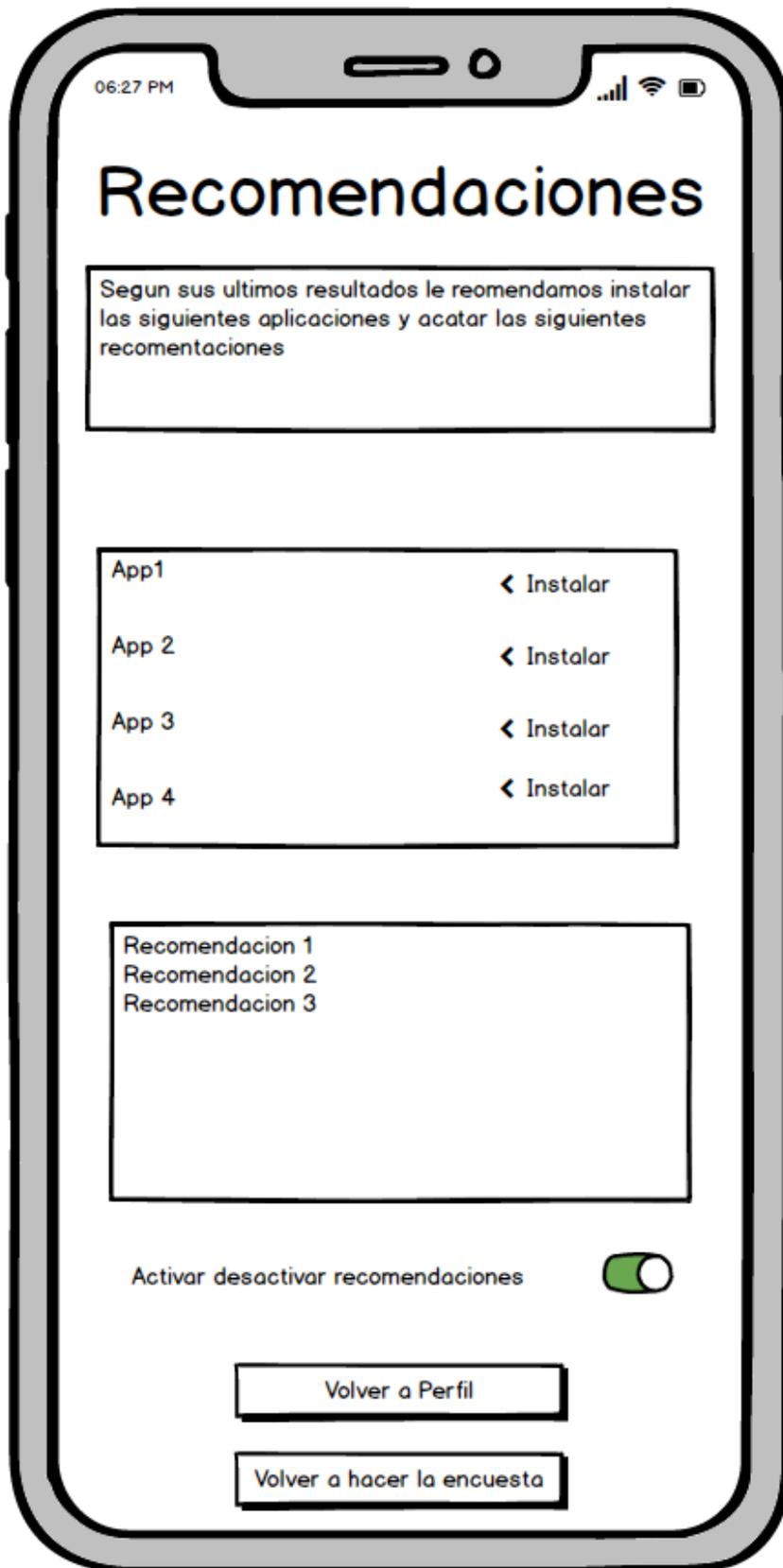


Figura 5 Mockup de recomendaciones



Figura 6 Mockup de estadísticas

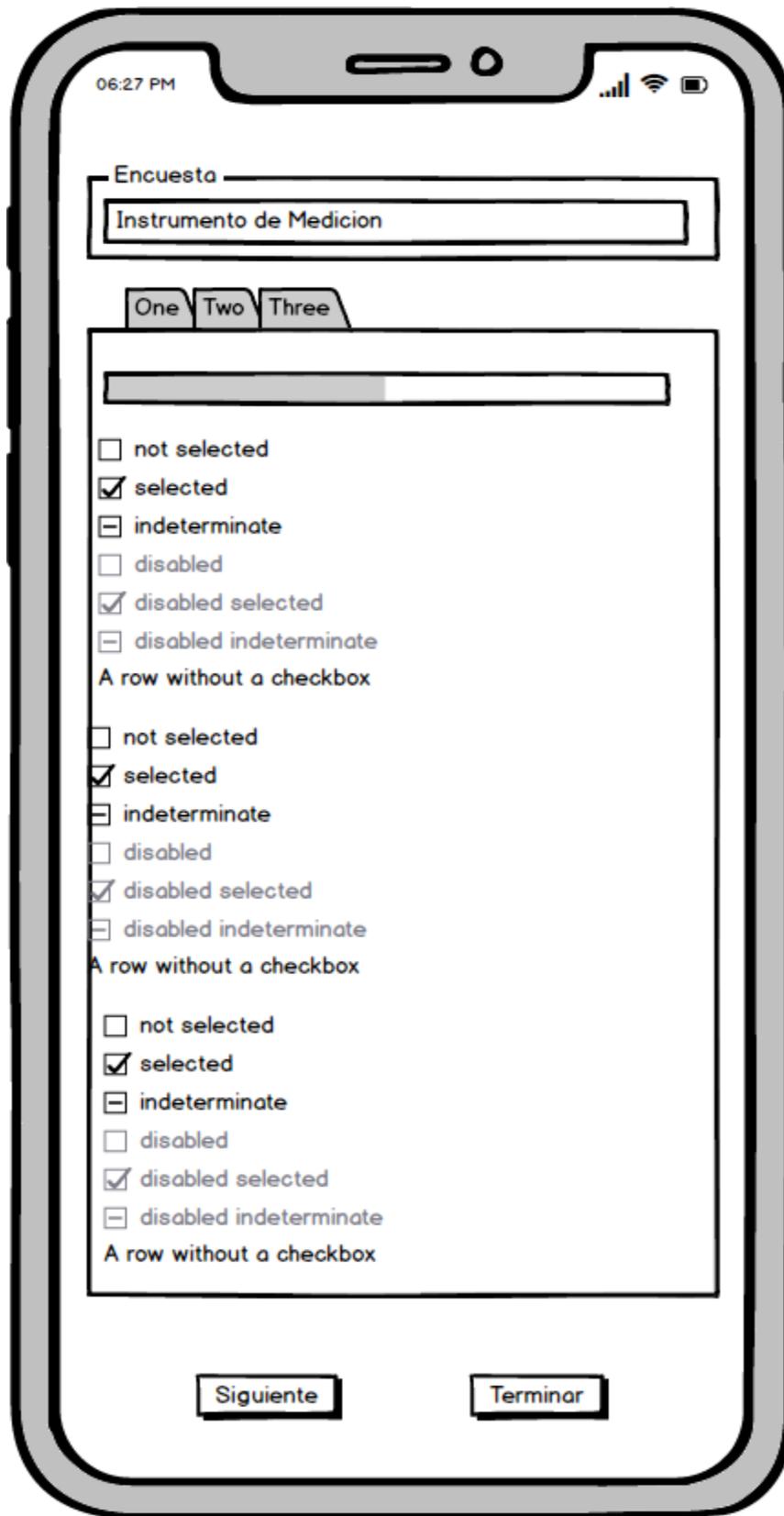


Figura 7 Mockup de encuesta (autoevaluación)

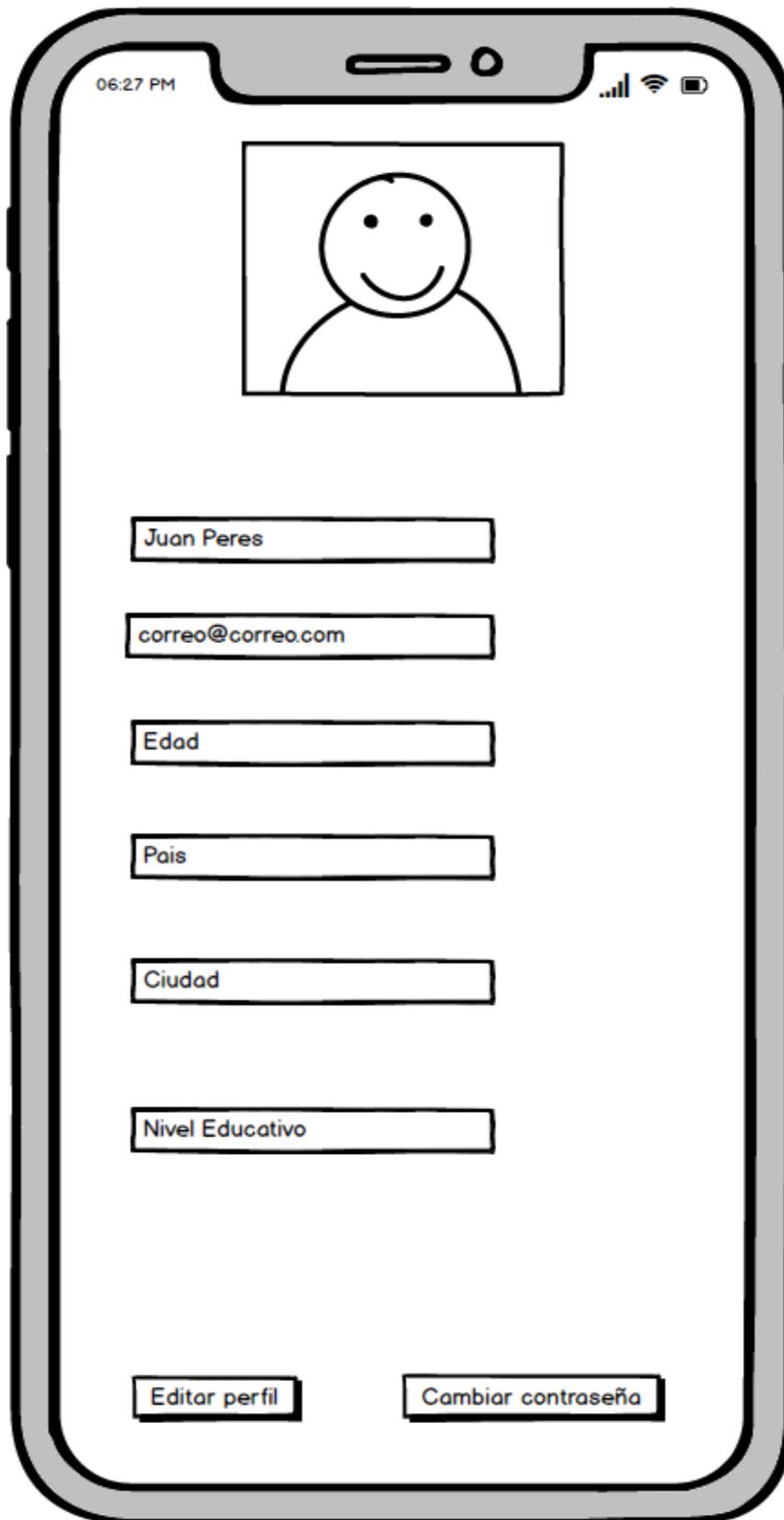


Figura 8 Mockup de perfil

6.2 Construcción del prototipo de Aplicación móvil

En este capítulo se describe como se realizó la construcción del prototipo de aplicación móvil, se describe cada uno de los pasos teniendo en cuenta el diseño que se planteó y las tareas propuestas en los objetivos específicos y diseño de la aplicación.

La aplicación móvil es construida utilizando una plataforma de construcción de aplicaciones en línea llamada **Appy Pie**² y una plataforma de gestión de encuestas en línea llamada **Type Form**³, a continuación, se describen las funcionalidades de estas plataformas, el método utilizado para la selección de estas plataformas y como se realizó la construcción y liberación de la aplicación móvil.

6.2.1 Selección de plataforma

Para escoger la plataforma usada para la construcción de la aplicación se utilizaron 3 criterios:

- **Costo de liberación de la aplicación.**

Se busca un costo económico que sea favorable pero que también ofrezca la mayoría de las funcionalidades que se buscan para que la aplicación se ejecute como se diseñó, cumpliendo todos los requerimientos funcionales planteados.

- **Robustez de la plataforma.**

Se busca una plataforma robusta, es decir, que cumpla correctamente con los servicios ofrecidos, que no presente fallas en sus funcionalidades, que presente un servicio técnico adecuado, en el caso en que se requiera solicitar servicio de asesoramiento en las funcionalidades de la plataforma.

- **Funcionalidad ofrecida.**

Es necesario que la plataforma ofrezca las funcionalidades esperadas para dar cumplimiento a todos los requerimientos de la aplicación planteados anteriormente.

Se hace la aclaración que en las funcionalidades aquí descritas en la tabla comparativa son las ofrecidas en el plan de precio full que ofrece cada plataforma, en el **Anexo 4** se puede conocer de forma detallada los planes y precios que ofrece cada plan de cada plataforma propuesta

Las plataformas evaluadas y sus características se presentan en la **Tabla 3**.

² <https://es.appypie.com/>

³ <https://www.typeform.com/product/>

Plataforma	Costo de liberación de la aplicación.	Robustez de la plataforma y Funcionalidad ofrecida* <small>*las funcionalidades aquí descritas son las ofrecidas en el plan de precio full que ofrece cada plataforma</small>
Plataforma Mob App creator⁴	Precio Más económico: \$19 USD/mes Precio Full: \$149 USD/mes	<ul style="list-style-type: none"> • App Nativa de Android • Notificaciones Push Ilimitadas • Instalaciones ilimitadas • Actualizaciones ilimitadas • Módulos ilimitados • Soporte Dedicado • Estadísticas de App • Google Analytics • Acceso a API
Plataforma App Makr⁵	Precio Más económico: \$2 USD/mes Precio Full: \$39 USD/mes	<ul style="list-style-type: none"> • Usuarios Ilimitados • Actualizaciones Ilimitadas • Apps Nativas iPhone y Android • Sitio Web Móvil HTML5 • Auto-Publicación desde cualquier sitio • Acceso al código fuente • Permite crear marca propia • Informe de Estadísticas en Vivo
App Yourself⁶	Precio Más económico: \$23 USD/mes Precio Full: \$93 USD/mes	<ul style="list-style-type: none"> • Usuarios activos ilimitados • Messenger • Gestión de clientes • Notificaciones Push⁷ • Smart Widget⁸ • Aplicación web progresiva • Aplicación en las tiendas de aplicaciones • Gestor de acceso

⁴ <https://www.mobappcreator.com/es/Inicio#pricing>

⁵ https://www.appmakr.com/?locale=es_US

⁶ <https://appyourself.net/es/precios-crear-aplicaciones/>

⁷ Notificaciones push es un sistema que te permite una comunicación instantánea con tu cliente. De esta manera, puedes mandar mensajes de hasta 255 caracteres a los usuarios de tu app. (Upplication, 2017)

⁸ Los Smart widget son las aplicaciones que se instalan en los Smart watch(dispositivos que son como relojs que son compatibles con los celulares) (Smart posts widget, 2016)

Good Barber⁹	Precio Más económico: \$32 USD/mes Precio Full: \$200 USD/mes	<ul style="list-style-type: none"> • Aplicación web progresiva ilimitadas para Desktop, Tablet y Móvil • Aplicaciones nativas para Android ilimitadas • Aplicaciones Nativas ilimitadas para iOS (cuenta de desarrollador empresa) • Coste de verificación adicional si se quiere distribuir en la App Store • Nombre de dominio personalizado • Seguridad SSL incluida • Tráfico ilimitado • Descargas ilimitadas • Marca blanca
Appy Pie¹⁰	Precio Más económico: Gratis Precio Full: \$45 USD/Mes	<ul style="list-style-type: none"> • ¡Appy Pie Sin Anuncios! • Editar tu Aplicación Ilimitadamente • Publicar bajo tu cuenta de desarrollador. • Cantidad de Notificaciones Push 25000/mensual • Espacio del disco 600 MB • Ancho de banda mensual 12 GB • Aplicación Analytics con Google Analytics • Gana dinero a través de publicidad • Atención al Cliente • Correo electrónico, Chat & Llamadas • Quitar Marca (su propia aplicación de marca blanca)
Desarrollo de aplicación sin usar ninguna plataforma	Precio Más económico: Gratis	<ul style="list-style-type: none"> • Gratuita • Compatibilidad limitada • Personalización de opciones, diseño e interfaz • Escalabilidad limitada al cambiar la aplicación de sistema operativo

Tabla 3. Plataformas de desarrollo de aplicaciones móviles.

Se aclara que la aplicación se liberó directamente en Google Play Store y no se utilizó el servicio de publicación que ofrece la plataforma Appy pie, debido a temas de seguridad de datos, para que

⁹ <https://es.goodbarber.com/pricing/>

¹⁰ <https://es.appypie.com/plan-de-precios>

solo los autores del presente trabajo tengan acceso a la cuenta de Google Play Store y la plataforma de construcción de aplicaciones Appy Pie

Finalmente, la aplicación escogida teniendo en cuenta las funcionalidades ofrecidas y un costo económico favorable en términos costo beneficio (relación calidad precio) fue la plataforma **Appy Pie**, se escogió un plan básico mensual de cuarentaicinco mil pesos colombianos (\$45.000 COP) o quince dólares americanos (\$15 USD) al mes de mayo de 2018. Esta opción no es la más económica, pero se contrata este servicio por ofrecer los servicios que son necesarios para dar cumplimiento con los requerimientos de la aplicación propuestos en la metodología. La plataforma **Appy Pie** ofrece las siguientes características, además de las ya descritas en la tabla comparativa:

- Hojas de cálculo de Google y Formularios de Google
- Plataforma multilinguaje
- Crear Aplicaciones Móviles educativas
- Crea tu propio CRM
- crear una aplicación de base de datos
- Nuevos Estilos
- Gane Dinero con Ads
- Analytics para aplicaciones
- Crear una App para Encuestas y Preguntas
- Generador de formularios
- Como crear una App para Colegios y Escuelas: Aplicaciones Educativas
- Cómo crear apps sin saber programar
- Agregado de notificaciones push a una app
- Herramientas de Bolsillo
- Crear aplicación móvil para bienes raíces y agencia inmobiliaria
- Hacer un prototipo de apps móviles

Las plataformas presentadas a continuación son plataformas para la gestión de encuestas, se evaluaron teniendo en cuenta los mismos criterios que se usaron para escoger la plataforma de creación de la Aplicación. Los resultados de la evaluación se presentan en la **Tabla 4**.

Se hace la aclaración que en las funcionalidades descritas en la **Tabla 4** comparativa son las ofrecidas en el plan de precio full que ofrece cada plataforma, en el **Anexo 4** se puede conocer a detalle los planes y precios que ofrece cada plan de cada plataforma propuesta.

Plataforma	Costo de liberación de la aplicación.	Robustez de la plataforma y Funcionalidad ofrecida* *las funcionalidades aquí descritas son las ofrecidas en el plan de precio full que ofrece cada plataforma
------------	---------------------------------------	---

Wufoo¹¹	Precio Más económico: Gratis Precio Full: \$ 99 USD/Mes	<ul style="list-style-type: none"> • Formularios Ilimitados • 5,000 entradas • Campos máximos • 5 usuarios • Informes ilimitados • 5GB Cargas • Seguimiento de Google Analytics • Página de confirmación personalizada • Reglas de formulario • Logotipo personalizado • Cifrado de campo • Proteger contraseña • Email de confirmación • Integraciones • 25,000 solicitudes de API
Jotform¹²	Precio Más económico: Gratis Precio Full: \$ 99 USD/Mes	<ul style="list-style-type: none"> • 100,000 presentaciones mensuales • Envíos seguros de SSL • Recibir pagos ilimitados • 1 TB de espacio disponible • Formularios ilimitados • Formulario mensual ilimitado • Vistas ilimitadas • Almacenamiento de envío total • Informes ilimitados, campos por formulario • Sin marca
Survey Monkey¹³	Precio Más económico: \$25USD/mes Precio Full: \$62USD/año	<ul style="list-style-type: none"> • Cantidad ilimitada de encuestas • Preguntas ilimitadas por encuesta • Respuestas ilimitadas por encuesta • Asistencia por teléfono y correo electrónico 24/7 • Cuestionarios con comentarios personalizados • Filtros y tabulaciones cruzadas ilimitados, datos de tendencias • Exportaciones de datos (CSV, PDF, PPT, XLS) • Lógica de exclusión, canalización de preguntas y respuestas • Análisis de textos e importancia estadística

¹¹ <https://www.wufoo.com/pricing/>

¹² <https://www.jotform.com/pricing>

¹³ https://es.surveymonkey.com/pricing/?ut_source=header

		<ul style="list-style-type: none"> • Exportaciones avanzadas de datos (SPSS) • Variables personalizadas • Carga de archivos • Encuestas con marca blanca • Encuestas en múltiples idiomas
Type Form¹⁴	<p>Precio Más económico: Gratis</p> <p>Precio Full: \$70 USD/mes</p>	<ul style="list-style-type: none"> • Campos de tipos de letra ilimitados • Tipos de preguntas avanzadas • Métricas y reportes • Auto notificaciones (correo electrónico) • Respuesta de tuberías • Integración de Hojas de cálculo de Google • Integración de HubSpot • Enviar datos a más de 500 aplicaciones (Zapier) • API de respuestas • Incrustar • Cerrar typeform incrustado después de enviar • Lógica condicional (salto lógico) • Notificaciones de los encuestados (correo electrónico) • Calculadora (puntuación y precios) • Pantalla de agradecimiento personalizado • Campos ocultos • Campo de pago • Integración de MailChimp • Campo de carga del archivo (4Gb / usuario) • Invitar a otros usuarios a espacios de trabajo • Soporte prioritario • Eliminar la marca Typeform • Redirigir al enviar • Gestion de resultados finales (para cuentas anuales con más de 10 usuarios)

Tabla 4. Plataformas de gestión de encuestas.

Finalmente, la plataforma de gestión de encuestas escogida fue **Type Form** por sus características ofrecidas acordes a los requerimientos de la aplicación y a un valor económico favorable en términos costo beneficio. Se escoge el **Plan Pro** que tiene un costo de cuarenta y cinco mil pesos colombianos (\$45.000 COP) mensuales al mes de mayo de 2018, a continuación, se describen más detalladamente las características que ofrece esta plataforma **Type Form**:

- Campos de tipos de letra ilimitados, pueden agregarse campos ilimitados en cada uno de sus tipos de letra.
- Tipos de preguntas avanzadas más todos los campos básicos.

¹⁴ <https://www.typeform.com/pricing/#>

- Métricas y reportes, información sobre los datos que se recopilan generando informes.
- Auto notificaciones (correo electrónico), respuestas del encuestado directamente en la bandeja de entrada tan pronto como completen su forma.
- Integración de Hojas de cálculo de Google que se sincroniza automáticamente cuando entran los resultados.
- Enviar datos a más de 500 aplicaciones (Zapier), permite crear flujos de trabajo al enviar automáticamente los datos de forma tipográfica a más de 500 aplicaciones, a través del conector Zapier.
- API de respuestas.
- Incrustar los tipos de letra sin problemas en su sitio web o blog.
- Webhooks empuja los datos de su forma de letra a sus propias aplicaciones y servicios, al instante.
- Cierra una forma una vez que el encuestado envía su respuesta final.
- Lógica condicional (salto lógico) entre las preguntas basadas en las respuestas de los encuestados y dirige a los encuestados a través de diferentes caminos.
- Calculadora (puntuación y precios) para asignar operadores y valores a las respuestas para calcular un puntaje o precio. Ideal para crear cuestionarios inteligentes, pruebas y formas de pago.
- Pantalla de agradecimiento personalizado, facilita a los encuestados compartir la forma o visiten otra página web.
- Campos ocultos, agregar variables al URL para completar sus preguntas con información personalizada y pasar los datos que ya tiene en el archivo a sus resultados.
- Integración de MailChimp Agregue los nombres y correos electrónicos de los encuestados a sus listas de suscriptores.
- Campo de carga del archivo (almacenamiento de 2GB).

6.2.2 Implementación y construcción de la aplicación

En esta sección se describe paso a paso como se realizó la construcción de la aplicación, utilizando las plataformas seleccionadas **AppyPie** y **TypeForm**, y todo el contenido que se incluye dentro de esta.

El primer paso es establecer una estructura para la aplicación para que sea más fácil organizar y agregar el contenido, la plataforma **AppyPie** ofrece diferentes estructuras que se adaptaron a los requerimientos de la aplicación. Primero se seleccionó un nombre para la aplicación que sea acorde al contexto mismo de la aplicación. Se escogió el nombre **Privatus** es una palabra en Latin que hace referencia a lo Privado.

En la **Figura 9** se presenta el diseño seleccionado y el **CMS (Content Management System)** de la aplicación a través del cual se edita todo el contenido. Para su diseño se escogió la estructura de matriz fija y la categoría de aplicación educativa, características de diseño que ofrece la plataforma **Appy Pie**.

En la **Figura 10** se muestra el logo, el Splash de inicio y la imagen de fondo para la aplicación. Cabe aclarar que el diseño del logo de la aplicación es creación propia del autor del actual trabajo de grado y la imagen de fondo es una imagen gratuita ofrecida por la plataforma **Appy Pie**.

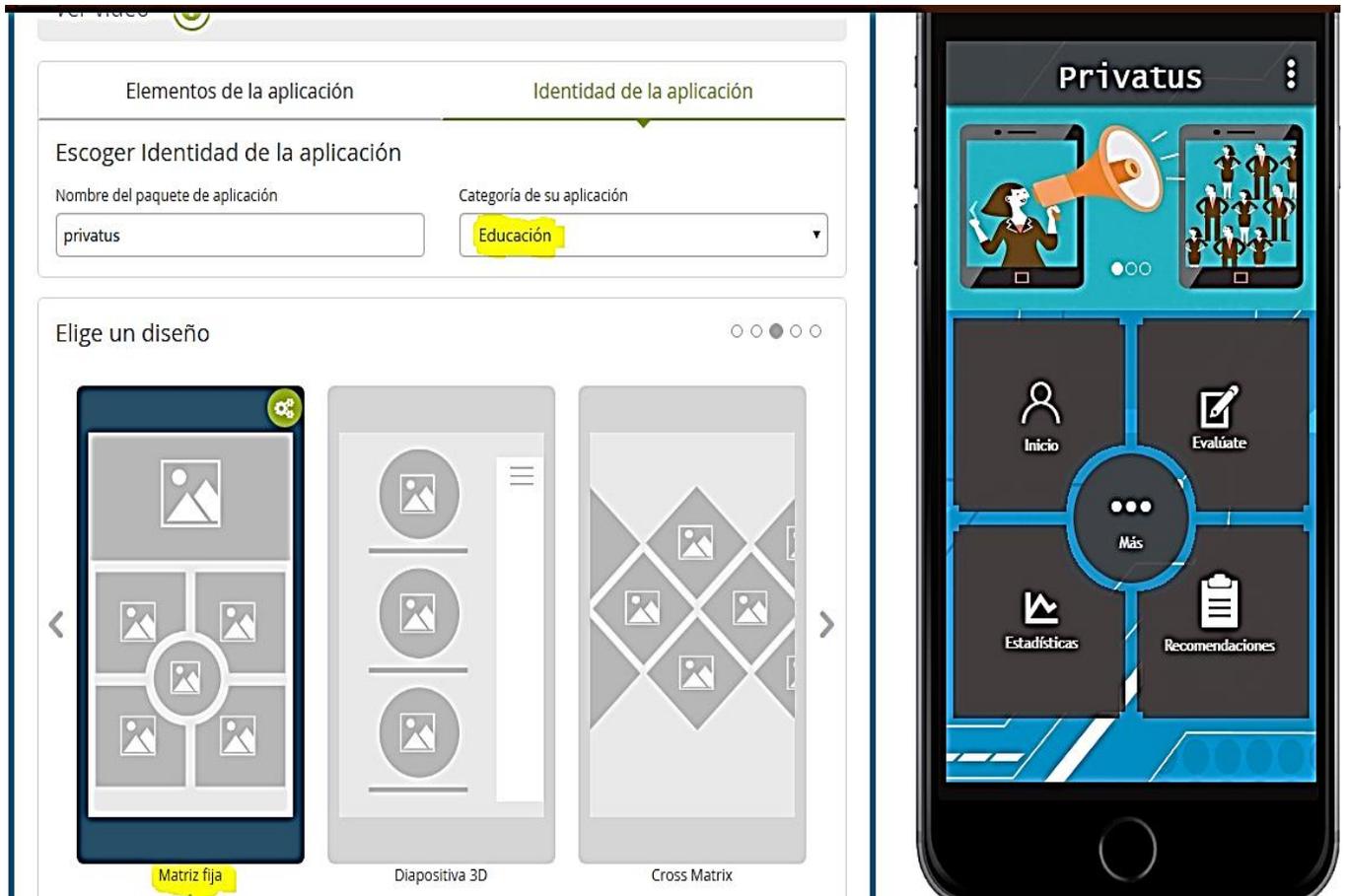


Figura 9. Diseño y estructura.

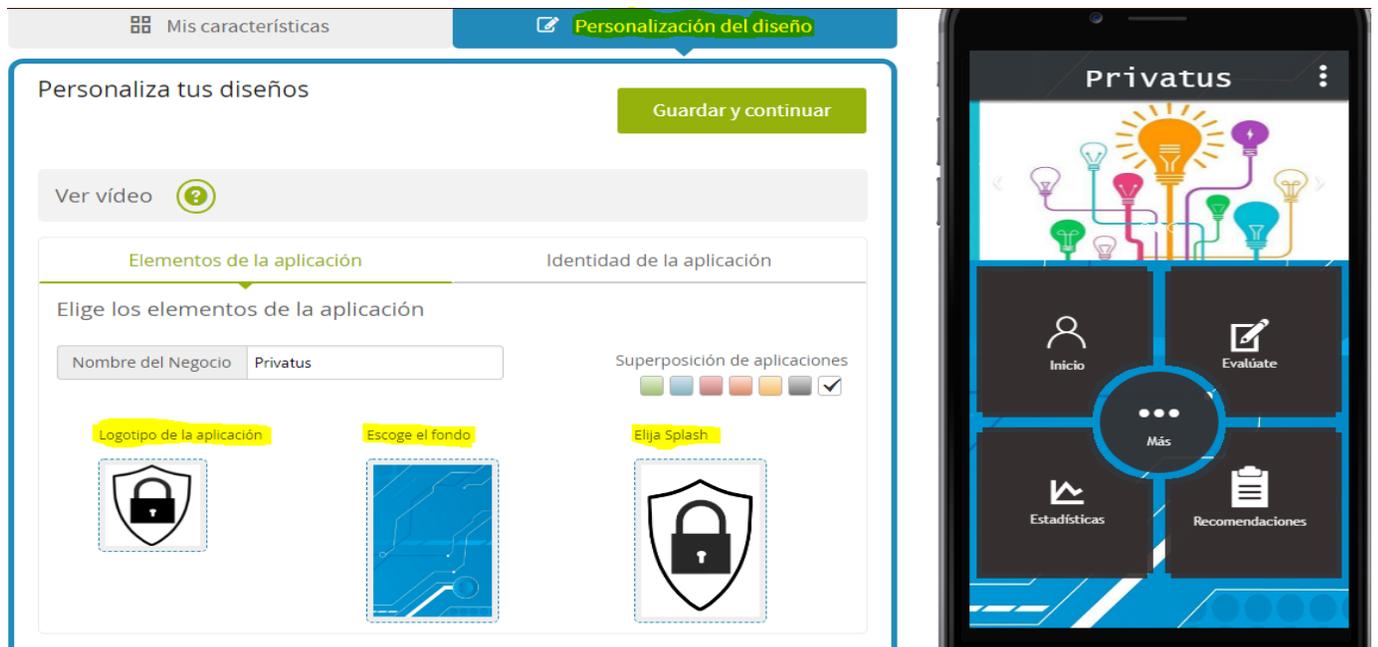


Figura 10. Elementos de aplicación.

En la **Figura 11** se muestra al lado izquierdo del **CMS (Content Managment System)** de la pantalla de inicio, en el cual se modifica y agrega información como: la descripción de la aplicación, instrucciones de uso, información sobre el autor y generalidades de la aplicación. En el lado derecho de la **Figura 11** se presenta una vista previa de la pantalla inicial o página principal de la aplicación, desde donde el usuario se redirige al resto de funciones de la aplicación.

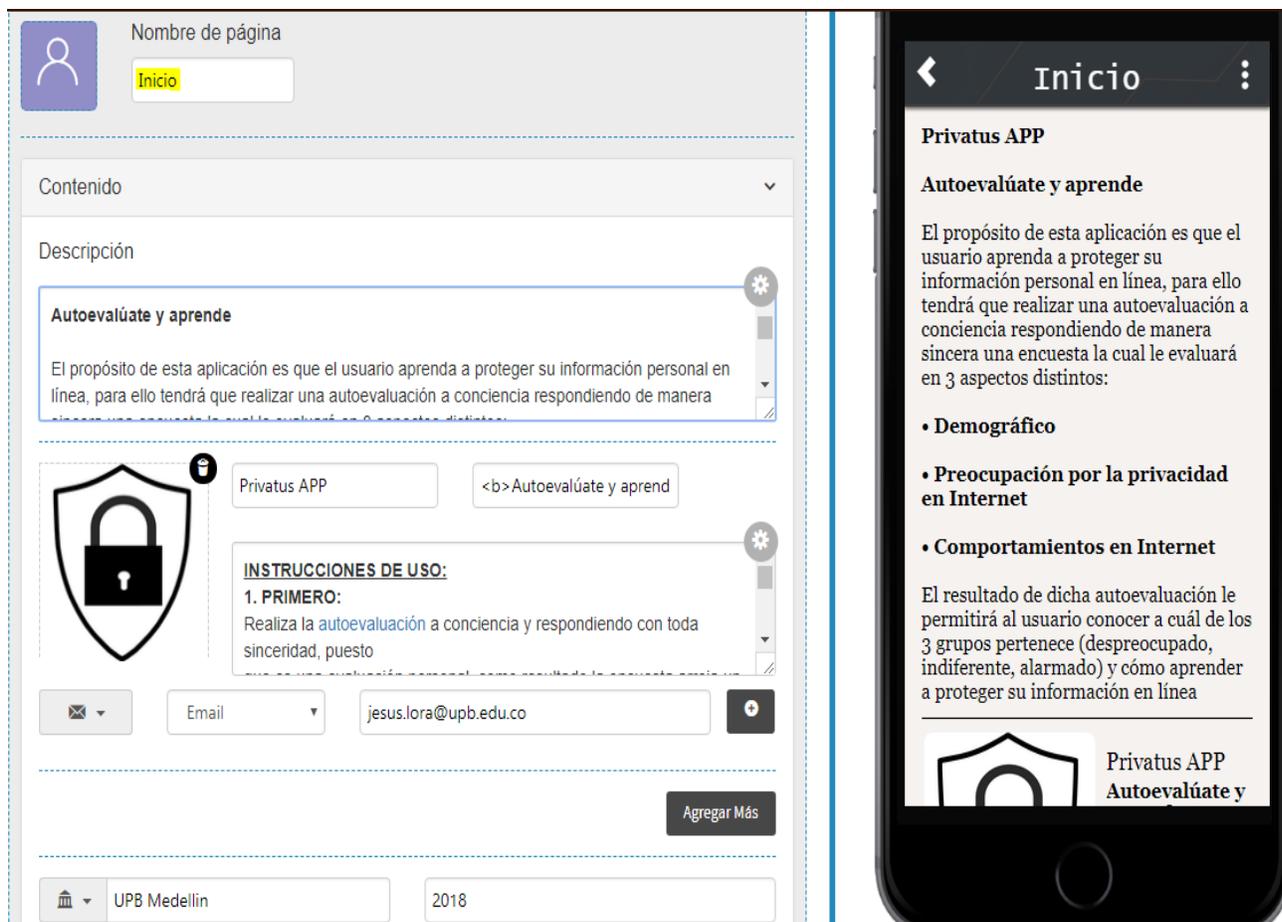


Figura 11. Pantalla inicial.

En la **Figura 12** se muestra el **CMS (Content Management System)** de la pantalla de Autoevaluación que es la pantalla donde se integra la evaluación realizada en la plataforma de gestión de formularios **Type Form** a la aplicación realizada en **Appy Pie** gracias a la funcionalidad de código insertado que ofrecen las dos plataformas: **Type Form** con la funcionalidad de exportar y compartir la encuesta en otras plataformas y **Appy Pie** con la funcionalidad de poder insertar la encuesta por código HTML y JavaScript. En la parte izquierda de la **Figura 12** se muestra la vista previa de la pantalla Autoevaluación. Esta pantalla fue la segunda en crearse para realizar la integración de las dos plataformas **Type Form con Appy Pie**. La implementación esta página da cumplimiento a los requerimientos de rendimiento en donde se propone contemplar el uso óptimo de recursos tales como conexiones a la base de datos y la correcta integración entre la base de datos y la aplicación para garantizar el óptimo rendimiento del sistema.

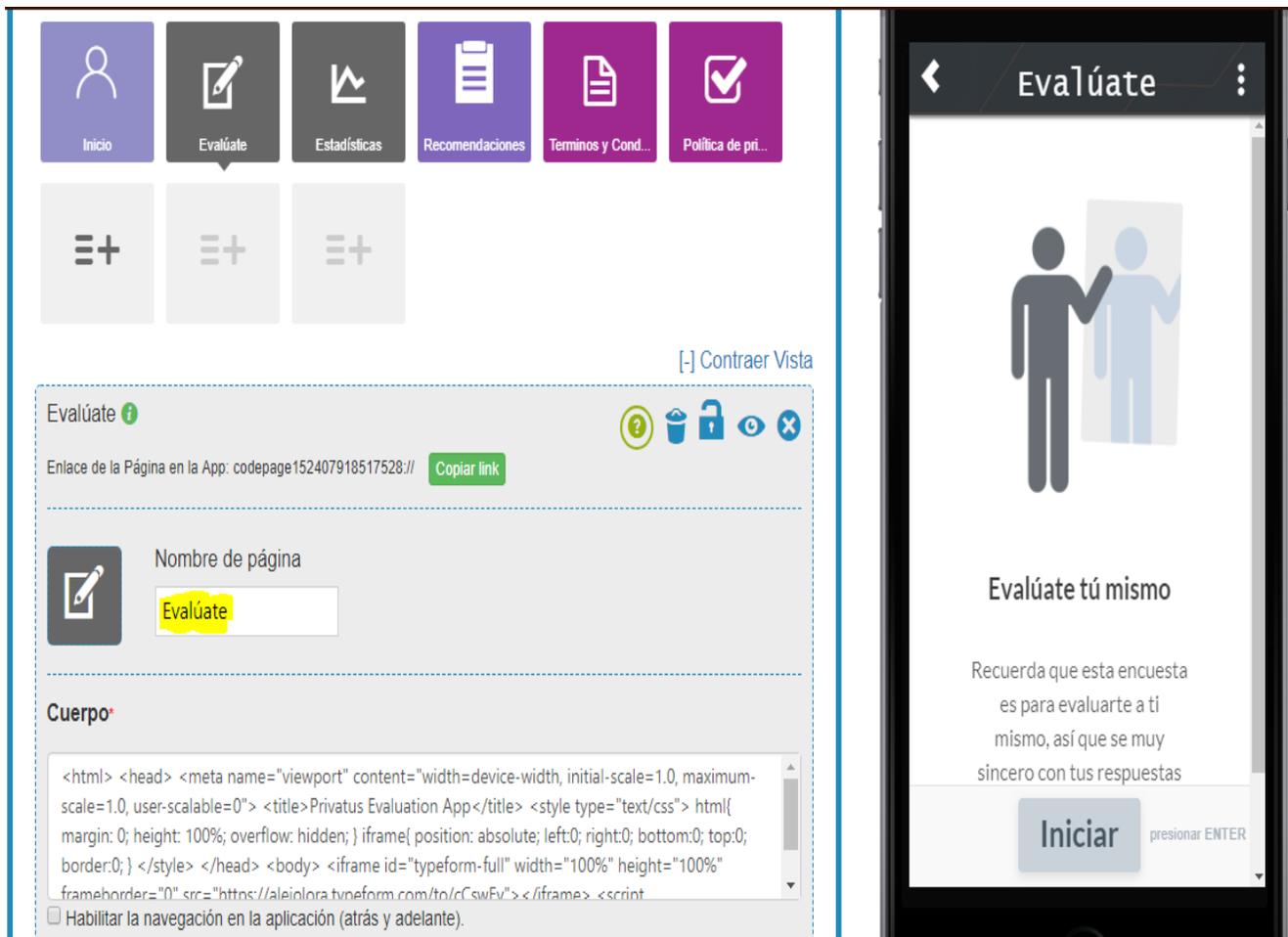


Figura 12. Evalúate.

En la **Figura 13** se muestra el **CMS (Content Managment System)** de la pantalla de estadísticas, que al igual que la pantalla de autoevaluación es una integración de las dos plataformas **Appy Pie** y **Type Form** para presentar las estadísticas en tiempo real de los resultados de las encuestas. Cabe aclarar que los resultados presentados son datos generales de todas las respuestas obtenidos en la evaluación. La integración de esta funcionalidad se logra con la inserción de un código HTML y javascript que permite mostrar las estadísticas generales generadas por la plataforma **Type For**, dentro de la funcionalidad de Codepage de la plataforma **Appy Pie**. En el lado derecho de la **Figura 13** se muestra una vista previa de la pantalla de estadísticas, esta pantalla se desarrolló posterior a la **pantalla de Autoevaluación** con el fin de dar un orden al desarrollo y poder verificar correctamente su funcionalidad después de realizar unas algunas encuestas de prueba. El informe general con los resultados de las evaluaciones se presenta en el **Anexo 2**.

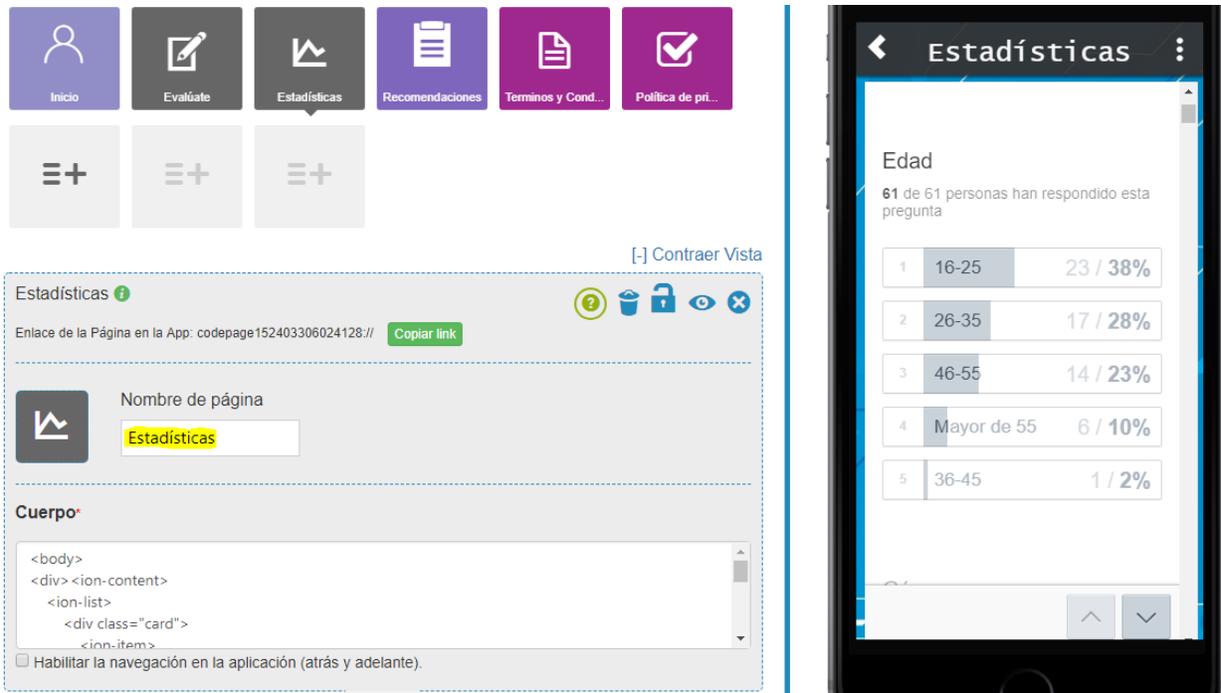


Figura 13. Estadísticas.

En la **Figura 14** se muestra el **CMS (Content Management System)** de la pantalla de recomendaciones que permite la creación de una página informativa por cada uno de los grupos de individuos según su clasificación de la evaluación. Para esto se crea una pantalla para cada uno de los usuarios: despreocupados, indiferentes y alarmados respectivamente. También se crea una pantalla instructiva la cual contiene las indicaciones de como el usuario accede a las recomendaciones según su grupo. Esta pantalla fue la cuarta en crearse para la aplicación siguiendo un orden establecido después de tener en funcionamiento la pantalla de autoevaluación y de estadísticas respectivamente. La pantalla de recomendaciones es aquella donde el usuario viene a consultar que información relevante para mejorar su privacidad en línea.



Figura 14. Recomendaciones.

La **Figura 15** muestra una vista previa de la pantalla de recomendaciones parte derecha y el acceso directo al **CMS (Content Managment System)** de recomendaciones en la parte izquierda. Esta pantalla es creada paralelamente con la pantalla de **CMS** de recomendaciones de la **Figura 14**.

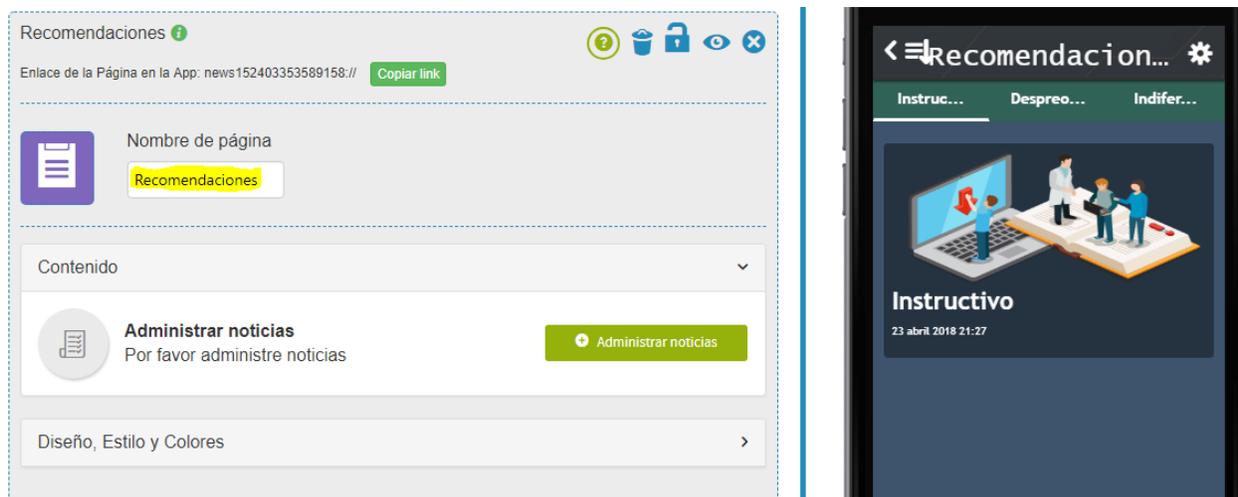


Figura 15. Página recomendaciones.

En la **Figura 16** se muestra el **CMS** de la página Términos y condiciones, es una página informativa que presenta al usuario los términos y condiciones del uso de la aplicación.

En la parte derecha de la **Figura 16** se muestra la vista previa de la pantalla y en la parte izquierda el **CMS** de edición y configuración de esta.

En la **Figura 17** se presenta el **CMS** de la pantalla de Políticas de privacidad de la aplicación, es una página informativa que muestra a través de un procesador de texto, al usuario cuales son las políticas de privacidad de la aplicación.

En la parte izquierda de la **Figura 17** se muestra el **CMS** de edición de texto y en la parte derecha de la figura se muestra una vista previa de la pantalla de Políticas de privacidad.

Las **Figuras 16 y 17** son las últimas funciones en ser diseñadas y creadas, debido a que son páginas netamente informativas y de consulta.

Las recomendaciones para cada grupo de usuarios se presentan en el **Anexo 5**.

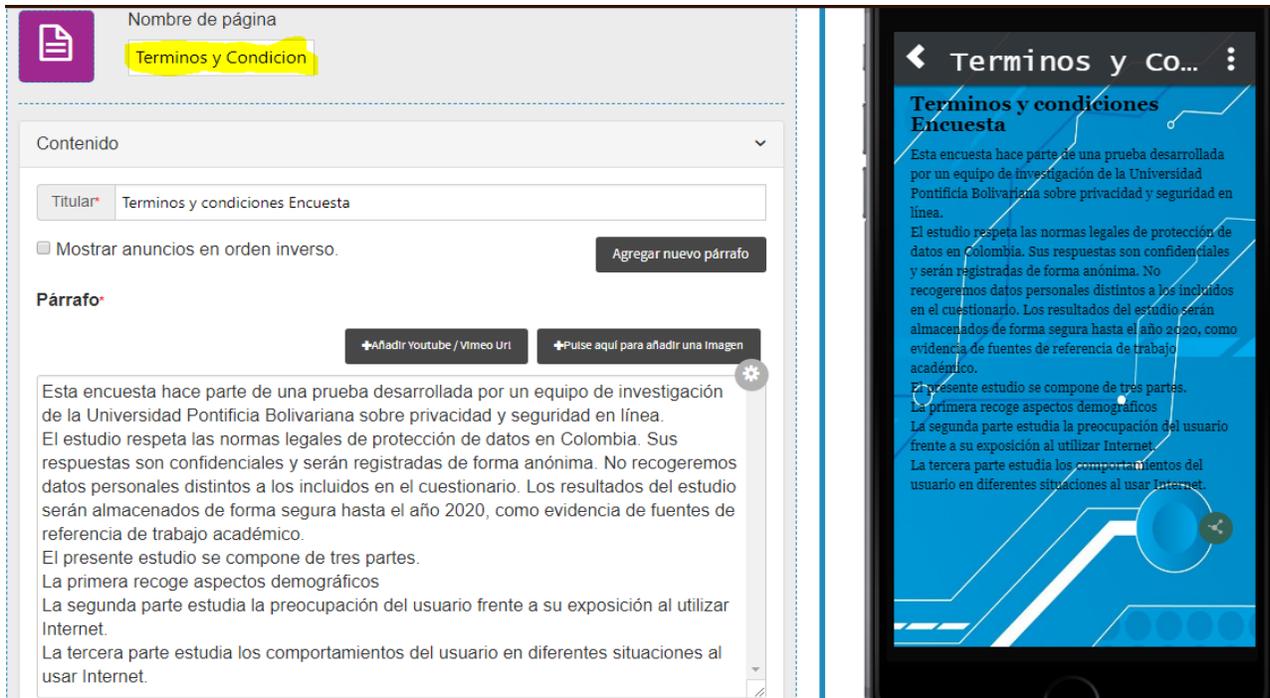


Figura 16. Términos y condiciones.

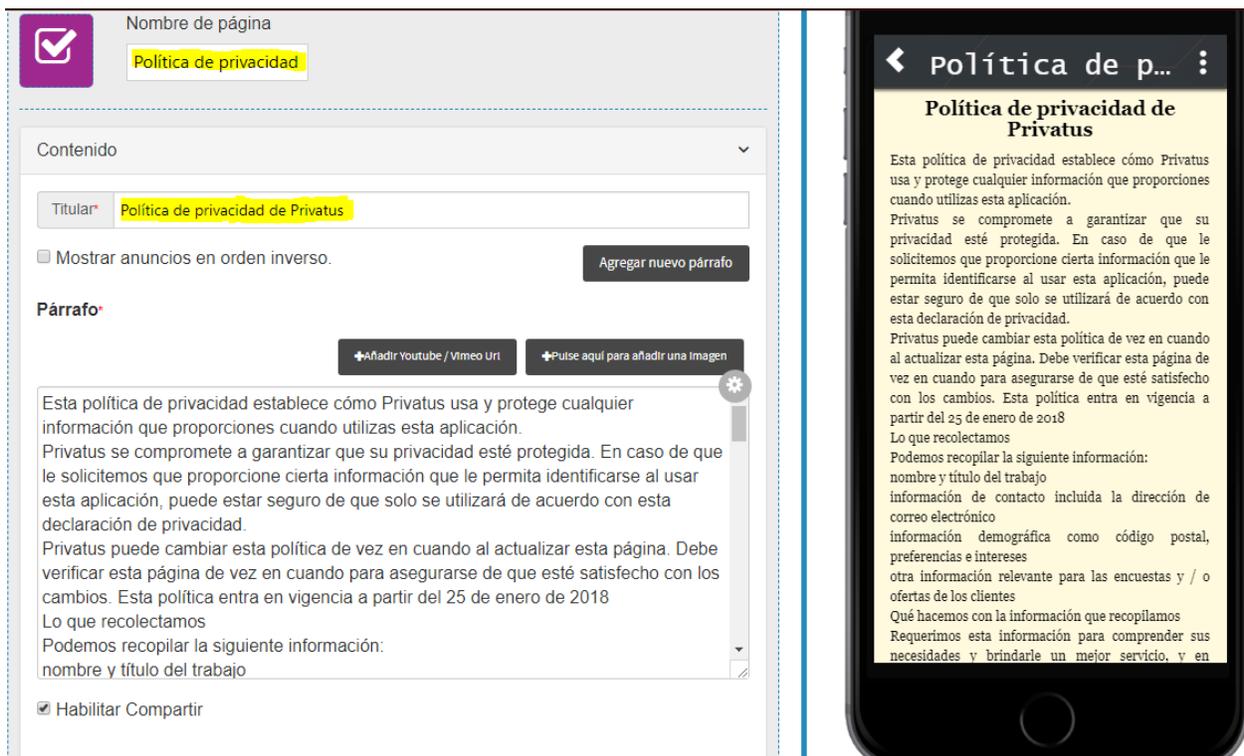


Figura 17. Políticas de privacidad.

Con la implementación de todas las páginas del Frontend (Aplicación) y Backend (**CMS Content Managment System**) de la aplicación se da cumplimiento a los requerimientos de rendimiento que definen que la aplicación debe tener un diseño y entorno funcional y usable para el usuario y también se da cumplimiento con el requerimiento de confiabilidad que propone que la aplicación debe manejar fuentes del alfabeto en español.

Las figuras que se presentan a continuación muestran la otra parte del **Backend de la Aplicación Privatus** correspondiente al **CMS** de gestión de la encuesta a través de la Plataforma **Type Form**.

En la **Figura 18** se muestra la interfaz de creación de formulario de la plataforma **Type Form**, que es una plataforma amigable con el usuario, de fácil uso, con una amplia gama de funcionalidades, las cuales cumplen con lo necesario para cubrir los requerimientos planteados para la Aplicación Privatus. Haciendo uso de esta funcionalidad de creación de formularios, se crea la evaluación (**instrumento de medición**) utilizando el instrumento con las 40 situaciones presentadas en el **Anexo 1**.

T > Privatus Evaluation App **Crear** Integrar Compartir Resultados Guardado Ver Hazte PRO+ A

BLOQUES

- Pantalla de Bienvenida
- Pantalla Final
- Elección Múltiple
- Respuesta corta
- Respuesta larga
- Texto
- Elección de Imágenes
- Si/No
- Email
- Escala de Opinión
- Puntuación
- Fecha
- Número

Evaluáte tú mismo

Recuerda que esta encuesta es para evaluarte a ti mismo, así que se muy sincero con tus respuestas

* 1 Dirección de correo electrónico

Enviaremos los resultados de la evaluación a tu correo al terminar.

2 Parte 1 Variables demográficas

La primera recoge información estadística respecto a aspectos demográficos, personales y mediciones generales en cuanto uso de Internet.

* 2a Edad

- 16-25
- 26-35
- 36-45
- 46-55
- Mayor de 55

Evaluáte tú mismo

Recuerda que esta encuesta es para evaluarte a ti mismo, así que se muy sincero con tus respuestas

Iniciar pulsa INTRO

Figura 18. Crear formulario.

En la **Figura 19** se muestra la funcionalidad compartir de la plataforma **Type Form**, a través de la cual es posible la interacción con la Plataforma **Appy Pie** y que la evaluación pueda ser vista y diligenciada por el usuario desde la aplicación utilizando código **HTML con Javascript** generado por la funcionalidad compartir. Es posible insertar el código generado dentro de la función Codepage de la plataforma Appy pie y así obtener la interacción completa de las dos plataformas. Esta funcionalidad en integración con la página **Evalúate** del **CMS** de la aplicación da cumplimiento a los requerimientos de rendimiento que propone implementar una correcta integración entre la base de datos y la aplicación para garantizar el óptimo rendimiento del sistema.

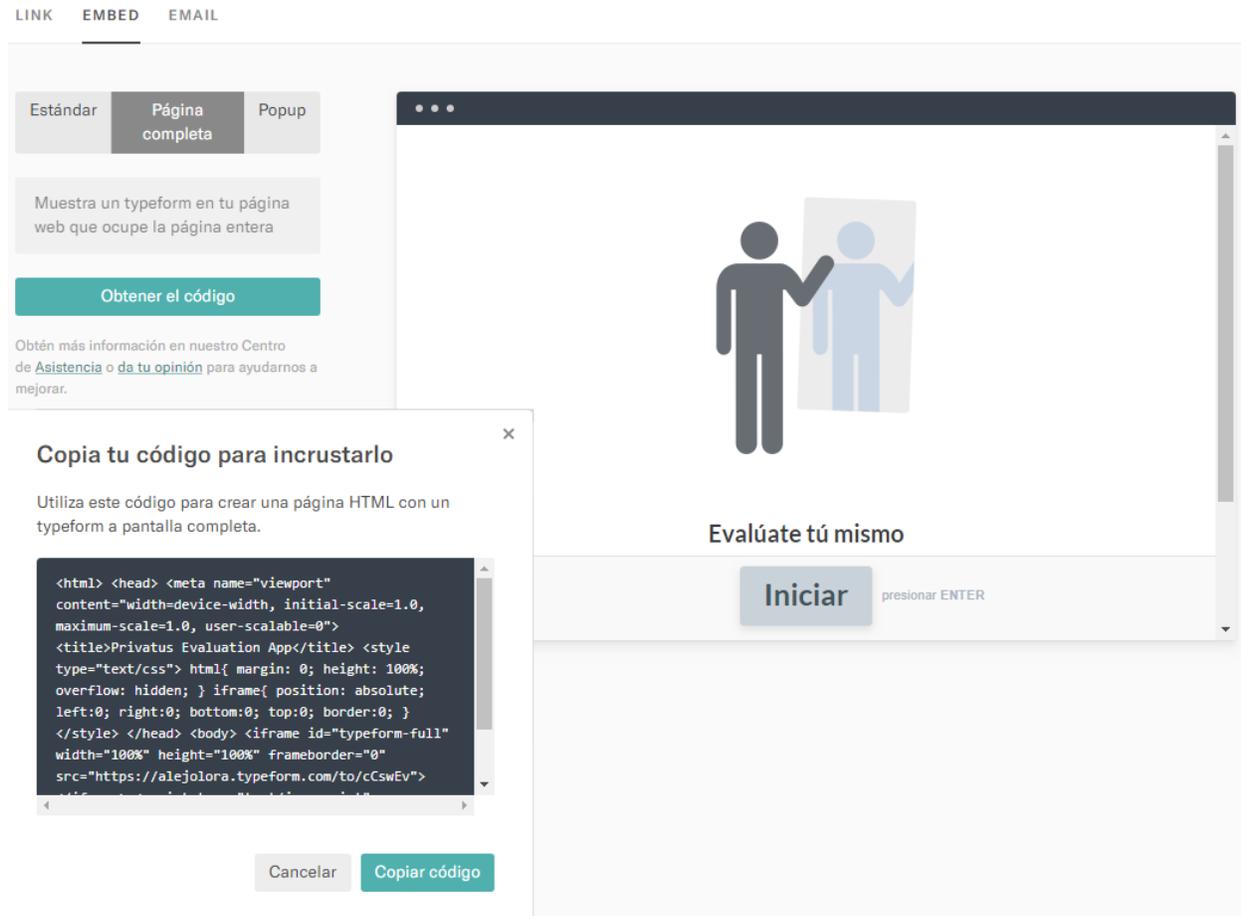


Figura 19. Compartir.

En la **Figura 20** se muestra la funcionalidad de resultados, las cuales abarca las funciones de consultar estadísticas detalladas, generales, individuales de la **Aplicación Privatus**. Esta funcionalidad permite generar reportes generales o individuales y hacer una gestión completa de la información de respuestas almacenadas en la plataforma, también ofrece una variedad de funciones en las cuales está la presentación de estadísticas y resultados.



RESUMEN INGLÉS RESPUESTAS

Fecha

1. Dirección de correo ...

Cualquier fecha

Buscar respuestas

- 61 respuestas en total
- 8 de mayo de 2018 [redacted]@[redacted].com
- 5 de mayo de 2018 [redacted]@gmail.com
- 4 de mayo de 2018 [redacted]@yahoo.es
- 4 de mayo de 2018 [redacted]@gmail.com
- 4 de mayo de 2018 [redacted]@hotmail.com
- 4 de mayo de 2018 [redacted]@hotmail.com
- 4 de mayo de 2018 [redacted]@gmail.com

Descargar todas las respuestas

8 de mayo de 2018 09:29 p.m.

1 Dirección de correo electrónico

[redacted]@[redacted].com

2 Parte 1 Variables demográficas

1a Edad
26-35

2b Género
Masculino

3a Estrato socioeconómico según escala de clasificación

Figura 20. Función Resultados.

6.2.3 Pruebas de funcionalidad

Esta sección describe las pruebas de funcionalidad y ajustes que se realizaron a la aplicación antes de ser lanzada y desplegada para ser descargada.

Con la aplicación terminada y todas las funcionalidades planeadas se realizan pruebas de funcionalidad. Para esto el autor del presente trabajo contacta con dos profesionales para que realicen pruebas de funcionalidad a la aplicación: un Ingeniero de Sistemas y un Abogado, José Antonio Tovar ingeniero de sistemas y programador con experiencia en desarrollo en de interfaces para aplicaciones web y de escritorio y Luis Felipe Lora, abogado trabaja en la gobernación de Nariño con experiencia en derechos humanos y de trabajo.

El ingeniero de sistemas realiza pruebas de funcionalidad comprobando que todas las funciones se ejecuten correctamente, también realiza aportes sobre el diseño gráfico de la aplicación, recomendando cambiar el diseño de funciones como la página de inicio, el formato de autoevaluación y la página de recomendaciones para que estas sean amigables y fáciles de interactuar con el usuario final.

El Abogado se encarga de evaluar el contenido de la aplicación desde los términos y condiciones, políticas de privacidad, formulario de autoevaluación e instrucciones de uso de la aplicación, haciendo recomendaciones para mejorar y optimizar las preguntas del formulario de autoevaluación para que sean más entendibles para el usuario final. También comprobó que las paginas informativas de políticas de privacidad y términos y condiciones estuvieran acordes a como establece la ley.

Una vez terminadas de hacer estas pruebas de funcionalidad, de corregir los errores encontrados y aplicar los cambios sugeridos por los dos profesionales, la aplicación esta lista para ser subida a las plataformas de Apps como Google Play y ser descargada por el usuario final.

6.3 Desplegar el prototipo de aplicación móvil.

En este capítulo se describe el proceso de liberación, instalación, seguimiento durante un mes y documentación de la aplicación Privatus.

6.3.1 Instalación y liberación de la aplicación.

Cuando la Aplicación esta lista para ser liberada después de haber pasado por el proceso de pruebas, correcciones, y mejoras, el siguiente paso es subir la aplicación a la plataforma de Apps de Google llamada Play Store para que puede ser descargada por cualquier usuario que tenga un celular con sistema operativo Android con cualquier versión hasta mayo de 2018, mes hasta que funcionó la aplicación. A continuación, se describe el proceso para liberar e instalar la aplicación.

1. Google Play Developer Console

Es la plataforma de Google creada para los desarrolladores de Aplicaciones. La **Figura 21** muestra la pantalla de registro y para acceder a ella hay que realizar los siguientes pasos:

- Registrarse para obtener una cuenta de desarrollador de Google Play.
- Aceptar el Acuerdo de Distribución para Desarrolladores.
- Paga la cuota de registro. es un valor que marca Google a todas las cuentas de desarrollador. Se realiza un único pago de 25 dólares.
- Incluir la información de la cuenta. Elegir un nombre de desarrollador que se mostrará a los clientes en Google Play.

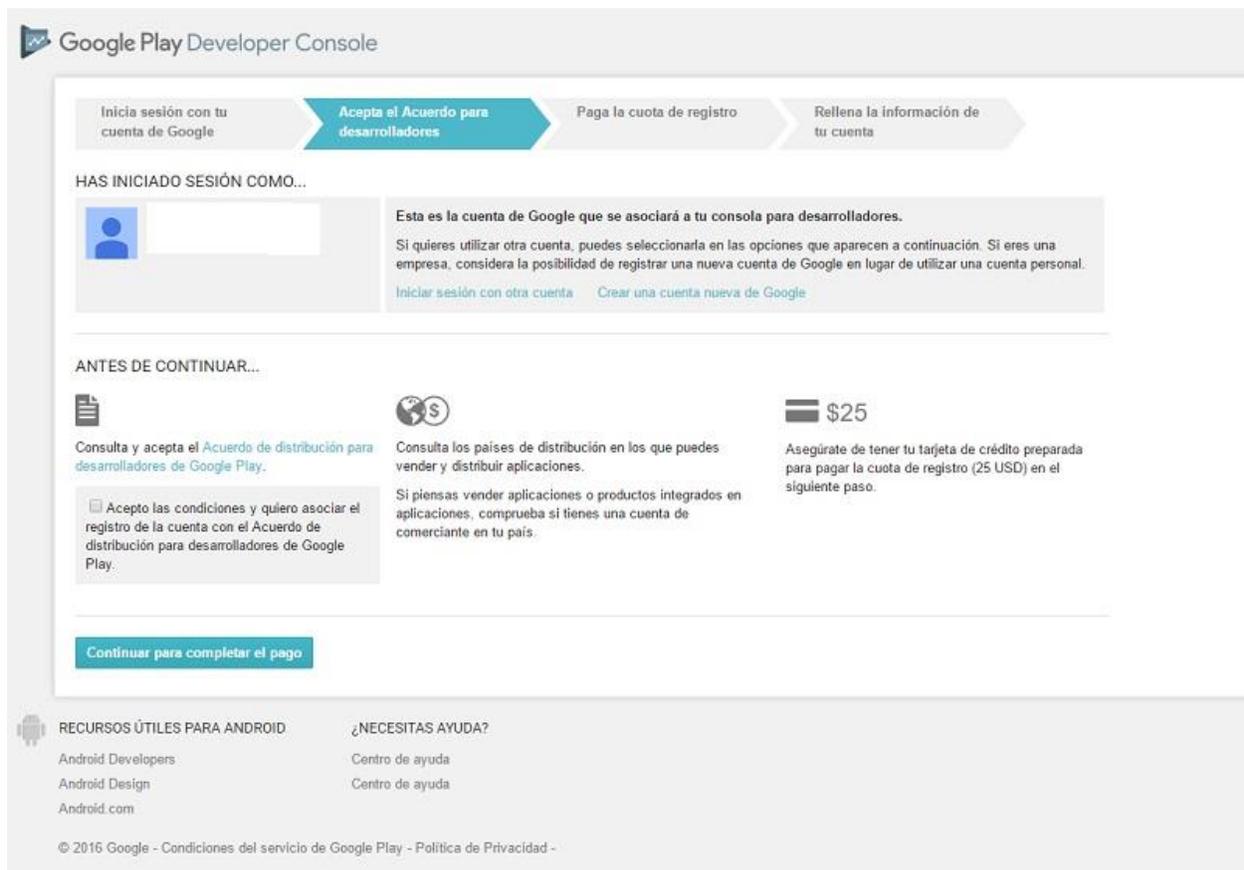


Figura 21. Google Play Developer Console (Antevenio, 2018).

2. Añadir una nueva aplicación

Después de crear la cuenta en Google Play Developer Console, se procede a subir la aplicación. Este paso consiste en subir los archivos APK, como se indica en la **Figura 22**. En el menú **Tus aplicaciones** se selecciona la opción de **Añadir nueva aplicación** y realizar lo siguiente:

1. En el menú desplegable, seleccionar idioma español.
2. Elegir el nombre de la aplicación, para el caso de esta investigación: Privatus.
3. Seleccionar Subir APK.
4. **Elegir entre los canales de producción, beta o alfa.** para el caso de la presente aplicación se selecciona la versión Alfa; Debido a que es la versiona final.
5. Seleccionar el archivo y **subir archivo APK.**

Después de subir el APK, al lado aparece un tick verde. Esto indica que Google da el visto bueno para publicar la Aplicación.

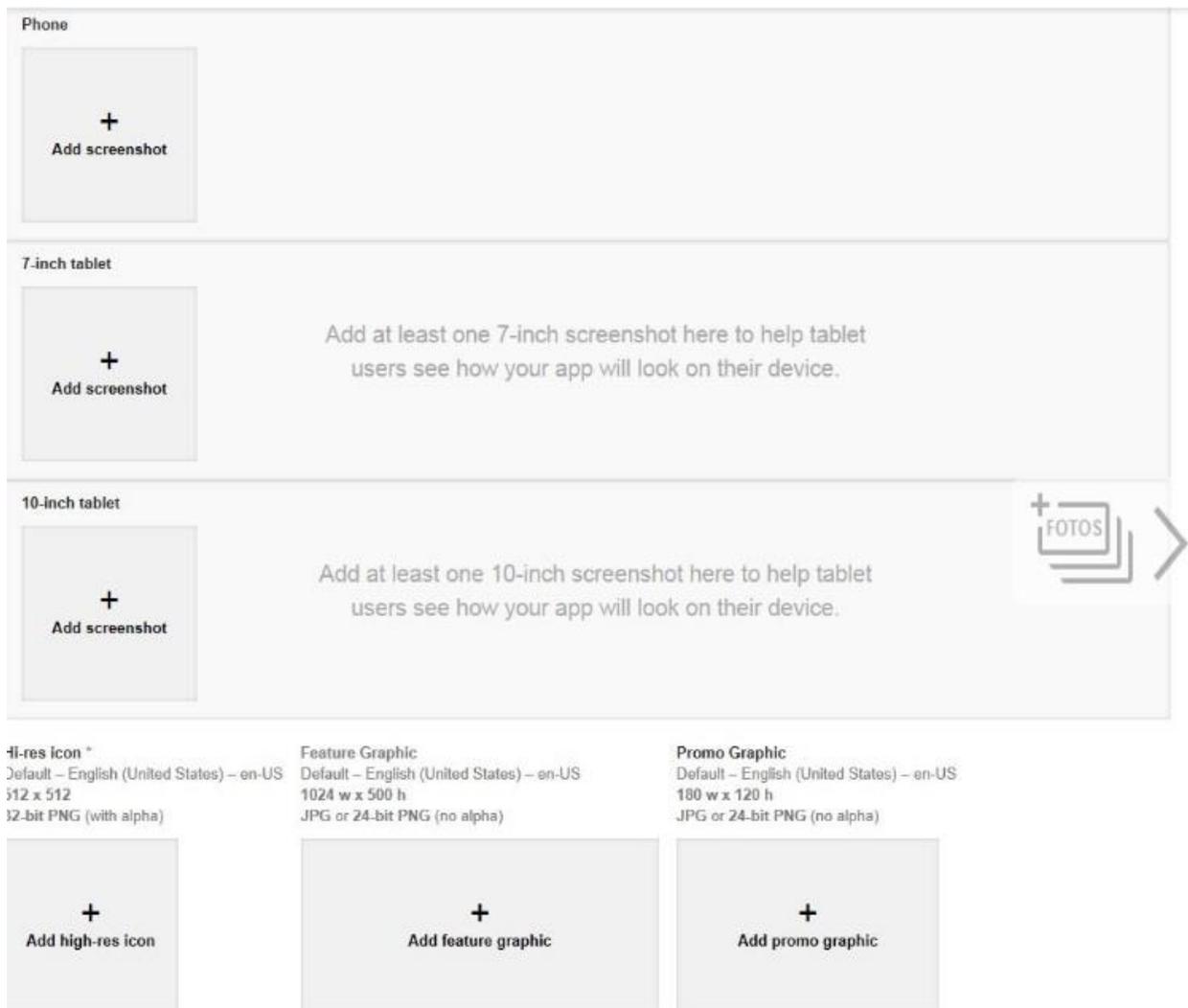


Figura 22. Añadir aplicación (Antevenio, 2018).

Cuando la Aplicación sea finalmente publicada aparece en la pantalla principal de **Google Play Console Developer** como muestra la **Figura 23** y el usuario final ya puede descargarla en su celular.

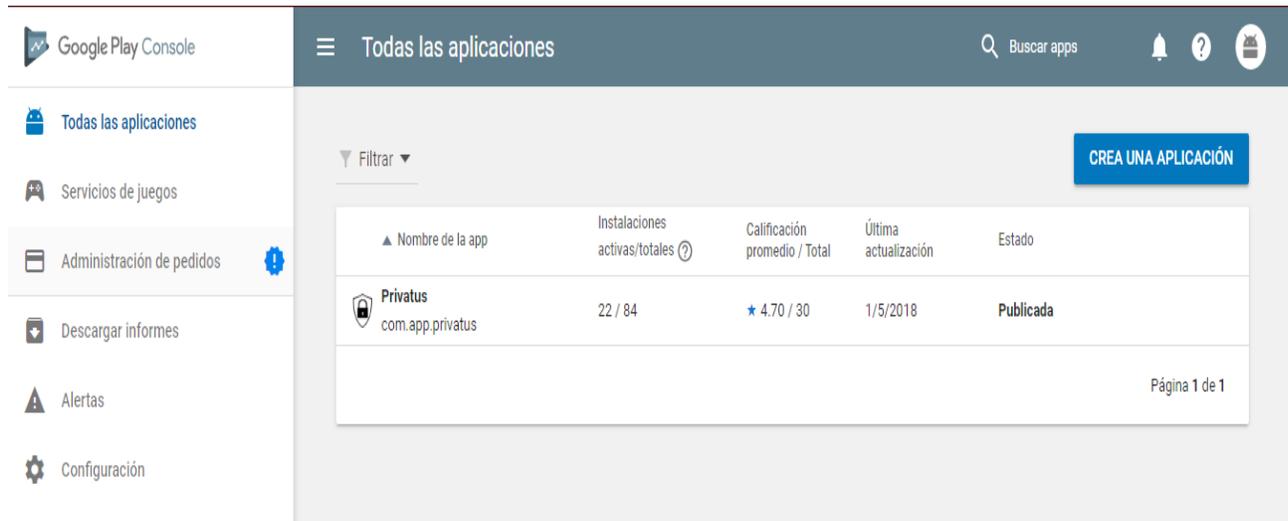


Figura 23. Pantalla principal Google Console.

3. Instalación de la aplicación

Finalmente, para instalar la aplicación en el celular con sistema operativo Android el usuario accede a la Play Store de Android y busca la aplicación, con el nombre Privatus, como se muestra en a **Figura 24**. Se aceptan los términos condiciones y se instala como cualquier aplicación descargada desde la Play Store.

Al momento de contactar con los usuarios que decidieron participar en la investigación, se les explico el propósito de la aplicación y que esta forma parte de un proyecto de investigación, así como de un trabajo de grado, después se envió a los usuarios el link el cual direcciona directamente a la ficha de la aplicación en la Play Store de Google para garantizar que no se descargue ninguna otra aplicación parecida o algún homónimo de esta. Durante la liberación de la aplicación no se encontraron homónimos.

Cuando el usuario accede por primera vez a la aplicación se muestra la pantalla de términos y condiciones, en donde se le explica al usuario nuevamente el propósito de la aplicación, de la encuesta, así como se menciona que los datos recolectados serán utilizados para fines académicos, los cuales solo serán accedidos por personas relacionadas por la investigación, se puede consultar los términos y condiciones en el **Anexo 6**.



Figura 24. Vista Previa Privatus.

6.3.2 Reportes y estadísticas del uso de la aplicación durante el mes de seguimiento

En esta sección se describe y presenta las estadísticas de uso generadas por distintas herramientas de análisis de datos en línea con las que se realizó el seguimiento a la aplicación Privatus durante un mes, desde el primero de mayo hasta el 31 de mayo del 2018. Se emplearon herramientas como Google Analytics, Estadísticas de Google console Developer y las estadísticas de uso generadas por las plataformas Appy Pie y Type Form.

Dentro de los datos recopilados y estadísticas de uso se analizaron datos como: número de instalaciones, lugares en los que se realizaron instalaciones, tiempo de uso de la aplicación, comentarios y calificación de la aplicación, dispositivos en los que fue instalada la aplicación, así como los datos estadísticos de los resultados de las evaluaciones que generaron los usuarios. La presentación de estos reportes, datos y estadísticas da cumplimiento al requerimiento no funcional de confiabilidad que propone que el sistema debe tener una disponibilidad del 99,99% de las veces en que un usuario intente accederlo debido a que la aplicación esta subida en la plataforma **Play store de Google** y corre sobre los servidores de **Appy Pie**, Estos servicios están diseñados para estar siempre en ejecución y cuentan con servidores de respaldo para garantizar a los usuarios el principio de disponibilidad.

La población que descargó y utilizó la aplicación constituye una población heterogénea de distintas edades, ubicadas en diferentes lugares de Colombia, ciudades principales como Medellín, Cali, Bogotá, Pasto, Pereira Manizales y Popayán como se detalla en las siguientes secciones.

6.3.2.1 Estadísticas Generadas por Google Analytics

Información general del uso de la aplicación

La **Figura 25** se presenta el informe que presenta Google Analytics en la estadística de datos generales con ubicaciones, en cuanto al informe se puede inferir que:

- Hubo un total de 162 usuarios que interactuaron con la aplicación en el mes de mayo del año 2018.
- Se realizaron 205 sesiones, entendiendo que una sesión es el tiempo que un usuario interactúa con la aplicación.
- Se realizaron 458 visualizaciones de pantalla con un promedio de visualización de 2.23 pantallas por sesión.
- La duración media de cada sesión comprende un tiempo de 10 minutos con 33 segundos.
- El 78.54 % de las sesiones durante el mes fueron sesiones nuevas de nuevos usuarios.
- Las ciudades desde donde hubo interacción con la aplicación son: Pasto, Cali, Medellín, Bogotá, Ibagué, Manizales, Pereira, Popayán, Portoviejo (Ecuador).

Visión general de los usuarios

Todos los usuarios
 100,00 % Usuarios

1 may. 2018 - 31 may. 2018

Visión general



Ciudad	Usuarios	% Usuarios
1. Pasto	43	25,90 %
2. Cali	37	22,29 %
3. Medellin	35	21,08 %
4. Bogota	19	11,45 %
5. (not set)	8	4,82 %
6. Ibague	5	3,01 %
7. Manizales	2	1,20 %
8. Pereira	2	1,20 %
9. Popayan	2	1,20 %
10. Portoviejo	2	1,20 %

Figura 25. Información general del uso de la aplicación.

Ubicación de los usuarios

Las Figuras 26 y 27 muestran las ciudades y departamentos en Colombia desde donde los usuarios interactuaron con la aplicación. Se aclara que los usuarios que participaron durante la ejecución de este trabajo son amigos, familiares y profesores UPB con alguna relación con el autor de la presente investigación, que voluntariamente accedieron a instalar e interactuar con la aplicación. Estas figuras hacen parte del reporte de **Google Analytics** y se puede inferir que las ciudades con más interacción de usuarios con la Aplicación Privatus son: Pasto con 43 usuarios, Cali con 37 usuarios, Medellín con 35 usuarios y Bogotá con 19 usuarios.

Ciudad	Usuarios	Usuarios nuevos	Sesiones	Visualizaciones de pantalla	Pantallas/sesión	Duración media de la sesión
	162 % del total: 100,00 % (162)	164 % del total: 101,86 % (161)	205 % del total: 100,00 % (205)	458 % del total: 100,00 % (458)	2,23 Media de la vista: 2,23 (0,00 %)	00:10:33 Media de la vista: 00:10:33 (0,00 %)
1. Pasto	43 (25,90 %)	42 (25,61 %)	52 (25,37 %)	161 (35,15 %)	3,10	00:14:22
2. Cali	37 (22,29 %)	37 (22,56 %)	49 (23,90 %)	83 (18,12 %)	1,69	00:09:20
3. Medellín	35 (21,08 %)	35 (21,34 %)	49 (23,90 %)	96 (20,96 %)	1,96	00:11:17
4. Bogotá	19 (11,45 %)	18 (10,98 %)	19 (9,27 %)	26 (5,68 %)	1,37	00:07:45
5. (not set)	8 (4,82 %)	8 (4,88 %)	8 (3,90 %)	52 (11,35 %)	6,50	00:02:38
6. Ibagué	5 (3,01 %)	4 (2,44 %)	6 (2,93 %)	10 (2,18 %)	1,67	00:10:10
7. Manizales	2 (1,20 %)	2 (1,22 %)	2 (0,98 %)	3 (0,66 %)	1,50	00:22:30
8. Pereira	2 (1,20 %)	3 (1,83 %)	5 (2,44 %)	4 (0,87 %)	0,80	00:05:16
9. Popayan	2 (1,20 %)	2 (1,22 %)	2 (0,98 %)	4 (0,87 %)	2,00	00:12:53
10. Portoviejo	2 (1,20 %)	2 (1,22 %)	2 (0,98 %)	3 (0,66 %)	1,50	00:04:32

Figura 26. Ubicaciones por ciudad.

Región	Usuarios	Usuarios nuevos	Sesiones	Visualizaciones de pantalla	Pantallas/sesión	Duración media de la sesión
	149 % del total: 91,98 % (162)	151 % del total: 93,79 % (161)	192 % del total: 93,66 % (205)	400 % del total: 87,34 % (458)	2,08 Media de la vista: 2,23 (-6,75 %)	00:11:04 Media de la vista: 00:10:33 (4,93 %)
1. Nariño	43 (28,10 %)	42 (27,81 %)	52 (27,08 %)	161 (40,25 %)	3,10	00:14:22
2. Valle del Cauca	39 (25,49 %)	39 (25,83 %)	51 (26,56 %)	88 (22,00 %)	1,73	00:09:29
3. Antioquia	35 (22,88 %)	35 (23,18 %)	49 (25,52 %)	96 (24,00 %)	1,96	00:11:17
4. Bogotá	19 (12,42 %)	18 (11,92 %)	19 (9,90 %)	26 (6,50 %)	1,37	00:07:45
5. Tolima	5 (3,27 %)	4 (2,65 %)	6 (3,12 %)	10 (2,50 %)	1,67	00:10:10
6. Caldas	4 (2,61 %)	4 (2,65 %)	4 (2,08 %)	5 (1,25 %)	1,25	00:11:17
7. Atlántico	2 (1,31 %)	2 (1,32 %)	2 (1,04 %)	2 (0,50 %)	1,00	00:03:22
8. Bolívar	2 (1,31 %)	2 (1,32 %)	2 (1,04 %)	4 (1,00 %)	2,00	00:14:38
9. Risaralda	2 (1,31 %)	3 (1,99 %)	5 (2,60 %)	4 (1,00 %)	0,80	00:05:16
10. Cauca	2 (1,31 %)	2 (1,32 %)	2 (1,04 %)	4 (1,00 %)	2,00	00:12:53

Figura 27. Ubicaciones por departamento.

Información General de los dispositivos y red

La **Figura 28** muestra métricas como las versiones del sistema operativo Android que más se usaron para interactuar con la aplicación Privatus, los principales operadores de red a través de los cuales los usuarios se conectaron para interactuar con la aplicación, los modelos de dispositivos que más se utilizaron para interactuar con la aplicación, marcas de dispositivo móviles que más se utilizaron para interactuar con la aplicación entre otras. De la **Figura 28** se puede inferir que:

- Las versiones del sistema operativo más utilizadas para interactuar con la aplicación en orden de más utilizada a menos utilizada son:
 - Android 7.0
 - Android 6.0
 - Android 6.0.1
 - Android 5.1.1
 - Android 7.1.1
 - Android 4.4.2
- Los principales operadores de red más utilizados para conectarse a la aplicación en orden de más utilizado a menos utilizado fueron:
 - Telmex colombia S.A.
 - EPM Telecomunicaciones S.A. E.S.P.
 - Colombia Telecomunicaciones S.A. E.S.P
 - Google llc
 - Comcel S.A.
 - Colombia móvil
- Los modelos de dispositivos móviles más utilizados por los usuarios para interactuar con la aplicación en orden de más utilizado a menos utilizado fueron:
 - Huawei P8 Lite 6 Usuarios con 3,70 %
 - Motorola Moto G (5) Plus 6 Usuarios 3,70 %
 - Samsung Galaxy J5 6 Usuarios 3,70 %
 - Motorola Moto G4 Play 5 Usuarios 3,09 %
 - Otras 125 Usuarios 77,16 %
 - Dispositivo no reconocido 14 Usuarios 8,64 %
- Las marcas de dispositivos móviles más utilizadas que interactuaron con la aplicación en orden de más utilizada a menos utilizada son:
 - Samsung 49 usuarios
 - Huawei 33 usuarios
 - Motorola 26 usuarios
 - Sony 15 usuarios

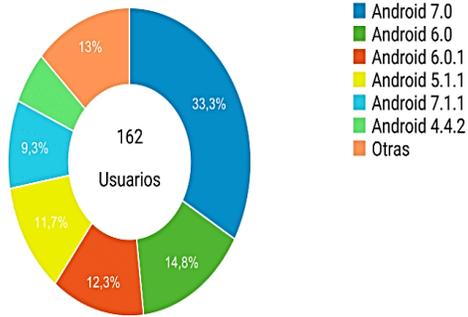
Información general de dispositivos y red

Todos los usuarios
 100,00 % Usuarios (100,00 % Usuarios nuevos)

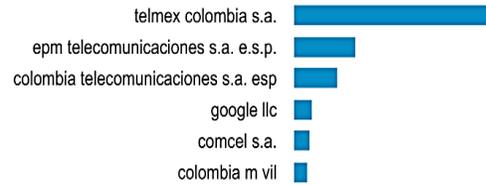
1 may. 2018 - 31 may. 2018

Métricas clave

Versiones del SO



Principales operadores de red



Modelos de dispositivos principales



Resolución de pantalla	Usuarios	Método de entrada del móvil	Usuarios	Marca del dispositivo móvil	Usuarios
(not set)	88	touchscreen	148	Samsung	49
360x640	55	(not set)	12	Huawei	33
320x534	4			Motorola	26
360x604	2			Sony	15
412x732	2			(not set)	12

Figura 28. Información general de dispositivos y red.

Versiones del SO (Sistema Operativo)

En la **Figura 29** se presentan las versiones que se utilizaron para interactuar con la aplicación

- De los 162 usuarios que utilizaron la aplicación Privatus en sistema operativo Android se puede observar que:
 - 33.3% utilizaron Android 7.0 equivalente a 54 usuarios
 - 14.8% utilizaron Android 6.0 equivalente a 24 usuarios
 - 12.3% utilizaron Android 6.0.1 equivalente a 20 usuarios
 - 11.7% utilizaron Android 5.1.1 equivalente a 19 usuarios
 - 9.3% utilizaron Android 7.1.1 equivalente a 15 usuarios
 - 5.6% utilizaron Android 4.4.2 equivalente a 9 usuarios
 - 3.75% utilizaron Android 5.1 equivalente a 6 usuarios
 - 3.75% utilizaron Android 8.0.0 equivalente a 6 usuarios
 - 1.25% utilizaron Android 4.4.4 equivalente a 2 usuarios
 - 1.25% utilizaron Android 5.0.1 equivalente a 2 usuarios
 - 1.25% utilizaron Android 5.0.2 equivalente a 2 usuarios
 - 0.62% utilizaron Android 4.1.2 equivalente a 1 usuarios

<input type="checkbox"/>	Versión del sistema operativo ?	Usuarios ? ↓	Usuarios nuevos ?	Sesiones ?	Visualizaciones de pantalla ?	Pantallas/sesión ?	Duración media de la sesión ?
		160 % del total: 98,77 % (162)	162 % del total: 100,62 % (161)	202 % del total: 98,54 % (205)	458 % del total: 100,00 % (458)	2,27 Media de la vista: 2,23 (1,49 %)	00:10:34 Media de la vista: 00:10:33 (0,15 %)
<input type="checkbox"/>	1. 7.0	54 (33,75 %)	54 (33,33 %)	60 (29,70 %)	112 (24,45 %)	1,87	00:10:36
<input type="checkbox"/>	2. 6.0	24 (15,00 %)	24 (14,81 %)	28 (13,86 %)	49 (10,70 %)	1,75	00:07:52
<input type="checkbox"/>	3. 6.0.1	20 (12,50 %)	20 (12,35 %)	20 (9,90 %)	60 (13,10 %)	3,00	00:16:10
<input type="checkbox"/>	4. 5.1.1	19 (11,88 %)	19 (11,73 %)	28 (13,86 %)	71 (15,50 %)	2,54	00:16:09
<input type="checkbox"/>	5. 7.1.1	15 (9,38 %)	17 (10,49 %)	21 (10,40 %)	38 (8,30 %)	1,81	00:05:52
<input type="checkbox"/>	6. 4.4.2	9 (5,62 %)	9 (5,56 %)	26 (12,87 %)	65 (14,19 %)	2,50	00:07:04
<input type="checkbox"/>	7. 5.1	6 (3,75 %)	6 (3,70 %)	6 (2,97 %)	13 (2,84 %)	2,17	00:08:01
<input type="checkbox"/>	8. 8.0.0	6 (3,75 %)	6 (3,70 %)	6 (2,97 %)	34 (7,42 %)	5,67	00:09:43
<input type="checkbox"/>	9. 4.4.4	2 (1,25 %)	2 (1,23 %)	2 (0,99 %)	6 (1,31 %)	3,00	00:12:38
<input type="checkbox"/>	10. 5.0.1	2 (1,25 %)	2 (1,23 %)	2 (0,99 %)	7 (1,53 %)	3,50	00:09:29
<input type="checkbox"/>	11. 5.0.2	2 (1,25 %)	2 (1,23 %)	2 (0,99 %)	3 (0,66 %)	1,50	00:16:19
<input type="checkbox"/>	12. 4.1.2	1 (0,62 %)	1 (0,62 %)	1 (0,50 %)	0 (0,00 %)	0,00	00:12:17

Figura 29. Versiones del SO.

Datos por dispositivo

La **Figura 30** muestra la marca de celulares y dispositivos con sistema operativo Android que descargaron la aplicación. Se comprueba que la aplicación funcionó en diferentes marcas de dispositivos. La marca de dispositivos que más instalaron la aplicación fue Samsung con un total de 49 instalaciones.

Marca del dispositivo móvil	Usuarios	Usuarios nuevos	Sesiones	Visualizaciones de pantalla	Pantallas/sesión	Duración media de la sesión
	160 % del total: 98,77 % (162)	162 % del total: 100,62 % (161)	202 % del total: 98,54 % (205)	458 % del total: 100,00 % (458)	2,27 Media de la vista: 2,23 (1,49 %)	00:10:34 Media de la vista: 00:10:33 (0,15 %)
1. Samsung	49 (30,62 %)	49 (30,25 %)	51 (25,25 %)	94 (20,52 %)	1,84	00:14:11
2. Huawei	33 (20,62 %)	33 (20,37 %)	56 (27,72 %)	122 (26,64 %)	2,18	00:07:44
3. Motorola	26 (16,25 %)	26 (16,05 %)	27 (13,37 %)	57 (12,45 %)	2,11	00:09:39
4. Sony	15 (9,38 %)	15 (9,26 %)	19 (9,41 %)	49 (10,70 %)	2,58	00:12:03
5. (not set)	12 (7,50 %)	12 (7,41 %)	14 (6,93 %)	19 (4,15 %)	1,36	00:07:11
6. Lenovo	9 (5,62 %)	11 (6,79 %)	19 (9,41 %)	63 (13,76 %)	3,32	00:17:03
7. LG	7 (4,38 %)	7 (4,32 %)	7 (3,47 %)	8 (1,75 %)	1,14	00:02:03
8. Alcatel	2 (1,25 %)	2 (1,23 %)	2 (0,99 %)	6 (1,31 %)	3,00	00:12:38
9. Asus	2 (1,25 %)	2 (1,23 %)	2 (0,99 %)	2 (0,44 %)	1,00	00:00:00
10. Google	2 (1,25 %)	2 (1,23 %)	2 (0,99 %)	27 (5,90 %)	13,50	00:04:29
11. ProntoTec	2 (1,25 %)	2 (1,23 %)	2 (0,99 %)	4 (0,87 %)	2,00	00:06:20
12. Xiaomi	1 (0,62 %)	1 (0,62 %)	1 (0,50 %)	7 (1,53 %)	7,00	00:02:12

Figura 30. Datos por dispositivo.

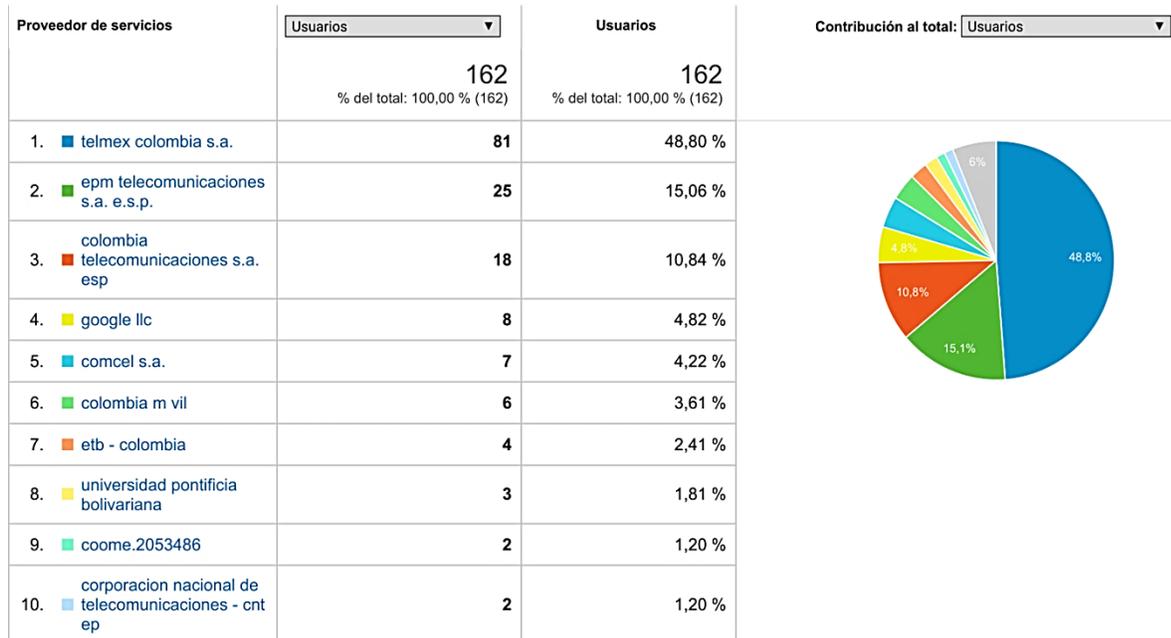


Figura 31. Datos por red.

Duración de la sesión

La **Figura 32** muestra el reporte sobre las sesiones, la cantidad, duración de las sesiones, pantallas por sesión y una clasificación de las sesiones según el tiempo de uso por cada usuario. De la **Figura 32** se puede inferir:

- Se realizaron un total de 205 sesiones durante el mes de mayo de 2018, durante el cual se le hizo seguimiento a la aplicación Privatus.
- La duración media de cada sesión fu de 10 minutos con 33 segundos por usuario.
- El número promedio de pantallas por sesión que los usuarios visualizaron por sesión fue de 2.23.
- Hubo 17 sesiones las cuales duraron más de 30 minutos, con un promedio de duración de 41 minutos con 25 segundos en promedio.
- Hubo 74 sesiones con una duración entre 10 y 30 minutos con un promedio de duración de la sesión de 15 minutos 37 segundos.

Duración de la sesión

Todos los usuarios
 100,00 % Usuarios (100,00 % Sesiones)

1 may. 2018 - 31 may. 2018

Distribución

Duración de la sesión

Sesiones	Duración media de la sesión	Pantallas/sesión	Tasa de conversión del objetivo
205 % del total: 100,00 % (205)	00:10:33 Media de la vista: 00:10:33 (0,00 %)	2,23 Media de la vista: 2,23 (0,00 %)	0,00 % Media de la vista: 0,00 % (0,00 %)

Duración de la sesión	Sesiones	Duración media de la sesión	Pantallas/sesión	Tasa de conversión del objetivo
0-10 segundos	45	00:00:01	0,96	0,00 %
11-30 segundos	8	00:00:21	1,75	0,00 %
31-60 segundos	5	00:00:48	2,60	0,00 %
61-180 segundos	19	00:01:56	3,00	0,00 %
181-600 segundos	37	00:06:58	1,76	0,00 %
601-1800 segundos	74	00:15:37	2,57	0,00 %
1801+ segundos	17	00:41:25	4,47	0,00 %

Figura 32. Duración de la sesión.

Datos de las pantallas

La **Figura 33** muestra el informe de Google Analytics sobre el uso de las pantallas de la aplicación como número de visualizaciones de pantalla, visitas únicas a la pantalla, tiempo medio de duración por pantalla. De la información presentada en la **Figura 33** se puede inferir:

- Hay un total de 458 visualizaciones de pantallas en total.
- Hay un total de 316 visitas únicas a alguna de las pantallas de la aplicación.
- El tiempo promedio de duración en las pantallas es de 3 minutos 33 segundos.
- La pantalla más visualizada es la pantalla de **Inicio**, es la pantalla principal, contiene las instrucciones de uso de la aplicación, con 154 visualizaciones de pantalla, 97 visitas únicas y un promedio de tiempo en la pantalla de 1 minuto 3 segundos.
- La pantalla **Evalúate** ocupa la segunda casilla en visualizaciones, es la pantalla que contiene el formulario de autoevaluación para el usuario, con 126 visualizaciones de pantalla en total, 92 visitas únicas, y un promedio de duración en la pantalla de 7 minutos con 54 segundos, esta es la página con mayor tiempo de permanencia de los usuarios, lo cual demuestra que los usuarios realizaron la encuesta con interés y de forma correcta.
- La pantalla **Recomendaciones** ocupa la tercera casilla en visualizaciones, pantalla que contiene las recomendaciones y consejos sobre privacidad en línea, se divide en 3 grupos despreocupados, indiferentes, y alarmados, con 99 visualizaciones de pantalla en total, 62

visitas únicas a la pantalla y una duración en la pantalla promedio de 2 minutos 29 segundos.

- La pantalla **Estadísticas** ocupa la cuarta casilla en número de visualizaciones, pantalla que muestra a los usuarios los resultados en forma general de todas las respuestas obtenidas en las evaluaciones, para que el usuario pueda hacer una comparación de su propio resultado con los resultados generales, 50 visualizaciones de pantalla en total, 43 visitas únicas a la pantalla, y una duración promedio en la pantalla de 3 minutos y 10 segundos.
- la pantalla **Términos y condiciones**, ocupa el sexto lugar en visualizaciones, pantalla informativa que contiene los términos y condiciones de uso de la aplicación, con 11 visitas en total, 10 visitas únicas, y una duración promedio en la pantalla de 3 minutos 57 segundos.
- La pantalla de **Políticas de privacidad** ocupa el séptimo y último lugar en número de visualizaciones con un total de 5 visualizaciones de pantalla, 5 visitas únicas, y un promedio de duración en la pantalla de 37 segundos, de esto se puede inferir que los usuarios que usaron la aplicación no están interesados en conocer a profundidad las políticas de privacidad.

Nombre en pantalla	Visualizaciones de pantalla	Visitas únicas a una pantalla	Media. El tiempo en la pantalla	Porcentaje de salidas
	458 % del total: 100,00 % (458)	316 % del total: 100,00 % (316)	00:03:33 Media de la vista: 00:03:33 (0,00 %)	33,39 % Media de la vista: 33,39 % (0,00 %)
1. Inicio	154 (33,62 %)	97 (30,70 %)	00:01:03	18,18 %
2. Evalúate	126 (27,51 %)	92 (29,11 %)	00:07:54	25,40 %
3. Recomendaciones	99 (21,62 %)	62 (19,62 %)	00:02:29	38,38 %
4. Estadísticas	50 (10,92 %)	43 (13,61 %)	00:03:10	34,00 %
5. Estadísticas	13 (2,84 %)	7 (2,22 %)	00:03:04	15,38 %
6. Terminos y Condiciones	11 (2,40 %)	10 (3,16 %)	00:03:57	27,27 %
7. Política de privacidad	5 (1,09 %)	5 (1,58 %)	00:00:37	20,00 %

Figura 33. Datos de pantallas de usuarios.

Las **Figuras 34 y 35** hacen una comparación de los usuarios que estuvieron activos durante la primera semana del mes de mayo y los usuarios que estuvieron activos todo el mes de mayo.

Respecto a la **Figura 34** se puede inferir que la mayor cantidad de usuarios estuvieron activos durante la primera semana de mayo con un número total de 159 usuarios activos durante esa primera semana.

De la **Figura 35** se puede inferir que durante las dos últimas semanas del mes de mayo hubo poca afluencia de usuarios que interactuaran con la aplicación, y al final del mes 40 usuarios estuvieron activos en total.

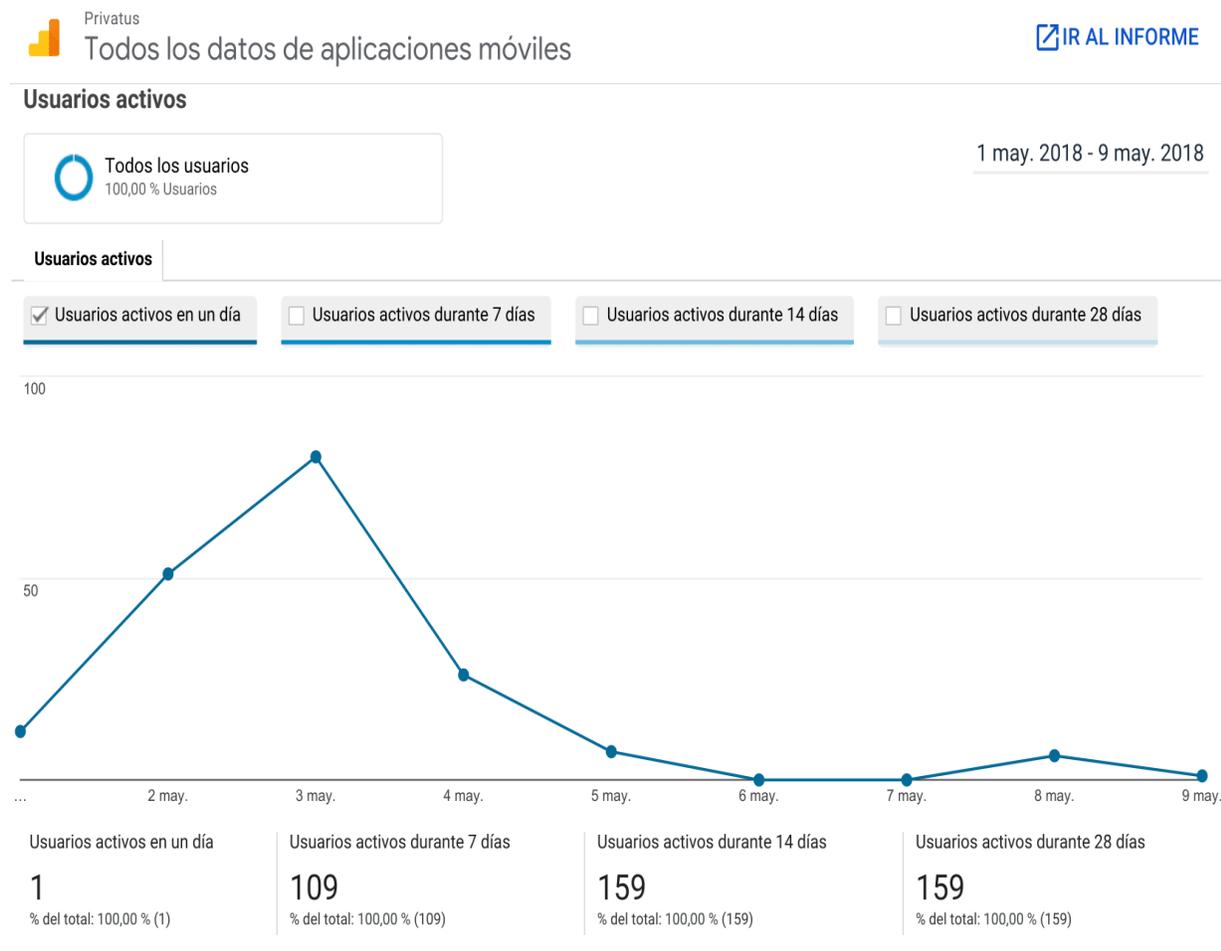


Figura 34. Usuarios semana 1.

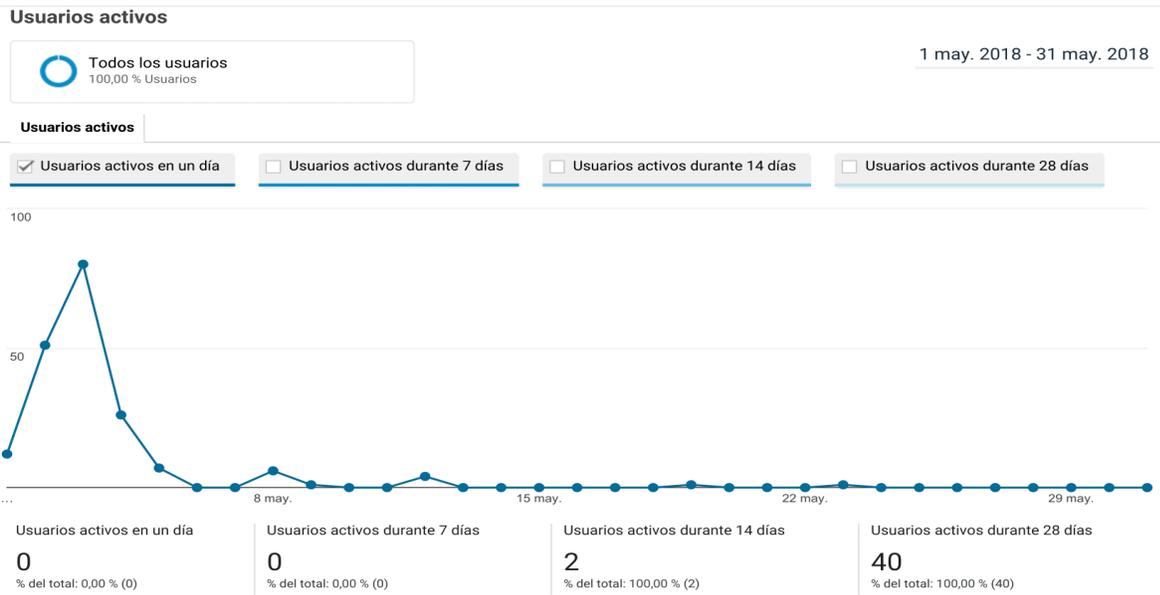


Figura 35. Usuarios semana 4.

6.3.2.2 Estadísticas generadas por Google Play Console

Las estáticas de Google Play Console son una herramienta de seguimiento de Apps gratuita de Google para los usuarios que utilizan la plataforma Google Play Console para subir una aplicación a la Play Store. Dentro de las estadísticas que la herramienta rastrea están calificaciones de la aplicación, instalaciones y desinstalaciones, usuarios que instalaron la aplicación por primera vez, instalaciones totales, estas estadísticas se reportan detalladamente a continuación.

Instalaciones en dispositivos activos por versión de Android

Se hizo un seguimiento de las instalaciones de la aplicación durante un mes, del 1 de mayo al 31 de mayo de 2018. La **Figura 36** muestra las instalaciones en dispositivos activos por versión de Android a la fecha del 31 de mayo del 2018, donde se puede inferir que:

- Las instalaciones al finalizar el mes en dispositivos activos son 32, la gráfica indica que el punto más alto de instalaciones activas en dispositivos fue 58 el viernes 4 de mayo.
- Se da cumplimiento al requerimiento no funcional de confiabilidad que propone que **la aplicación móvil será desarrollada para las plataformas Android**, la cual fue utilizada en diferentes versiones; el total de versiones de dispositivos Android que instalaron la aplicación fueron 58, discriminado por versiones como se indica a continuación:
 - Android versión 7.0 con 23 dispositivos equivalente a un 39.7%
 - Android versión 6.0 15 25 dispositivos equivalente a un 9%
 - Android versión 5.1 10 dispositivos equivalente a un 17.2%
 - Android versión 4.4 4 dispositivos equivalente a un 6.9%

- Android versión 5.0 2 dispositivos equivalente a un 3.4%
- Android versión 7.1 2 dispositivos equivalente a un 3.4%
- Android versión 8.0 2 dispositivos equivalente a un 3.4%



Figura 36. Instalaciones en dispositivos activos por versión de Android.

Usuarios que instalaron la Aplicación por primera vez

Las Figuras 37 y 38 muestran los usuarios que instalaron la aplicación por primera vez en cada una de las semanas del mes de mayo. Los visitantes a la ficha de la Aplicación Privatus en la Play Store y se puede inferir que:

- 141 usuarios Visitaron la ficha de la Aplicación Privatus en la Play Store en el mes de mayo.
- 81 usuarios instalaron la Aplicación por primera vez en el mes de mayo.
- 57 usuarios que equivalen a un 70.4% instalaron la Aplicación por primera vez durante la primera semana del mes de mayo.
- 40 usuarios que equivalen a un 49.4% instalaron la Aplicación por primera vez durante la segunda semana del mes de mayo.
- 36 usuarios que equivalen a un 44.4% instalaron la Aplicación por primera vez durante la tercera semana del mes de mayo.
- 31 usuarios que equivalen a un 38.3% instalaron la Aplicación por primera vez durante la cuarta semana del mes de mayo.

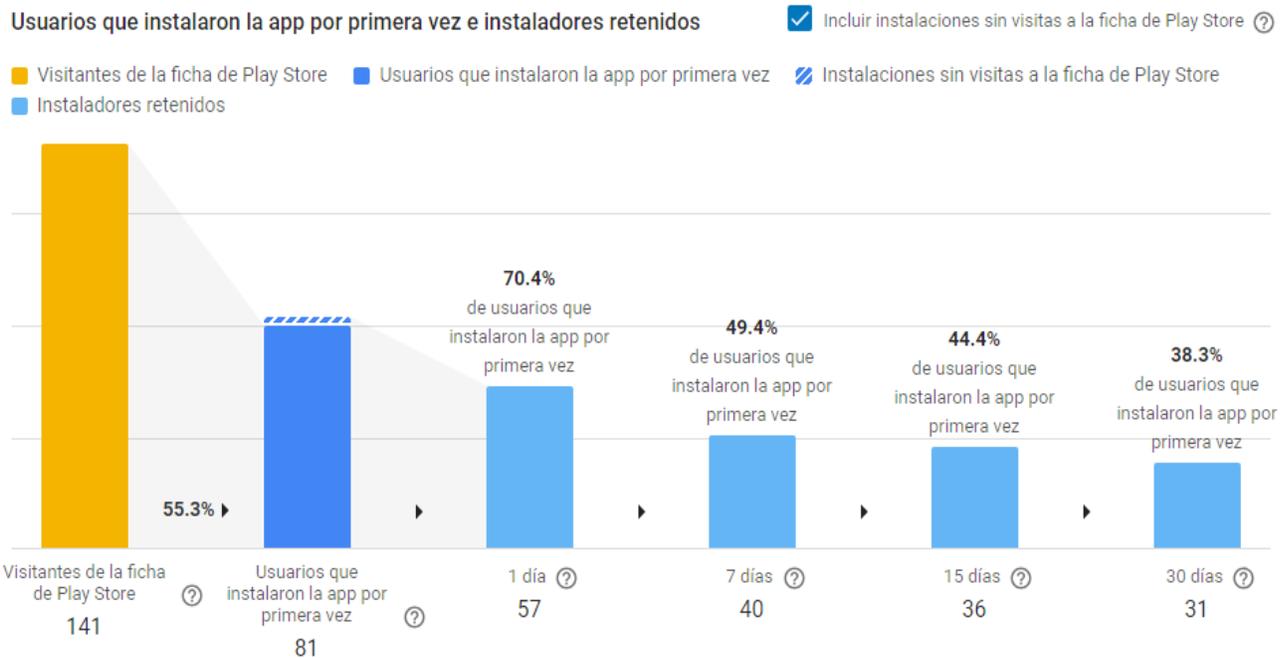


Figura 37. Usuarios que instalaron la Aplicación por primera vez gráfica.

Visitantes de la ficha de Play Store	Usuarios que instalaron la app por primera vez	1 día	7 días	15 días	30 días
141	81	57	40	36	31
-	55.3%	70.4%	49.4%	44.4%	38.3%

Figura 38. Usuarios que instalaron la Aplicación por primera vez tabla.

Instalaciones y desinstalaciones por usuario por versión de Android.

Las **Figuras 30 y 40** muestran las instalaciones y desinstalaciones totales respectivamente de la aplicación Privatus durante el mes de mayo de 2018.

De la **Figura 39** se puede inferir que durante el mes de mayo de 2018 se realizaron un total 85 instalaciones de la Aplicación Privatus. De la **Figura 40** se puede inferir que durante el mes de mayo de 2018 se realizaron 52 desinstalaciones, con respecto a las 85 instalaciones que se realizaron en total, hubo una reducción de 61% en las instalaciones.

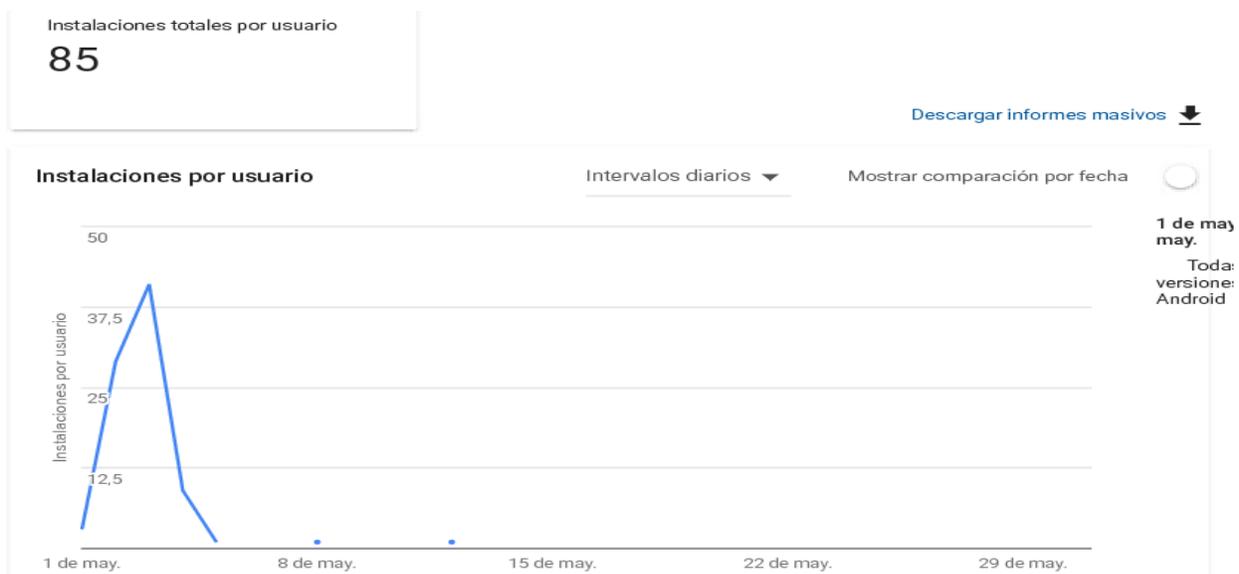


Figura 39. Instalaciones totales por usuarios.

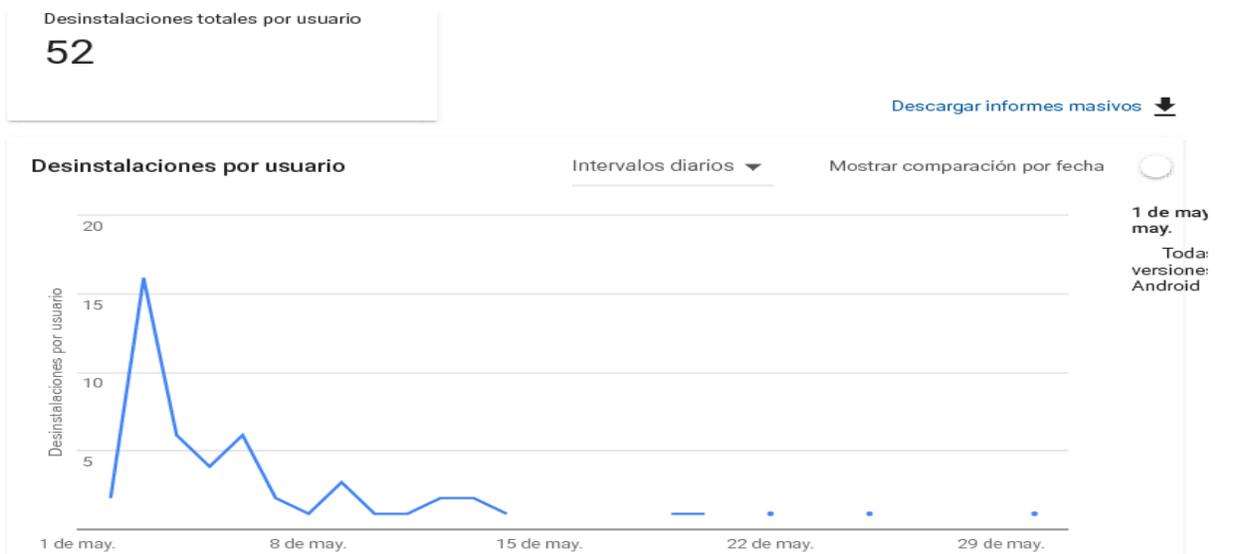


Figura 40. Desinstalaciones totales por usuarios.

Calificaciones de la Aplicación Privatus

La **Figura 41** muestra las calificaciones que la aplicación recibió durante el mes de mayo, mes designado para realizar seguimiento de uso a la aplicación Privatus. Se presenta un promedio de

todas las calificaciones, número de calificaciones totales y número de calificaciones con opiniones. El listado completo con las opiniones de los usuarios se presenta en el *Anexo 3*. De la *Figura 41* se puede inferir que:

- La calificación en promedio es de 4.7 sobre 5, lo que indica que la aceptación de los usuarios para la aplicación es alta.
- Hay 30 calificaciones en total de las cuales hay 19 calificaciones con opiniones.
- El promedio acumulativo de las calificaciones es de 4.641.
- Hay un total de 22 calificaciones con 5 estrellas, 5 calificaciones con 4 estrellas, cero calificaciones con 3 y 2 estrellas respectivamente y 1 calificación con una estrella.



Figura 41. Calificaciones a lo largo del tiempo.

6.3.2.3 Estadísticas Generadas por Type Form y Appy Pie

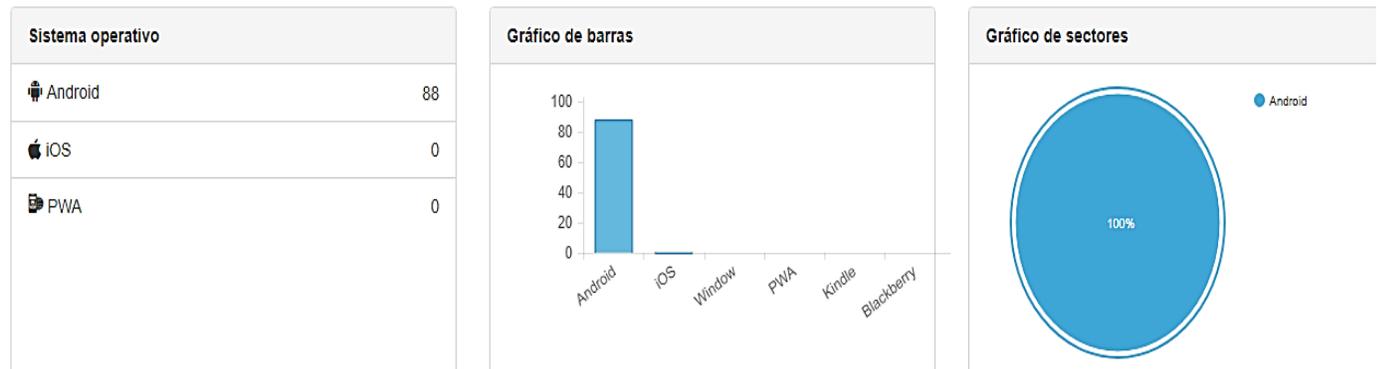
Las plataformas Type Form y Appy Pie utilizadas para la construcción de la aplicación también tienen herramientas para hacer seguimiento a la información de sus aplicaciones, la Plataforma **Appy Pie** hace seguimiento de las instalaciones de la aplicación en diferentes dispositivos y la Plataforma **Type Form** hace seguimiento a los resultados de las autoevaluaciones de los usuarios.

La *Figura 42* muestra los resultados del reporte generado por la herramienta de análisis de la plataforma Appy Pie respecto a las instalaciones en distintos sistemas operativos. De la *Figura 42*

se puede inferir que hubo un total de 88 instalaciones de la aplicación en celulares con sistemas operativos Android.

App Analytics te permite realizar un seguimiento de la interacción del usuario dentro de tu aplicación. Desde el descubrimiento hasta la descarga, puede obtener una visión clara del comportamiento del usuario para tomar las medidas necesarias.

Dispositivo de instalación Descripción general : 05/01/2018 - 05/31/2018



Nota: El recuento de instalación variará con regularidad a medida que eliminamos recuentos de tokens no válidos / desinstalados, proporcionándole la cantidad real de instalaciones.

Figura 42. Appy Pie Analytics.

La **Figura 43** hace referencia a los resultados generales de las autoevaluaciones realizadas por los usuarios, estas estadísticas son un reporte general. El reporte completo de todas las respuestas de los usuarios se presenta en el **Anexo 2**. De la **Figura 43** se puede inferir que:

- El número total de respuestas obtenidas en la autoevaluación fue 61.
- Hubo 176 visitas totales al formulario de autoevaluación.
- Hubo 117 visitas únicas al formulario de autoevaluación.
- El porcentaje de finalización de la autoevaluación fue de 52.1%.
- El tiempo promedio que tardo cada usuario en completar la encuesta fue de 10 minutos con 2 segundos.

El siguiente análisis se realiza en cuanto a la clasificación de los usuarios en Internet y sus diferencias

- Los usuarios de Internet despreocupados muestran una preocupación mínima por la privacidad en línea. Son algo mayores que el promedio y tienden a tener una educación de licenciado o menos.
- Los usuarios prudentes de Internet tienen una preocupación mínima con la privacidad en línea en general, aunque algunas situaciones pueden hacer que tengan mayores niveles de preocupación. Son algo más jóvenes que el promedio, y tienden a tener niveles más bajos de educación (es decir, licenciatura o menos).
- Los usuarios cautelosos de Internet tienen un nivel moderado de preocupación por su privacidad en muchas situaciones, y varias situaciones les hacen experimentar una

preocupación superior a la media con respecto a la privacidad. Estos usuarios tienden a ser más jóvenes y mejor educados, este grupo también estaba muy preocupado por las prácticas clandestinas de recolección de información.

- Los usuarios alarmados de Internet están muy preocupados por su privacidad en línea. Tienden a ser mayores con mayores niveles de educación.

Métricas

Todos los dispositivos					Escritorio	Teléfono	Tablet	Otros
Respuestas	Visitas totales	Visitas únicas	Porcentaje de finalización	Tiempo medio para completar				
61	176	117	52.1%	10:02				

Figura 43. Métricas de Type Form.

La **Figura 44**, presenta datos de la aplicación instalada en un dispositivo Android donde muestra el espacio que memoria que ocupa en el dispositivo, representa un total de **63.30 MB**, estos datos se componen de **29.27 MB** que representa el **46%** de espacio que ocupa la aplicación en total y **34.04 MB** que representa el **54%** de espacio que ocupan los datos de la aplicación, esta estadística da cumplimiento a los requerimientos de confiabilidad que proponen **que la aplicación deberá consumir menos de 500 Mb de memoria RAM y no podrá ocupar más de 500 Mb de espacio en disco.**

Información de la aplicación



Privatus
versión 1.0

Forzar detención

Desinstalar



Mostrar notificaciones

Memoria

Total

63,30 MB

Aplicación

29,27 MB

Datos

34,04 MB

Borrar datos

Memoria caché

Memoria caché

100 KB

Figura 44. Datos de instalación.

6.3.2.4 Resultados estadísticos de las autoevaluaciones

Esta sección presenta los resultados de las 61 encuestas obtenidas durante el mes de evaluación de la aplicación **Privatus**, no se pretende hacer una estadística avanzada pues no es el objetivo de este proyecto, pero si dar una descripción general de los resultados obtenidos a través de gráficas y estadísticas generales.

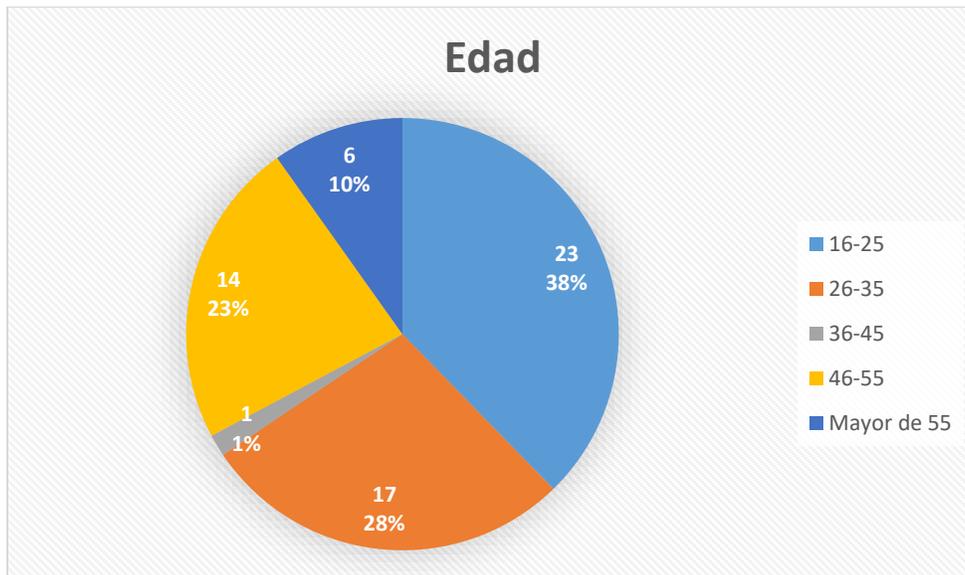


Figura 45 Edad de los encuestados.

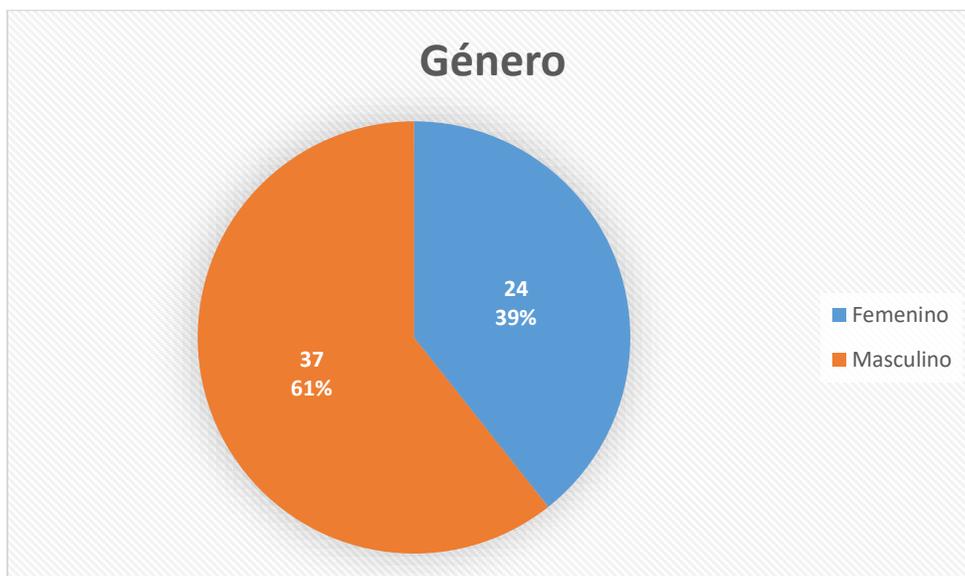


Figura 46 Género de los encuestados.

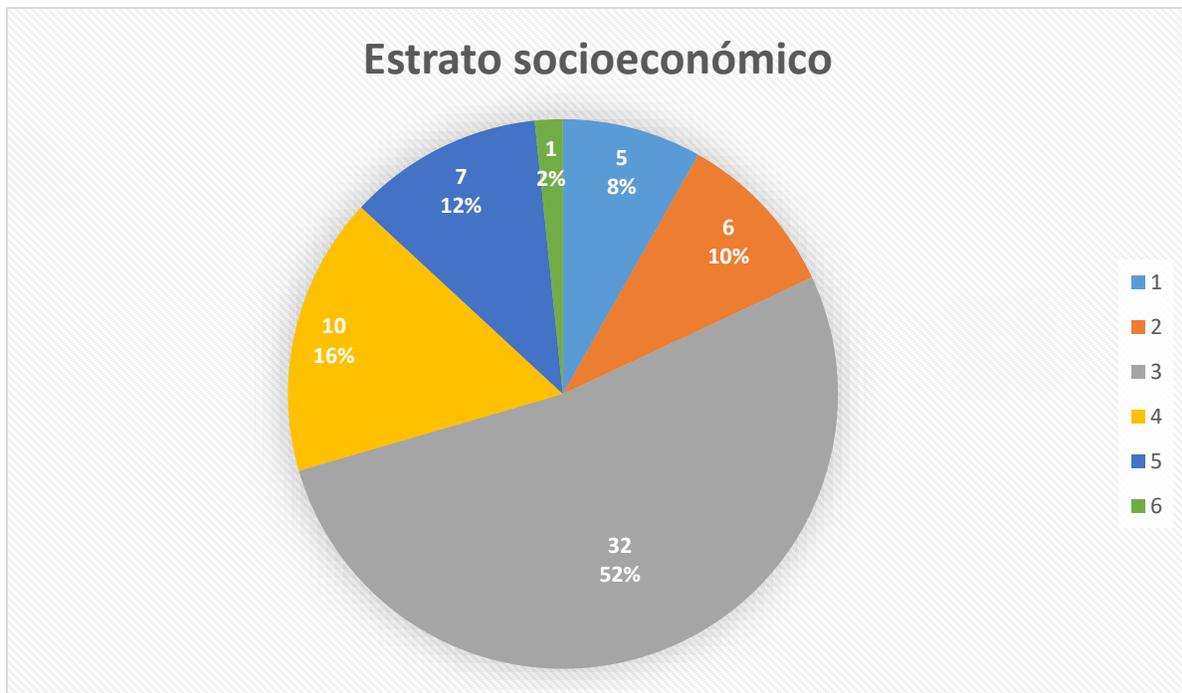


Figura 47 Estrato socioeconómico de los encuestados.

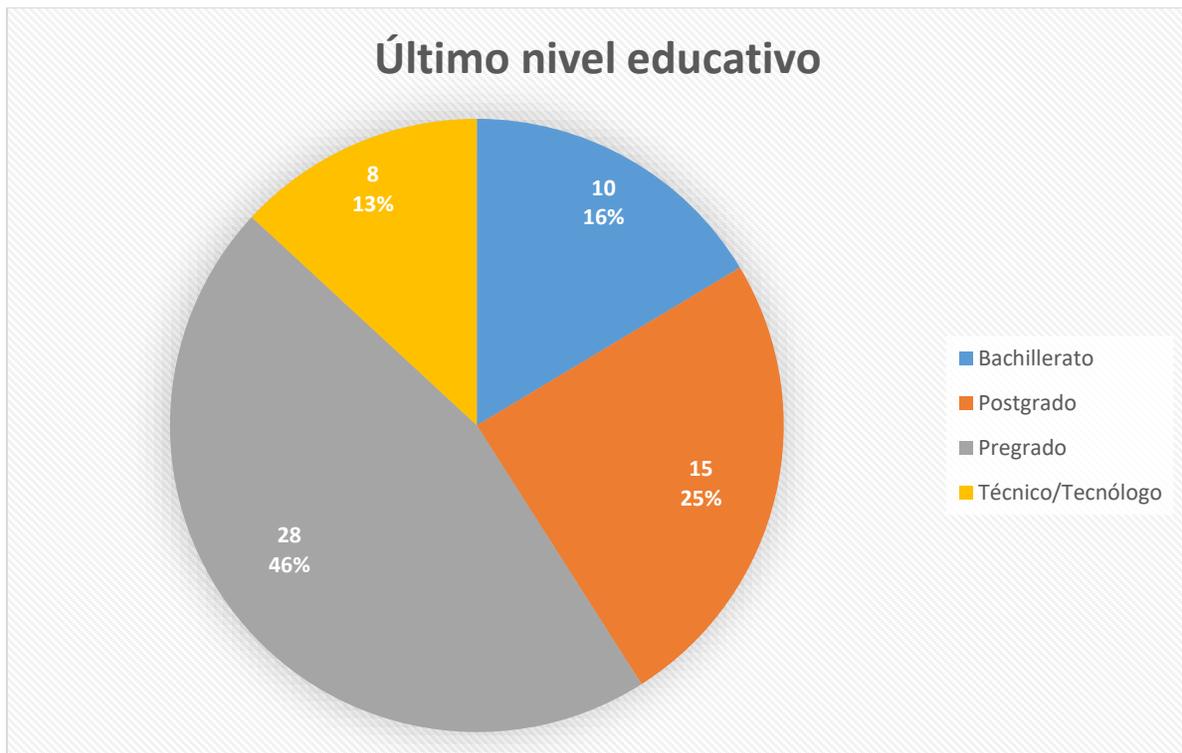


Figura 48 Último nivel educativo de los encuestados.

¿Cuánto tiempo lleva usando internet?

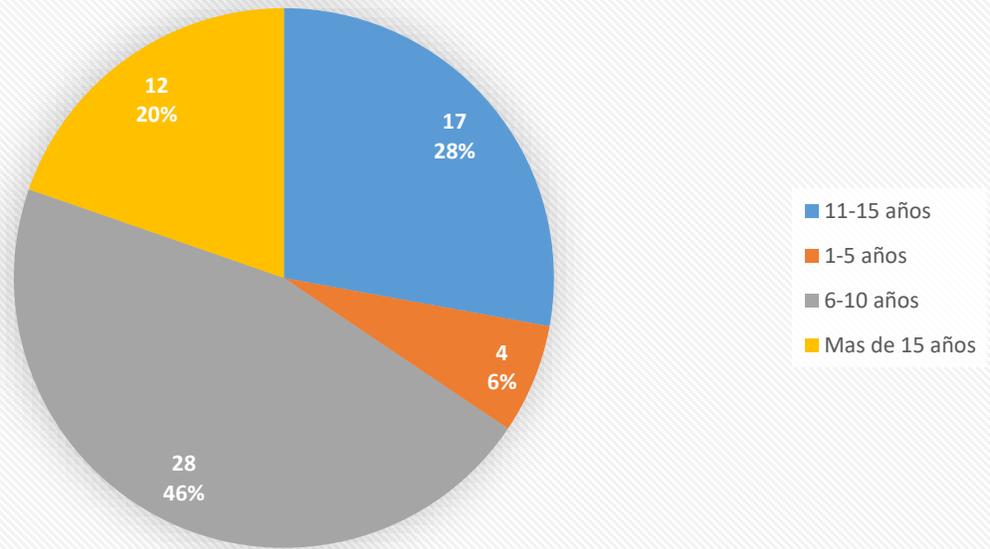


Figura 49 ¿Cuánto tiempo lleva usando internet?

¿Cuánto tiempo lleva haciendo compras en línea?

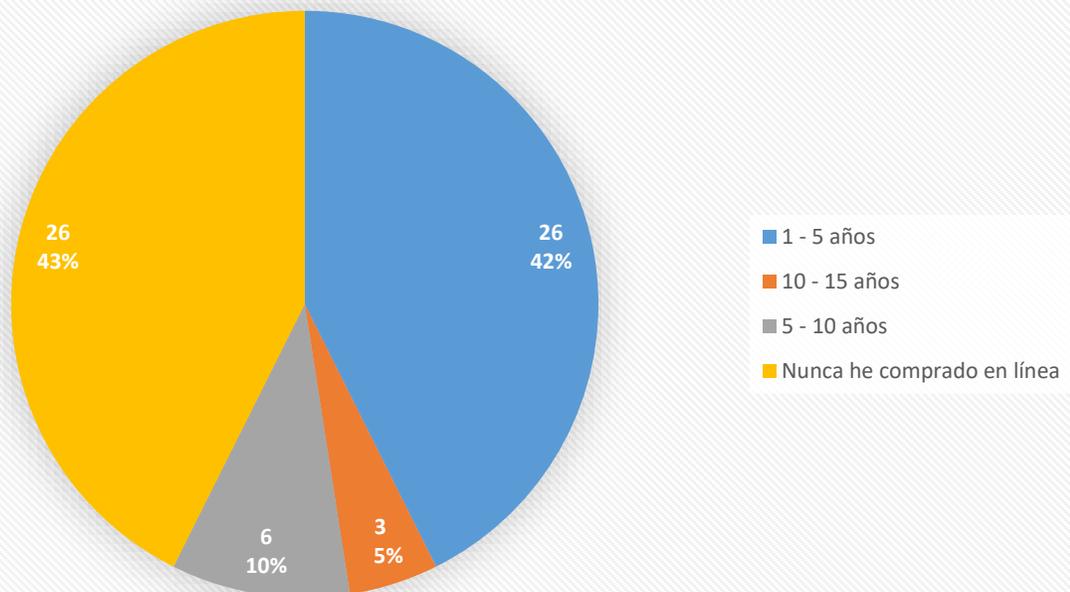


Figura 50 ¿Cuánto tiempo lleva haciendo compras en línea?

¿Cuáles de las siguientes actividades realiza con más frecuencia al acceder a Internet?

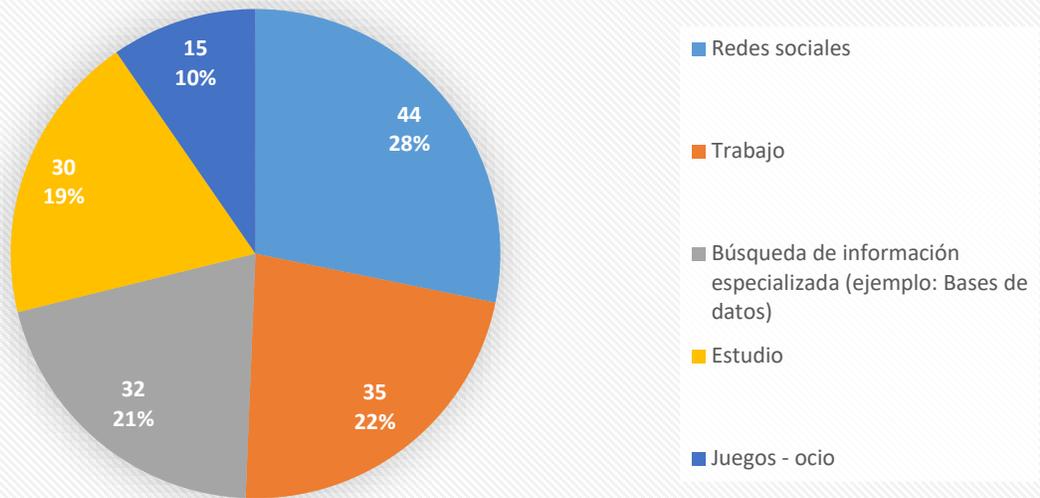


Figura 51 ¿Cuáles de las siguientes actividades realiza con más frecuencia al acceder a Internet?

¿Hace cuánto tiene cuenta en redes sociales?

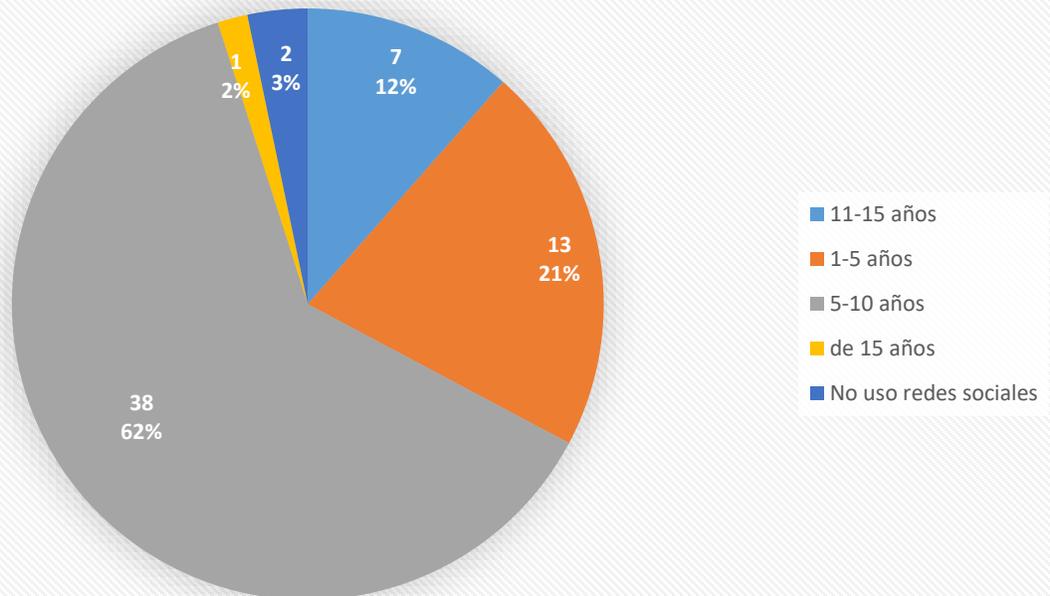


Figura 52 ¿Hace cuánto tiene cuenta en redes sociales?

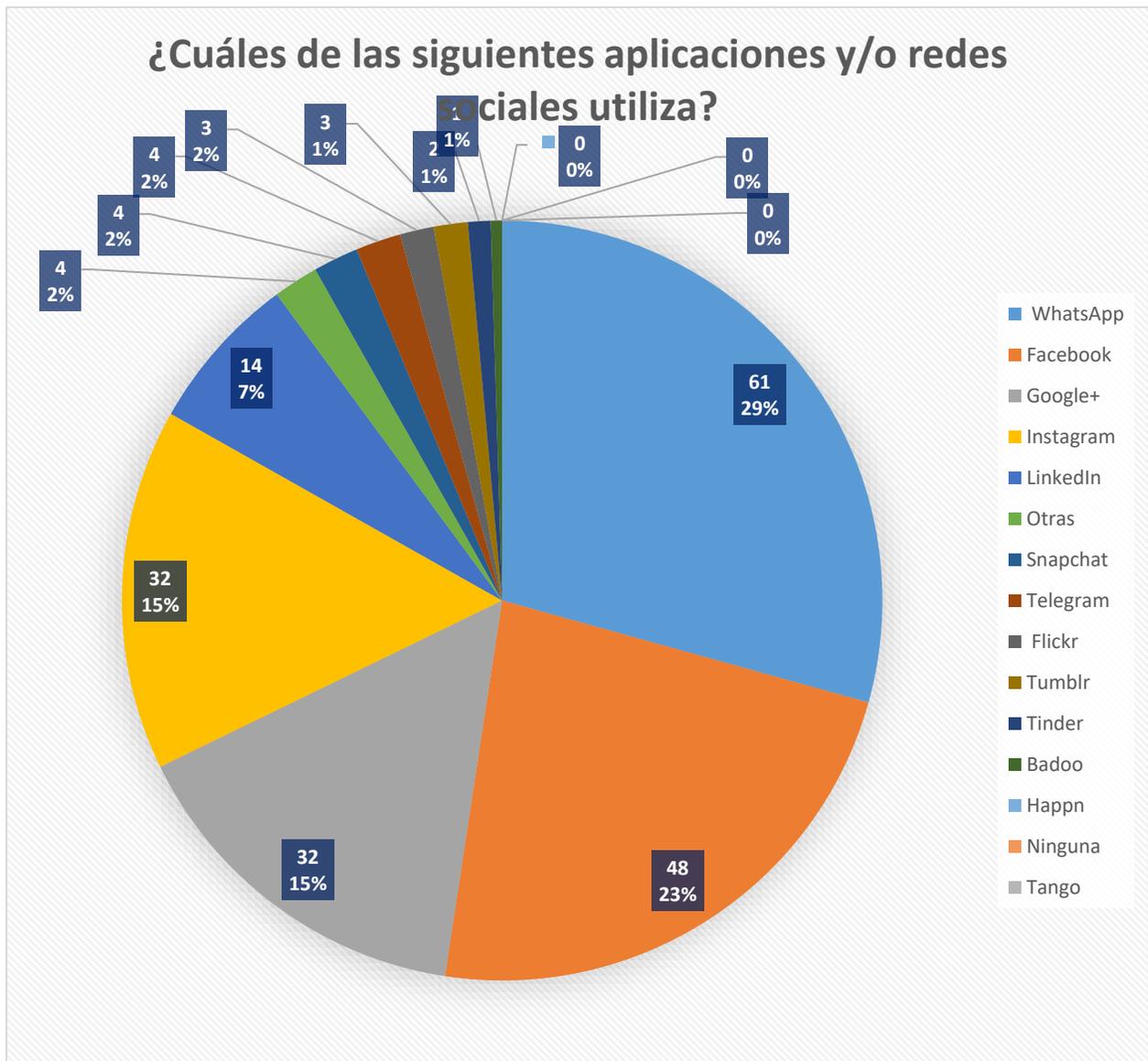


Figura 53 ¿Cuáles de las siguientes aplicaciones y/o redes sociales utiliza?

¿Cuándo está o ha estado en una relación afectiva, comparte alguna de la siguiente información con la otra persona?

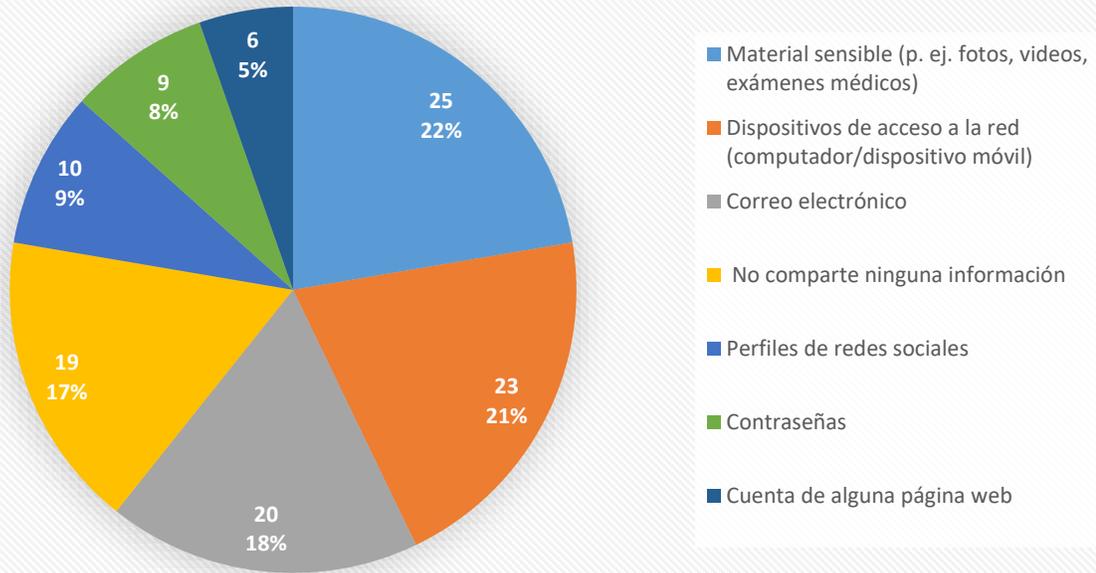


Figura 54 ¿Cuándo está o ha estado en una relación afectiva, comparte alguna de la siguiente información con la otra persona?

Clasificación de usuarios

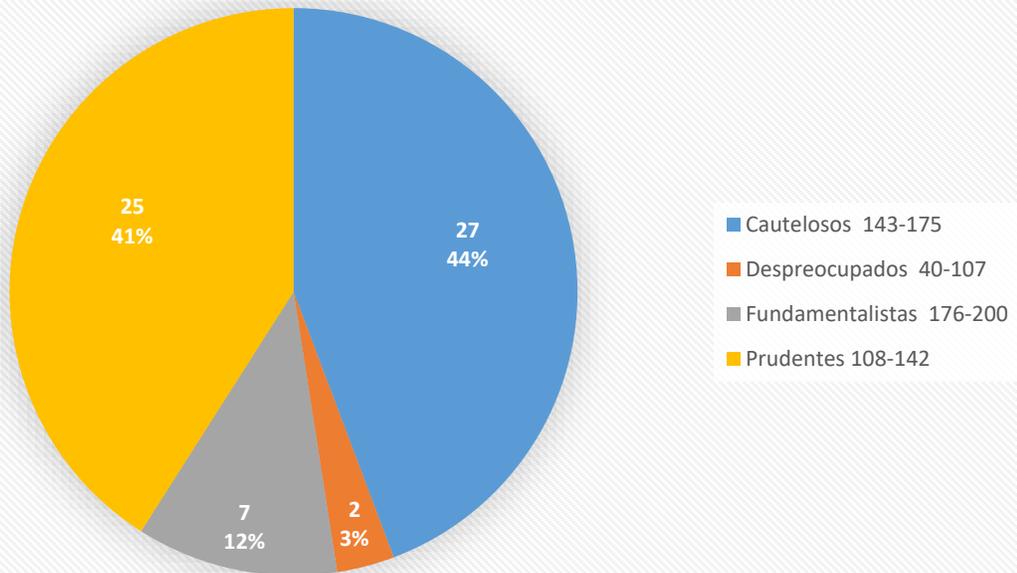


Figura 55 Clasificación de usuarios encuestados.

6.3.3 Manual de la aplicación para dar mantenimiento

Este último capítulo hace referencia a la documentación y realización del manual de mantenimiento de la Aplicación Privatus, la razón para hacer este manual es dejar una guía para posteriores estudiantes interesados en seguir con esta investigación puedan retomar la aplicación que es en esta instancia un primer prototipo tal como lo refiere el título de esta investigación y seguir con su desarrollo, añadiendo funciones, buscando más afluencia de público, construyendo una versión definitiva, que sea nativa en el lenguaje Android y pueda expandirse a otros sistemas operativos como IOS.

1. Comprender la estructura de la aplicación

La aplicación Privatus es construida utilizando dos plataformas web, una plataforma llamada Appy Pie, diseñada para la construcción de aplicaciones móviles, la plataforma Appy Pie controla todo el contenido informativo que se muestra al usuario final, controla La página de inicio, la página de evaluación, que es una integración que ofrece Appy Pie para conectarse con Type Form, la Pagina de estadísticas que funciona de la misma forma que la página de Evaluación, la página de recomendaciones que es una funcionalidad que ofrece Appy Pie llamada noticias en la que se puede crear distintos artículos y ser mostrados a los usuarios, y por ultimo las Paginas de Términos y condiciones y la página de Políticas de privacidad que son paginas netamente informativas.

La segunda plataforma llamada Type Form plataforma que gestiona encuestas, formularios y evaluaciones en línea, esta plataforma controla y gestiona el Formulario de autoevaluación diseñado para ser resuelto por los usuarios el cual se encuentra en el *Anexo I*, se hace la aclaración que estas dos plataformas tienen planes pago y planes gratis, desde las cuales la aplicación podría funcionar usando los planes gratuitos de las Plataformas o bien contratando un plan mensual ganando más características y funcionalidades, actualmente la aplicación funciona utilizando los planes pago de estas Plataformas, se realiza un pago mensual, para mantener la aplicación funcionando con los requerimientos funcionales establecidos en el diseño de la misma.

2. Manejo de la aplicación

El manejo de la aplicación es relativamente fácil de aprender, las plataformas Apy Pie y Type form son plataformas diseñadas para ser amigables y cómodas con el cliente, en el caso que se requiera aprender a manejar las Plataformas, cada una cuenta con tutoriales, e información completa para aprender a usar todas las funcionalidades que brindan las plataformas a sus clientes, en el caso necesario de necesitar soporte profesional, las plataformas cuentan con un excelente servicio técnico.

3. Servicio técnico

Cada una de las plataformas Appy Pie y Type Form cuentan con servicio de soporte técnico, personal altamente capacitado, que está disponible las 24 horas del día para resolver los problemas de sus clientes, el servicio se hace por medio de chat y correo electrónico, en los planes pago intermedios; las plataformas prestan un servicio de asistencia por video llamada, contratando el plan de pago más costoso en cada plataforma.

4. Transferencia de titularidad

Para la construcción de la Aplicación Privatus, el autor de la presente investigación contrato bajo su nombre y recursos propios los servicios de las dos Plataformas Appy Pie y Type form, quedando registrada la aplicación bajo su nombre y correos electrónicos, las plataformas cuentan con la característica de poder nombrar administradores de la aplicación a otras personas, utilizando esta función se puede transferir la titularidad de la Aplicación a la persona que se requiera.

El pago se realizaría de la siguiente manera, para utilización de tipo netamente académica, se realiza un traspaso libre de titularidad de la aplicación determinando que su uso será para fines investigativos y académicos, para una transferencia con fines lucrativos, se debe realizar un contrato formal de compra venta con el autor de la investigación

6.3.4 Cumplimiento de los requerimientos

Esta sección verifica que se dé cumplimiento a los requerimientos de rendimiento (requerimientos funcionales) y los requerimientos de confiabilidad (requerimientos no funcionales) propuestos en el diseño de la aplicación.

Requerimientos de rendimiento

Con la implementación de todas las páginas Frontend (**Aplicacion**) y Backend (**CMS Content Managment System**) de la aplicación se da cumplimiento a los requerimientos de rendimiento que definen que la aplicación debe tener un diseño y entorno gráfico agradable para el usuario, esto se verifica en las calificaciones de los usuarios (*Anexo 3*) y en las estadísticas de uso y funcionalidad (*sección 6.3.2.1*) que se realizaron a la aplicación, una segunda instancia para verificar este requerimiento son los comentarios de los usuarios donde calificaron a la aplicación de tener una interfaz agradable esto se comprueba en el *Anexo 3*.

En las *Figuras 12* y *13*, donde se presenta la implementación de las páginas de **evaluación y resultados generales** se verifica el cumplimiento de los requerimientos en donde se propone contemplar el uso óptimo de recursos tales como conexiones a la base de datos y la correcta integración entre la base de datos y la aplicación para garantizar el óptimo rendimiento del sistema. Esto se verifica cuando el usuario accede a la aplicación y diligencia la encuesta, debido a que la

encuesta esta creada en otra plataforma y la integración de las dos plataformas permiten al usuario diligenciar la encuesta desde la aplicación móvil.

En la **Figura 19** se muestra la funcionalidad compartir de la plataforma **Type Form**, a través de la cual es posible la integración con la Plataforma **Appy Pie** y que la evaluación pueda ser vista y diligenciada por el usuario desde la aplicación; utilizando código HTML con JavaScript generado por la funcionalidad compartir. Es posible insertar el código generado dentro de la función Codepage de la plataforma Appy pie y así obtener la integración completa de las dos plataformas. Esta funcionalidad en integración con la página **Evalúate** del **CMS** de la aplicación da cumplimiento a los requerimientos de rendimiento que propone implementar una correcta integración entre la base de datos y la aplicación para garantizar el óptimo rendimiento del sistema. Se verifica a través del uso de la aplicación, cuando el usuario realiza la **autoevaluación** la cual se integra desde otra plataforma (plataforma de gestión de formularios), también cuando el usuario consulta las **estadísticas generales** que son estadísticas que se actualizan y se integran a la aplicación desde la plataforma de gestión de encuestas.

Requerimientos de Confiabilidad

La presentación de los reportes, datos y estadísticas del numeral 6.3.2 da cumplimiento al requerimiento no funcional de confiabilidad que propone que **el sistema debe tener una disponibilidad del 99,99% de las veces en que un usuario intente accederlo debido a** que la aplicación esta subida en la plataforma **Play store de Google** y corre sobre los servidores de **Appy Pie**, Estos servicios están diseñados para estar siempre en ejecución y cuentan con servidores de respaldo para garantizar a los usuarios el principio de disponibilidad. De igual forma se garantiza este requerimiento debido a que la aplicación esta subida en la plataforma Play store de Google, estos servidores nunca se caen ni pierden conexión, por eso el 99% de disponibilidad.

La **Figura 36** muestra las instalaciones en dispositivos activos por versión de Android a la fecha del 31 de mayo del 2018, donde se da cumplimiento al requerimiento no funcional de confiabilidad que propone que **la aplicación móvil será desarrollada para las plataformas Android. La versión mínima de Android en la que se instaló la aplicación es la** Android versión 4.4 4 y la versión más reciente de Android en la que se instaló la aplicación es la versión 8.0 2. El total de versiones de dispositivos Android que instalaron la aplicación fueron 58.

7 CONCLUSIONES

Este capítulo se genera a partir de los resultados presentados en el capítulo de presentación y **análisis de resultados** numeral 6. Las conclusiones aquí escritas corresponden a dos ejes fundamentales de la aplicación y del objetivo general de esta investigación, que son los resultados del seguimiento a la Aplicación Privatus durante un mes y los resultados de las encuestas generadas por los usuarios cuando interactuaron con la aplicación.

El análisis realizado en este documento demostró que al usuario de Internet le preocupa la privacidad de sus datos, esto se puede corroborar en que el promedio de puntaje obtenido en el total de las 61 encuestas recibidas fue de 144. Esto quiere decir que los usuarios se ubican dentro del grupo llamado **usuarios cautelosos**, que según la literatura este grupo sentía un nivel moderado de preocupación en la mayoría de las situaciones en las que interactúa a través de Internet.

Esta investigación cumple el objetivo de analizar mediante una encuesta a los usuarios de Internet según la preocupación de la exposición de sus datos personales. El estudio se enfoca en el nivel de preocupación que el usuario tiene respecto a los comportamientos que el mismo realiza cuando navega en Internet, este sistema permite al usuario conocer el nivel de exposición de sus datos y compararse frente al nivel de exposición de otros usuarios, esto permite que el mismo usuario pueda tomar conciencia de proteger de manera adecuada sus datos personales. Los resultados del análisis y la tipología en este estudio son aplicables solo a Colombia.

Puede concluirse que el grupo de personas participante es joven y con un buen nivel de educación. Esto se verifica al observar que el rango de edad con más participación en la encuesta es de 16 a 25 años con el 38% de la participación total, el estrato socioeconómico nivel 3 según la escala colombiana con 52% del total de encuestados, el grupo presenta un nivel de educación alto, 46% conformado de personas con pregrado y un 25% de personas tienen un postgrado.

El 46% de los encuestados lleva usando internet entre 6 y 10 años, lo que quiere decir que este grupo tiene un conocimiento sobre el manejo de las nuevas tecnologías, pero tiene miedo a utilizarlas, el 43% de los encuestados nunca ha realizado una compra en internet, otro 42%, hace compras recientes, entre 1 y 5 años, solo el 15% de los encuestados, hace compras en internet hace más de 5 años.

Se observa que las actividades que los usuarios realizan en Internet son muy variadas: uso de redes sociales 72%, trabajo 57%, búsqueda de información especializada 52%, estudio 49% y juegos u ocio un 25%, lo que lleva a concluir que las personas utilizan internet para distintas tareas y no solo se enfoca en una sola actividad.

La mayoría de los usuarios (62%) utilizan redes sociales hace un periodo medianamente moderado, entre 5 a 10 años, lo que lleva a concluir que es un grupo que ha vivido la evolución, el crecimiento y el surgimiento de las redes sociales que conectan al mundo, en cuanto al uso de las redes el 100% de los encuestados utiliza la red social “WhatsApp”, seguida de Facebook” con el 78%, “Google

+” e “Instagram” con el 52%, cada una lideran la lista de las redes sociales más utilizadas por los usuarios, estos resultados apoyan el estudio realizado por (MinTIC, 2018), que anuncia a WhatsApp, Facebook, e Instagram como las redes sociales más usadas en Colombia.

La información que las personas comparten a través de internet es moderada, el 41% de los usuarios afirmo compartir material sensible con su pareja como videos, fotos, el 38% de las personas afirmo compartir con su pareja el dispositivo móvil y/o computador, bajo esta información se concluye que las personas que están en una relación, es menos de la mitad, lo cual significa que las personas guardan su privacidad aun en una relación afectiva.

Desplegar la aplicación y liberarla fue un proceso ágil y sencillo. Las cifras de seguimiento presentadas demuestran la buena aceptación de la aplicación, durante el mes de mayo del 2018 hubieron 162 usuarios que interactuaron con la aplicación, estas personas fueron contactadas y capacitadas en cuanto al contenido y objetivo de la aplicación, se les explico el propósito de la aplicación y su contexto investigativo, que esta forma parte de un proyecto de investigación así como de un trabajo de grado, después se envió a los usuarios el link el cual direcciona directamente a la ficha de la aplicación en la Play Store de Google.

En cuanto al uso de la aplicación hubo un total de 205 sesiones de interacción usuario aplicación, las ciudades donde hubo mayor interacción fueron Medellín, Bogotá, Manizales, Ibagué, Pereira, Popayán; Las ciudades con más interacción de usuarios con la Aplicación Privatus son: Pasto con 43 usuarios, Cali con 37 usuarios, Medellín con 35 usuarios y Bogotá con 19 usuarios. La duración promedio de cada sesión es de 10 minutos y 33 segundos, entendiendo la sesión como el tiempo que el usuario interactúa con la aplicación la aplicación obtuvo un buen concepto por parte de los usuarios al obtener una calificación de 4.7 sobre 5 en la escala de calificación que presenta Google Play durante el mes de seguimiento, por lo que se concluye que la aplicación es de agrado para quienes interactúan con ella.

La aplicación funciona en diferentes versiones del sistema operativo para móviles Android, las versiones del sistema operativo más utilizadas para interactuar con la aplicación son Android 7.0 con 33,3% o 54 usuarios, Android 6.0 con 14,6% o 24 usuarios y Android 6.0.1 con 12,3% o 20 usuarios, Android 5.1.1 con 11.7% o 19 usuarios, y Android 7.1.1 con 9.3% o 15 del total de usuarios que interactuaron durante el mes de seguimiento.

La interacción de los usuarios con la aplicación fue variante durante el mes de seguimiento, la mayor cantidad de usuarios estuvieron activos durante la primera semana de mayo con un número total de 159 usuarios activos, durante las dos últimas semanas del mes de mayo hubo poca afluencia de usuarios que interactuaran con la aplicación, y al final del mes 40 usuarios estuvieron activos en total.

En cuanto al número de usuarios hubo un total de 141 usuarios Visitaron la ficha de la Aplicación Privatus en la Play Store en el mes de mayo. De los cuales 81 usuarios instalaron la Aplicación por primera vez en el mes de mayo. 57 usuarios (70.4%) instalaron la Aplicación por primera vez

durante la primera semana del mes de mayo. 40 usuarios (49.4%) instalaron la Aplicación por primera vez durante la segunda semana del mes de mayo. 36 usuarios (44.4%) instalaron la Aplicación por primera vez durante la tercera semana del mes de mayo. y 31 usuarios (38.3%) instalaron la Aplicación por primera vez durante la cuarta semana del mes de mayo.

La aplicación no presentó fallas de tipo técnico durante el mes de seguimiento, se mantuvo siempre en línea y funcionando correctamente en todas sus funcionalidades, como se presenta en el análisis realizado por Google Play. El correcto funcionamiento de la aplicación se evidencia en que se dio por cumplido los requerimientos funcionales y no funcionales propuestos, también en que siempre estuvo disponible como evidencia el seguimiento en tiempo real durante un mes presentado en las estadísticas de recolección de datos de Google Analytics.

8 TRABAJOS FUTUROS

En este capítulo se plantean alternativas de futuros proyectos o trabajos que pueden desarrollarse posterior a esta investigación.

Las aplicaciones y los dispositivos móviles están marcando una nueva tendencia en la forma como las personas viven actualmente, generar medidas de protección para los datos, y despertar la conciencia de los usuarios de internet para proteger su información en línea es fundamental para mantener el Internet seguro y seguir aprovechando todas las ventajas que ofrece vivir en un mundo moderno. La propuesta que se hace para futuros estudios es continuar con el objetivo general propuesto, pasar de construir un prototipo de aplicación a una aplicación completa, nativa, que se adapte a los distintos sistemas operativos ofrecidos en el mercado actual, añadir nuevas funcionalidades, mejorar la interacción con el usuario y simplificar la usabilidad del prototipo propuesto en esta investigación.

Aunque este estudio se encuentra entre los primeros en ser desarrollados en el país, se enfoca solo en ciudades principales. Con una muestra reducida, Todavía se necesitan estudios en otras ciudades o en otros países para probar la solidez de la metodología propuesta.

Este proyecto construyo y propuso una nueva metodología de clasificación de usuarios de internet con el propósito de medir el **nivel de exposición total**, utilizando las variables de **nivel de preocupación y comportamientos frente a la privacidad en línea**. Los estudios futuros podrían incluir estudios en otros países de la región o podrían usar nuevas metodologías para observar y evaluar a los usuarios de Internet a medida que su comportamiento cambia con el tiempo.

Optimizar el instrumento de medición (encuesta), las variables preocupación y comportamientos de la privacidad, agregar nuevas variables par ser medidas, la percepción de la privacidad y la forma en como las personas se comportan al enfrentar distintas situaciones que comprometan la seguridad de sus datos depende de muchas variables como la edad, ubicación geográfica, nivel de educación, estrato socioeconómico entre muchas otras, buscar estudios que expongan cuales son estas nuevas variables es fundamental para poder desarrollar un sistema que permita conocer el nivel de preocupación y percepción de los datos personales en línea, en los usuarios de internet de hoy en día.

Uno puede esperar ver crecer las aplicaciones de Internet en tantas plataformas tecnológicas como estén disponibles, y el comportamiento de los usuarios será un factor importante que determinará el uso de Internet en el futuro. La seguridad en las aplicaciones dependerá de cómo el usuario sea exigente en la protección de sus datos personales, para estudios futuros puede incluir

9 REFERENCIAS

- Abad, D. (6 de Mayo de 2015). *Latamclick* . Obtenido de Estadísticas de Facebook y Twitter en Colombia (2015): <https://www.latamclick.com/estadisticas-de-facebook-y-twitter-en-colombia-2015/>
- ABC Aplicaciones. (01 de 04 de 2018). <https://www.abc.es>. Obtenido de Google endurece sus exigencias para subir aplicaciones a la Play Store: https://www.abc.es/tecnologia/moviles/aplicaciones/abci-google-endurece-exigencias-para-subir-aplicaciones-play-store-201712212203_noticia.html
- Aguirre Jaramillo, L. M., & Amaya Fernández, F. O. (2016). *Privacidad siglo XXI: ¿reliquia o necesidad?* Medellín: UPB Innova.
- Ahn, A. (30 de 01 de 2018). *Product Manager, Google Play* . Obtenido de Cómo luchamos contra aplicaciones malas y desarrolladores maliciosos en 2017: <https://android-developers.googleblog.com/2018/01/how-we-fought-bad-apps-and-malicious.html>
- Alaminos Chica, A., & Castejón Costa, J. (2006). *ELABORACIÓN, ANÁLISIS E INTERPRETACIÓN DE ENCUESTAS, CUESTIONARIOS Y ESCALAS DE OPINIÓN*. ALICANTE: ICE/VICERRECTORADO DE CALIDAD Y ARMONIZACIÓN EUROPEA UNIVERSIDAD DE ALICANTE.
- Alvarado, D. (19 de Mayo de 2014). *Cuántos usuarios tiene facebook*. Obtenido de <https://www.laneros.com/>: <https://www.laneros.com/temas/%C2%BFcu%C3%A1ntos-usuarios-tiene-facebook-en-colombia.212031/>
- Antevenio. (2018). <https://www.antevenio.com/>. Obtenido de <https://www.antevenio.com/wp-content/uploads/2016/09/Información.jpg>
- Antevenio. (2018). <https://www.antevenio.com/wp-content/uploads/2016/09/GooglePlayDeveloperConsole.jpg>. Obtenido de <https://www.antevenio.com/wp-content/uploads/2016/09/GooglePlayDeveloperConsole.jpg>
- Apexlauncher. (2018). www.apexlauncher.com. Obtenido de <https://www.apexlauncher.com>
- Appyourself. (2018). <https://appyourself.net/>. Obtenido de <https://appyourself.net/es/precios-crear-aplicaciones/>
- Appypie. (2018). <https://es.appypie.com/plan-de-precios>. Obtenido de <https://es.appypie.com/plan-de-precios>
- Armor text. (2018). <https://armortext.com> . Obtenido de <https://armortext.com>

- Bandura, A. (1989). Regulation of cognitive processes through perceived self-efficacy. . *Developmental Psychology*, págs. 725–739.
- Bandura, A. (2012). On the Functional Properties of Perceived Self-Efficacy Revisited. *Journal of Management*, 38(1), 9-44.
- Barnes, S. J., Bauer, H., Neumann, M., & Huber, F. (2007). Segmenting cyberspace: A customer typology for the Internet. *European Journal of Marketing*, 41(1), 71-93.
- Becker, J., & Chen, H. (2009). Measuring Privacy Risk in Online Social Networks. *UC Davis*, 1-8.
- Bedoya Laguna, C. A., & Reyes Roncancio, J. D. (2017). *Diseño de un instrumento tipo escala Likert para la descripción de las actitudes hacia la tecnología por parte de los profesores de un colegio público de Bogotá*. Bogotá: Universidad Distrital Francisco José de Caldas.
- Bernhard Debatin, J. P., Ann-Kathrin Horn, M., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, 83-108.
- Boxcryptor. (2018). *www.boxcryptor.com/*. Obtenido de <https://www.boxcryptor.com/es/>
- Brandeis, L., & Warren, S. (1890). The right to privacy. . *Harvard Law Review*, 4:193.
- Brandtzæg, P. B., & Heim, J. (2010). Social network sites - A typology of users. *Journal of Web-Based Communities*, 6(3), 231-253.
- Brandtzæg, P. B., Heim, J., Kaare, B. H., Endestad, T., & Torgersen, B. H. (Junio 29 a Julio 3 de 2005). Gender differences and the digital divide in Norway - Is there really a gendered divide? *Presented at the International Conference of Childhoods: Children and youth in Emerging and Transforming Societies*.
- Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *JOURNAL OF THE AMERICAN SOCIETY FOR INFORMATION SCIENCE AND TECHNOLOGY*, 157-165.
- Byer, B. (20 de Junio de 2018). *Internet Users Worry About Online Privacy but Feel Powerless to Do Much About It*. Obtenido de <https://www.entrepreneur.com:https://www.entrepreneur.com/article/314524>
- Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). responses, A multinational study on online privacy: global concerns and local. *New Media & Society*, 394-416.
- Citizenme. (2018). *www.citizenme.com*. Obtenido de <https://www.citizenme.com/public/wp/>
- Cliqz. (2018). *cliqz.com*. Obtenido de <https://cliqz.com>

- CM Locker. (2018). *www.cmcm.com*. Obtenido de <http://www.cmcm.com/es-es/cm-locker/>
- Congreso de Colombia, G. N. (2012). *Ley estatutaria No 1581*. Bogota.
- Consejo Superior de la Judicatura, S. A. (1991). Constitución Política de Colombia. En S. A. Consejo Superior de la Judicatura, *Título de la colección: Normatividad 5* (pág. 15). Bogota: ISSN: 2344-8997.
- Corte Constitucional, R. d. (2011). *Sentencia C-748/11*. Obtenido de <http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm>
- Del Valle, L. (12 de Diciembre de 2016). *Cómo programar una app para móviles*. Obtenido de <https://www.marketingandweb.e>: <https://www.marketingandweb.es/marketing/como-crear-una-app/>
- Deloitte. (15 de Junio de 2017). *Samsung y Huawei, los celulares más comprados del país*. Obtenido de <https://www.eltiempo.com>: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/marcas-de-celulares-mas-compradas-en-colombia-99088>
- DeYoung, C. G., & Spence, I. (2004). Profiling information technology users: En route to dynamic personalization,. *Computers in Human Behavior*, 20(1), 6-55.
- Diario oficial Unión Europea. (04 de 05 de 2016). *Reglamento general para la proteccion de datos RGPD*. Obtenido de ISSN 1977-0685: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=ES>
- Duck DuckGo. (2018). *duckduckgo.com*. Obtenido de <https://duckduckgo.com>
- Electronic Frontier Foundation . (2018). *www.eff.org*. Obtenido de <https://www.eff.org/privacybadger>
- Equifax, I., & Harris Louis, a. A. (1991). Equifax-Harris consumer privacy survey. *Atlanta, Ga. : Equifax ; New York, NY : L. Harris & Associates*.
- ESET. (2016). *ESET prensa* . Obtenido de <http://www.eset-la.com/>: <http://www.eset-la.com/centro-prensa/prensa/2016>
- Eshagh, E., Carosi, M., & Shanthikumar, H. (2014). *US Patente n° US20180181378A1*.
- Ferreira, C. M., Peixoto, M. J., Duarte, P. A., Torres, A. B., Junior, M. L., Rocha, L. S., & Viana, W. (Abril de 2018). An Evaluation of Cross-Platform Frameworks for Multimedia Mobile Applications Development. *IEEE Latin America Transactions*, 16(4), 1206 - 1212.
- Ganti, R. K., Ye, F., & Lei, H. (2011). Raghu K. Ganti, Fan Ye, and Hui Lei. *IEEE Communications Magazine* , 1-9.

- Ghostery. (2018). *ghostery.com*. Obtenido de <https://www.ghostery.com/>
- Gilbert, P., Chun, B.-G., Cox, L. P., & Jung, J. (2011). Vision: automated security validation of mobile apps at app markets. *Proceeding MCS '11 Proceedings of the second international workshop on Mobile cloud computing and services*, 21-26.
- Google LLC . (26 de Febrero de 2018). <https://play.google.com>. Obtenido de Acuerdo de Distribución para Desarrolladores de Google Play: https://play.google.com/intl/es_es/about/developer-distribution-agreement.html
- Griswoldv. Connecticut. , 381 US 479. (U.S. Supreme Court 1965).
- Hoffman, L. (1980). *Computers and privacy in the next decade*. . New York: Academic Press.
- Horrigan, J. B. (2007). A typology of information and communication technology users, Pew Internet and American Life Report, Washington, DC. *Pew Internet Report*.
- Howard, P. E., Rainie, L., & Jones, S. (2001). Days and nights on the Internet. The impact of a diffusing technology. *American Behavioral Scientist*, 45(3), 382-404. Obtenido de American Behavioral Scientist, vol. 45, no. 3, pp. 382-404, 2001.
- Hushmail. (2018). *www.hushmail.com* . Obtenido de <https://www.hushmail.com>
- Internet World Stats. (Junio de 2016). *Estadísticas de internetworldstats*. Obtenido de <http://www.internetworldstats.com/>: <http://www.internetworldstats.com/south.htm#co>
- ISMS Forum Spain. (2018). www.ismsforum.es/. Obtenido de <https://www.ismsforum.es/quien/index.php>
- Jagtap, S. S., & Hanchate, D. B. (Julio de 2017). Development of Android Based Mobile App for PrestaShop eCommerce Shopping Cart (ALC). *International Research Journal of Engineering and Technology (IRJET)*, 4(7), 2248–2254.
- Jepsen, A. L. (2006). Information search in virtual communities: Is it replacing use of off-line communication? *Journal of Marketing Communications*, 12(4), 247-261.
- Johnson, G. M., & Kulpa, A. (2007). Dimensions of online behavior: Toward a user typology. *CyberPsychology and Behavior*, 10(6), 773-779.
- Joinson, A. N., Reips, U.-D., Buchanan, T. a., & Schofield, P. (2008). Privacy, Trust And Self-Disclosure Online . *IN PRESS, HUMAN-COMPUTER INTERACTION*, 1-46.
- Jotform. (2018). <https://www.jotform.com/pricing>. Obtenido de <https://www.jotform.com/pricing>: <https://www.jotform.com/pricing>
- Keep safe. (2018). *www.getkeepsafe.com*. Obtenido de <https://www.getkeepsafe.com>

- Kim Bartel, S. (2002). *Toward a Typology of Internet Users and Online Privacy Concerns*. Oregon, USA: School of Journalism and Communication, University of Oregon, Eugene.
- Kimmel, A. J. (1996). *Ethical issues in behavioral research: A study*. Cambridge, MA: Blackwell.
- Krairit, D. (2018). The New Face of Internet User Typology: The Case of Thailand. *Journal of Theoretical and Applied Electronic Commerce Research*, 13(2), 58-79.
- Latch. (2018). *latch.elevenpaths.com*. Obtenido de <https://latch.elevenpaths.com/www/index.html>
- Li, C., Bernoff, J., Fiorentino, R., & Glass, S. (2007). Social technographics mapping participation in activities forms, Forrester, New York. *A Forrester Research Report*.
- Makr, A. (2018). <https://www.appmakr.com>. Obtenido de <https://www.appmakr.com>: https://www.appmakr.com/?locale=es_US
- McLean, D. (1993). *Privacy and its invasion*. Westport, CT: Praeger.
- Meyer., D. B. (2006). *Síntesis de "Estrategia de la investigación descriptiva" en Manual de técnica de la investigación educacional*.
- Mincomercio, i. y., & Presidente de la republica, d. C. (Super intendencia de industria y comercio de 2013). *Decreto 1317 DE 2013 Sobre la protección de datos personales*. Obtenido de www.sic.gov.co: <http://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>
- MINTIC. (Marzo de 2015). *Boletín trimestral de las tic*. Obtenido de <http://colombiatic.mintic.gov.co/>: http://colombiatic.mintic.gov.co/602/articles-8598_archivo_pdf.pdf
- MinTIC. (20 de Marzo de 2018). *¿Cuáles son las redes sociales que más se usan en su región?* Obtenido de www.mintic.gov.co: <https://www.mintic.gov.co/portal/604/w3-article-70369.html>
- MinTIC. (23 de Abril de 2018). *Tres operadores manejan el 88% de los usuarios de celular*. Obtenido de <https://www.elnuevosiglo.com.co>: <https://www.elnuevosiglo.com.co/articulos/04-2018-tres-operadores-manejan-el-88-de-los-usuarios-de-celular>
- MINTIC, M. D. (Marzo de 2017). *BOLETÍN TRIMESTRAL DE LAS TIC Marzo de 2017*. Obtenido de <http://colombiatic.mintic.gov.co/>: http://colombiatic.mintic.gov.co/602/articles-51235_archivo_pdf.pdf
- MINTIC; Infométrika S.A.S, consultores. (Diciembre de 2016). *Diseño y medición Indicador Terminales por cada 100 habitantes*. Obtenido de <http://www.mintic.gov.co>: http://www.mintic.gov.co/portal/604/articles-51641_recurso_1.pdf

- MobApp Creator. (2018). *https://www.mobappcreator.com*. Obtenido de <https://www.mobappcreator.com>: <https://www.mobappcreator.com/es/Inicio#pricing>
- Moceyunas, A. K. (1996). *Privacy laws for technology business UCLA Institute for Cyberspace Law and Policy*. Obtenido de <http://www.gse.ucla.edu/iclp>
- Mozilla Corp. (9 de Marzo de 2017). *Hackers, Trackers and Snoops: Our Privacy Survey Results*. Obtenido de <https://medium.com/>: <https://medium.com/mozilla-internet-citizen/hackers-trackers-and-snoops-our-privacy-survey-results-1bfa0a728bd5>
- Mozilla Corp. (Febrero de 2017). *Privacy Survey Analysis*. Obtenido de <https://drive.google.com>: https://drive.google.com/file/d/0B5UMbl9u1_wQdGZGQ05mUjRxLVE/view
- My Permissions. (2018). *mypermissions.com*. Obtenido de <https://mypermissions.com/about/>
- My permissions. (2018). *mypermissions.com/*. Obtenido de <https://mypermissions.com/about/>
- Nowak, G., & Phelps, J. (1995). Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When “Privacy” Matters. *Journal of Direct Marketing*, 9, 46-60. 10.1002/dir.4000090307.
- OFCOM, V. (2008). Social Networking. A Quantitative and Qualitative Research Report into Attitudes, Behaviours and Use. *London UK: Office of Communication*.
- Ortega Egea, J. M., Menéndez, M. R., & González, M. V. (2007). Diffusion and usage patterns of Internet services in the European Union, informations research. *International Electronic Journal*, 12(2), 302.
- Panoptick Electronic Frontier Foundation . (2018). *panoptick.eff.org*. Obtenido de <https://panoptick.eff.org>
- Park, I., Sharman, R., Raghav Rao, H., & Upadhyaya, S. (2016). The Effect of Spam and Privacy Concerns on E-mail Users' Behavior. *ACM Transactions on Information and System Security - TISSEC* .
- Pérez Porto, J., & Merino, M. (Junio de 2010). *DEFINICIÓN DE PRIVACIDAD*. Obtenido de <http://definicion.d>: <http://definicion.de/privacidad/>
- Picchi, A. (21 de Marzo de 2018). *CBS news*. Obtenido de Facebook: Your personal info for sale in MONEYWATCH: <https://www.cbsnews.com/news/facebook-your-personal-info-for-sale/>
- Picchi, A., & Carissimo, J. (20 de Marzo de 2018). *CBS news*. Obtenido de 3 states open investigations into Cambridge Analytica, Facebook: <https://www.cbsnews.com/live-news/facebook-under-fire-the-latest-on-cambridge-analytica-scandal-live-updates/>

- Platzi. (2018). *platzi.com*. Obtenido de <https://platzi.com/blog/proteger-datos-personales/>
- Popken, B. (10 de Mayo de 2018). *NBC news*. Obtenido de Google sells the future, powered by your personal data: <https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501>
- Regan, P. (1995). *Legislating privacy: Technology, social values and public policy*. . Chapel Hill: University of North Carolina Press.
- Rifon, N. J., LaRose, R., & Lewis, M. L. (20 de Octubre de 2007). *Resolving the Privacy Paradox: Toward a Social-Cognitive Theory of Consumer Privacy Protection*. Obtenido de www.msu.edu: <http://www.msu.edu/wirthch1/privacyparadox07.pdf>
- Rimal, R. (2000). Closing the Knowledge–Behavior Gap in Health Promotion: The Mediating Role of Self-efficacy. *Health Communication*, 3(12), 219–237.
- Rogers, J. L. (1996). Mail advertising and consumer behavior. *Psychology & Marketing*, 211-233 volumen 13, Numero 2.
- Rogers, R. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology*, 93–114.
- Rogers, R. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change:. En J. Cacioppo, & R. Petty, *A Revised Theory of Protection Motivation* (págs. 153–76). New York: (eds) Social Psychophysiology: a Sourcebook, Guilford Press.
- Romero Landeros, C., González Suárez, E., & Anabalón, M. (2016). Expectativas de autoeficacia respecto al uso de tics y nuevas tecnologías, relacionado a los cumplimientos de demandas de la organización. *Universidad academia de humanismo cristiano facultad de ciencias sociales escuela de psicología*, 1-167.
- Rouse, M. (junio de 2017). *Privacidad de datos (privacidad de información)*. Obtenido de <http://searchdatacenter.techtarg.com>: <http://searchdatacenter.techtarg.com/es/definicion/Privacidad-de-datos-privacidad-de-informacion>
- Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook Users’ Online Privacy Protection: Risk, Trust, Norm Focus Theory, and the Theory of Planned Behavior. *The Journal of Social Psychology*, 154(4), 352-369.
- Samsung, E. (18 de Abril de 2016). *Cómo proteger tu móvil ante malware e intrusiones*. Obtenido de <http://www.samsung.com/>: <http://www.samsung.com/es/a-fondo/contenidos-y-servicios/como-proteger-tu-movil-ante-malware/>

- Schoeman, F. (1984). Philosophical dimensions of privacy. . *American Philosophical Quarterly*, 199 - 213.
- Schoeman, F. (1992). *Privacy and social freedom*. . Cambridge: Cambridge University Press.
- Schwarzer, R. (. (1992). *Self-efficacy: Thought control of action*. Washington DC: Hemisphere.
- Shah, D., Kwak, N., & Holbert, R. (2001). Connecting and ‘disconnecting with civic life: Patterns of Internet use and the production of social capital. *Political Communication*, 18(2), 141-162.
- Sheehan, K. B. (2010). Toward a typology of internet users and online privacy concerns. *The Information Society*, 18(1), 21-32.
- Shih, C.-F., & Venkatesh, A. (2004). Beyond adoption: Development and application of a use-diffusion model. *Journal of Marketing*, 68(1), 59-72.
- Sikur. (2018). *www.sikur.com* . Obtenido de <https://www.sikur.com>
- Silent Circle. (2018). *www.silentcircle.com*. Obtenido de <https://www.silentcircle.com>
- Smart posts widget. (2016). *wordpress.org/plugins/*. Obtenido de <https://es.wordpress.org/plugins/smart-posts-widget/>
- Sommerville, I. (2005). Ingeniería del software. En *Ingeniería del software* (pág. 687). Pearson Educación.
- Sophos Mobile Security . (2018). *www.sophos.com*. Obtenido de <https://www.sophos.com/en-us.aspx>
- Stat Counter Global Stats. (25 de 09 de 2017). https://www.abc.es/tecnologia/informatica/software/abci-google-android-sistemas-operativos-201604202207_noticia.html. Obtenido de https://www.abc.es/tecnologia/informatica/software/abci-google-android-sistemas-operativos-201604202207_noticia.html
- Statista. (Mayo de 2017). <https://www.statista.com>. Obtenido de Most concerning issues about online usage according to internet users in the United States as of May 2017: <https://www.statista.com/statistics/248488/frequency-with-which-us-internet-users-worry-about-online-privacy/>
- SurveyMonkey. (2018). https://es.surveymonkey.com/pricing/?ut_source=header. Obtenido de https://es.surveymonkey.com/pricing/?ut_source=header: https://es.surveymonkey.com/pricing/?ut_source=header

- Tor Project. (2018). *www.torproject.org*. Obtenido de <https://www.torproject.org/about/overview.html>
- Type Form. (2018). *https://www.typeform.com/pricing/#*. Obtenido de <https://www.typeform.com/pricing/#>: <https://www.typeform.com/pricing/#>
- Ugarte Cataldo, J. L. (2013). Privacidad, trabajo y derechos fundamentales. *Estudios constitucionales*, 9(1), 13-36.
- Ultrasurf. (2018). *https://ultrasurf.us/*. Obtenido de <https://ultrasurf.us/about/>
- Upplication. (2017). *www.upplication.com*. Obtenido de <https://www.upplication.com/blog/question-las-notificaciones-push/>
- Velásquez Durán, A. M. (18 de Enero de 2018). *Aprenda a crear aplicaciones sin saber programar*. Obtenido de <https://www.eltiempo.com/tecnosfera/apps/como-crear-aplicaciones-sin-saber-programar-172218>
- Verma, N., Kansal, S., & Malvi, H. (2018). Development of Native Mobile Application Using Android Studio for Cabs and Some Glimpse of Cross Platform Apps. *International Journal of Applied Engineering Research*, 13(16), 12527-12530.
- Whalen v. Roe , 429 U.S. 589 (U.S. Supreme Court 1977).
- Witte, K. (1992). Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. *Communication Monographs*, 59(4): 329–49.
- Wufoo. (2018). *https://www.wufoo.com/pricing/*. Obtenido de <https://www.wufoo.com/pricing/>: <https://www.wufoo.com/pricing/>
- Yao, M. Z., & Linz, D. G. (2008). Predicting Self-Protections of Online Privacy. *CYBERPSYCHOLOGY & BEHAVIOR*, 615-617.
- Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *The Journal of Consumer Affairs*, Vol. 43, No. 3, 389-418.
- Zhou, Y., Zhang, X., Jiang, X., & Freeh, V. W. (2011). Taming Information-Stealing Smartphone Applications (on Android). *Trust and Trustworthy Computing*, 93-107.

10 ANEXOS

ANEXO 1

Instrumento de medición

Evalúate tú mismo

Parte 1 Variables demográficas

La primera recoge información estadística respecto a aspectos demográficos, personales y mediciones generales en cuanto uso de Internet.

Edad

- 16-25
- 26-35
- 36-45
- 46-55
- Mayor de 55

Género

- Masculino
- Femenino

Estrato socioeconómico según escala de clasificación en Colombia

- 1
- 2
- 3
- 4
- 5
- 6

Estado civil

- Soltero
- Casado
- Otro

Último nivel educativo

- Bachillerato
- Técnico/Tecnólogo
- Pregrado
- Postgrado

¿Cuánto tiempo lleva usando Internet?

- 1-5 años
- 6-10 años
- 11-15 años
- Mas de 15 años

¿Cuáles de las siguientes actividades realiza con más frecuencia al acceder a Internet?

Búsqueda de información especializada (ejemplo: Bases de datos)

- Redes sociales
- Trabajo
- Estudio
- Juegos - ocio

¿Cuánto tiempo lleva haciendo compras en línea?

- Nunca he comprado en línea
- 1 - 5 años
- 5 - 10 años
- 10 - 15 años
- Más de 15 años

¿Cuántas veces al mes realiza compras en línea?

- 0
- 1-5
- 5-10
- 11-15
- Mas de 15

¿Cuántos correos electrónicos no deseados (spam) recibe al día?

- 0
- 1-5
- 5-10

- 11-15
- Mas de 15

¿Hace cuánto tiene cuenta en redes sociales?

- No uso redes sociales
- 1-5 años
- 5-10 años
- 11-15 años
- de 15 años

¿Cuáles de las siguientes aplicaciones y/o redes sociales utiliza?

- Facebook
- Google+
- Badoo
- WhatsApp
- Telegram
- Instagram
- Snapchat
- Tinder
- Happn
- Tango
- Flickr
- Tumblr
- LinkedIn
- Ninguna
- Otras

¿Cuándo está o ha estado en una relación afectiva, comparte alguna de la siguiente información con la otra persona?

Dispositivos de acceso a la red (computador/dispositivo móvil)

- Contraseñas
- Correo electrónico
- Cuenta de alguna página web
- Perfiles de redes sociales
- Material sensible (p. ej. fotos, videos, exámenes médicos)
- No comparte ninguna información

Parte 2: Preocupación por la privacidad

La segunda parte estudia la preocupación del usuario frente a su exposición al utilizar Internet.

Cada pregunta se califica en una escala de 1 a 5 siendo 1 la escala más baja de preocupación denominada “Para nada me preocupa”, y 5 la escala más alta de preocupación denominada “Me preocupa mucho”.

1. A manera general cuánto me preocupa la privacidad de mi información en Internet.
2. Me preocupa la exposición de mi información personal en redes sociales como Facebook, Instagram, Snapchat, WhatsApp.
3. Me preocupa que dentro de 5 años se pueda encontrar información mía que para entonces me pueda avergonzar o perjudicar a nivel laboral o social.
4. Me preocupa que, al buscar un servicio o empresa en línea, el sitio web no sea realmente el que estoy buscando sino uno fraudulento.
5. Me preocupa que me solicitan demasiada información personal al registrarme en Redes sociales o al realizar compras en línea.
6. Me preocupa que las redes sociales y páginas web donde estoy registrado puedan vender a terceros datos mis datos.
7. Me preocupa que la gente con quien interactúo en línea no sea quien dice ser y pueda engañarme.
8. Me preocupa que mi información disponible en línea pueda ser vista por personas de mi entorno, familiar, laboral o académico y pueda perjudicarme en alguna forma.
9. Me preocupa que persona desconocida pueda obtener información personal acerca de mí, de mis actividades en línea, o de mis redes sociales sin que me entere.
10. Me preocupa que personas con intenciones engañosas envíen solicitudes de amistad o para conectarse conmigo en las redes sociales que utilizo.
11. Me preocupa que un tercero pueda interceptar mi conexión y robarme información, además de hacerse pasar por mí con intenciones delictivas (suplantación de identidad).
12. Me preocupa que, si utilizo mis datos bancarios para comprar algo en Internet, estos sean obtenidos / interceptados por otra persona.
13. Me preocupa que un virus informático pueda enviar Correos electrónicos, Mensajes, o Chats falsos a mi nombre.
14. Me preocupa dejar abierta una sesión de mis redes sociales o correos en un dispositivo o computador público o de otra persona.
15. Me preocupa que los Correos electrónicos, Mensajes y Chats que recibo no sean de quienes dicen enviarlos.
16. Me preocupa que el gobierno de mi país o de otros países puedan obtener información sobre mis actividades en línea sin que yo sea advertido.
17. En una relación afectiva me preocupa que la otra persona exponga material privado e íntimo (contenido sexual explícito).

Parte 3: Comportamiento para la protección de la privacidad

Estudia los comportamientos de los usuarios frente a diferentes situaciones que afronta al utilizar Internet o compartir información a través del mismo.

Cada pregunta se califica en una escala de 1 a 5 siendo 1 la escala más baja denominada “Nunca”, 3 la escala intermedia denominada “Algunas veces” y 5 la escala más alta de preocupación denominada “Siempre”.

1. Al ingresar a una página web me aseguro de que el sitio tenga al menos una marca de confianza (Certificado SSL) o que la conexión sea segura (https).
2. Leo, entiendo y apruebo las “cookies” de los sitios web y aplicaciones a las que accedo.
3. Borro las "cookies" de mi navegador después de cada sesión en línea o después de cada cierto tiempo.
4. Utilizo programas o software que bloqueen las "cookies" de los sitios web a los que accedo.
5. Utilizo aplicaciones o software que permitan navegación anónima en Internet (p. ej. navegador Tor, Redes VPN).
6. Asigno contraseñas distintas para cada sitio web que uso con frecuencia (Correos electrónicos, redes sociales, Cuentas bancarias).
7. Utilizo direcciones de correo electrónico distintas a Yahoo!, Gmail o Hotmail para buscar mayor garantía de seguridad y privacidad.
8. Uso diferentes correos electrónicos para distintos fines (trabajo, estudio, personal, etc.).
9. Consulto las políticas de privacidad, leo los términos y condiciones antes de acceder a un sitio web o de comercio electrónico.
10. Rechazo las opciones automáticas para recibir Boletines electrónicos (correo con publicidad comercial) de los sitios web en los que me registro.
11. Opto por controlar y no revelar información personal a terceros para que la utilicen con fines de mercadeo y publicidad.
12. Evito realizar transacciones electrónicas que no me generan suficiente confianza
13. Elimino solicitudes de contacto de personas que no conozco en mis redes sociales como Facebook, Instagram, Snapchat, WhatsApp u otros que utilizo.
14. Evito abrir sesión de mis redes sociales en dispositivos que no son de mi propiedad.
15. Reviso que no existan sesiones abiertas en dispositivos diferentes a los que sean de confianza.
16. Cambio las contraseñas de mis redes sociales y correos periódicamente.
17. Leo los cambios en las políticas de seguridad y términos de servicio cuando me llega notificación de algún cambio.
18. Limito el contenido que pueden ver las personas que acceden a mis redes sociales utilizando las opciones de seguridad que ofrecen Facebook, Instagram, WhatsApp.
19. Denuncio al proveedor de redes sociales las malas conductas de personas que violan los términos de uso, las políticas de privacidad en cuanto al comportamiento y publicaciones que atentan contra mi privacidad e integridad o la de otros.

20. Utilizo las opciones de seguridad para inicio de sesión, como el envío de códigos de verificación al correo o celular (autenticación de dos pasos), en redes sociales como Facebook e Instagram.
21. En una relación afectiva hablo con mi pareja sobre compartir contraseñas, acceso a perfiles de redes sociales y material íntimo o sensible (por ejemplo, fotos, videos, información médica).
22. Al terminar una relación afectiva me aseguro de mi expareja elimina toda mi información privada o de los dos a la que tiene acceso incluidas cuentas comunes (de redes, páginas web, teléfonos y otros dispositivos) y yo también tomo las mismas medidas.
23. Tomo medidas de protección cuando detecto una advertencia de acceso no deseado o no autorizado a mis cuentas de redes sociales o de correo electrónico.

ANEXO 2

INFORME DE RESULTADOS DEL INSTRUMENTO

Edad

61 de 61 personas han respondido esta pregunta

1	16-25	23 / 38%
2	26-35	17 / 28%
3	46-55	14 / 23%
4	mayor de 55	6 / 10%
5	36-45	1 / 2%

Género

61 de 61 personas han respondido esta pregunta

1	masculino	37 / 61%
2	femenino	24 / 39%

Estrato socioeconómico según escala de clasificación en Colombia

61 de 61 personas han respondido esta pregunta

1	3	32 / 52%
2	4	10 / 16%
3	5	7 / 11%

4	2	6 / 10%
5	1	5 / 8%
6	6	1 / 2%

Estado civil

61 de 61 personas han respondido esta pregunta

1	soltero	37 / 61%
2	casado	20 / 33%
3	otro	4 / 7%

Último nivel educativo

61 de 61 personas han respondido esta pregunta

1	pregrado	28 / 46%
2	postgrado	15 / 25%
3	bachillerato	10 / 16%
4	técnico/Tecnólogo	8 / 13%

¿Cuánto tiempo lleva usando Internet?

61 de 61 personas han respondido esta pregunta

1	6-10 años	28 / 46%
2	11-15 años	17 / 28%
3	más de 15 años	12 / 20%
4	1-5 años	4 / 7%

¿Cuáles de las siguientes actividades realiza con más frecuencia al acceder a Internet?

61 de 61 personas han respondido esta pregunta

1	Redes sociales	44 / 72%
2	Trabajo	35 / 57%
3	Búsqueda de información especializada (ejemplo: Bases de datos)	32 / 52%
4	Estudio	30 / 49%
5	Juegos - ocio	15 / 25%

¿Cuánto tiempo lleva haciendo compras en línea?

61 de 61 personas han respondido esta pregunta

1	1 - 5 años	26 / 43%
---	------------	-----------------

2	Nunca he comprado en línea	26 / 43%
3	5 - 10 años	6 / 10%
4	10 - 15 años	3 / 5%
5	Más de 15 años	0 / 0%

¿Cuántas veces al mes realiza compras en línea?

61 de 61 personas han respondido esta pregunta

1	0	32 / 52%
2	1-5	27 / 44%
3	5-10	2 / 3%
4	11-15	0 / 0%

¿Cuántos correos electrónicos no deseados (spam) recibe al día?

61 de 61 personas han respondido esta pregunta

1	1-5	31 / 51%
2	5-10	18 / 30%
3	0	6 / 10%
4	Más de 15	5 / 8%
5	11-15	1 / 2%

¿Hace cuánto tiene cuenta en redes sociales?

61 de 61 personas han respondido esta pregunta

1	5-10 años	38 / 62%
2	1-5 años	13 / 21%
3	11-15 años	7 / 11%
4	no uso redes sociales	2 / 3%
5	más de 15 años	1 / 2%

¿Cuáles de las siguientes aplicaciones y/o redes sociales utiliza?

61 de 61 personas han respondido esta pregunta

1	WhatsApp	61 / 100%
2	Facebook	48 / 79%
3	Google+	32 / 52%
4	Instagram	32 / 52%
5	LinkedIn	14 / 23%
6	Otras	4 / 7%
7	Snapchat	4 / 7%
8	Telegram	4 / 7%
9	Flickr	3 / 5%
10	Tumblr	3 / 5%
11	Tinder	2 / 3%
12	Badoo	1 / 2%
13	Happn	0 / 0%
14	Ninguna	0 / 0%
15	Tango	0 / 0%

¿Cuándo está o ha estado en una relación afectiva, comparte alguna de la siguiente información con la otra persona?

61 de 61 personas han respondido esta pregunta

1	Material sensible (p. ej. fotos, videos, exámenes médicos)	25 / 41%
2	Dispositivos de acceso a la red (computador/dispositivo móvil)	23 / 38%
3	Correo electrónico	20 / 33%
4	No comparte ninguna información	19 / 31%
5	Perfiles de redes sociales	10 / 16%
6	Contraseñas	9 / 15%
7	Cuenta de alguna página web	6 / 10%

A manera general cuánto me preocupa la privacidad de mi información en Internet

61 de 61 personas han respondido esta pregunta

Media: 4.31

- 5 31 / **51%**
- 4 21 / **34%**
- 3 7 / **11%**
- 1 1 / **2%**
- 2 1 / **2%**

Me preocupa la exposición de mi información personal en redes sociales como Facebook, Instagram, Snapchat, WhatsApp

61 de 61 personas han respondido esta pregunta

Media: 4.21

- 5 30 / **49%**
- 4 20 / **33%**
- 3 6 / **10%**
- 2 4 / **7%**
- 1 1 / **2%**

Me preocupa que dentro de 5 años se pueda encontrar información mía que para entonces me pueda avergonzar o perjudicar a nivel laboral o social

61 de 61 personas han respondido esta pregunta

Media: 3.51

- 5 22 / **36%**
- 3 13 / **21%**
- 4 10 / **16%**
- 2 9 / **15%**
- 1 7 / **11%**

Me preocupa que, al buscar un servicio o empresa en línea, el sitio web no sea realmente el que estoy buscando sino uno fraudulento

61 de 61 personas han respondido esta pregunta

Media: 4.21

- 5 34 / **56%**
- 3 12 / **20%**
- 4 11 / **18%**
- 2 3 / **5%**
- 1 1 / **2%**

Me preocupa que me solicitan demasiada información personal al registrarme en Redes sociales o al realizar compras en línea

61 de 61 personas han respondido esta pregunta

Media: 4.26

- 5 31 / **51%**
- 4 20 / **33%**
- 3 6 / **10%**
- 2 3 / **5%**
- 1 1 / **2%**

Me preocupa que las redes sociales y páginas web donde estoy registrado puedan vender a terceros datos mis datos

61 de 61 personas han respondido esta pregunta

Media: 4.05

- 5 29 / **48%**
- 4 14 / **23%**

3 11 / 18%

2 6 / 10%

1 1 / 2%

Me preocupa que la gente con quien interactúo en línea no sea quien dice ser y pueda engañarme

61 de 61 personas han respondido esta pregunta

Media: 3.89

5 28 / 46%

4 13 / 21%

2 9 / 15%

3 8 / 13%

1 3 / 5%

Me preocupa que mi información disponible en línea pueda ser vista por personas de mi entorno, familiar, laboral o académico y pueda perjudicarme en alguna forma

61 de 61 personas han respondido esta pregunta

Media: 3.44

5 18 / 30%

3 14 / 23%

4 13 / 21%

2 10 / 16%

1 6 / 10%

Me preocupa que persona desconocida pueda obtener información personal acerca de mí, de mis actividades en línea, o de mis redes sociales sin que me entere

61 de 61 personas han respondido esta pregunta

Media: 4.21

5 33 / 54%

4 13 / 21%

3 10 / 16%

2 5 / 8%

Me preocupa que personas con intenciones engañosas envíen solicitudes de amistad o para conectarse conmigo en las redes sociales que utilizo

61 de 61 personas han respondido esta pregunta

Media: 3.89

- 5 27 / **44%**
- 4 14 / **23%**
- 3 9 / **15%**
- 2 8 / **13%**
- 1 3 / **5%**

Me preocupa que un tercero pueda interceptar mi conexión y robarme información, además de hacerse pasar por mí con intenciones delictivas (suplantación de identidad)

61 de 61 personas han respondido esta pregunta

Media: 4.28

- 5 35 / **57%**
- 4 13 / **21%**
- 3 9 / **15%**
- 2 3 / **5%**
- 1 1 / **2%**

Me preocupa que, si utilizo mis datos bancarios para comprar algo en Internet, estos sean obtenidos / interceptados por otra persona

61 de 61 personas han respondido esta pregunta

Media: 4.43

- 5 39 / **64%**
- 4 14 / **23%**
- 3 5 / **8%**
- 1 2 / **3%**
- 2 1 / **2%**

Me preocupa que un virus informático pueda enviar Correos electrónicos, Mensajes, o Chats falsos a mi nombre

61 de 61 personas han respondido esta pregunta

Media: 4.31

- 5 37 / **61%**
- 4 12 / **20%**
- 3 7 / **11%**

2 4 / 7%

1 1 / 2%

Me preocupa dejar abierta una sesión de mis redes sociales o correos en un dispositivo o computador público o de otra persona

61 de 61 personas han respondido esta pregunta

Media: 4.36

5 40 / 66%

4 10 / 16%

3 6 / 10%

2 3 / 5%

1 2 / 3%

Me preocupa que el Correos electrónico, Mensajes y Chats que recibo no sean de quienes dicen enviarlos

61 de 61 personas han respondido esta pregunta

Media: 3.84

5 23 / 38%

4 16 / 26%

3 14 / 23%

2 5 / 8%

1 3 / 5%

Me preocupa que el gobierno de mi país o de otros países pueda obtener información sobre mis actividades en línea sin que yo sea advertido

61 de 61 personas han respondido esta pregunta

Media: 3.95

5 24 / 39%

4 18 / 30%

3 14 / 23%

1 3 / 5%

2 2 / 3%

En una relación afectiva me preocupa que la otra persona exponga material privado e íntimo (contenido sexual explícito)

61 de 61 personas han respondido esta pregunta

Media: 3.80

- 5 28 / **46%**
- 4 13 / **21%**
- 1 8 / **13%**
- 3 8 / **13%**
- 2 4 / **7%**

Al ingresar a una página web me aseguro de que el sitio tenga al menos una marca de confianza (Certificado SSL) o que la conexión sea segura (https)

61 de 61 personas han respondido esta pregunta

Media: 3.38

- 5 18 / **30%**
- 3 13 / **21%**
- 4 13 / **21%**
- 1 9 / **15%**
- 2 8 / **13%**

Leo, entiendo y apruebo las "cookies" de los sitios web y aplicaciones a las que accedo

61 de 61 personas han respondido esta pregunta

Media: 2.80

- 3 23 / **38%**
- 1 12 / **20%**
- 2 11 / **18%**
- 5 8 / **13%**
- 4 7 / **11%**

Borro las "cookies" de mi navegador después de cada sesión en línea o después de cada cierto tiempo

61 de 61 personas han respondido esta pregunta

Media: 2.57

- 1 18 / **30%**
- 3 17 / **28%**
- 2 12 / **20%**

5 8 / 13%

4 6 / 10%

Utilizo programas o software que bloqueen las "cookies" de los sitios web a los a accedo

61 de 61 personas han respondido esta pregunta

Media: 2.56

1 20 / 33%

3 19 / 31%

2 8 / 13%

4 7 / 11%

5 7 / 11%

Utilizo aplicaciones o software que permitan navegación anónima en Internet (p. ej. navegador Tor, Redes VPN)

61 de 61 personas han respondido esta pregunta

Media: 2.08

1 27 / 44%

3 16 / 26%

2 11 / 18%

4 5 / 8%

5 2 / 3%

Asigno contraseñas distintas para cada sitio web que uso con frecuencia (Correos electrónicos, redes sociales, Cuentas bancarias)

61 de 61 personas han respondido esta pregunta

Media: 3.33

3 20 / 33%

5 17 / 28%

4 9 / 15%

1 8 / 13%

2 7 / 11%

Utilizo direcciones de correo electrónico distintas a Yahoo!, Gmail o Hotmail para buscar mayor garantía de seguridad y privacidad

61 de 61 personas han respondido esta pregunta

Media: 2.54

- 1 23 / **38%**
- 3 16 / **26%**
- 5 10 / **16%**
- 2 7 / **11%**
- 4 5 / **8%**

Uso diferentes correos electrónicos para distintos fines (trabajo, estudio, personal, etc.)

61 de 61 personas han respondido esta pregunta

Media: 3.52

- 3 18 / **30%**
- 5 18 / **30%**
- 4 14 / **23%**
- 1 7 / **11%**
- 2 4 / **7%**

Consulto las políticas de privacidad, leo los términos y condiciones antes de acceder a un sitio web o de comercio electrónico

61 de 61 personas han respondido esta pregunta

Media: 2.74

- 1 17 / **28%**
- 3 17 / **28%**
- 5 11 / **18%**
- 2 10 / **16%**
- 4 6 / **10%**

Rechazo las opciones automáticas para recibir Boletines electrónicos (correo con publicidad comercial) de los sitios web en los que me registro

61 de 61 personas han respondido esta pregunta

Media: 3.89

- 5 30 / **49%**
- 3 16 / **26%**
- 2 6 / **10%**
- 4 6 / **10%**

1 3 / 5%

Opto por controlar y no revelar información personal a terceros para que la utilicen con fines de mercadeo y publicidad

61 de 61 personas han respondido esta pregunta

Media: 4.02

5 24 / 39%

4 18 / 30%

3 16 / 26%

2 2 / 3%

1 1 / 2%

Evito realizar transacciones electrónicas que no me generan suficiente confianza

61 de 61 personas han respondido esta pregunta

Media: 4.39

5 41 / 67%

4 10 / 16%

3 6 / 10%

1 3 / 5%

2 1 / 2%

Elimino solicitudes de contacto de personas que no conozco en mis redes sociales como Facebook, Instagram, Snapchat, WhatsApp u otros que utilizo

61 de 61 personas han respondido esta pregunta

Media: 4.31

5 39 / 64%

3 10 / 16%

4 8 / 13%

1 2 / 3%

2 2 / 3%

Evito abrir sesión de mis redes sociales en dispositivos que no son de mi propiedad

61 de 61 personas han respondido esta pregunta

Media: 4.20

5 31 / 51%

4 16 / 26%

3 10 / 16%

2 3 / 5%

1 1 / 2%

Reviso que no existan sesiones abiertas en dispositivos diferentes a los que sean de confianza

61 de 61 personas han respondido esta pregunta

Media: 3.92

5 27 / 44%

4 15 / 25%

3 11 / 18%

1 5 / 8%

2 3 / 5%

Cambio las contraseñas de mis redes sociales y correos periódicamente

61 de 61 personas han respondido esta pregunta

Media: 2.64

3 18 / 30%

1 15 / 25%

2 14 / 23%

5 8 / 13%

4 6 / 10%

Leo los cambios en las políticas de seguridad y términos de servicio cuando me llega notificación de algún cambio

61 de 61 personas han respondido esta pregunta

Media: 2.70

1 16 / 26%

3 16 / 26%

2 14 / 23%

5 13 / 21%

4 2 / 3%

Limito el contenido que pueden ver las personas que acceden a mis redes sociales utilizando las opciones de seguridad que ofrecen Facebook, Instagram, WhatsApp

61 de 61 personas han respondido esta pregunta

Media: 3.79

- 5 25 / **41%**
- 3 15 / **25%**
- 4 12 / **20%**
- 1 5 / **8%**
- 2 4 / **7%**

Denuncio al proveedor de redes sociales las malas conductas de personas que violan los términos de uso, las políticas de privacidad en cuanto al comportamiento y publicaciones que atentan contra mi privacidad e integridad o la de otros

61 de 61 personas han respondido esta pregunta

Media: 2.74

- 1 20 / **33%**
- 3 14 / **23%**
- 5 11 / **18%**
- 4 9 / **15%**
- 2 7 / **11%**

Utilizo las opciones de seguridad para inicio de sesión, como el envío de códigos de verificación al correo o celular (autenticación de dos pasos), en redes sociales como Facebook e Instagram

61 de 61 personas han respondido esta pregunta

Media: 3.38

- 5 18 / **30%**
- 3 16 / **26%**
- 4 11 / **18%**
- 1 8 / **13%**
- 2 8 / **13%**

En una relación afectiva hablo con mi pareja sobre compartir contraseñas, acceso a perfiles de redes sociales y material íntimo o sensible (por ejemplo, fotos, videos, información médica)

61 de 61 personas han respondido esta pregunta

Media: 2.23

- 1 27 / 44%
- 2 13 / 21%
- 4 8 / 13%
- 3 7 / 11%
- 5 6 / 10%

Al terminar una relación afectiva me aseguro de mi expareja elimina toda mi información privada o de los dos a la que tiene acceso incluidas cuentas comunes (de redes, páginas web, teléfonos y otros dispositivos) y yo también tomo las mismas medidas

61 de 61 personas han respondido esta pregunta

Media: 2.75

- 1 18 / 30%
- 3 12 / 20%
- 5 12 / 20%
- 2 11 / 18%
- 4 8 / 13%

Tomo medidas de protección cuando detecto una advertencia de acceso no deseado o no autorizado a mis cuentas de redes sociales o de correo electrónico

61 de 61 personas han respondido esta pregunta

Media: 3.79

- 5 26 / 43%
- 3 15 / 25%
- 4 10 / 16%
- 2 6 / 10%
- 1 4 / 7%

ANEXO 3 COMENTARIOS DE LOS USUARIOS

- Venur Garzón 4/5/2018 a la(s) 19:20
★★★★★
Excelente felicitaciones muy buena app
Dispositivo: Moto G4 Play (harpia)
Versión de la aplicación: —
SO: Android 6.0

- Johan Osorio 3/5/2018 a la(s) 23:33

★ ★ ★ ★ ★

Muy buena app ayuda a tu seguridad 😊

Dispositivo: Moto G (5) Plus (potter_n)

Versión de la aplicación: 72 (1.0)

SO: Android 7.0
- Darío Insuasty Ramos 3/5/2018 a la(s) 22:41

★ ★ ★ ★ ★

Una app muy funcional, me lleva a estar más pendiente de la importancia de la protección de mis datos en internet. ¡Excelentes recomendaciones!

Dispositivo Xperia Z3 (D6653)

Versión de la aplicación 72 (1.0)

SO Android 6.0
- Luisa María Vela Tobar 3/5/2018 a la(s) 21:50

★ ★ ★ ★ ★

Muy buena aplicación

Dispositivo: Galaxy J2 (j2lte)

Versión de la aplicación: 72 (1.0)

SO: Android 5.1
- 3/5/2018 a la(s) 19:53

★ ★ ★ ★ ★

Esta super... muy útil

Dispositivo: Galaxy J5 Prime (on5xelte)

Versión de la aplicación: 72 (1.0)

SO: Android 7.0
- Stefania Enríquez 3/5/2018 a la(s) 16:11

★ ★ ★ ★ ★

Una excelente app que nos concientiza de la manera en la que manejamos nuestra información personal. Mediante la encuesta podemos identificar en qué factores estamos fallando y tomar medidas para proteger nuestra información. Felicitaciones por esta app.

Dispositivo: B6000-H (B6000)

Versión de la aplicación: 72 (1.0)

SO: Android 4.4
- David Eduardo Ordoñez García 3/5/2018 a la(s) 14:38

★ ★ ★ ★ ★

Ayuda. A comprender como nuestra seguridad informática está comprometida.

Dispositivo: Galaxy S6 Edge (zerolte)

Versión de la aplicación: 72 (1.0)

SO: Android 7.0
- 3/5/2018 a la(s) 12:32 0

★ ★ ★ ★ ★

Muy buena Me Gusto La App

Responder este comentario
Dispositivo: 4013M (Pixi3-4)
Versión de la aplicación: —
SO: Android 4.4

- Tulio Victoria G 3/5/2018 a la(s) 8:56

★★★★★

Esta interesante la aplicación
Dispositivo: Galaxy J7 (j7elte)
Versión de la aplicación: 72 (1.0)
SO: Android 6.0

- Fabio Coral 3/5/2018 a la(s) 7:56

★★★★★

¡Excelente! Hay datos que a veces no tenemos en cuenta a la hora de proteger nuestra info y es necesario tener el cuidado necesario para evitar sorpresas en un futuro. App fácil y muy intuitiva

Dispositivo: Xperia Z3+ (E6553)
Versión de la aplicación: 72 (1.0)
SO: Android 7.1

- Diana Vela 3/5/2018 a la(s) 7:28

★★★★★

¡Gran aplicación!
Dispositivo: Galaxy J1 Ace (j1acevelte)
Versión de la aplicación: 72 (1.0)
SO: Android 5.1

- Arigvame 3/5/2018 a la(s) 5:37

★★★★★

Interesante encuesta, recuerda algunas cosas que pasa uno por alto en su seguridad informática

Dispositivo: NOS Roya (Alto45)
Versión de la aplicación: —
SO: Android 4.4

- Francisco Montenegro 2/5/2018 a la(s) 23:20

★★★★★

Esta chingona la app, la recomiendo
Dispositivo Xperia Z1 (C6903)
Versión de la aplicación 72 (1.0)
SO Android 5.1

- Jorge Geoffrey Vela Ortiz 2/5/2018 a la(s) 22:53

★★★★★

La aplicación es buenísima
Dispositivo: Moto C (namath)

Versión de la aplicación: 72 (1.0)

SO: Android 7.0

- David Portilla 2/5/2018 a la(s) 22:51

★★★★★

Muy buena app califica y da recomendaciones para alertar te ayudar a proteger nuestros datos en la red

Dispositivo: Galaxy S6 Edge (zerolte)

Versión de la aplicación: 72 (1.0)

SO: Android 7.0

- Jean Tovar 2/5/2018 a la(s) 22:49

★★★★★

Excelente. Muy buena para conocer cómo estoy manejando mi información

Dispositivo: Moto G (5th Gen) (cedric)

Versión de la aplicación: 72 (1.0)

SO: Android 7.0

- melissa alejandra 2/5/2018 a la(s) 22:13

★★★★★

Recomendada Preocupación por la privacidad que existe en el mundo informático

Dispositivo: Moto G (5) Plus (potter_n)

Versión de la aplicación: 72 (1.0)

SO: Android 7.0

- Dan Skurety 2/5/2018 a la(s) 21:55

★★★★★

ufffff lo mejor al fin una app buena

Dispositivo: Galaxy J2 (j2lte)

Versión de la aplicación: —

SO: Android 5.1

ANEXO 4 PLATAFORMAS DISPONIBLES

1. Mobapp Creator

Link: <https://www.mobappcreator.com/es/Inicio#pricing>

Precio Más económico: 19 USD/Mes

Precio Full: 149 USD/Mes

BASIC	PRO	ADVANCED
<p style="text-align: center;">USD 19.00/mes facturado mensualmente</p> <p style="text-align: center;">1 APP INCLUIDA</p>	<p style="text-align: center;">USD 49.00/mes facturado mensualmente</p> <p style="text-align: center;">1 APP INCLUIDA</p>	<p style="text-align: center;">USD 149.00/mes facturado mensualmente</p> <p style="text-align: center;">5 APPS INCLUIDAS</p>
CREAR CUENTA GRATUITA	CREAR CUENTA GRATUITA	CREAR CUENTA GRATUITA
<p>App Nativa de Android ¹</p> <hr/> <p>App Nativa de iPhone ²</p> <hr/> <p>1000 Notificaciones Push por mes ³</p> <hr/> <p>Instalaciones ilimitadas</p> <hr/> <p>Actualizaciones ilimitadas</p> <hr/> <p>Módulos ilimitados</p> <hr/> <p>Soporte Online</p> <hr/> <p>Estadísticas de App</p> <hr/> <p>2 Apps en Construcción</p> <hr/> <p>2 Colaboradores</p> <hr/>	<p>App Nativa de Android ¹</p> <hr/> <p>App Nativa de iPhone ²</p> <hr/> <p>Notificaciones Push ilimitadas ³</p> <hr/> <p>Instalaciones ilimitadas</p> <hr/> <p>Actualizaciones ilimitadas</p> <hr/> <p>Módulos ilimitados</p> <hr/> <p>Soporte Dedicado</p> <hr/> <p>Estadísticas de App</p> <hr/> <p>2 Apps en Construcción</p> <hr/> <p>10 Colaboradores</p> <hr/> <p>App Marca Blanca</p>	<p>App Nativa de Android ¹</p> <hr/> <p>App Nativa de iPhone ²</p> <hr/> <p>Notificaciones Push ilimitadas ³</p> <hr/> <p>Instalaciones ilimitadas</p> <hr/> <p>Actualizaciones ilimitadas</p> <hr/> <p>Módulos ilimitados</p> <hr/> <p>Soporte Dedicado</p> <hr/> <p>Estadísticas de App</p> <hr/> <p>10 Apps en Construcción</p> <hr/> <p>100 Colaboradores</p> <hr/> <p>App Marca Blanca</p>

Figura 56. Plataforma MobApp Creator (MobApp Creator, 2018).

2. Appmak

Link: https://www.appmakr.com/?locale=es_US

Precio Más económico: Gratis

Precio Full: 99 USD/Mes

Mobile Website	App Básico	App Pro	Reseller 10-Pack
FREE	\$2 / mes*	\$99 / year*	\$39 / mes
No Credit Card Required	<i>*billed annually</i>	<i>Regularly \$130 / year</i>	
Sitio Web Móvil HTML5	App Nativa de Android en el AppMakr Market	<i>*billed annually</i>	Publish up to 10 Apps
Viewable in 1+ Billion Smartphone Browsers	Sitio Web Móvil HTML5	Apps Nativas iPhone y Android + Sitio Web Móvil HTML5	Usuarios Ilimitados
Usuarios Ilimitados	Usuarios Ilimitados	Envía tu app a iTunes, Google Play.*	Actualizaciones Ilimitadas
SIN ANUNCIOS	Actualizaciones Ilimitadas	Sitio Web Móvil HTML5	Apps Nativas iPhone y Android
Informe de Estadísticas en Vivo	SIN ANUNCIOS	Usuarios Ilimitados	Sitio Web Móvil HTML5
Custom URL & QR Code	Marca AppMakr	Actualizaciones Ilimitadas	Empieza tu propio negocio de apps, y vende tus servicios de creación de apps a tus clientes al precio que desees
User Forum & FAQ Support	Informe de Estadísticas en Vivo	SIN ANUNCIOS	SIN ANUNCIOS
Todas las Funciones Incluidas (see complete list below)	Soporte por Email	Publica Bajo tu Propia Marca	Auto-Publicación desde cualquier sitio te gusta **
	Sin Contratos, Cancela en Cualquier Momento	Cargo por App	Consigues el código fuente
	Todas las Funciones Incluidas (comprueba la lista completa más abajo)	Informe de Estadísticas en Vivo	Publica Bajo tu Propia Marca o la de tu Cliente ***
Comienza Ya		Sin Contratos, Cancela en Cualquier Momento	Informe de Estadísticas en Vivo
		Soporte Prioritario por Chat en Directo	Soporte Prioritario al Revendedor 24/7
	¡Vamos Allá!	Todas las Funciones Incluidas (comprueba la lista completa más abajo)	¡Empieza Ya!

Figura 57. App Makr (Makr, 2018).

3. Appyourself

Link: <https://appyourself.net/es/precios-crear-aplicaciones/>

Precio Más económico: 20 Euros/Mes

Precio Full: 80 Euros/Mes

The image shows three pricing plans for Appyourself, presented in a grid layout. Each plan is contained within a white box with a blue border. The Starter plan is on the left, Business in the middle, and Enterprise on the right. The Business plan has a green 'TOP' badge in its top right corner. Each plan lists its price per month and a list of features with checkmarks.

Plan	Price (€/mes)	Key Features
STARTER	20 €	<ul style="list-style-type: none">✓ Hasta 200 usuarios activos✓ Campañas: 1✓ Messenger✓ Gestión de clientes✓ Notificaciones Push✓ Smart Widget✓ Progressive Web App
BUSINESS	40 €	<ul style="list-style-type: none">✓ Hasta 2.000 usuarios activos✓ Campañas: 5✓ Messenger✓ Gestión de clientes✓ Notificaciones Push✓ Smart Widget✓ Progressive Web App
ENTERPRISE	80 €	<ul style="list-style-type: none">✓ Usuarios activos ilimitados✓ Campañas: 20✓ Messenger✓ Gestión de clientes✓ Notificaciones Push✓ Smart Widget✓ Progressive Web App✓ App en Google Play y Apple App Store✓ Success Manager

Figura 58. Appyourself (Appyourself, 2018).

4. Good Barber

Link: <https://es.goodbarber.com/pricing/>

Precio Más económico: 32 USD/Mes

Precio Full: 200 USD/Mes

ANDROID STANDARD	ANDROID FULL	IOS PREMIUM	RESELLER NATIVO
US\$ 32 /mes Facturación anual	US\$ 48 /mes Facturación anual	US\$ 96 /mes Facturación anual	US\$ 200 /mes Facturación anual
<ul style="list-style-type: none">✓ 1 Progressive Web App para Desktop, Tablet y Móvil✓ 1 App Nativa para Android✓ Nombre de dominio personalizado✓ Seguridad SSL incluida✓ Tráfico ilimitado✓ Descargas ilimitadas	<ul style="list-style-type: none">✓ 1 Progressive Web App para Desktop, Tablet y Móvil✓ 1 App Nativa para Android✓ Nombre de dominio personalizado✓ Seguridad SSL incluida✓ Tráfico ilimitado✓ Descargas ilimitadas✓ Add-ons avanzados	<ul style="list-style-type: none">✓ 1 Progressive Web App para Desktop, Tablet y Móvil✓ 1 App Nativa para Android✓ 1 App Nativa para iOS✓ Nombre de dominio personalizado✓ Seguridad SSL incluida✓ Tráfico ilimitado✓ Descargas ilimitadas✓ Add-ons avanzados	<ul style="list-style-type: none">✓ Progressive Web Apps ilimitadas para Desktop, Tablet y Móvil✓ Apps nativas para Android ilimitadas✓ App Nativas ilimitadas para iOS (cuenta de desarrollador empresa)✓ Coste de verificación adicional si se quiere distribuir en la App Store✓ Nombre de dominio personalizado✓ Seguridad SSL incluida✓ Tráfico ilimitado✓ Descargas ilimitadas✓ Add-ons avanzados

Figura 59. Good Barber (Appyourself, 2018).

5. Appy Pie

Link: <https://es.appypie.com/plan-de-precios>

Precio Más económico: 32 USD/Mes

Precio Full: 200 USD/Mes

GRATIS con anuncios	\$45000 /aplicación/mês	\$90000 /aplicación/mês	\$150000 /aplicación/mês
ELIJA EL PLAN	ELIJA EL PLAN	ELIJA EL PLAN	ELIJA EL PLAN
Plataformas soportadas 	Plataformas soportadas 	Plataformas soportadas 	Plataformas soportadas 
Distribución ** X	Distribución ** 	Distribución ** 	Distribución ** 
Anuncios de Appy Pie anuncios relevantes	Anuncios de Appy Pie Sin Anuncios!	Anuncios de Appy Pie Sin Anuncios!	Anuncios de Appy Pie Sin Anuncios!
Puedes Editar tu App Durante las primeras 48 hrs	Puedes Editar tu App Ilimitadamente	Puedes Editar tu App Ilimitadamente	Puedes Editar tu App Ilimitadamente
Publicar bajo tu cuenta de desarrollador. X	Publicar bajo tu cuenta de desarrollador. <input checked="" type="checkbox"/>	Publicar bajo tu cuenta de desarrollador. <input checked="" type="checkbox"/>	Publicar bajo tu cuenta de desarrollador. <input checked="" type="checkbox"/>
Asistencia One to One (En la aplicación de publicación a la tienda de Apple) X	Asistencia One to One (En la aplicación de publicación a la tienda de Apple) X	Asistencia One to One (En la aplicación de publicación a la tienda de Apple) X	Asistencia One to One (En la aplicación de publicación a la tienda de Apple) <input checked="" type="checkbox"/>
Cantidad de Notificaciones Push 0/mensual X	Cantidad de Notificaciones Push 5000/mensual 	Cantidad de Notificaciones Push 10000/mensual 	Cantidad de Notificaciones Push 25000/mensual 
Espacio del disco 100 MB	Espacio del disco 200 MB	Espacio del disco 400 MB	Espacio del disco 600 MB
Ancho de banda mensual 2 GB	Ancho de banda mensual 4 GB	Ancho de banda mensual 8 GB	Ancho de banda mensual 12 GB
Aplicación Analytics con Google Analytics X	Aplicación Analytics con Google Analytics <input checked="" type="checkbox"/>	Aplicación Analytics con Google Analytics <input checked="" type="checkbox"/>	Aplicación Analytics con Google Analytics <input checked="" type="checkbox"/>
Gana dinero a través de publicidad X	Gana dinero a través de publicidad <input checked="" type="checkbox"/>	Gana dinero a través de publicidad <input checked="" type="checkbox"/>	Gana dinero a través de publicidad <input checked="" type="checkbox"/>
Atención al cliente X	Atención al cliente Correo electrónico & Chat	Atención al Cliente Correo electrónico, Chat & Llamar	Atención al Cliente Correo electrónico, Chat & Llamar
Quitar Appy Pie Marca (su propia aplicación de marca blanca) X	Quitar Appy Pie Marca (su propia aplicación de marca blanca) X	Quitar Appy Pie Marca (su propia aplicación de marca blanca) <input checked="" type="checkbox"/>	Quitar Appy Pie Marca (su propia aplicación de marca blanca) <input checked="" type="checkbox"/>

Figura 60. Appy Pie (Appypie, 2018)

Plataformas De Gestión De Encuestas

6. Wufoo

Link: <https://www.wufoo.com/pricing/>

Precio Más económico: Gratis

Precio Full: 99 USD/Mes

GRATIS	MOTOR DE ARRANQUE	PROFESIONAL	AVANZADO
GRATIS para siempre ¡REGÍSTRATE!	\$ 19 .00 mes Ir anual, guardar 25%! → ¡REGÍSTRATE!	\$ 39 .00 mes Ir anual, guardar 25%! → ¡REGÍSTRATE!	\$ 99 .00 mes Ir anual, guardar 25%! → ¡REGÍSTRATE!
5 formas	10 formas	Formas Ilimitadas	Formas Ilimitadas
100 entradas	1,000 entradas	5,000 entradas	25,000 entradas
10 campos	Max Fields	Max Fields	Max Fields
1 usuarios	1 usuarios	5 usuarios	20 usuarios
Informes ilimitados	Informes ilimitados	Informes ilimitados	Informes ilimitados
-	Subidas de 1GB	5GB Cargas	10GB Cargas
-	-	Aceptar pagos!	

Figura 61. Wufoo (Wufoo, 2018).

7. Jotform

Link: <https://www.jotform.com/pricing>

Precio Más económico: Gratis

Precio Full: 99 USD/Mes

Motor de arranque	Bronce	Plata	Oro
GRATIS	\$ 19 / mes	\$ 39 / mes	\$ 99 / mes
100 Presentaciones mensuales Envíos seguros SSL Recibe 3 pagos	1,000 Presentaciones mensuales Envíos seguros SSL Reciba 10 pagos	10,000 Presentaciones mensuales Envíos seguros SSL Reciba 100 pagos	100,000 Presentaciones mensuales Envíos seguros SSL Reciba pagos ilimitados
100 MB Espacio disponible	10 GB Espacio disponible	100 GB Espacio disponible	1 TB Espacio disponible
5 Formularios	25 Formularios	100 Formularios	Ilimitado Formularios
1,000 Vistas de formulario mensuales	10,000 Vistas de formulario mensuales	Ilimitado Vistas de formulario mensuales	Ilimitado Vistas de formulario mensuales
500 Almacenamiento de envío total	Ilimitado Almacenamiento de envío total	Ilimitado Almacenamiento de envío total	Ilimitado Almacenamiento de envío total
Ilimitado Informes, campos por formulario	Ilimitado Informes, campos por formulario	Ilimitado Informes, campos por formulario	Ilimitado Informes, campos por formulario
Sin cumplimiento	Sin cumplimiento	 Conformidad HIPAA 	 Conformidad HIPAA 
JotForm Branding 	Sin marca	Sin marca	Sin marca

Figura 62. JotForm (Jotform, 2018).

8. Survey Monkey

Link: https://es.surveymonkey.com/pricing/?ut_source=header

Precio Más económico: 75.000 COP/mes

Precio Full: 2.160.000 COP/año

ESTÁNDAR	AVANZADO	PREMIER
\$ 75.000 COP/mes	\$ 960.000 COP/año	\$ 2.160.000 COP/año
FACTURACIÓN MENSUAL AHORRA con un plan anual	FACTURACIÓN ANUAL DE \$ 960.000 COP	FACTURACIÓN ANUAL DE \$ 2.160.000 COP
SUSCRÍBETE	SUSCRÍBETE	SUSCRÍBETE
<ul style="list-style-type: none"> • Cantidad ilimitada de encuestas • Preguntas ilimitadas por encuesta • 1000 respuestas al mes* • Atención al cliente 24/7 por correo electrónico • Cuestionarios con comentarios personalizados • Filtros y tabulaciones cruzadas ilimitados, datos de tendencias • Logotipo, colores y URL de encuestas personalizados • Exportaciones de datos (CSV, PDF, PPT, XLS) • Lógica de exclusión • Análisis de texto 	<ul style="list-style-type: none"> • Cantidad ilimitada de encuestas • Preguntas ilimitadas por encuesta • Respuestas ilimitadas por encuesta • Asistencia rápida por correo electrónico 24/7 • Cuestionarios con comentarios personalizados • Filtros y tabulaciones cruzadas ilimitados, datos de tendencias • Logotipo, colores y URL de encuestas personalizados • Exportaciones de datos (CSV, PDF, PPT, XLS) • Lógica de exclusión, canalización de preguntas y respuestas • Análisis de textos e importancia estadística • Exportaciones avanzadas de datos (SPSS) • Pruebas A/B, asignación aleatoria, cupos • Variables personalizadas • Carga de archivos • SurveyMonkey Industry Benchmarks 	<ul style="list-style-type: none"> • Cantidad ilimitada de encuestas • Preguntas ilimitadas por encuesta • Respuestas ilimitadas por encuesta • Asistencia por teléfono y correo electrónico 24/7 • Cuestionarios con comentarios personalizados • Filtros y tabulaciones cruzadas ilimitados, datos de tendencias • Logotipo, colores y URL de encuestas personalizados • Exportaciones de datos (CSV, PDF, PPT, XLS) • Lógica de exclusión, canalización de preguntas y respuestas • Análisis de textos e importancia estadística • Exportaciones avanzadas de datos (SPSS) • Pruebas A/B, asignación aleatoria, cupos • Variables personalizadas • Carga de archivos • SurveyMonkey Industry Benchmarks • Bifurcación y canalización avanzadas, bloques aleatorios • Encuestas con marca blanca • Encuestas en múltiples idiomas

Figura 63. Survey Monkey (Surveymonkey, 2018).

9. Type Form

Link: <https://www.typeform.com/pricing/#>

Precio Más económico: Gratis

Precio Full: 70 USD/mes

BÁSICO (gratis)	PRO USD 35 / mes	PRO + A partir de USD 70 / mo para 1 usuario ?
100 respuestas / mes	Respuestas ilimitadas	Respuestas ilimitadas
<ul style="list-style-type: none"> ✓ 10 campos por tipografía ✓ Tipos básicos de preguntas ✓ Métricas y reportes ✓ Auto notificaciones (correo electrónico) ✓ Respuesta de tuberías ✓ Integración de Hojas de cálculo de Google ✓ Integración de HubSpot ✓ Enviar datos a más de 500 aplicaciones (Zapier) ✓ API de respuestas ✓ Incrustar ✓ Webhooks ✓ Cerrar typeform incrustado después de enviar 	<ul style="list-style-type: none"> ✓ Campos de tipos de letra ilimitados ✓ Tipos de preguntas avanzadas ✓ Métricas y reportes ✓ Auto notificaciones (correo electrónico) ✓ Respuesta de tuberías ✓ Integración de Hojas de cálculo de Google ✓ Integración de HubSpot ✓ Enviar datos a más de 500 aplicaciones (Zapier) ✓ API de respuestas ✓ Incrustar ✓ Webhooks ✓ Cerrar typeform incrustado después de enviar + Lógica condicional (salto lógico) + Notificaciones de los encuestados (correo electrónico) + Calculadora (puntuación y precios) + Pantalla de agradecimiento personalizado + Campos ocultos + Campo de pago + Integración de MailChimp + Campo de carga del archivo (almacenamiento de 2Gb) 	<ul style="list-style-type: none"> ✓ Campos de tipos de letra ilimitados ✓ Tipos de preguntas avanzadas ✓ Métricas y reportes ✓ Auto notificaciones (correo electrónico) ✓ Respuesta de tuberías ✓ Integración de Hojas de cálculo de Google ✓ Integración de HubSpot ✓ Enviar datos a más de 500 aplicaciones (Zapier) ✓ API de respuestas ✓ Incrustar ✓ Webhooks ✓ Cerrar typeform incrustado después de enviar ✓ Lógica condicional (salto lógico) ✓ Notificaciones de los encuestados (correo electrónico) ✓ Calculadora (puntuación y precios) ✓ Pantalla de agradecimiento personalizado ✓ Campos ocultos ✓ Campo de pago ✓ Integración de MailChimp + Campo de carga del archivo (4Gb / usuario) + Invitar a otros usuarios a espacios de trabajo + Soporte prioritario + Eliminar la marca Typeform + Redirigir al enviar + Customer Outcomes Manager (para cuentas anuales con más de 10 usuarios)

Figura 64. Type Form (Type Form, 2018).

ANEXO 5

RECOMENDACIONES PARA USUARIOS

En este anexo se presentan las recomendaciones que se usan en la aplicación, estas recomendaciones se dividen en 3 grupos, recomendaciones para despreocupados, recomendaciones para indiferentes o pragmáticos, y recomendaciones para alarmados o fundamentalistas, en la aplicación el usuario accede a las recomendaciones según el puntaje obtenido en su evaluación, la información de los puntajes se observa en la **Tabla 1**, algunas recomendaciones se repiten entre grupos, esto es debido que la recomendación aplica para los 3 grupos, se aclara que dentro de la aplicación las recomendaciones están separadas por paginas según el grupo asignado a cada usuario, para efectos de este anexo se presentan las recomendaciones separadas por títulos:

Recomendaciones texto general

A continuación, presentamos las recomendaciones para el grupo, las cuales consisten entre aplicaciones para móviles, para pc y consejos sobre cómo proteger tu información y privacidad en línea, desde ahora depende de ti usar estas herramientas de manera adecuada.

Las aplicaciones que recomendamos son seguras, sin embargo, consultas sus páginas oficiales para obtener mayor información sobre ellas, antes de instalar una aplicación, consulta sus términos de uso y condiciones

Las aplicaciones que recomendamos pueden ayudarte a proteger de manera más efectiva tu privacidad e identidad en la red, pero no reemplazan al sentido común ni te hacen impune. Su uso no te exime de la responsabilidad de lo que hagas en Internet. Y, por otro lado, no son infalibles, sobre todo cuando se usan sin experiencia previa.

Algunas aplicaciones se repiten en más de un grupo, porque consideramos que son útiles para todo tipo de usuario

Recomendaciones para despreocupados

A continuación, presentamos las recomendaciones para el grupo, las cuales consisten entre aplicaciones para móviles, para pc y consejos sobre cómo proteger tu información y privacidad en línea, desde ahora depende de ti usar estas herramientas de manera adecuada.

Aplicaciones para Smartphone

1. MyPermissions

La siguiente información es tomada de (My Permissions, 2018).

Una excelente aplicación para móviles que te ayuda a proteger la privacidad de tus redes sociales, **MyPermissions** permite a los usuarios controlar y controlar el acceso a su información personal en dispositivos móviles y en línea. MyPermissions supervisa todas las aplicaciones conectadas en

los sitios de redes sociales, incluidos Facebook, Twitter, Google, Dropbox y más. Le damos a los usuarios control sobre los datos a los que las aplicaciones pueden acceder. MyPermissions protege a los usuarios de compartir, sin saberlo, fotos, documentos, ubicaciones, contactos, correos electrónicos o cualquier otra información confidencial, y les permite aprobar o revocar qué aplicaciones acceden a sus datos, y cómo.

Funciones:

- **Descubre quién puede acceder a tus datos.**
- **La única protección de privacidad de las redes sociales.**
- **Recibe alertas 24/7.**

Para más información visita: <https://mypermissions.com/about/>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial, como **MyPermissions**

2. Duck DuckGo

La siguiente información es tomada de (Duck DuckGo, 2018).

Desde el tema de buscadores es ampliamente conocido Duck DuckGo, un **motor de búsqueda que no recopila ni comparte tu información, y no ofrece resultados “promovidos”**. Los datos personales derivados de las búsquedas no están a disposición de terceros. El buscador no almacena ningún tipo de información personal, como la dirección IP, correo electrónico, que permite hacer una segmentación por localización, y que en buscadores como Google esos datos son usados para ofrecer todo tipo de publicidad.

Para mayor información visita: <https://duckduckgo.com>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial, también puedes instalar el buscador en tu PC de escritorio

3. Ghostery

La siguiente información es tomada de (Ghostery, 2018)

Una aplicación que no deja de sorprenderme es Ghostery la cual es una herramienta que se instala a tu navegador, y nos permite ver que empresas rastrean tus datos. Con Ghostery puede elegir si quiere hacer bloqueos rastreadores por rastreador, sitio por sitio o mezclando ambos sistemas. Puede pasar el bloqueo en los momentos en los que quiera desactivarlo por completo.

Para mayor información visita: <https://www.ghostery.com/>

Puedes descargar el plugin desde la página oficial.

4. Cliqz

La siguiente información es tomada de (Cliqz, 2018)

Cliqz es un navegador seguro para móviles que trabajan bajo la premisa: “Nosotros, por otro lado, tenemos una visión muy diferente de Internet. Creemos en una Internet donde los valores, como la transparencia, la privacidad, la apertura, la seguridad y el respeto importan. Una Internet donde los datos personales permanecen en poder de los usuarios y estos usuarios llegan a su destino por la ruta más corta, incluso si esto significa menos oportunidades de publicidad.”

Para mayor información visita: <https://cliqz.com>

Puedes descargar el navegador para Móviles y PC desde la página oficial.

5. Privacy Badger

La siguiente información es tomada de (Electronic Frontier Foundation , 2018)

La EFF, o Electronic Frontier Foundation reconocida organización que protege la privacidad, ha generado herramientas como **Privacy Badger**, la cual también **permite bloquear los trackers o empresas que recolectan información**. Privacy Badger es un complemento del navegador que **impide** que los anunciantes y otros rastreadores de terceros realicen un seguimiento en secreto a dónde va y qué páginas mira en la Web. Si un anunciante parece estar rastreando en varios sitios web sin su permiso, Privacy Badger bloquea automáticamente que ese anunciante cargue más contenido en su navegador. Para el anunciante, es como si de repente desapareciera.

Para mayor información visita: <https://www.eff.org/privacybadger>

Puedes descargar el navegador para PC desde la página oficial.

6. Panopticlick

La siguiente información es tomada de (Panopticlick Electronic Frontier Foundation , 2018)

La EFF, también ha lanzado la iniciativa Panopticlick, que consiste en realizar una prueba de privacidad a su navegador. Panopticlick analizará qué tan bien su navegador y complementos lo protegen contra las técnicas de seguimiento en línea. También veremos si su sistema está configurado de forma única, y por lo tanto identificable, incluso si está utilizando un software de protección de la privacidad.

Para mayor información visita: <https://panopticlick.eff.org>

Puedes descargar el navegador para PC desde la página oficial.

7. Sophos Antivirus

La siguiente información es tomada de (Sophos Mobile Security , 2018)

Sophos Mobile Security es una aplicación que protege los dispositivos Android sin afectar al rendimiento ni a la duración de la batería. La sincronización en tiempo real con SophosLabs garantiza que su dispositivo móvil esté siempre protegido contra los programas maliciosos y las amenazas de Internet más recientes, igual que con nuestros productos empresariales. Identifica las aplicaciones maliciosas o no deseadas que podrían causar, por ejemplo, robos de datos, pérdida de datos y costes excesivos del uso de la red. Si el dispositivo se pierde o es objeto de un robo, el bloqueo o el borrado remotos protegen la información personal contra curiosos

Para mayor información visita: <https://www.sophos.com/en-us.aspx>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial, como **Sophos**

8. Boxcryptor

La siguiente información es tomada de (Boxcryptor, 2018)

Boxcryptor cifra sus archivos y carpetas sensibles en Dropbox, Google Drive, OneDrive y muchos otros almacenes en la nube. Combina los beneficios de la mayoría de los servicios de almacenamiento en nube fácil de usar con los mejores estándares de seguridad en todo el mundo. Cifre sus datos directamente en su dispositivo antes de sincronizarlos con los proveedores de la nube de su elección.

Para más información visita: <https://www.boxcryptor.com/es/>

Puedes descargar Boxcryptor para PC desde la página oficial.

9. KeepSafe

La siguiente información es tomada de (Keep safe, 2018)

KeepSafe, una herramienta sencilla que organiza tus fotos en carpetas protegidas por contraseña. De este modo, para acceder a cualquier foto o vídeo que hayas decidido proteger tendrás que introducir un código PIN.

Para mayor información visita: <https://www.getkeepsafe.com>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial, como **KeepSafe**

10. Apex Launcher

La siguiente información es tomada de (Apexlauncher, 2018)

Para un cambio más radical, mejora tu *launcher* de defecto a uno más personalizable. La mayoría de los *launchers* poseen botones bonitos y fondos de pantalla impresionantes, pero Apex Launcher te ofrece mucho más en cuanto a funcionalidad: podrás esconder la *app* que desees.

Para mayor información visita: <https://www.apexlauncher.com>

Puedes descargar la aplicación desde la playstore, y la página oficial, como **Apex Launcher**

11. CM Locker

La siguiente información es tomada de (CM Locker, 2018)

CM Locker Añade un patrón de desbloqueo o un código numérico como primera línea de defensa. Gracias a la opción de “Intruder Selfie”, la *app* hará una foto con la cámara frontal cada vez que alguien introduzca la contraseña incorrecta. La fotografía te llegará con una notificación.

Para mayor información visita: <http://www.cmcm.com/es-es/cm-locker/>

Puedes descargar la aplicación desde la playstore, y la página oficial, como **CM Locker**

Recomendaciones para pragmáticos

A continuación, presentamos las recomendaciones para el grupo, las cuales consisten entre aplicaciones para móviles, para pc y consejos sobre cómo proteger tu información y privacidad en línea, desde ahora depende de ti usar estas herramientas de manera adecuada.

Aplicaciones para Smartphone

1. MyPermissions.

La siguiente información es tomada de (My permissions, 2018)

Una excelente aplicación para móviles que te ayuda a proteger la privacidad de tus redes sociales, **MyPermissions** permite a los usuarios controlar y controlar el acceso a su información personal en dispositivos móviles y en línea. MyPermissions supervisa todas las aplicaciones conectadas en los sitios de redes sociales, incluidos Facebook, Twitter, Google, Dropbox y más. Le damos a los usuarios control sobre los datos a los que las aplicaciones pueden acceder. MyPermissions protege a los usuarios de compartir, sin saberlo, fotos, documentos, ubicaciones, contactos, correos

electrónicos o cualquier otra información confidencial, y les permite aprobar o revocar qué aplicaciones acceden a sus datos, y cómo.

Funciones:

- **Descubre quién puede acceder a tus datos.**
- **La única protección de privacidad de las redes sociales.**
- **Recibe alertas 24/7.**

Para mayor información visita: <https://mypermissions.com/about/>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial, como **MyPermissions**

2. Citizenme

La siguiente información es tomada de (Citizenme, 2018)

En el teléfono celular se puede descargar aplicaciones como Citizenme, la cual permite tener un control sobre qué datos personales que toman las aplicaciones. La aplicación se descarga en el teléfono y por medios iconos de nuestras redes sociales, cada uno con un color que indica si protegen bien nuestros datos (verde) o no (rojo). Pulsando cada icono podremos ver las políticas de privacidad como entender como gestionan los datos personales.

Para mayor información visita: <https://www.citizenme.com/public/wp/>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial, como **Citizenme**

3. Duck DuckGo

La siguiente información es tomada de (Duck DuckGo, 2018)

Desde el tema de buscadores es ampliamente conocido **Duck DuckGo**, un **motor de búsqueda que no recopila ni comparte tu información, y no ofrece resultados “promovidos”**. Los datos personales derivados de las búsquedas no están a disposición de terceros. El buscador no almacena ningún tipo de información personal, como la dirección IP, correo electrónico, que permite hacer una segmentación por localización, y que en buscadores como Google esos datos son usados para ofrecer todo tipo de publicidad.

Para mayor información visita: <https://duckduckgo.com>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial, también puedes instalar el buscador en tu PC de escritorio

4. Ghostery

La siguiente información es tomada de (Ghostery, 2018)

Una aplicación que no deja de sorprenderme es Ghostery la cual es una herramienta que se instala a tu navegador, y nos permite ver que empresas rastrean tus datos. Con Ghostery puede elegir si quiere hacer bloqueos rastreadores por rastreador, sitio por sitio o mezclando ambos sistemas. Puede pasar el bloqueo en los momentos en los que quiera desactivarlo por completo.

Para mayor información visita: <https://www.ghostery.com/>

Puedes descargar el plugin desde la página oficial, para móvil existe un navegador llamado:

5. Cliqz

La siguiente información es tomada de (Cliqz, 2018)

Cliqz es un navegador seguro para móviles que trabajan bajo la premisa: “Nosotros, por otro lado, tenemos una visión muy diferente de Internet. Creemos en una Internet donde los valores, como la transparencia, la privacidad, la apertura, la seguridad y el respeto importan. Una Internet donde los datos personales permanecen en poder de los usuarios y estos usuarios llegan a su destino por la ruta más corta, incluso si esto significa menos oportunidades de publicidad.”

Para mayor información visita: <https://cliqz.com>

Puedes descargar el navegador para Mviles y PC desde la página oficial.

6. Privacy Badger

La siguiente información es tomada de (Electronic Frontier Foundation , 2018)

La EFF, o Electronic Frontier Foundation reconocida organización que protege la privacidad, ha generado herramientas como **Privacy Badger**, la cual también **permite bloquear los trackers o empresas que recolectan información**. Privacy Badger es un complemento del navegador que **impide** que los anunciantes y otros rastreadores de terceros realicen un seguimiento en secreto a dónde va y qué páginas mira en la Web. Si un anunciante parece estar rastreando en varios sitios web sin su permiso, Privacy Badger bloquea automáticamente que ese anunciante cargue más contenido en su navegador. Para el anunciante, es como si de repente desaparecieras.

Para mayor información visita: <https://www.eff.org/privacybadger>

Puedes descargar el navegador para PC desde la página oficial.

7. Panopticlick

La siguiente información es tomada de (Panopticlick Electronic Frontier Foundation , 2018)

La EFF, también ha lanzado la iniciativa Panopticlick, que consiste en realizar una prueba de privacidad a su navegador. Panopticlick analizará qué tan bien su navegador y complementos lo protegen contra las técnicas de seguimiento en línea. También veremos si su sistema está configurado de forma única, y por lo tanto identificable, incluso si está utilizando un software de protección de la privacidad.

Para mayor información visita: <https://panopticlick.eff.org>

Puedes descargar el navegador para PC desde la página oficial.

8. Sophos Antivirus

La siguiente información es tomada de (Sophos Mobile Security , 2018)

Sophos Mobile Security es una aplicación que protege los dispositivos Android sin afectar al rendimiento ni a la duración de la batería. La sincronización en tiempo real con SophosLabs garantiza que su dispositivo móvil esté siempre protegido contra los programas maliciosos y las amenazas de Internet más recientes, igual que con nuestros productos empresariales. Identifica las aplicaciones maliciosas o no deseadas que pudieran causar, por ejemplo, robos de datos, pérdida de datos y costes excesivos del uso de la red. Si el dispositivo se pierde o es objeto de un robo, el bloqueo o el borrado remotos protegen la información personal contra curiosos

Para más información visita: <https://www.sophos.com/en-us.aspx>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial, como **Sophos**

9. Tor

La siguiente información es tomada de (Tor Project, 2018)

La utilidad **Tor**, disponible para muchos sistemas operativos, encamina tu tráfico por una serie de nodos, haciendo que la navegación sea anónima. Gracias a su paquete instalable, es muy fácil de usar y configurar. Pero Tor no hace que el tráfico esté a prueba de escuchas. Para eso, has de cifrar tu conexión, hacerla pasar por un túnel. Es lo que hacen los llamados VPN. Los más famosos son **HotSpot Shield** y **UltraSurf**.

Para mayor información visita: <https://www.torproject.org/about/overview.html>

Puedes descargar el navegador para PC desde la página oficial.

10. UltraSurf

La siguiente información es tomada de (Ultrasurf, 2018)

INTIMIDAD: Proteja su privacidad en línea con navegación y navegación anónimas. Ultra Surf esconde su dirección IP, borra el historial de navegación, cookies y más.

SEGURIDAD: Uso de cifrado de extremo a extremo para proteger su transferencia de datos de ser visto por un tercero.

LIBERTAD: Omite la censura de internet para navegar por internet libremente.

Para mayor información visita: <https://ultrasurf.us/about/>

Puedes descargar para PC desde la página oficial.

11. Boxcryptor

La siguiente información es tomada de (Boxcryptor, 2018)

Boxcryptor cifra sus archivos y carpetas sensibles en Dropbox, Google Drive, OneDrive y muchos otros almacenes en la nube. Combina los beneficios de la mayoría de los servicios de almacenamiento en nube fácil de usar con los mejores estándares de seguridad en todo el mundo. Cifre sus datos directamente en su dispositivo antes de sincronizarlos con los proveedores de la nube de su elección.

Para mayor información visita: <https://www.boxcryptor.com/es/>

Puedes descargar Boxcryptor para PC desde la página oficial.

12. KeepSafe

La siguiente información es tomada de (Keep safe, 2018)

KeepSafe, una herramienta sencilla que organiza tus fotos en carpetas protegidas por contraseña. De este modo, para acceder a cualquier foto o vídeo que hayas decidido proteger tendrás que introducir un código PIN.

Para mayor información visita: <https://www.getkeepsafe.com>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial, como **KeepSafe**

13. CM Locker

La siguiente información es tomada de (CM Locker, 2018)

CM Locker Añade un patrón de desbloqueo o un código numérico como primera línea de defensa. Gracias a la opción de “Intruder Selfie”, la *app* hará una foto con la cámara frontal cada vez que alguien introduzca la contraseña incorrecta. La fotografía te llegará con una notificación.

Para mayor información visita: <http://www.cmcm.com/es-es/cm-locker/>

Puedes descargar la aplicación desde la playstore, y la página oficial, como **CM Locker**

Recomendaciones para Fundamentalistas

Para los fundamentalistas, tú como usuario avanzado en el uso de la red, y preocupado por la seguridad y privacidad de tus datos en Internet, presentamos recomendaciones más serias y profesionales, las cuales puedes utilizar para ampliar tus conocimientos, conocer los últimos avances en materia de seguridad de la información

ISMS Forum Spain

La siguiente información es tomada de (ISMS Forum Spain, 2018)

Un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información. Toda su actividad se desarrolla en base a los valores de transparencia, independencia, objetividad y neutralidad.

Para mayor información visita su página oficial: <https://www.ismsforum.es/quien/index.php>

A continuación, presentamos las recomendaciones para el grupo, las cuales consisten entre aplicaciones para móviles, para pc y consejos sobre cómo proteger tu información y privacidad en línea, desde ahora depende de ti usar estas herramientas de manera adecuada.

Aplicaciones para Smartphone

1. MyPermissions

La siguiente información es tomada de (My Permissions, 2018)

Una excelente aplicación para móviles que te ayuda a proteger la privacidad de tus redes sociales, **MyPermissions** permite a los usuarios controlar y controlar el acceso a su información personal en dispositivos móviles y en línea. MyPermissions supervisa todas las aplicaciones conectadas en los sitios de redes sociales, incluidos Facebook, Twitter, Google, Dropbox y más. Le damos a los usuarios control sobre los datos a los que las aplicaciones pueden acceder. MyPermissions protege a los usuarios de compartir, sin saberlo, fotos, documentos, ubicaciones, contactos, correos electrónicos o cualquier otra información confidencial, y les permite aprobar o revocar qué aplicaciones acceden a sus datos, y cómo.

Funciones:

- **Descubre quién puede acceder a tus datos.**
- **La única protección de privacidad de las redes sociales.**
- **Recibe alertas 24/7.**

Para más información visita: <https://mypermissions.com/about/>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial, como **MyPermissions**

2. Citizenme

La siguiente información es tomada de (Citizenme, 2018)

En el teléfono celular se puede descargar aplicaciones como Citizenme, la cual permite tener un control sobre qué datos personales que toman las aplicaciones. La aplicación se descarga en el teléfono y por medios iconos de nuestras redes sociales, cada uno con un color que indica si protegen bien nuestros datos (verde) o no (rojo). Pulsando cada icono podremos ver las políticas de privacidad como entender como gestionan los datos personales.

Para mayor información visita: <https://www.citizenme.com/public/wp/>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial, como **Citizenme**

3. Duck DuckGo

La siguiente información es tomada de (Duck DuckGo, 2018)

Desde el tema de buscadores es ampliamente conocido **Duck DuckGo**, un **motor de búsqueda que no recopila ni comparte tu información, y no ofrece resultados “promovidos”**. Los datos personales derivados de las búsquedas no están a disposición de terceros. El buscador no almacena ningún tipo de información personal, como la dirección IP, correo electrónico, que permite hacer una segmentación por localización, y que en buscadores como Google esos datos son usados para ofrecer todo tipo de publicidad.

Para mayor información visita: <https://duckduckgo.com>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial, también puedes instalar el buscador en tu PC de escritorio

4. Latch

La siguiente información es tomada de (Latch, 2018)

Telefónica también le está apostando a la privacidad y por medio de la empresa **Latch**, se ha inventado un **interruptor digital**. Permite activar las tarjetas de crédito solo cuando las necesites. Latch te permite implementar un pestillo de seguridad en tus servicios online. De esta manera, podrás bloquear temporalmente funcionalidades del servicio como el mecanismo de inicio de sesión, los pagos con tarjeta de crédito, el acceso a correo electrónico, etc. Además, el sistema de alerta de Latch te permite identificar, en tiempo real, comportamientos sospechosos en las cuentas de tus usuarios.

Para mayor información visita: <https://latch.elevenpaths.com/www/index.html>

Puedes descargar la aplicación desde la playstore, appstore y la página oficial,

5. Blackphone

La siguiente información es tomada de (Silent Circle, 2018)

Si cuenta con un poco más de dinero, por 600 dólares, puede comprar el **Blackphone un teléfono inteligente diseñado para ofrecer niveles de seguridad**. El teléfono cuenta con aplicaciones, controles y cifrado de datos.

Para más información visita: <https://www.silentcircle.com>

6. Sikur

La siguiente información es tomada de (Sikur, 2018)

En países como Colombia, México y Brasil, está tomando mucha fuerza servicios como el que ofrece la empresa **Sikur**, el cual **encripta la información, ofrece correo electrónico, chat seguro, el cual se puede instalar en dispositivos Android o IOS**. Sikur funciona bajo una nube pública y privada y sirve para que las empresas mitiguen la fuga de datos e información.

Para mayor información visita: <https://www.sikur.com>

7. Tor

La siguiente información es tomada de (Tor Project, 2018)

La utilidad **Tor**, disponible para muchos sistemas operativos, encamina tu tráfico por una serie de nodos, haciendo que la navegación sea anónima. Gracias a su paquete instalable, es muy fácil de usar y configurar. Pero Tor no hace que el tráfico esté a prueba de escuchas. Para eso, has de cifrar tu conexión, hacerla pasar por un túnel. Es lo que hacen los llamados VPN. Los más famosos son **HotSpot Shield** y **UltraSurf**.

Para más información visita: <https://www.torproject.org/about/overview.html>

Puedes descargar el navegador para PC desde la página oficial.

8. UltraSurf

La siguiente información es tomada de (Ultrasurf, 2018)

INTIMIDAD: Proteja su privacidad en línea con navegación y navegación anónimas. Ultra Surf esconde su dirección IP, borra el historial de navegación, cookies y más.

SEGURIDAD: Uso de cifrado de extremo a extremo para proteger su transferencia de datos de ser visto por un tercero.

LIBERTAD: Omita la censura de internet para navegar por internet libremente.

Para más información visita: <https://ultrasurf.us/about/>

Puedes descargar para PC desde la página oficial.

9. Hushmail

La siguiente información es tomada de (Hushmail, 2018)

Hushmail es como su servicio de correo electrónico actual, puede leer y redactar su correo electrónico en la web, teléfono inteligente y en cualquier lugar donde trabaje, pero hemos agregado importantes funciones de seguridad para ayudarlo a mantener la seguridad de sus datos. Recupere el control de sus datos y experimente una bandeja de entrada limpia sin publicidad. Elija qué correos electrónicos desea enviar utilizando nuestro potente cifrado y mantenga sus conversaciones más personales en privado y confidencial.

Para más información visita: <https://www.hushmail.com>

Puedes descargar para Hushmail PC y iphone desde la página oficial.

10. ArmorText

La siguiente información es tomada de (Armor text, 2018)

ArmorText permite a los usuarios enviar y recibir mensajes seguros en múltiples dispositivos simultáneamente. Con una representación criptográfica única para cada dispositivo + usuario, cuando un dispositivo se pierde o es robado, los usuarios continúan trabajando de forma segura desde sus dispositivos restantes mientras sus administradores borran y desactivan mensajes y claves en el dispositivo errante de forma remota.

Para más información visita: <https://armortext.com>

Puedes descargar para Hushmail PC, Android y iPhone desde la página oficial.

11. Boxcryptor

La siguiente información es tomada de (Boxcryptor, 2018)

Boxcryptor cifra sus archivos y carpetas sensibles en Dropbox, Google Drive, OneDrive y muchos otros almacenes en la nube. Combina los beneficios de la mayoría de los servicios de almacenamiento en nube fácil de usar con los mejores estándares de seguridad en todo el mundo. Cifre sus datos directamente en su dispositivo antes de sincronizarlos con los proveedores de la nube de su elección.

Para más información visita: <https://www.boxcryptor.com/es/>

Puedes descargar Boxcryptor para PC desde la página oficial.

Recomendaciones para alarmados

Consejos para aplicar en tu trabajo y empresa Información presentados por la empresa (Platzi, 2018), información que contiene información útil para los usuarios alarmados o fundamentalistas:

- 1. HAZ TU DEBER: LOS DATOS PERSONALES DE TUS CLIENTES SE DEBEN PROTEGER** Es importante que entiendas que **tienes la obligación jurídica de proteger los datos personales que te entrega un cliente**, como lo son el nombre, correo electrónico, datos de contacto, etc. En Latinoamérica **casi todos los países cuentan con normas de protección de datos personales**, las cuales te obligan a que tengas la autorización expresa e informada de tus usuarios para enviarles información de tus productos.
- 2. RECOGE SOLO LOS DATOS QUE SEAN NECESARIOS Y CREA POLÍTICAS DE PROTECCIÓN DE DATOS** Como consejo, es bueno que **solo recojas los datos necesarios**: entre más datos personales recojas tendrás que protegerlos de mejor forma. La protección de datos también lleva el principio de calidad del dato, el cual se traduce en que tienes que recoger datos exactos de tus clientes, evitando errores en datos de carácter personal como lo pueden ser un nombre y un correo electrónico. Es recomendable que utilices herramientas del tipo CRM (del inglés Customer Relationship Management), y que en ellas tengas una casilla para guardar la autorización de cuando la persona te entregó el dato.
- 3. UTILIZA MEDIDAS TÉCNICAS Y JURÍDICAS PARA PROTEGER LA INFORMACIÓN** Empieza utilizando medidas técnicas y jurídicas para la protección de la información personal y empresarial. **Exige de tus empleados y proveedores que firmen cláusulas de confidencialidad**. Por regulación existe la figura de responsable y encargado del tratamiento de datos. Imagina el caso de que eres una empresa y le entregas tu base de datos en Excel a un tercero para que te haga un envío de correo electrónico; si este tercero por desconocimiento empieza a utilizar la base de datos de tus clientes para enviar publicidad de otro negocio, te podría llevar a un riesgo de queja o demanda.

4. **MÁS VALE PREVENIR QUE CURAR** La protección de datos y la seguridad de la información tiene que ser una de las mayores preocupaciones que debe tener cualquier empresa, y la desconfianza es la mejor prevención. No es lo mismo un colegio que guarda datos sensibles de menores de edad o un portal de comercio electrónico que solo pide un correo electrónico y que no recoge información. **Analiza los riesgos de tu negocio:** en la actualidad existen metodologías como la ISO 31001, la cual te recomienda que analices los factores de riesgo y que te definas objetivos y medidas concretas para mitigar el riesgo.

5. **LAS PERSONAS, EN EL CENTRO** La protección de datos personales y la seguridad de la información son parte un proceso global, el cual es centrado en las personas. Algunos consideran que **la protección de datos se limita a cumplir con los aspectos legales, pero esto es un error: la protección de datos es un tema cultural, tecnológico y jurídico.** Lo mismo pasa con la seguridad de la información, que es **mucho más que hardware o software**, como lo explicó el hacker Kevin Mitnick: “Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil que son las personas.”

ANEXO 6

La **Figura 65** presenta la pantalla de los términos y condiciones del uso de la aplicación, esta pantalla aparece al usuario la primera vez que utiliza la aplicación

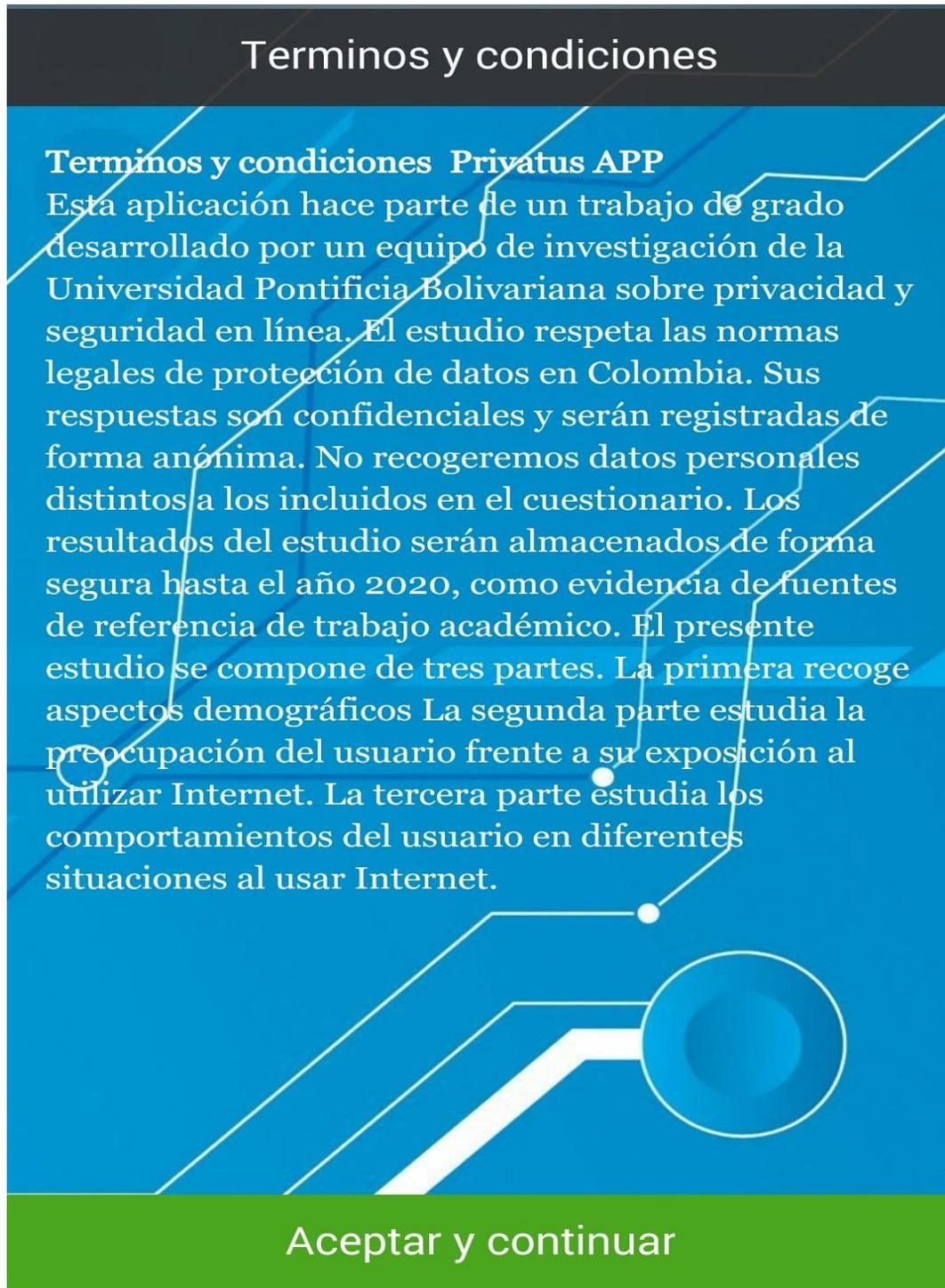


Figura 65 Términos y condiciones