PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE ARQUITECTURA DISEÑO Y ARTES

CARRERA DE DISEÑO

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE DISEÑADOR/A PROFESIONAL CON MENCIÓN EN DISEÑO GRÁFICO Y COMUNICACIÓN VISUAL

“Diseño de material gráfico informativo e interactivo sobre la protección virtual de datos privados, dirigido a los estudiantes de la Pontificia Universidad Católica del Ecuador (PUCE).”

Nombre:

Esteban Fernando Muela Betancourt

Director:

Ing. Mariana Lozada Mtr.

Quito D.M., julio 2018

Diseño de material gráfico informativo e interactivo sobre la protección virtual de datos privados, dirigido a los estudiantes de la Pontificia Universidad Católica del Ecuador (PUCE).

Tabla de contenidos

Índice de figuras

Índice de tablas

Generalidades

I. Tema

Diseño de material gráfico informativo e interactivo sobre la protección virtual de datos privados, dirigido a los estudiantes de la Pontificia Universidad Católica del Ecuador (PUCE).

II. Resumen

El uso masivo del Internet y de otras herramientas electrónicas ha traído una infinidad de ventajas pero también una serie de impactos negativos en la sociedad. El Ecuador no es ajeno a esta realidad, convirtiendo a las instituciones académicas en blancos vulnerables. Esta tesis de disertación considera de manera particular a los estudiantes de la Pontificia Universidad Católica del Ecuador (PUCE). Aunque no de manera suficiente, existen políticas y normativas internacionales, nacionales e institucionales relacionadas con el derecho a la protección de la privacidad, las mismas que son desconocidas por la mayoría de estudiantes. Frente a ello la tesis propone un producto gráfico que informe a los estudiantes de la PUCE sobre la importancia de mantener protegidos sus datos privados.

Para abordar esta situación, ha sido necesario elaborar la tesis con tres componentes, uno de investigación, otro de diseño y un tercero de validación, cada uno con sus respectivos respaldos teóricos y metodológicos. A través de la aplicación de técnicas cuantitativas y cualitativas en el primer componente se pudo constatar que los estudiantes de la PUCE han sido víctimas de diversos ataques cibernéticos, frente a lo cual, una amplia mayoría tienen una limitada adopción de medidas

para preservar la privacidad. El estudio detectó las principales causas de este fenómeno. Una de ellas, el desconocimiento sobre las estrategias o mecanismos para la protección de información privada en Internet. Siendo central, la ausencia de una herramienta ágil de diseño informativo e interactivo para la protección de datos privados. La elaboración de este producto y la presentación de los detalles teórico-metodológicos son los contenidos principales del segundo componente de esta tesis. El tercer componente tiene que ver con el proceso de validación del producto de diseño, con la finalidad de conocer su viabilidad y corregir los aspectos centrales que arroje esa prueba.

Con el propósito de preservar el derecho a la privacidad se ha visto la necesidad de promover en la Institución una herramienta que produzca un diseño de experiencia y se sirva del Diseño Centrado en el Usuario (DCU), para generar un producto informativo e interactivo con características de gamificación.

Abstract

The massive use of the Internet and other electronic tools has brought an infinity of advantages, but also some negative impacts on society. Ecuador is no stranger to this reality, turning academic institutions into vulnerable targets. This thesis dissertation includes students of the Pontificia Universidad Católica de Ecuador (PUCE) in a particular way. Although not enough, there are international, national and institutional policies and regulations related to the right to privacy protection, however, these are unknown by most students. The thesis proposes a graphic product that informs students of PUCE about the importance of keeping their private data protected. The study detected the main causes of this phenomenon. One of them, the ignorance about the strategies or mechanisms for the protection of private information on the Internet. The absence of an agile tool of informative and interactive design for the protection of private data is central. The elaboration of this product and the presentation of the theoretical-methodological details are the main contents of the thesis second component. The third component is related with the validation process of the design product, in order to know its viability and correct the central aspects that this test throws. With the purpose of preserving the right to privacy, we promote in the Institution a tool that produces an experience design that uses the User Centered Design (DCU), this to generate an informative and interactive product with gamification characteristics.

III. Introducción

El Internet es una herramienta que funciona como una ventana abierta hacia el mundo. No solamente habilita el desarrollo, la participación social, política y el ejercicio de derechos humanos, también permite el acceso a una gran cantidad de información de forma instantánea y constituye un medio de comunicación crucial en el entorno cotidiano. Sin embargo, sin el cuidado suficiente, la información privada que se comparte en el día a día puede ser fácilmente vulnerada.

El desarrollo vertiginoso del Internet y las nuevas tecnologías de la información y comunicación (TIC) han supuesto una serie de implicaciones positivas y negativas en las interacciones sociales posmodernas y en el ejercicio de derechos fundamentales.

El Internet ha presentado nuevos alcances en la difusión de información y se ha constituido en un medio de expresión y participación social y política que propicia el desarrollo humano. Sin embargo, muchos de los derechos vinculados a la preservación de la autonomía, integridad y poder de decisión del usuario digital sobre su información personal y privada, no siempre se ven respetados por otros individuos en la Red o distintas entidades gubernamentales y no gubernamentales.

Esta situación toma relevancia en el medio estudiantil universitario, en el cual los usuarios de Internet empiezan a compartir información privada, en términos institucionales, profesionales y personales, inclusive datos de cuentas bancarias. Por esta razón es indispensable comprender las consecuencias y repercusiones de un mal manejo de la información privada en línea, así como la importancia de la generación de hábitos adecuados que aseguren el bienestar de las personas.

La presente disertación busca ofrecer recursos útiles para la comunidad universitaria de la Pontificia Universidad Católica del Ecuador (PUCE), orientados a informar sobre la importancia de proteger la privacidad en línea y a promover la adopción de hábitos en el manejo de información privada en Internet, como un método de prevención y resguardo de la integridad de un usuario.

Este trabajo de tesis tiene tres componentes, uno de investigación, otro de diseño y un tercero, de validación. El primero tiene la finalidad de sustentar las características que debe tener un proyecto de diseño, de cualquier tipo que sea y dirigido a cualquier usuario. En este caso, era necesario conocer las particularidades de la población estudiantil de la PUCE, en lo que respecta al conocimiento sobre la protección de la información personal y al uso de las herramientas más adecuadas para esos fines. El segundo componente es el de diseño propiamente dicho, el de un producto gráfico, respaldado por los resultados de la investigación y expresado en una herramienta de utilidad tanto para los estudiantes como para la Institución. El tercer componente se refiere a la evaluación de la eficacia y demás características del producto de diseño (herramienta), propuesto para el uso de los estudiantes de la PUCE.

Cada uno de estos componentes tiene sus particularidades teóricas y metodológicas que serán desarrollados en los espacios correspondientes.

IV. Justificación

El manejo inadecuado de información en Internet puede llevar a un usuario cibernético a situaciones que violenten su privacidad e incluso comprometan su integridad física y emocional, vulnerándose los derechos fundamentales.

Según la revista Computer World y de Vinton Cerf, Vicepresidente de Google, el Internet es un espejo de la sociedad, incluyendo amenazas como fraudes y delitos en línea. Tomando en cuenta esta afirmación, dentro de la red se da muchos casos de estafas, ataques, violaciones de privacidad, pérdidas de información, suplantación de identidad e incluso situaciones que comprometen la integridad física y emocional de la víctima. Aún así, muchos de estos casos pueden ser evitados con un manejo adecuado de la información privada en la Red. (Computer World, 2007).

La Organización de Derechos de Privacidad, Privacy International (2014), sostiene que “la privacidad es un derecho fundamental, esencial a la autonomía y protección de la dignidad humana, una base sobre la cual muchos otros derechos humanos se construyen”

Tomando en cuenta que la privacidad es un derecho humano, éste se ve articulado en una gran cantidad de acuerdos e instrumentos de derechos humanos internacionales y regionales. Un ejemplo, el artículo 12 de la Declaración Universal de Derechos Humanos de la Organización de las Naciones Unidas (1948) establece que:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (p. 4).

La privacidad se presenta de manera similar en disposiciones de otros instrumentos internacionales. Por ejemplo, en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, así como en el artículo 8 de la Convención Europea de Derechos Humanos (Nyst, 2013). Cabe recalcar, que más de 130 países cuentan con declaraciones relativas a la protección de la privacidad en cada región del mundo (Privacy International, 2014).

Ecuador también contempla dentro de su Constitución el derecho a la privacidad. En el artículo 66, numerales 19, 20, 21 se garantiza:

> El derecho a la protección de datos de carácter personal… el derecho a la intimidad personal y familiar… el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual para cualquier tipo o forma de comunicación… (Constitución del Ecuador, 2008, p. 32).

La protección de la información privada significa el preservar una serie de derechos y espacios cuyo resguardo lleva a una mejor calidad de vida de la persona. El tema de los derechos se encuentra también en el Plan Nacional de Desarrollo toda una vida (2017), dentro del cual se plantean objetivos nacionales de desarrollo como ejes de la planificación. Se presenta en el objetivo 1: Garantizar una vida digna con iguales oportunidades para todas las personas, en el cual se especifica que:

> El hablar de una vida digna con igualdad de oportunidades para todas las personas, implica también garantizar a las personas el derecho a la integridad personal, lo cual incluye: la integridad física, psíquica, moral y sexual; una vida libre de violencia en el ámbito público y privado, así como la obligación del Estado de adoptar las medidas necesarias para prevenir, eliminar y sancionar toda forma de violencia. (p. 60).

En el mismo sentido se incluye la política 1.17 que busca “Asegurar el acceso a la justicia, la seguridad integral, la lucha contra la impunidad y la reparación integral a las víctimas, bajo el principio de igualdad y no discriminación”. Es interesante analizar el objetivo 7: En el cual se busca el incentivar a una sociedad más participativa, con un Estado cercano al servicio de la ciudadanía; y la política 7.9, con la finalidad de “Promover la seguridad jurídica y la defensa técnica del Estado” y “Aumentar la cobertura, calidad y acceso a servicios de justicia y seguridad integral” (p. 58-100).

Lo señalado tiene especial importancia en el contexto nacional y dentro de este trabajo de titulación ya que son referentes para generar métodos de denuncia y recuperación para casos que vulneren la privacidad e integridad personal en medios digitales.

El diseño toma relevancia en el proyecto, además, como actividad interdisciplinaria que apoya al ejercicio de los derechos especificados anteriormente. Con esta estrategia es posible alcanzar estos ideales, a través del aporte de distintos enfoques, que incluyen soluciones conservadoras e innovadoras, apropiadas para diversas comunidades de usuarios (Bennet y Vulpinari, 2001).

Este proyecto encuentra su campo de acción dentro del área del diseño de información, donde la detección y comprensión de la información es esencial para generar una mejor acción de los usuarios. Según Frascara (2011), “el buen diseño de información invita a ser usado, reduce cansancio y errores en el procesamiento de información, agiliza el trabajo, y hace que la información sea atractiva y adecuada a la situación en la que se presenta” (p. 11).

Es importante generar un sistema de acceso fácil y de uso eficaz para apoyar a la generación de hábitos de protección y conciencia para mejorar el manejo de información privada en los estudiantes de la PUCE.

Se debe considerar que éstos deben estar implicados o sumergidos en la información que para Frascara (2012):

> El diseño de información consiste en dos distintos aspectos: la organización de la información (el contenido), y la planificación de su presentación visual. Esto requiere habilidad para procesar, organizar, y presentar la información en forma verbal y no verbal (p. 128).

Con el creciente uso de nuevas tecnologías y nuevos medios de comunicación, cada vez es más importante tener un control adecuado de la información que se proporciona y cómo se lo hace, además de métodos de protección ante amenazas externas. Es importante generar apoyo mediante el diseño hacia la protección de la información privada, en vista que la integridad del estudiante no solamente se ve vulnerada por cibercriminales potenciales que buscan extorsionar o estafar a las personas, sino también por violaciones de derechos por parte de distintas entidades estatales y no estatales, que pueden tomar lugar en el medio nacional, debido a la falta de control o de normativas aplicables a la realidad del Ecuador.

A diario somos testigos de noticias que hacen referencia a la violación de los sistemas electrónicos e informáticos a todo nivel. Muchas personas dedican tiempo y recursos para una diversidad de actos ilícitos, estudiando y diseñando herramientas y estrategias para ello. Por el contrario, pocos son los que dedican esfuerzos para disponer también de herramientas y estrategias para la protección de esos u otros ataques. Con el trabajo de esta disertación se tiene el interés de aportar en alguna forma para ir cubriendo estos necesarios campos.

V. Planteamiento del problema

Para entender mejor el medio en el que se desenvuelven los estudiantes de la PUCE como usuarios de la Red y su papel dentro de la preservación de sus derechos, es importante entender el contexto jurídico y legislativo en cuanto a la privacidad en línea. Se toma como referente a la privacidad como un derecho humano, reconocido en la Declaración Universal de Derechos Humanos y por varios instrumentos y acuerdos a nivel mundial.

Desde este punto de vista, los internautas deben encontrarse protegidos desde la ley y deben contar con formas de protección y recuperación en caso de una situación que atente contra su derecho a la privacidad. Este derecho también se encuentra en la Constitución de la República del Ecuador de 2008.

El Informe de la Oficina del Alto Comisionado de las Naciones Unidas (2014), para los Derechos Humanos, titulado 'El derecho a la privacidad en la era digital', menciona que:

> Las prácticas en muchos Estados han puesto de manifiesto una carencia de leyes nacionales adecuadas y/o de aplicación de las mismas, insuficientes garantías procesales y capacidades de supervisión ineficaces, elementos que han contribuido a la falta de rendición de cuentas por las injerencias arbitrarias o ilegales en el derecho a la privacidad (p. 17).

En alguna medida es cierto lo que se presenta dentro de este documento de la ONU. A pesar de contar con algunas normativas, regulaciones y políticas en cuanto a la protección de la información de las personas, el derecho a la privacidad puede verse vulnerado incluso por el Estado ecuatoriano.

> Paradójicamente, Ecuador tiene una amplia regulación en cuanto a interceptación de datos, llamadas y mensajes. En todos los casos se exige una orden judicial y se prohíbe el espionaje con fines políticos. Sin embargo, la práctica parece distar mucho del panorama normativo. (Pérez de Acha, 2016, p. 39).

Según Pérez de Acha: el 5 de julio del 2015 se filtró 400 GB de información en las WikiLeaks, acerca de la empresa de tecnología de información, Hacking Team, creadora de una herramienta denominada Remote Control System (RCS), un malware para vigilancia masiva hecho para organizaciones gubernamentales alrededor del mundo. Dentro de los documentos revelados, se encuentra negociaciones hasta entonces secretas, entre la empresa italiana y distintos gobiernos de América Latina, incluyendo al Ecuador.

A pesar de disponer de varias normativas al respecto, en el Ecuador no se implementa políticas adecuadas, normativas o métodos de denuncia o recuperación que permitan al internauta ejercer sus derechos a la privacidad en línea con plena libertad en caso de vulneración de los mismos. Por esta razón, los funcionarios públicos y las personas que comparten información privada en Internet necesitan entender y capacitarse en la instauración de medidas que permitan fortalecer una cultura de protección de información en el país. Además, es importante concientizar a las personas acerca de las repercusiones de compartir información privada de manera indiscriminada.

Es importante entender la realidad en la que se ve vulnerado el derecho a la privacidad. En el Ecuador existe una realidad vigente de ataques cibernéticos. Esto se debe una diversidad de determinantes y factores de igualmente de distinto grado de complejidad. Entre otras cosas se puede mencionar a la falta de conocimiento de las personas en cuanto a la

protección de su información en medios digitales. Según Digiteen (2008), empresa de seguridad informática, en el 2015 Ecuador fue el cuarto país de la región latinoamericana con mayor número de ciberataques, con un porcentaje del 11,22% de usuarios afectados en un monitoreo de más de trece mil dispositivos.

Una de las mayores amenazas dentro del país son los ataques por phising[1]. Según Securelist (2016), el país se posicionó en 2015 en cuarto lugar de ataques por phishing en Latinoamérica, con un 20,03% de afectación de usuarios de la compañía de protección y seguridad digital Kaspersky, según amenazas registradas por la misma empresa.

Otra de las grandes amenazas cibernéticas dentro del país es el malware[2]. Según Dmitry Bestuzhev[3] (2015), una gran parte de usuarios de Internet del Ecuador, específicamente el 40,8%, son atacados vía USB y también vía web. En la provincia de Pichincha se registra el 43% de los casos de ataques del país.

Todo esto sucede a pesar de que existen normativas que permiten sancionar a infractores en este campo. Por ejemplo, el Artículo 229 descrito a continuación del Código Orgánico Integral Penal (2014) se sanciona la revelación ilegal de bases de datos:

1 El phishing se trata de un tipo de fraude por internet, el cual busca la adquisición de credenciales de usuario e información de contraseñas, números de tarjeta de crédito, información de cuentas bancarias, entre otros (Securelist, 2010).

2 Se entiende por malware, el software malicioso que tiene por objeto generar daño informático y comprende a los más variados virus informáticos, tales como los gusanos, troyanos y otros tantos con gran potencial destructivo.” (Tomeo, 2014, p. 209).

3 Director de Investigación y Análisis para Kaspersky Lab en América Latina.

> La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años… Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años (p. 36).

En el caso de la PUCE, la mayor parte de estudiantes se conecta a Internet por medio de sus teléfonos inteligentes. Además, cada día utiliza múltiples aparatos tecnológicos para navegar por la red. Esto hace que los estudiantes se encuentren vulnerables en cuanto a su privacidad, tanto dentro del campus universitario, como en su integridad y autonomía personal por fuera de ese espacio.

En el medio estudiantil, por las razones señaladas anteriormente y por a las condiciones del manejo de Internet en el país, la falta de protección información privada constituye un serio problema. Como se mencionó con anterioridad, la privacidad es un derecho fundamental, el cual dentro del país se ve muchas veces transgredido debido a casos de ataques cibernéticos y una normativa difícil de aplicar en el entorno.

En la figura número 1 se condesa lo señalado en líneas anteriores. Como se puede ver, en la base se han colocado las principales causas de la inadecuada protección de la información, tomando como punto de partida lo

que sucede en el ámbito universitario y en los estudiantes (seguramente en otros usuarios del sistema de red). Se incluye en esta síntesis de las causas a las dimensiones más macro, esto es, a las normativas y políticas del país.

En la parte intermedia del esquema se hace referencia al problema central que resulta de las causas identificadas. En el tercer nivel se registra, igualmente de manera sintética, las consecuencias que conlleva esta problemática.

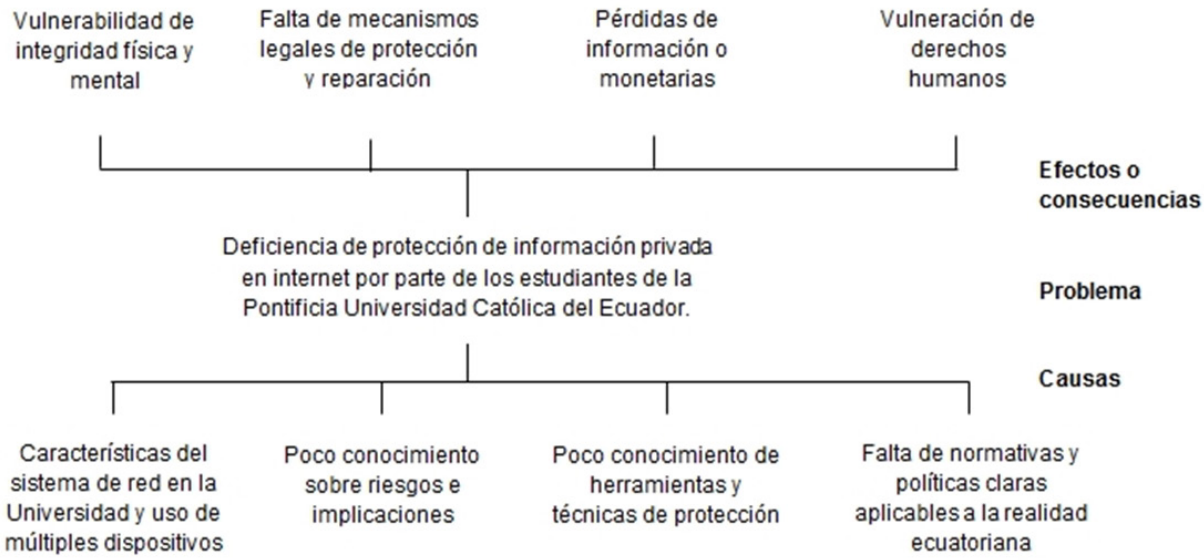


Fig.1. Árbol de problemas

Elaboración: Autor

Con base a lo identificado y sintetizado en el árbol de problemas, en lo que concierne a la disciplina del Diseño Gráfico, las áreas de acción más directas que pueden ser abordadas mediante el diseño de información son el conocimiento acerca de riesgos e implicaciones y disponer de las herramientas y técnicas de protección adecuadas para la generación de una mejor protección.

El trabajo sobre estas causas incide de manera directa en los hábitos de protección y en el conocimiento a futuro del manejo de información por parte del usuario, incluso fuera del entorno estudiantil. Además, son los elementos sobre los que el Diseño tendría más control para comunicar los aspectos pertinentes de manera efectiva y objetiva. Esto evita depender o actuar de manera directa con el sistema de Red dentro de la Institución o de los cambios de normativas y políticas a nivel nacional. Lo último no significa que se soslaye de su importancia, simplemente se está señalando lo factible y lo que mejor se pueda controlar.

Por lo dicho, también se interactúa sobre las normativas y políticas poco aplicables a la realidad nacional, colocadas en la base del árbol de problemas. Los usuarios pueden llegar a conocer de mejor manera, entender y, fundamentalmente, exigir los derechos que tienen al momento de utilizar Internet y la importancia de preservarlos, sobre cualquier contexto.

Así, es importante protegerse en un medio en el que, como estudiante y persona, el usuario y la comunidad universitaria se encuentran expuestos mediante diversos aparatos tecnológicos a la vulneración de su información privada. Este es el sustento teórico y el propósito de los cuales parten los objetivos para el desarrollo del proyecto.

VI. Objetivos

Objetivo General

Desarrollar a través de planteamientos teóricos y prácticos, un producto gráfico que informe a los estudiantes de la PUCE sobre la importancia de mantener protegidos sus datos privados que circulan a través de Internet y fortalezca las prácticas y hábitos orientados a ello.

Objetivos específicos

1. Identificar mediante herramientas de investigación las razones por las que los estudiantes de la PUCE realizan un mal manejo de la información privada en Internet y que sirvan como insumo para el planteamiento de la propuesta gráfica.
2. Establecer una propuesta gráfica que considere las características propias del público objetivo y su entorno y permita su implementación efectiva en el espacio de estudio
3. Verificar la viabilidad del producto diseñado, considerando los estándares teóricos propuestos para el mismo y que satisfaga las necesidades identificadas tanto por el comitente como por los usuarios.

Capítulo 1

1.1. Marco teórico y conceptual

Para efectos de este proyecto de titulación y como ya se ha mencionado, se toma como referente a la privacidad como un derecho humano, reconocido en la Declaración Universal de Derechos Humanos y en los instrumentos de derecho internacional. Se basa, además, en la noción de 'privacidad de forma predeterminada´, acerca de la cual se hablará posteriormente, como la manera de aplicación de ese derecho en la tecnología de información y comunicación.

Los límites para el ejercicio del derecho a la privacidad deben ser proporcionados con base al debido proceso y de acuerdo a lo que está establecido en la ley. Además, en este planteamiento se parte del entendido que las configuraciones de forma predeterminada en la concepción, diseño, desarrollo e implementación de la tecnología de información y comunicación deben garantizar el mayor nivel de privacidad posible para los usuarios.

1.1.1. Antecedentes

A pesar de los esfuerzos de los últimos años a nivel nacional por la preocupación de preservar la privacidad en este campo, aún queda mucho por hacer para que las personas conozcan maneras prácticas de protegerse. Muestras de esta preocupación creciente son los pronunciamientos de grupos nacionales e internacionales exigiendo la protección de su privacidad.

Dentro de éstos se encuentra el 'Pronunciamiento en Defensa de la Privacidad en Ecuador', realizado por organizaciones de activistas dentro del

continente, por ejemplo, de Electronic Frontier Foundation (EFF), Asociación para el Progreso de las Comunicaciones (APC), Usuarios Digitales, Access, entre otras. Demandaron la realización de investigaciones y mecanismos de control y transparencia en referencia al caso del contrato realizado con el Hacking Team por parte de la Secretaría Nacional de Inteligencia, SENAIN, para la vigilancia y monitoreo a nivel de todo el Ecuador (Bogado, 2015).

De igual manera, después de varias críticas por parte de las autoridades del gobierno del Ecuador hacia el anonimato en Internet, diversas organizaciones realizaron el 'Manifiesto por la libertad de expresión, el anonimato y la privacidad en línea en Ecuador'.

Access Now (2015), expone que "El anonimato es una herramienta fundamental para ejercer plenamente el derecho a la libre expresión, ya sea en Internet o fuera de ella. La difusión de datos personales de quienes usan legalmente el anonimato constituye una amenaza a la integridad de las personas…los recursos públicos deben brindar las garantías suficientes para promover el libre ejercicio de nuestros derechos también en plataformas digitales" .

Como otra forma de protección y garantía jurisdiccional es posible apelar al Habeas Data, un recurso establecido en el artículo 92 de la Constitución y que garantiza el derecho al acceso y conocimiento del uso de información personal en cualquier medio, con autorización de su titular o de la ley. (Constitución de la República del Ecuador, 2008).

A pesar que la protección de la información privada consta dentro de las políticas y normativas de la legislación ecuatoriana en pro de los derechos humanos, en la práctica la aplicación de las normativas planteadas no es adecuada para la realidad ecuatoriana.

En vista que las políticas y acuerdos de derechos no son aplicables al entorno del Ecuador, es necesario realizar un análisis de la importancia de la privacidad en Internet, así como de los métodos de protección de la información privada.

Por otro lado, es bueno señalar que se ha desarrollado gran cantidad de herramientas en línea con el afán de generar conciencia y de apoyar de distintas maneras para proteger la privacidad en Internet.

Un ejemplo de ello es 'La caja de herramientas', una guía desarrollada por las organizaciones Tactical Tech y Front Line, en conjunto con una red de miles de activistas, facilitadores y expertos en seguridad digital, para asegurar la protección en línea de activistas y defensores de derechos humanos. La guía cubre desde principios básicos de protección, hasta la instalación de varias herramientas y servicios esenciales para la seguridad digital. (Security in a box, 2009).

También se encuentra iniciativas como 'ItrainOnline' (http://www.itrainonline.org), una guía web creada por ocho organizaciones expertas en el manejo de TICs. Contiene una selección de recursos para el desarrollo y manejo de nuevas tecnologías de manera segura.

También está el Kit de Primeros Auxilios para la Seguridad Digital de Defensores de Derechos Humanos (https://www.apc.org/en/irhr/digital-security-first-aid-kit). Se trata de un kit desarrollado por activistas y para activistas, que los ayuda a mantener su seguridad en las prácticas digitales. Sin embargo es una herramienta especializada y la mayoría de personas desconoce de ella. (Association for Progressive Communications, 2017).

De igual manera, es importante realizar un trabajo ideado hacia las necesidades de los estudiantes y para la protección de la información

que proporcionan diariamente sin tener en cuenta riesgos, ni formas de protegerse de amenazas cibernéticas.

1.1.2. La privacidad y el anonimato en Internet como derechos fundamentales

Para entender mejor la importancia de la privacidad como derecho y por qué exigirlo, es necesario definir qué es.
La privacidad es un derecho humano fundamental que permite a las personas salvaguardar su autonomía y dignidad. “La privacidad representa el concepto que los individuos tienen el derecho a determinar quién tiene información acerca de ellos y controlar cómo, cuándo y en qué medida esa información es comunicada” (Nyst, 2013).

Entonces, la privacidad, en el caso de la información, es el derecho de los individuos a determinar cómo se maneja su información personal, quién cuenta con esa información, cómo se la controla y en qué medida es comunicada.

Cabe recalcar que la privacidad permite a las personas establecer límites y barreras para protegerse de manera individual y como miembro de una sociedad de elementos no deseados en su vida y del uso de poder arbitrario e injustificado por parte de otros. Se considera un derecho esencial que determina quiénes somos como seres humanos, pues brinda un espacio individual libre de discriminación y juicios para pensar, ser uno mismo y definirse como persona.

Según la organización Privacy International (2014):

> Tomando en cuenta esta postura, un elemento importante dentro del derecho a la privacidad es el derecho a la protección de información personal. Además, sostiene que en el caso de la información personal es necesario que los individuos tengan los medios necesarios para ejercer su derecho a la privacidad y que se puedan proteger de cualquier tipo de abuso o violación al mismo.

Tomando en cuenta esta postura, la información a ser protegida puede ser cualquier información relativa a una persona física identificada o identificable. (Consejo de Europa, 1981).

Las nuevas tecnologías brindan un espacio intercultural mediante el cual los usuarios ya no se ven limitados por problemas de los sistemas de comunicación tradicionales. Esto propicia un entorno ideal para compartir ideas y evolucionar como sociedad. El Internet tiene un profundo valor sobre la libertad de expresión. Kaye (2015), explica que el Internet magnifica las opiniones de las personas y multiplica el alcance de la información hacia los usuarios de la red. (OHCHR, 2015)

Sin embargo, la masificación social en la red constituye una realidad distinta en términos del manejo de las libertades individuales, por lo tanto, no es posible asegurar una total garantía para el ejercicio de los derechos fundamentales como los de la privacidad y de la libertad de expresión. García (2014), asegura que por esta razón es importante que un Internet seguro y abierto pueda ser contado entre los prerrequisitos para el ejercicio de la libertad de expresión.

La privacidad fortalece la libertad de expresión[4], tanto lo uno como lo otro son pilares de las sociedades democráticas. Por lo señalado, es fundamental hacer ejercicio de la libertad y, al mismo tiempo, tener la capacidad para mantener el anonimato en la red[5]. Se ve cada vez con más frecuencia a víctimas de delincuencia, violencia y discriminación; a humoristas, activistas y a otro tipo de personas descubriendo su sexualidad y buscando información para afrontarla; clientes disconformes; individuos que han sufrido abuso de poder víctimas de acoso y bullying; trabajadores que denuncian malas condiciones laborales; periodistas y estudiantes afectados de distintas maneras al ser la información sus herramientas de trabajo; a enfermos y adictos buscando consejos de pacientes similares, etc.

Según la organización derechos digitales, todos los usuarios de Internet que brindan y proveen información en la red, deben ser capaces de preservar y manejar su intimidad, así mismo:

“El derecho al anonimato es una de las garantías básicas de la democracia: nos permite expresar nuestras opiniones sin temor a represalias. Ya sea con fines políticos, críticos, humorísticos o satíricos, históricamente el anonimato ha sido uno de los garantes de la libertad de expresión y en Internet no es diferente.” (Garay, 2016).

4 Es el derecho a la difusión, investigación y recepción de opiniones, ideas y posturas, sin limitaciones en cualquier medio de expresión y sin ser discriminado por ello (ONU, 1948).

5 Derecho a mantener oculta la personalidad, nombre e información acerca de un individuo en Internet. Es indispensable para preservar y manejar la intimidad personal. Es una garantía en línea para expresar una opinión o postura sin temor a represalias. (Derechos Digitales, 2016).

Las nuevas tecnologías ofrecen a los distintos gobiernos, corporaciones y hasta a los criminales una gran capacidad de interferir con los derechos de libertad de expresión. La censura en línea, la vigilancia masiva, recolección de datos y ataques digitales a la sociedad civil, que resultan de la expresión en línea, fuerzan a los usuarios de Internet a buscar formas de mantener su seguridad y a la vez sostener posturas y opiniones públicas que les permitan asegurar el ejercicio de sus derechos. Tomando esto en cuenta, es importante conocer sobre la información que debe ser protegida, por qué razones y por cuáles medios.

1.1.3. La importancia de proteger la información privada en Internet

La privacidad electrónica hace difícil la salvaguarda de información privada, en cuanto a riesgos como pérdida, alteración o destrucción de ella, así como acceso y difusión no autorizada por parte de terceros. (Ballesteros, 2006, p. 152).

Es importante entender la forma en la que un usuario de Internet deja rastros en línea de sí mismo y de sus interacciones con otros usuarios y medios. La mayoría de personas dejan cientos de rastros digitales[6] todos los días. Éstos pueden ser intencionales, como e-mails, fotografías, comentarios, entradas de blogs, etc., o involuntarios, como registros de visitas a sitios web, búsquedas en la red, historiales web y de llamadas telefónicas, entre

6 Información que se proporciona voluntaria o involuntariamente en Internet. Desde entradas de blogs, correos electrónicos, tweets, fotografías, comentarios en redes sociales, hasta registros de visitas a sitios web e historiales de búsqueda.

otros. En su conjunto, los rastros digitales proporcionan mucha información personal del usuario, la cual en muchas ocasiones se asume como privada.

Es bueno recordar que existen dos tipos de rastros digitales, los contenidos de un mensaje y los denominados metadatos. Los primeros, es decir, los contenidos de un mensaje encierran la información que se proporciona de manera consciente, lo que la persona que los emite desea comunicar, por ejemplo lo que se escribe dentro de un mensaje de texto. En cambio, los metadatos[7] hacen referencia a los detalles de los primeros, es decir, contienen información diversa sobre los contenidos de un mensaje que han sido objeto de análisis. Tactical Tech (2016), menciona que muchas veces los metadatos se generan de manera automática. Por ejemplo un registro de algún número telefónico, nombres de usuario, geolocalización, fechas y horas de mensajes y llamadas, archivos, etc.

Una gran cantidad de metadatos son generados sin que el usuario lo sepa. Permiten analizar, reconocer patrones y establecer un perfil acerca de la persona y de sus actividades. Empresas que centralizan la comunicación y la información que es transmitida mediante las TICs logran construir historiales detallados y bases de datos con información de los individuos, incluyendo datos que quizás la persona no quiera revelar (EFF, 2015).

> La tecnología informática pone a disposición de los prestadores de servicios en Internet, procedimientos que permiten acceder a datos personales de los usuarios con conocimiento y también sin conocimiento de los mismos y almacenarlos, clasificarlos, manipulándolos de mil formas. (Muñoz, 2000, p. 175).

7 Se trata de los datos sobre otros datos. Información generada automáticamente acerca de un contenido específico. Por ejemplo registros de llamadas telefónicos, direcciones de correo electrónico, datos de geolocalización, fechas, entre otros.

Las consecuencias de no controlar o proteger la información que se provee en línea van más allá de fraudes, estafas, y casos de cibercrimen. Se ve vulnerada la autonomía, integridad y confidencialidad de la persona y de sus relaciones con el entorno. En definitiva, su derecho a la privacidad no se cumple.

Por lo señalado, es importante entender qué tipo de información debe ser protegida para asegurar una buena protección de la privacidad. El Departamento de Seguridad Nacional de los Estados Unidos (DHS), define la información de carácter personal como 'Personally Identifiable Information' (PII). El PII consiste en "cualquier tipo de información que permite que la identificación de un individuo sea directa o indirectamente inferida, incluyendo cualquier información ligada o vinculable hacia ese individuo… (DHS, 2012).

En definitiva, el PII es la información de carácter personal, que permite la identificación, contacto o localización de una persona. Existe una gran variedad de herramientas y métodos que se puede utilizar para proteger este tipo de información. Pero también es necesario considerar su papel en el ejercicio de Internet como usuario y cómo proteger el PII en consonancia con los derechos de privacidad y a la vez de expresión humana

EFF asegura que la protección de metadatos, de colecciones externas, es un problema técnicamente complicado. Sin embargo existen distintas herramientas y métodos que se puede utilizar para proteger la privacidad del usuario.

1.1.4. Herramientas para la seguridad digital

Bajo la premisa de que es indispensable preservar la privacidad de la información y fomentar la seguridad de lo que la persona dispone como un bien preciado, es necesario saber con qué estrategias y herramientas es factible alcanzar estos justos propósitos, aspecto no del todo sencillo. “Los gobiernos y las empresas aseguran que la anonimización efectiva de datos es posible. Sin embargo, el segundo que examinas esta afirmación bajo lupa, empieza a desmoronarse”. (Tactical Tech, 2016).

Uno de los mayores retos en la protección de la información privada es el tipo y el tamaño de la información que se almacena y la facilidad con la que esa información puede ser arrebatada por agentes externos. Por esta razón, los expertos recomiendan ocultar los datos para recuperarlos a través de una clave que solo conoce el interesado; en otras palabras, es aconsejable encriptar la información por medio de diversos métodos de autenticación y utilizando software de anonimato en línea. EFF, 2015).

Las soluciones de seguridad digital[8], como la encriptación[9] de información y software de anonimato, son necesarias para asegurar el derecho a la privacidad del usuario y el anonimato en la red. Esto permite a los individuos protegerse de la vigilancia digital y del espionaje masivo, así como prevenir ciberataques. Se logra crear una zona de privacidad que protege la opinión

8 Hace referencia al bienestar de una persona y su seguridad en línea. Se trata de las medidas y precauciones que preponderan la integridad del usuario en Internet. (Digiteen, 2008).

9 Proceso de codificar comunicaciones para que no puedan ser interceptadas por un tercero. Por lo general se accede a mensajes encriptados por medio de claves o llaves electrónicas.

de la persona y sus acciones en entornos sociales, políticos, religiosos, que podrían estar controlados y atacados.

Desde otro ángulo, el anonimato también puede funcionar como un medio de evasión y camuflaje en casos de ataques cibernéticos[10], utilizado con mucha frecuencia por el perpetrador del ataque. Por esta razón es importante utilizar diversas tácticas para la protección de la información privada en internet, marcando una diferenciación entre las buenas intenciones de esas tácticas y las de tipo delincuencial.

Es importante implementar y aplicar distintos métodos de protección en internet, en vista que la privacidad no es un elemento cuya protección se encuentra considerada de forma predeterminada en el diseño de los distintos medios web. La Dra. Cavoukian, A., Comisionada canadiense en Información y Privacidad, afirma que la protección de la privacidad debe convertirse en el modo de operación “por defecto” (de forma predeterminada) de una organización. (Cavoukian, 2015).

Finalmente, es indispensable considerar distintos métodos de protección digitales para asegurar el anonimato en línea y la protección de la información privada, así como el ejercicio de la libertad de expresión, en un medio en el que la noción de privacidad planteada en acuerdos e instrumentos de derechos no son aplicables y la privacidad se debe conseguir idealmente de forma predeterminada.

10 Ataques realizados por Internet, que tienen motivaciones económicas, sociales o políticas. Pueden encontrarse dirigidos a ciudadanos, organizaciones o incluso gobiernos. Su difusión por lo general es mediante malwares, sitios web falsos y otros medios difundidos por plataformas como correo electrónico para perjudicar a las distintas entidades. (Trend Micro Incorporated, 2015).

1.1.5. Diseño Centrado en el Usuario (DCU)

El diseño juega un papel relevante en el ejercicio de los derechos, especialmente en jóvenes estudiantes en los que es necesario generar una serie de hábitos y difundir métodos de protección de su privacidad. En esta perspectiva, el diseño debe trabajar para preservar la integridad y mejorar el manejo de información que puede ser considerada delicada o sensible y que va tomando relevancia con el tiempo. Posteriormente será de mucho valor al momento del ejercicio profesional en cualquier campo.

Es importante que el manejo y tratamiento de información privada y personal, así como las formas de protección en la Red, sean considerados dentro del medio estudiantil en un contexto muy específico. Por todo lo dicho, el Diseño Centrado en el Usuario (DCU) se convierte en un eje esencial en el desarrollo del presente proyecto. Es una estrategia que, además, puede ofrecer herramientas útiles para beneficios individuales y colectivos, en este caso, de los estudiantes y de la Institución.

El propósito central del DCU es el de apoyar a los estudiantes de la PUCE para que se mejore el entendimiento de la importancia de preservar el derecho a la privacidad, sobre el conocimiento de amenazas y para que sepa que existen herramientas y métodos de protección que pueden ser usados de manera sencilla.

El DCU, a más de responder a un referente teórico-metodológico señalado en líneas anteriores, se considera una estrategia de diseño para el desarrollo y testeo de un producto que se encuentre acorde a las necesidades y características específicas de un usuario determinado. Como lo especifican Pratt y Nuñez (2013):

> Conocer al usuario, saber qué quiere exactamente, qué necesita y en qué contexto utilizará el producto no sólo es una buena manera de garantizar que funcionará, sino que además contribuye en cierta medida en crear una sociedad más segura y saludable. (p. 16).

Tomando en cuenta el contexto en el que se da el manejo de la privacidad y los medios que son utilizados cotidianamente en el entorno universitario, el DCU debe ser considerado en su aplicación dentro de los medios digitales de manera interactiva y lúdica.

1.1.6. Diseño interactivo

En las plataformas actuales es indispensable el diseño de sistemas interactivos que permitan un mejor relacionamiento entre el usuario y el medio digital. Para esto es importante tomar en cuenta un proceso interactivo y de retroalimentación de interacciones entre el estudiante y el producto que se desarrolla, que incluye diseño de la interfaz de usuario, las formas de uso del mismo, incorporados dentro de una experiencia que busca ser satisfactoria. En este sentido, se debe considerar los elementos y aspectos centrales de diseño que configuran la experiencia interactiva y que parte de las necesidades específicas del usuario.

Como explica Benyon (2010). “El diseño de sistemas interactivos concierne al desarrollo de sistemas interactivos de alta calidad, productos y servicios que calcen con la gente y su modo de vida” (p. 6). De esta manera, el diseño interactivo debe atender a servicios y productos digitales cotidianos, como es el caso de la protección de la privacidad.

1.1.7. Diseño de información

Para la generación de contenido adecuado dentro del diseño interactivo y con base a las necesidades específicas y a los retos y dificultades que se presentan en los usuarios de Internet de la PUCE, es necesario gestionar información y conocimientos de otras disciplinas. Esto es indispensable para generar una interpretación, asimilación y posterior acción en torno a ella, por medio de las percepciones y entendimiento de aquel contenido. Así lo explica Frascara (2011):

> El diseño de información es necesariamente diseño centrado en el usuario [...] No hay recetas en el diseño de información: hay conocimientos aplicables, pero la aplicación siempre debe hacerse con intensa atención prestada a quien nos dirigimos, para qué lo hacemos, dónde, cuándo y por medio de qué (p.9).

Además, el diseño de información permite en primer lugar organizar la información de manera interdisciplinaria y sistematizada y planificar la implementación de la misma. Es importante el uso de recursos visuales para hacerla asimilable y atractiva para el usuario, considerando, además, el contexto en el que se desenvuelve. Se utiliza métodos que permiten evaluar de manera objetiva la eficacia del producto planteado y entender los elementos que se pueden mejorar (Frascara, 2011). Son precisamente estos planteamientos los que se han tomado en cuenta para el componente de diseño de este trabajo.

1.1.8. Gamificación y el juego

Asimismo, dentro del ámbito del diseño, es necesario incluir dinámicas y recursos relativos al juego, de manera que se pueda generar motivación para modificar ciertos comportamientos que no son del todo fácil susceptibles de cambiar. A esto se le conoce como gamificación.

> La gamificación es la aplicación de recursos propios de los juegos (diseño, dinámicas, elementos, etc.) en contextos no lúdicos, con el fin de modificar los comportamientos de los individuos, actuando sobre su motivación, para la consecución de objetivos concretos. (Ferrán, 2015, p. 18).

El juego es importante como un medio para conseguir objetivos concretos, trabajando sobre la motivación, sobre todo si se implementa como actividades en entornos ajenos, como el caso de un producto informativo. Así lo indica Aranda, Goméz y Navarro, (2015), “La experiencia de juego es [...] una pieza clave de nuestro deseo por el descubrimiento y la superación como civilización. [...] el juego se define como un factor distintivo y de vital importancia en el mundo social y cultural de los humanos” (p.13).

Por lo visto, el diseño interactivo debe ir de la mano con actividades lúdicas que motiven al usuario hacia cierto fin. Es también otro de los principios que ha servido de referencia para la elaboración del instrumento de diseño para los estudiantes de la PUCE.

PRIMER COMPONENTE: INVESTIGACIÓN

Un aspecto importante en la formación de los futuros diseñadores en la FADA ha sido la inclusión del pensamiento sistémico y de las teorías de la complejidad de Morin, (1981) ,como marco de referencia para la estructuración de un proyecto de diseño. Y, como herramienta metodológica, la importancia de la investigación, cuyos resultados sirvan para ubicar al usuario en sus necesidades y en el contexto en donde él se desenvuelve. De esta manera, el diseño no se reduce a un proceso mecánico, alejado de la realidad en donde va a ser aplicado o utilizado.

Uno de los propósitos del componente de investigación ha sido la búsqueda de evidencias sobre el inadecuado manejo de la información privada en los estudiantes universitarios de la Pontificia Universidad Católica del Ecuador (PUCE), los cuales dentro de un medio institucional comparten información y refuerzan hábitos que los pueden dejar expuestos a situaciones de vulnerabilidad fuera de la Universidad. Sobre este supuesto, se ha tomado el reto de elaborar y ofrecer una herramienta que coadyuve a la protección de ataques cibernéticos a los que se encuentran expuestos los estudiantes.

1.2. Respuesta tentativa a un problema de investigación

Para este proyecto se ha considerado al diseño como un medio para potenciar y facilitar el entendimiento y la asimilación de información que posibilite la generación de hábitos de protección y un mejor manejo de la privacidad en línea de los estudiantes de la PUCE. La investigación previa ha servido de base para definir las características del proyecto de diseño. Se parte de la premisa que existe una deficiencia en la protección de la privacidad por parte de los estudiantes de la PUCE. Debido, posiblemente, a la falta de conocimiento de amenazas, riesgos e implicaciones y a la ausencia de herramientas de protección que faciliten un mejor manejo de la información privada en línea.

Mediante un mejor conocimiento de las repercusiones y técnicas adecuadas de protección se mejoraría el manejo de la información por parte de los estudiantes, como una respuesta tentativa a esta problemática. La investigación previa se ha considerado como paso fundamental para corroborar o modular estas apreciaciones.

1.3 Operacionalización de la investigación

El componente de investigación parte de cómo se ha concebido el planteamiento del problema. Ha sido indispensable sistematizar esos pensamientos en hipótesis, variables, indicadores y en la metodología que se utilizaría para la recolección de los datos. Ha sido necesario elaborar una matriz de operacionalización que consta a continuación:

Hipótesis			Variables	Indicadores	Metodología/ técnicas
Problema / Premisa	Verbo condicional	Respuestas / Causas	…existe una variación de:	Evidencias / Medibles:	Marco metodológico
Deficiencia de protección de información privada en Internet por parte de los estudiantes de la Pontificia Universidad Católica del Ecuador.	Esto se debería al mal manejo de la información privada en Internet por parte de los estudiantes de la PUCE	Normativas y políticas poco claras, y no aplicables a la realidad ecuatoriana.	1. Conocimiento de las leyes 2. Aplicación de las leyes	¿Qué leyes hay?	Entrevista Revisión de fuentes secundarias
				¿Cuántas personas conocen acerca de derechos de la privacidad y protección de la intimidad en la constitución y leyes secundarias?	Focus Group, encuesta
				¿Se toman o no en cuenta las normativas para el sistema de red de la Universidad?	Entrevista
		Poco conocimiento sobre riesgos e implicaciones.	1. Riesgos 2. Implicaciones	Amenazas cibernéticas que los usuarios conocen	Encuesta, Focus Group
				¿Hasta qué punto es riesgoso compartir información privada?	Entrevista
				Casos de ciberataques en estudiantes	Focus Group, encuesta
		Falta de conocimiento de herramientas y técnicas de protección.	1. Conocimiento de las personas acerca de las herramientas 2. Desinterés	Herramientas que las personas conocen y utilizan	Focus group, encuesta
				Técnicas de protección que la gente implementa	Etnografía, focus group
				Preocupación por mantener privacidad en Internet	Encuesta
		Características del sistema de red en la Universidad y uso de múltiples dispositivos.	1. Seguridad del sistema 2. Hábitos de los usuarios al usar el Internet	¿Qué medidas implementa la red de la Universidad?	Entrevista
				¿Qué actividades realiza el estudiante al utilizar Internet dentro de la Universidad?	Seguimiento, foto-diario
				¿Qué uso se les da a distintos dispositivos?	Seguimiento, foto-diario
Explicación (Se obtienen de un análisis teórico conceptual para poder explicar el problema y saber qué hacer para eliminarlo) MT1. Ingeniería en Sistemas MT2. Sociología MT3. Derecho					

Tabla 1: Operacionalización de las variables.

Elaboración: Autor

1.4. Procedimiento - metodología del componente de investigación

Para un adecuado diagnóstico del problema de estudio se recurrió a distintas metodologías para la recolección, clasificación, procesamiento y análisis de la información. Se tomó como referencia principal la metodología de la investigación de Hernández, Fernández, Baptista (2006). En este componente de investigación se aplicaron técnicas cuantitativas y cualitativas; se usaron fuentes primarias y fuentes secundarias.

Dentro de las técnicas cuantitativas se aplicó una encuesta a la población de estudio. Ésta consistió en un conjunto de preguntas, la mayoría estructuradas como preguntas cerradas que incluían diversas variables susceptibles a ser valoradas (Hernández, Fernández y Baptista, 2006). Se diseñó el instrumento para que sea un cuestionario autoadministrado. Se procesó la información de manera manual y con la ayuda de herramientas digitales.

Dentro de las técnicas cualitativas se realizaron entrevistas a informantes claves y trabajo con grupos focales. Esto con la finalidad de obtener información de relevancia en torno a percepciones, hábitos e información clave acerca de algunas variables del estudio. También se recurrió a metodologías de investigación observacionales, apoyado por lo que se plantea en el libro 'Métodos de Investigación del Diseño de Productos' de Rodgers y Milton (2013). Dentro del componente etnográfico del estudio se utilizó entrevistas, seguimientos y foto diarios, con la finalidad de obtener información relacionada con el comportamiento, hábitos, entorno y percepción de los usuarios. Estas técnicas se plantearon en vista de la importancia de entender patrones de uso y características de éste, desde distintos dispositivos, así como el desenvolvimiento del usuario en la red.

Todas las técnicas citadas en líneas anteriores correspondieron a fuentes primarias; las fuentes secundarias fueron especialmente documentos de las normativas con que cuenta el país en el tema de estudio (legislaciones, normativas institucionales y generales, la Constitución de la República del Ecuador, estrategias, etc.).

La metodología del diseño se detalla en la parte correspondiente del segundo componente.

Universo y muestra

De un universo de 10680 estudiantes en la Universidad se seleccionó una muestra propositiva y aleatoria de 84 estudiantes de distintas carreras y niveles de la PUCE, en los cuales se aplicaron las diversas técnicas de recolección de datos señaladas en la metodología. Los resultados se muestran en siguiente acápite.

1.5 Resultados de la investigación

En esta sección se presentarán los resultados más relevantes del estudio, tanto los obtenidos de fuentes primarias como secundarias, a través de la técnica de encuesta como de las técnicas cualitativas. Con varios de ellos se procede a realizar el análisis respectivo.

1.5.1 Normativas y políticas de privacidad en internet

La PUCE, como institución privada, que debe preservar y realizar un manejo adecuado de la información de la comunidad universitaria, cuenta con su propia política y normas en cuanto a información procesada mediante sistemas informáticos para asegurar la integridad y autonomía de los estudiantes y personal administrativo

Al no conocer las distintas políticas y estándares sobre los cuales se debería ejercer sus derechos, los estudiantes no exigen que el manejo por parte de entidades públicas y privadas sea realizado de manera trasparente, ni que se implementen políticas públicas que reflejen en el adecuado manejo de la información de carácter personal.

Según el ingeniero Pazmiño[11], una de las mayores razones para hacer del país un entorno fértil para amenazas cibernéticas es que las leyes y normativas, en cuanto a la privacidad en línea, son muy genéricas y por lo tanto no aplican al contexto social del Ecuador. Además, hace falta políticas y sanciones claras. (A. Pazmiño, comunicación personal, 2016).

Andrés Delgado, activista y miembro de la organización Apertura Radical, para los derechos de privacidad en Internet, afirma que dentro del país no se ejerce un control adecuado de la información y no se respeta la normativa existente. Indica también que no se actualiza la información, debido a que una gran mayoría de usuarios en el Ecuador, por múltiples razones no entienden cómo funciona la tecnología. Por lo tanto, es necesario generar una conciencia alrededor de la información privada que se provee en Internet. (A. Delgado, comunicación personal, 2016).

11 Oficial de Seguridad Informática de la PUCE.

1.5.1.1. Conocimiento y aplicación de las normas y reglamentos por parte de la comunidad universitaria

Las TICs brindan un espacio intercultural y propician un entorno ideal para compartir ideas y evolucionar como sociedad. Sin embargo, es necesario entender y conocer las políticas y normativas para exigir y poder ejercer de manera plena los derechos humanos aplicables a Internet.

En un sondeo realizado a 85 personas de la PUCE, se determinó que aproximadamente un 95% de los estudiantes no se encuentran familiarizados con alguna legislación de derecho de privacidad de la información. De igual manera, alrededor del 99% no conoce el trabajo de la Institución en relación a temas de privacidad.

Al realizar un Grupo Focal con 7 estudiantes de la Facultad de Arquitectura, Diseño y Artes de la PUCE se determinó que ninguno de ellos conocía legislación en cuanto a privacidad, ni métodos de reparación o denuncia fuera de la Universidad. Tampoco conocían las políticas y normativas de la Institución en cuanto al manejo de información.

Esto se debe a la poca concientización que se realiza, no solamente a nivel Universidad, sino también a nivel país. El Ingeniero Pazmiño explicó que en el caso de la PUCE no se han realizado campañas de difusión de las políticas aplicadas por la misma Institución, debido a cambios estructurales y administrativos que fueron realizados en el momento de la implementación de la normativa.

1.5.1.2. Medidas de protección de la PUCE

El 20 de enero del 2012 la Universidad aprobó la 'Política Detallada y Normas de Seguridad Lógica de la Información Procesada con Sistemas Informáticos', desarrollada por la Oficina de Seguridad de la Información.

El objetivo de la política consiste en "normar la recolección, transmisión, almacenamiento, proceso y distribución de información por medio de sistemas informáticos, dirigida a salvaguardarla de eventos adversos que pudieran ocasionar la suspensión de los servicios de la Universidad basados en sistemas de información automatizados, del uso o divulgación no autorizados, o de alteraciones intencionales o no." (Oficina de seguridad de la información [OSI PUCE], 2012)

La normativa ayuda a sistematizar y a orientar el manejo y la circulación de la información dentro de la Universidad. Todo esto, con la finalidad de que sea menos vulnerable a situaciones que pudieran comprometer la integridad de algún miembro de la Institución y para mejorar la percepción que las personas puedan tener sobre el manejo de la información.

Además, busca proteger información de carácter confidencial, que verifique o conduzca a la identificación de personas. Por ejemplo, apellidos, número de cédula, fotografías, dirección, lugar, fecha de nacimiento, huella digital, información financiera, cuentas bancarias, etc., todo los cual se puede encontrar sujeta a pérdida de privacidad, robo o suplantación de identidad, entre otras amenazas.

Sin embargo, debido a cuestiones de cambios institucionales, según el Ingeniero Pazmiño, la política no ha podido ser implementada y difundida en los estudiantes como se señala en líneas anteriores.

Raúl Zapata, Administrador de Redes de la Institución, explica que la Red de la Universidad se encuentra sujeta a un constante trabajo de protección y vigilancia en vista de amenazas externas. Éste es uno de los puntos que permite que la Red sea de gran seguridad para los estudiantes.

La Política Detallada y Normas de Seguridad Lógica de la Información Procesada con Sistemas Informáticos complementan y sistematiza el trabajo de protección de la información confidencial en la Universidad. Estos datos deben ser clasificados por personas designadas específicamente para manejar esta información y clasificarla de forma que agentes externos no tengan acceso a ella de manera no autorizada. Finalmente, según el tipo de contenido, es importante tomar medidas para evitar filtraciones o alteraciones, como cifrar la información.

Por otro lado, según el administrador de la Red de la PUCE, lo que sí se ha realizado son campañas de concientización en cuanto a la amenaza cibernética de Phishing, sobre la cual se comentará más adelante. Esto se debe a la cantidad de correos electrónicos que llegaban a las cuentas de la Institución, sobre todo al personal administrativo y que pedían el ingreso de información privada con la amenaza de cerrar la cuenta del usuario si no se respondía al mensaje y con una finalidad lucrativa.

La Universidad cuenta con un sistema de Intranet y correo muy seguro, constantemente monitoreado y el cual, en términos informáticos no es fácil de vulnerar. Desde este punto de vista los estudiantes se encuentran protegidos en cuanto a lo que la Institución respecta, sin embargo, Pazmiño considera necesario e importante generar hábitos de protección en los estudiantes, que ayuden complementar y solventar falencias dentro del resguardo de información privada en la Universidad y en la cotidianidad.

1.5.2. Riesgos e implicaciones de compartir información privada en Internet

1.5.2.1. Riesgos

La empresa Trend Micro Incorporated (2015) explica que los ataques cibernéticos como ataques realizados por Internet tienen motivaciones económicas, sociales o políticas. Pueden encontrarse dirigidos a ciudadanos, organizaciones o incluso gobiernos. Su difusión por lo general es mediante malwares, sitios web falsos y otros medios difundidos por plataformas como correo electrónico para perjudicar a las distintas entidades.

Ecuador cuenta con uno de los índices más altos de ataques cibernéticos dentro de Latinoamérica, dentro de los 10 países más atacados de la región.

> Ecuador es el tercer país de Latinoamérica que más ciberataques sufre anualmente. 'Hackers' de Estados Unidos, Italia, Francia, Alemania, Rusia, Sudráfrica, China y Argentina encabezan estas operaciones ilegales. Empresas de seguridad incluso advierten que el país está en el ranking de las ocho naciones más vulnerables a escala mundial. En esa lista también aparecen México y Brasil. (Fernando Medina, 2016)

De igual manera, en el 2015 el país se posicionó en el cuarto lugar de ataques por phishing dentro del sector (Véase Fig. 2). El Phishing es un tipo de fraude por internet mediante el cual busca la adquisición de credenciales de usuario e información de contraseñas, números de tarjeta de crédito, información de cuentas bancarias, entre otros, es una de las mayores amenazas cibernéticas en el Ecuador (Encyclopedia, 2010).

Por lo general, los atacantes imitan plataformas o notificaciones de sistemas de pago y solicitan al usuario entregar información personal de manera inmediata. A menudo también se trata de correo electrónico basura, el cual llega a la bandeja de entrada del usuario y busca redireccionarlo a alguna página web señuelo para que la persona proporcione sus datos.

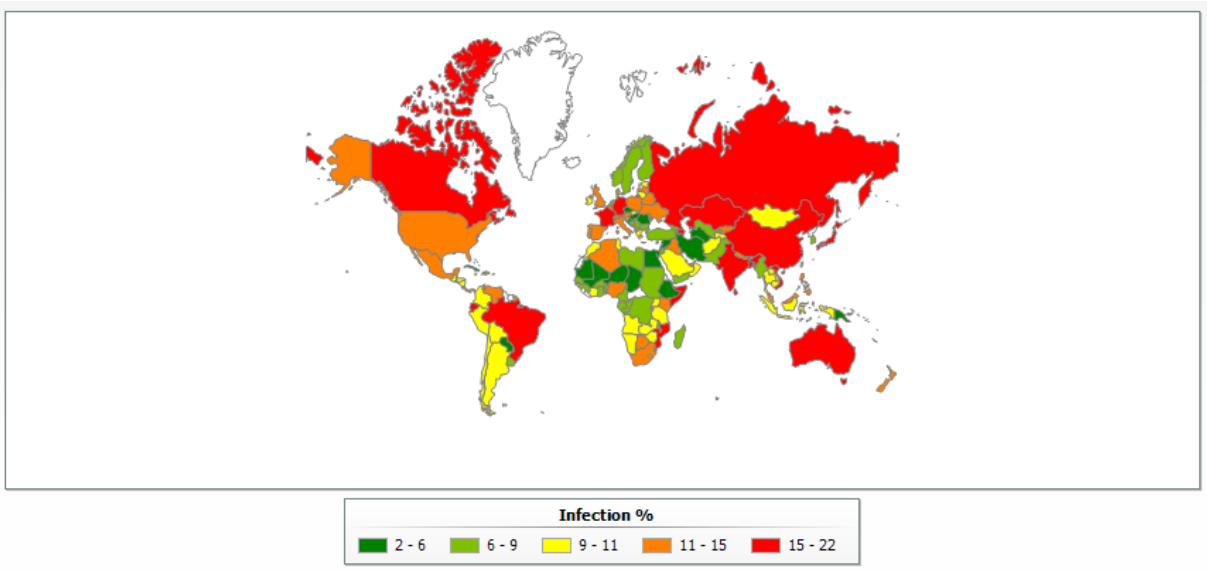


Fig. 2: Países más afectados por Phishing a nivel mundial.

Fuente: Secure list, (2016).

Otra de las grandes amenazas dentro del país, en términos de amenazas cibernéticas, es el **malware**. “Se entiende por malware, el software malicioso que tiene por objeto generar daño informático y comprende a los más variados virus informáticos, tales como los gusanos, troyanos y otros tantos con gran potencial destructivo.” (Tomeo, 2014, p. 209).

En cuanto a los malware, según Dmitry Bestuzhev, (2015), Director de Investigación y Análisis para Kaspersky Lab en America Latina, en Pichincha se registra un total de 43% de los casos dentro del país.

En el caso de la Pontificia Universidad Católica del Ecuador, la mayor cantidad de ataques viene por parte de atacantes de China que buscan vulnerar información y entrar a los servidores de la PUCE. Esto se determinó en la entrevista realizada a Raúl Zapata. Afortunadamente no se ha dado casos dentro de la Universidad, en los que se haya perdido información académica.

Más de la mitad de estudiantes han experimentado alguna situación de vulnerabilidad en Internet en su cotidianidad. Entre otras cosas, se debe a que muchos no conocen y/o no disponen de herramientas para hacerlo, ignorando también las repercusiones de compartir información privada en la red. No se ha desarrollado hábitos de protección, como analizar sus aparatos electrónicos en busca de software malicioso periódicamente, o tener cuidados especiales en las contraseñas que se utiliza. Es importante que el estudiante o cualquier usuario piensen en su protección pero, también, piensen en la protección de los demás.

Zapata y Pazmiño coinciden en que uno de los mayores problemas dentro de la Universidad es el manejo de contraseñas por parte de la comunidad estudiantil, puesto que la técnica utilizada para entrar a la Intranet con un 'PIN' de seguridad, no es muy seguro. Además, muchos estudiantes utilizan claves muy genéricas y las comparten para sus distintas cuentas. (Comunicación personal, 2016).

Por consiguiente, los estudiantes quedan expuestos a extorsiones, suplantaciones de identidad y estafas. De igual manera al no contar con hábitos adecuados de protección, las amenazas van más allá de fraudes y diversas modalidades de cibercrimen. Se ve vulnerada la autonomía, integridad y confidencialidad de la persona y de sus relaciones con el entorno. En definitiva, su derecho a la privacidad no se cumple.

1.5.2.2. Implicaciones

Kaye (2015), explica que las nuevas tecnologías ofrecen a los distintos gobiernos, corporaciones y criminales una gran capacidad de interferir con los derechos de libertad de expresión. La censura en línea, la vigilancia masiva, recolección de datos y ataques digitales a la sociedad civil, que resultan de la expresión en línea, fuerzan a los usuarios de Internet a buscar formas de mantener su seguridad y a la vez sostener posturas y opiniones públicas que les permitan asegurar el ejercicio de sus derechos. Tomando esto en cuenta, es importante entender qué tipo de información debe ser protegida y por qué razones.

En el sondeo realizado a estudiantes de la Universidad se determinó que para los estudiantes de la Universidad es sumamente importante proteger su información personal en línea. Alrededor del 70% de los encuestados calificaron a la importancia de mantener su privacidad en la Red con el valor más alto. De igual manera se considera de mayor importancia el resguardo de información bancaria, contraseñas y direcciones domiciliarias.

Información acerca de la familia, fotografías personales y teléfonos quedaron relegados hacia un segundo plano y opiniones personales, historiales médicos y académicos, preferencias, edad, género y correos electrónicos fueron los ámbitos de menos importancia en términos de protección.

Asimismo, siendo las contraseñas uno de los ámbitos que se consideran más importantes, paradójicamente, el problema más común dentro de la Universidad en los estudiantes es el robo de contraseñas y acceso no autorizado a cuentas personales.

En una entrevista realizada a la abogada Daniela Salazar de la Universidad San Francisco de Quito (USFQ) en el 2016, se concluyó que hace falta

mayor protección en temas de Internet a nivel nacional. Los recursos no son suficientemente rápidos, puesto que el Internet avanza a un paso más rápido que la legislación. Esto constituye el mayor desafío en cuanto a la regulación de la información, debido a que los funcionarios públicos, al igual que la sociedad civil, no están plenamente capacitados en las maneras de protección de su privacidad en línea ni en mecanismos de recuperación. (Salazar, D. Comunicación personal, 2016).

Finalmente, para esta misma abogada, parte de la solución se encuentra en capacitar a quienes comparten información y a funcionarios públicos en entender los riesgos y dimensiones de la deficiencia de protección en la privacidad en línea y en la instauración de políticas públicas claras.

Al realizar el grupo focal con los estudiantes de la PUCE surgió un caso de extorsión un tanto diferente a los comunes. En una ocasión fue robado el teléfono celular de uno de los estudiantes. El teléfono tenía una serie de fotografías personales guardadas en su memoria. Después de unos días, la persona que robó el celular, mediante redes sociales, intentó amenazar al chico con hacer públicas esas fotografías. Afortunadamente no constituyó un elemento que afecte a la integridad emocional del muchacho y la persona cesó con sus amenazas.

Por esta razón no se recurrió a hacer una denuncia formal, el caso no tuvo mayor trascendencia ni serias implicaciones, y en vista del poco conocimiento acerca de normativas y leyes y que la Universidad no cuenta con métodos de recuperación o denuncia para la protección de información privada en Internet, la persona afectada no recurrió a ningún otro método para proteger su información. Esto es un ejemplo de cómo puede afectar una vulneración de este tipo a la cotidianidad del usuario.

Asimismo, las publicaciones que se realiza dentro de las redes sociales, como Facebook o Twitter pueden compartirse con fines mercadológicos hacia otras entidades. La mayoría de empresas de este tipo cuentan con derechos sobre la información personal, por lo que puede analizarla e incluso compartirla. De esta manera es posible crear perfiles mercadológicos en base al modo de comportarse del usuario en la red.

1.5.3. Herramientas y técnicas de protección

Aunque la protección de metadatos es un problema técnicamente complicado y en vista que varias de las políticas de la legislación ecuatoriana no son aplicables a la realidad del país, es importante protegerse en un medio en el que, como estudiante de la PUCE y como persona, el usuario se encuentra expuesto a la vulneración de su información privada. Se debe tomar en consideración distintos métodos de protección digitales para asegurar el anonimato en línea y la protección de la información privada, así como el ejercicio de la libertad de expresión.

La privacidad viene de la mano con dos derechos muy importantes en la preservación de la autonomía humana. Uno de ellos es la libertad de expresión, es decir el derecho a la difusión, investigación y recepción de opiniones, ideas y posturas, sin limitaciones en cualquier medio de expresión y sin ser discriminado por ello (Naciones Unidas, 1948). También se encuentra el anonimato en la Red, indispensable para garantizar la intimidad y la libertad de expresión. (Peréz de Acha, 2016).

1.5.3.1. Medidas de protección adecuadas

Kaye, (2015), asegura que implementar medidas de protección adecuadas puede afianzar y reforzar la libertad de expresión y el derecho al anonimato en la red. Para esto se puede utilizar distintos métodos, como la encriptación de información y software de anonimato.

La **encriptación** consiste en codificar comunicaciones para que no puedan ser interceptadas por un tercero. Por lo general se accede a mensajes encriptados por medio de claves o llaves electrónicas.

De todas maneras, el anonimato también puede funcionar como un medio de evasión y camuflaje en casos de ataques cibernéticos, por parte del perpetrador del ataque. Por esta razón es importante utilizar diversas tácticas para la protección de la información privada en internet.

Según Tactical Techo (2009), algunas de estas tácticas son:

- Proteger tu computadora de software malicioso (malware) y piratas informáticos (hackers)
- Proteger tu información de amenazas físicas
- Crear y mantener contraseñas seguras
- Proteger los archivos sensibles en tu computadora
- Recuperar información perdida
- Destruir información sensible
- Mantener privada tu comunicación en Internet
- Mantenerse en el anonimato y evadir la censura en Internet
- Protegerte a ti mismo y a tus datos cuando utilizas sitios de redes sociales
- Utilizar los teléfonos móviles de la manera más segura posible
- Utilizar los teléfonos inteligentes de la manera más segura posible

Para lograr estos cometidos y llegar a un mejor resguardo de la privacidad, es importante también considerar una serie de herramientas. Aquí encontramos algunas:

- Antivirus
- Anti-espías
- Anti-malwares
- Cortafuegos
- Herramientas para almacenamiento seguro de contraseñas
- Herramientas para almacenamiento seguro de archivos
- Herramientas para recuperación de archivos
- Herramientas para eliminación segura de archivos
- Herramientas para eliminación segura de archivos y limpieza de sesiones de trabajo
- Software de mensajería instantánea segura de texto, audio y video
- Clientes de correo seguro
- Cifrado de archivos y textos de correo electrónico
- Navegadores web seguros
- Navegadores web de anonimato digital y evasión

La doctora Ann Cavoukian señala algunos principios de las estrategias para proteger la privacidad:

1) Proactivo, no reactivo y preventivo, no remedial
2) Privacidad como una configuración por defecto
3) Privacidad incrustada en el Diseño
4) Funcionalidad completa – Suma positiva, no suma igual a cero
5) Seguridad de fin a fin – Protección del ciclo de vida completo
6) Visibilidad y transparencia – Mantenerlo abierto
7) Respeto de la privacidad de usuario – Mantenerlo centrado en el usuario

Bajo estos referentes, qué de ello existe en la PUCE. Según los ingenieros, Pazmiño y Zapata, la Institución implementa varios métodos de autenticación, lo que fortalece la Red de la Universidad. Uno de ellos son las contraseñas, sin embargo el más seguro es la autenticación biométrica, es decir que requiere una parte del cuerpo del usuario para permitir el acceso a alguna parte del sistema, por ejemplo la huella digital. Ambos recomiendan llevar un manejo seguro de contraseñas, con más de ocho caracteres que incluyan números, símbolos y mayúsculas y minúsculas.

El ingeniero Zapata recomienda también revisar la autenticidad de los sitios que se visita y si son seguros. Para realizar esta verificación, se debe fijar que en la dirección se encuentre escrito HTTPS. Además es importante no guardar información de gran importancia en memorias USB o en teléfonos celulares. (Zapata. Comunicación personal, 2016).

Por otra parte, para la abogada Daniela Salazar el principal desafío para la protección de la privacidad en línea en el país es el ritmo vertiginoso en

el que avanza Internet. Por esta razón es necesario para los estudiantes exigir la instauración de políticas públicas que atiendan a las necesidades de protección de la privacidad aplicables a la realidad ecuatoriana, así como métodos de recuperación y promover una correcta capacitación de los funcionarios públicos para el manejo ético de la información. Es necesaria la implementación de medidas de acción necesarias en el caso de una vulneración de los derechos humanos mientras el mismo estudiante haga conciencia de la información que comparte. (Salazar, D. Comunicación personal, 2016).

1.5.3.2. Conocimiento por parte de la comunidad universitaria

En la encuesta realizada dentro de la Universidad se determinó que cerca de la mitad de los estudiantes no conocen herramientas que les permita asegurar de manera efectiva los derechos de libertad de expresión y anonimato en la red. Sin embargo el 80% se encuentra protegido con antivirus en sus dispositivos e incluso un pequeño porcentaje utiliza autenticación biométrica como método de protección.

Esto refleja que existe una conciencia de protección en los estudiantes, sin embargo, no conocen herramientas adecuadas y tienen una confusión en ciertas técnicas. Por ejemplo, más del 50% de estudiantes considera que al navegador seguro es una forma de proteger su información privada, a pesar que se siguen generando metadatos. De igual manera, consideran que tienen un manejo seguro de contraseñas, a pesar que la mayor parte de conflictos en línea son de robo de claves, acceso no autorizado a cuentas y suplantación de identidad.

En el grupo focal se logró observar de igual manera que todos consideraban importante protegerse y estaban conscientes de las repercusiones y riesgos mayores a los que estaban expuestos. Asimismo, todos tenían sus propias maneras de protegerse de situaciones que ellos consideran amenazas o de beneficio para sus dispositivos en base a cuestiones que han aprendido por experiencia propia u otros medios. Por ejemplo, borrar ciertos metadatos, asegurarse que entrar a sitios HTTPS e incluso manejar distintas contraseñas, como algunos ya lo hacen. A pesar de lo señalado, al compartir esa información, algunos no sabían de las técnicas que los otros utilizaban. También parece que existe un problema extendido en el uso del teléfono celular, puesto que se mantienen varias cuentas abiertas al mismo tiempo y en varias ocasiones las claves tienen solamente pequeñas o ninguna variación.

1.5.4. Manejo de la información en los estudiantes

En una entrevista al ingeniero Orlando Acosta, encargado de Redes de la PUCE, se determinó que, de un total de 10.680 estudiantes, casi la mitad de ellos se encuentran conectados a la red de la institución durante las horas de mayor uso de Internet dentro de la Universidad. De este número de personas, el 50% se encuentra conectado mediante celular, el 30% por laptop y el 20% por otros dispositivos (O. Acosta, comunicación personal, 2016).

En términos generales, los entrevistados Pazmiño y Zapata coinciden en que el manejo de la información privada por parte de los estudiantes de la PUCE es inadecuado. Aportan con algunas recomendaciones, entre ellas, que es importante generar en los estudiantes mejores hábitos de protección,

pesar que la Red e Intranet de la Universidad se encuentran sujetos a un constante trabajo y monitoreo para asegurar la integridad de los mismos. (Pazmiño y Zapata. Comunicación personal, 2016).

Otro problema es que con frecuencia se comparte información privada importante en redes sociales. Distintos tipos de cuentas se dejan abiertos en computadoras de la Institución sin ningún cuidado, se maneja una misma o contraseñas similares para todo y se guarda mucha información abierta en teléfonos inteligentes. Por todo ello es imperativo elevar la conciencia sobre las repercusiones de un manejo inadecuado de la información personal, a pesar que al analizar los datos del estudio con la muestra de estudiantes se vio que los hábitos y la conciencia de ellos sobre el tema, se detecta un nivel de importancia alto, en contraste con falta de información, acceso y entendimiento de cómo protegerse según distintos tipos de riesgos.

1.5.4.1. Hábitos y manejo de cuentas y dispositivos

En la Pontificia Universidad Católica del Ecuador, coincidiendo con la opinión del ingeniero Acosta, el ingeniero Pazmiño opina que la mayor parte de estudiantes se conectan a internet por medio de sus teléfonos inteligentes. Señala que los celulares en la actualidad son una puerta a la información privada, susceptible de ser invadida. Esto se debe a que los aparatos son más propensos a perderse o a ser robados. Muchas cuentas e información personal se ven vinculadas entre sí en los teléfonos. (Pazmiño, A. Comunicación personal, 2016).

También se utiliza múltiples aparatos tecnológicos dentro de la Institución para navegar por la red cada día. En otros resultados de la encuesta realizada a los estudiantes se encontró que el 98,7% tiene acceso a Internet

en su celular. De igual manera el 92% utiliza computadoras para acceder a la Red de la Institución. Esto hace que los estudiantes se encuentren vulnerables en cuanto a su privacidad, tanto dentro del campus universitario, como en su integridad y autonomía personal, precisamente por el uso de sus dispositivos personales como por los de la Institución.

Gran parte de los accesos es hacia redes sociales y cuentas de correo electrónico y, el ingeniero Pazmiño considera que los estudiantes no son cautos y no manejan su información de manera crítica o sensible. Muchos chicos o chicas son generosos con la información que brindan, sobre todo en redes sociales y no hay conciencia de que la información puede verse alterada, por ejemplo al compartir fotografías. (Pazmiño, A. Comunicación personal, 2016).

En una observación realizada a una estudiante de la PUCE se determinó que entre las 13h00 horas hasta las 18h30, revisó su teléfono un aproximado de 7 veces, con distintas duraciones, de 2 hasta 10 minutos. En cada ocasión miró aunque sea una vez la red social Facebook. En ninguna ocasión se conectó a la Red de la Institución, puesto que cuando intentó conectarse no funcionó. Por otro lado sí se conectó al Internet de la Universidad desde una computadora portátil y accedió de igual manera a redes sociales. (Fig. 3)

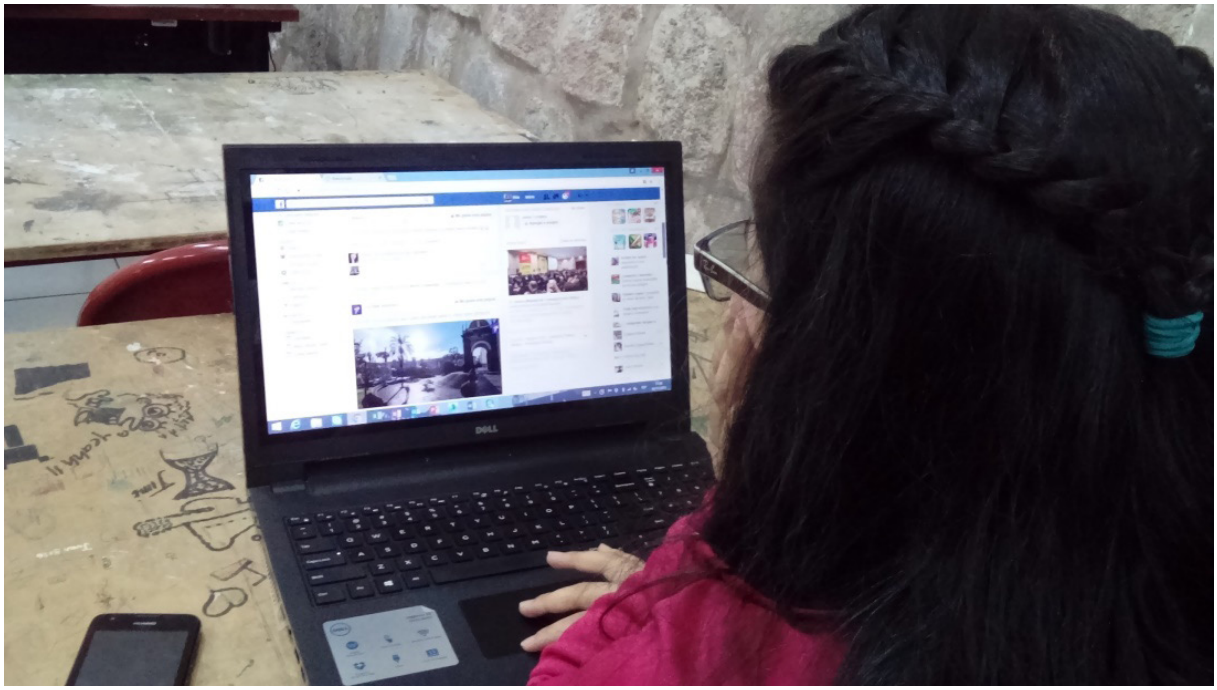


Fig. 3: Manejo de distintos dispositivos casi simultáneamente.

Elaboración: Autor

La persona a la que se estudió tenía en su teléfono celular abiertas cuentas de redes sociales y correo electrónico simultáneamente. De igual manera, las claves que utilizaba para cada una variaban en el uso de mayúsculas y minúsculas, mientras que lo demás se mantenía igual. Posteriormente se conectó a la red de la Universidad con una computadora para hacer un trabajo académico con una duración aproximada de una hora. Si bien no utilizó la computadora y el teléfono inteligente a la vez, sus cuentas se encontraban abiertas en ambos aparatos.

Asimismo en el grupo focal realizado en la Facultad de Arquitectura, Diseño y Artes, FADA, se encontró que los estudiantes acceden a Internet mediante varios dispositivos como computadoras, tabletas y teléfonos inteligentes. De igual manera, se mantienen vinculadas y abiertas una gran cantidad de cuentas, especialmente en los teléfonos celulares.

También consideran que utilizan contraseñas seguras, es decir con más de ocho caracteres, incluyendo mayúsculas y minúsculas y otros símbolos. Sin embargo, no se tiene la costumbre de cambiarlas y entre las distintas cuentas las contraseñas son las mismas o parecidas, generando un margen de inseguridad más grande, susceptibles de la vulneración de alguna de las fuentes.

Por otro lado, los estudiantes comentaron que en repetidas ocasiones se han encontrado con descuidos, que se dejan las cuentas de correo y redes sociales abiertas en las computadoras de la universidad.

Aun así, gran parte de los estudiantes se encuentran conscientes y le brindan importancia al tema de la privacidad en línea. De la encuesta surge el dato que aproximadamente el 71% de personas calificaron con el puntaje más alto, en una escala del uno al cinco, a la pregunta de qué tan importante es para ellos proteger su privacidad. En vista de esto, es necesario analizar qué es lo que genera los malos hábitos de protección.

1.5.4.2. Conciencia e intereses

En primer lugar, para entender la apreciación y el manejo de los estudiantes de su información, es importante distinguir entre la información confidencial, por ejemplo la que maneja la Universidad, y la privada, es decir, información personal que incluye intereses, gustos, opiniones. Hay puntos en las cuales ambas se solapan o coinciden, sin embargo el manejo de ambas es realizado de manera diferente.

> Cuando hablamos de lo privado es lo que está en el círculo interno de una persona, porque lo confidencial un poco parecería

> lo mismo. Lo confidencial es un poco más generoso el término, menos estricto, […] Confidencial de una empresa por ejemplo, su lista de clientes es confidencial, […] Pero ya las apetencias sexuales de una persona o su historial médico, eso entra en el ámbito privado e íntimo (Pazmiño, A. comunicación personal, 2016).

Pazmiño concluye que la confidencialidad se centra más bien en el manejo de la información de índole institucional. Si bien se encuentra PII dentro de la información confidencial, que permite identificar a una persona, la privacidad se encuentra más ligada hacia lo personal, que puede afectar a la intimidad y autonomía del individuo.

Como se explicó anteriormente, los estudiantes tienen conciencia acerca de los riesgos que corren al exponer su información privada en Internet. Cada uno conoce ciertos métodos de protección o herramientas que los ayudan a sentirse seguros dentro de Internet, sin embargo, no todos conocen métodos adecuados o de forma completa y tienen confusiones en ciertas técnicas y nociones, al igual que el uso inadecuado y el abuso de información que se brinda en ciertos dispositivos y medios.

Esta situación se ve en parte influenciada por los intereses de los estudiantes. Por ejemplo de entretenimiento e interacción social en redes sociales o por cuestiones de conveniencia. En el grupo focal se concluyó que en los teléfonos se mantienen varias cuentas abiertas por que es más fácil el manejo de las mismas y el acceso a la información de esa manera. Además, las cuentas muchas veces son vinculadas de manera predeterminada. También, a algunos no les interesaba leer términos y cláusulas de condiciones y uso, debido a que son muy largos.

Respecto a la Universidad y por cuestiones institucionales, los estudiantes consideran que el sistema de Red e Intranet es seguro, pero lento. Además, consideran que es de importancia proteger sus trabajos, por ejemplo al enviarlos o al subirlos a Internet, por correo o por redes sociales.

En cuanto al correo de la Universidad se opina que es muy poco revisado y utilizado, puesto que se tiene la percepción que es lento, no permite subir o enviar algunos archivos y tiene poco espacio en la nube, sin embargo según el ingeniero Zapata, es un correo sumamente seguro y tiene un terabyte (1000 gigas) de espacio en la nube para almacenar archivos.

Concluyendo, los usuarios de Internet de la Universidad Católica tienen conciencia de protección de información privada en la Red, sin embargo surge con reiterada presencia una deficiencia en el conocimiento y uso de técnicas y herramientas para realizarlo, al igual que un desconocimiento en la parte legislativa y por tanto de sus derechos.

1.5.5. Conclusión de la investigación

Al realizar un análisis del uso de Internet y del manejo de información por parte de los estudiantes dentro de la PUCE y en correspondencia con la situación del país y de la institución, en cuanto a derechos de privacidad y el desarrollo de una cultura de protección de información personal, se identificó una serie de aspectos que limitan la adopción de medidas adecuadas que preserven la privacidad del individuo de manera efectiva.

Cabe destacar que existe conciencia de protección de información privada en la Red en los usuarios de Internet de la Universidad Católica. Aun así, cada estudiante se protege de maneras que ha conocido mediante la experiencia o su aprendizaje personal, en varias ocasiones sin entender de manera precisa cómo se maneja la información que comparte y que busca proteger.

Se cuenta con una deficiencia en el conocimiento y uso de técnicas y herramientas para el resguardo adecuado de la información privada. Esto se debe en parte a un desconocimiento de los derechos y en la parte legislativa, lo que provoca que los estudiantes no exijan la preservación de los mismos. Además se debe a una cultura de protección poco desarrollada a nivel nacional, por lo que los usuarios de Internet no reciben suficiente información o por los medios adecuados que les ayude a defenderse mejor de amenazas en la Red.

Se ha visto que los estudiantes de la PUCE, posiblemente de la misma manera que sucede con estudiantes de otras universidades, han sido víctimas de diversos ataques informáticos, a pesar de ello, no se dispone de una herramienta ágil de diseño informativo e interactivo para la protección de datos privados.

Se genera un vacío en el entendimiento del manejo de información personal y privada en medios digitales y por lo tanto, de técnicas y herramientas que faciliten la protección de los estudiantes no solamente dentro de la Universidad, sino también en otros contextos y entornos tecnológicos.

A más de lo señalado, la investigación arroja el dato que la mayoría de los estudiantes de la PUCE usan el teléfono celular, inteligente o no para ingresar a las diversas herramientas electrónicas, haciendo más factible la vulneración de la privacidad individual y colectiva.

Por lo dicho, para preservar el derecho a la privacidad se ha visto la necesidad de promover en la Institución una herramienta que se sirva del Diseño Centrado en el Usuario (DCU), para generar un producto informativo e interactivo con características de gamificación.

Capítulo 2

SEGUNDO COMPONENTE: DISEÑO

Por otro lado, en el campo del diseño fueron orientadoras las ideas consignadas en el libro de Diseño Interactivo, Teoría y aplicación del DCU, de Pratt y Nunes (2013), que habla acerca del Diseño Centrado en el Usuario (DCU). De esta fuente se obtuvo parte del enfoque teórico-metodológico central para el desarrollo del proyecto.

Es un enfoque de diseño que se centra en el usuario de un producto o una aplicación para crear un determinado producto digital. El DCU implica que el diseñador estudie a fondo las necesidades, los deseos y las limitaciones del público objetivo al que va dirigido el producto final, y a partir de ese análisis toma las decisiones que procedan para confeccionar su creación. (Pratt, Nunez, p. 12).

Complementariamente, se tomaron en cuenta metodologías basadas principalmente en el diseño interactivo, que según Steane (2016), abarca sistemas y entornos complejos e inmersivos en la creación de productos de índole digital.

En ellas se detallan puntos de análisis del escenario y toma de decisiones para la generación del diseño y realización de prototipos, planteados en los libros ‘Fundamentos del Diseño Interactivo’ (Steane, 2016) y ‘Diseño de Interfaces’ (Wood, 2015).

Se presenta a continuación una tabla en la que se expone la metodología desarrollada a partir de los modelos planteados por los autores expuestos previamente.

Etapa	Proyecto
Investigación de Usuario	- Análisis de las necesidades y entorno del usuario
Definición de usuario y objeto de diseño	- Usuario y entorno - Requerimientos de usuario - Requerimientos de diseño
Definición de concepto de diseño	- Definición - Aplicación en vectores de la forma
Definición de contenido y generación de propuestas	- Contenido del objeto de diseño y su relación con el usuario.
Usabilidad y navegabilidad	- Definición de organización e interacciones - Arquitectura de la información Mapa de navegación Wireframes
Prototipo	- Principios de diseño Navegación Maquetación y retícula Ergonomía (hablar de botones) Tipografía Color Imagen Iconografía lustraciones - Definición de elementos formales - Definición de elementos dramáticos - Detalles constructivos - Costos de producción
Análisis heurístico y validación profesional	- Teórica - Comitente
Retroalimentación de usuario	- Prueba de usabilidad

Tabla 2: Metodología para el desarrollo de los componentes del proyecto de Diseño.

Elaboración: Autor.

Durante la etapa previa se identificó -a manera de diagnóstico- una deficiencia en el manejo de información privada en Internet por parte de los estudiantes de la PUCE, que se debe en gran medida a la falta de conocimiento acerca de los riesgos, amenazas y medidas de protección adecuadas, en el medio digital.

Habiendo finalizado la etapa investigativa, se procedió al siguiente segmento dentro de la metodología propuesta de diseño, basada en el DCU y en el diseño interactivo, en la cual se analizaron los requerimientos de usuario y de diseño para plantear un producto que se ajuste al medio en el que se desenvuelve el estudiante y ayude a la disminución del problema encontrado.

2.1. Planteamiento del proyecto en función del problema

En vista del manejo inadecuado de la información privada del usuario en la red, junto a los malos hábitos de protección en el contexto universitario, se encontró la importancia de generar un producto de diseño que conste de tres objetivos en términos de forma y funcionalidad.

El primero de ellos fue informar a los estudiantes acerca de las principales amenazas encontradas y métodos que permitan tomar medidas de protección y precautelares. Esto buscó ser realizado mediante la transmisión de las ideas y conceptos relacionados con la protección de información privada en Internet, de manera lúdica e interactiva, que permita una fácil asimilación de la información brindada.

Al relacionar la información con un sistema gamificado, es posible “motivar jugadores a interrogar y conciliar sus propios modelos del mundo, con modelos presentados en un juego” (Fullerton, 2008, p.57)

El segundo objetivo fue el de brindar herramientas que puedan ser utilizadas por los estudiantes de manera práctica en la cotidianidad, las cuales debían ir relacionadas a los problemas más comunes encontrados en campos del primer componente. Es decir, el conocimiento acerca del manejo de datos y los hábitos de protección.

Por último, se buscó generar interés y motivación para aprender más acerca de la privacidad como un derecho, por medio de la apropiación del producto generado. Para lograrlo, se entendió el producto como parte de una experiencia, en la que el aprendizaje se genera mediante la forma en la que los usuarios experimentan un producto interactivo, en vez de evaluar el producto por qué tan útil o productivo es, como lo plantea Preece et. al (Preece, Rogers & Sharp, 2002, p. 19).

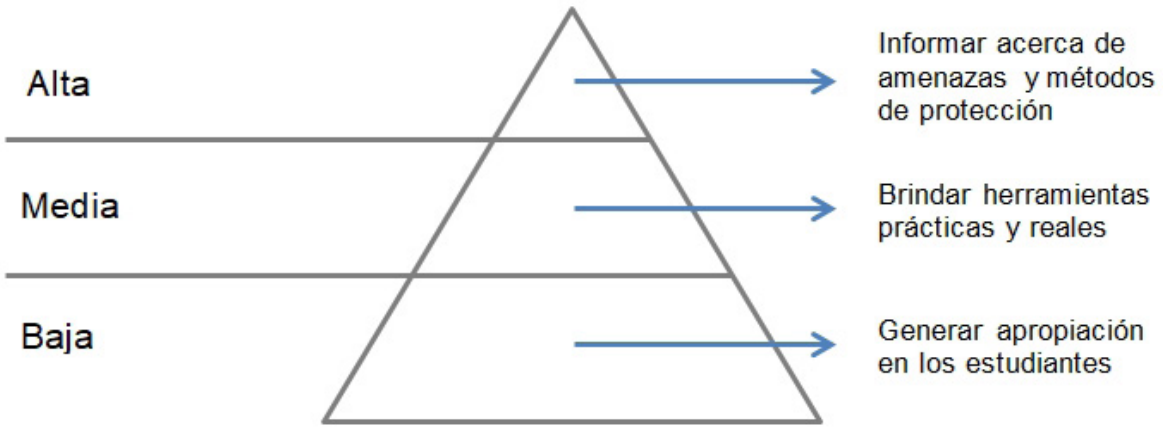


Figura 4: Pirámide de prioridades

Fuente: (Pratt & Nunez, Diseño Interactivo: Teoría y aplicación del DCU, 2013, p. 37).

2.1.1. Análisis del escenario

En base a las determinantes generales de forma y funcionalidad planteadas anteriormente, fue necesario analizar la relación entre usuario y entorno en el que el producto tuvo cabida. De esta manera fue posible plantear un producto accesible al estudiante y determinar las cualidades más específicas del mismo.

2.1.1.1. Mapa de públicos

En primer lugar se realizó un mapa tipológico de públicos, con la finalidad de establecer el alcance del proyecto y determinar el medio más eficaz para implementar el producto, así como definir los campos de acción del diseño y el medio utilizado para llevar a cabo los objetivos del producto. Se identificó los públicos, internos y externos, que podrían potencialmente tomar participación dentro del proyecto.

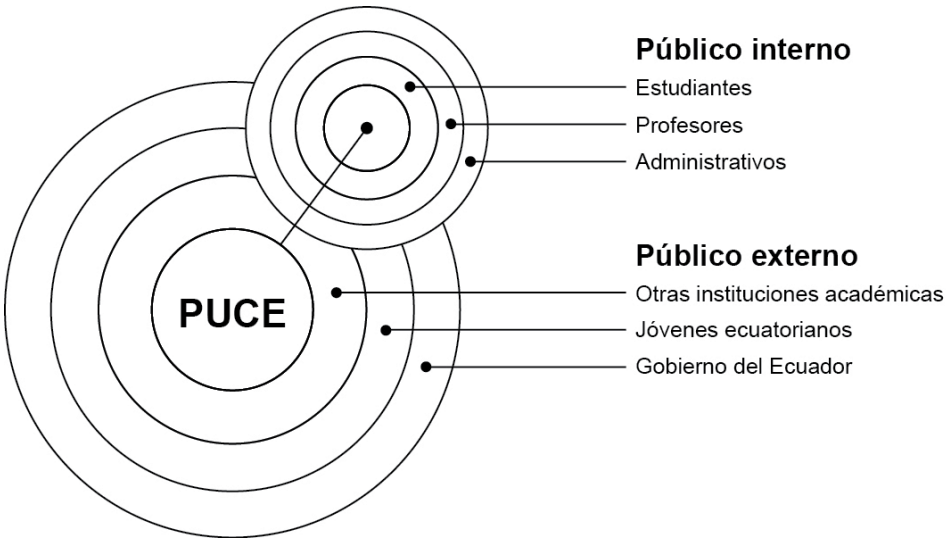


Figura 5: Mapa tipológico de públicos.

Fuente: (Costa, El DirCom hoy, Dirección y Gestión de la Comunicación en la nueva economía, 2014, pág. 109)

El responsable del proyecto, es decir la Pontificia Universidad Católica del Ecuador, con sus distintos componentes, consta como el público interno. La Institución toma parte importante dentro del manejo de información privada en los estudiantes, como intermediario entre el usuario y el acceso a Internet en plataformas digitales. Como ya se ha mencionado anteriormente utiliza métodos de protección seguros y fuertes en contra de diversos tipos de ciberataques y amenazas en la red, que podrían vulnerar la privacidad de los estudiantes.

La información personal se maneja con mucha cautela y de forma seria y responsable bajo políticas desarrollada por la misma institución. La PUCE busca demostrar excelencia y confianza en este ámbito, además de incentivar a los estudiantes a formar parte de la Red de la Universidad. En este contexto se ven involucrados estudiantes, profesores y personal administrativo.

El usuario principal, dentro del público interno, consiste en estudiantes que forman parte de la comunidad universitaria de la PUCE. En su mayoría jóvenes con malos hábitos de protección de su información privada en Internet y con poca conciencia de las amenazas a las que se ven expuestos en el momento de compartir ciertos datos en línea.

Por otro lado, como se puede observar en el gráfico, la Institución consta dentro de un sistema externo más grande. Dentro del público externo se tomó en cuenta públicos distintos, pero que comparten características similares en cuanto al entorno y por ende, pueden salir beneficiados con el producto de diseño propuesto. Este es el caso de otras instituciones educativas o de jóvenes independientes para los que el producto de diseño podría funcionar de igual manera, aunque no con la misma eficacia.

Igualmente al ser una propuesta que trabaja en distintos ámbitos de protección, como la información transmitida y una herramienta funcional y práctica, podría ser adaptada por el Gobierno del Ecuador para mejorar la protección de información privada en distintos contextos.

Entonces, tomando en cuenta los diferentes públicos internos y externos, se definió el campo de acción del producto como un medio digital, debido a su capacidad de rápida difusión y versatilidad de interacción con públicos similares.

2.1.1.1. Análisis FODA

A continuación, se realizó un análisis de las fortalezas, debilidades, amenazas y oportunidades (FODA), de los hechos que conforman la realidad estudiantil en cuanto a la protección de su privacidad. Esto sirvió para determinar el medio digital más adecuado para la implementación del producto. Para el análisis FODA se utilizó el formato propuesto por Andrés Aljure (2015), contemplado dentro del plan estratégico de comunicación: método y recomendaciones prácticas para su elaboración.

Hecho, circunstancia o situación relevante	Consecuencia	Amenaza u oportunidad	Impacto para la PUCE)	Plazo de impacto
Los estudiantes cuentan con una conciencia de protección, sin embargo no cuentan con suficiente conocimiento para protegerse adecuadamente	Los estudiantes se protegen parcialmente	Oportunidad	Medio	Medio
Los estudiantes conocen algunas herramientas de protección de información, pero en algunos casos se dan malentendidos en cuanto a su funcionalidad	Los estudiantes no saben cómo protegerse de forma eficaz	Oportunidad	Medio	Largo
Se dan varios intentos de violar el derecho a la privacidad en Red hacia los estudiantes por parte de agentes externos.	La integridad del estudiante se ve expuesta	Amenaza	Medio	Corto
Un gran número de estudiantes se conecta a la Red universitaria diariamente y con varios dispositivos	La protección se debilita si el estudiante no conoce métodos adecuados de protección	Amenaza	Medio	Corto

Tabla 3: Amenazas y Oportunidades.

Elaboración: Autor.

Hecho, circunstancia o situación relevante	Consecuencia	Debilidad o fortaleza	Impacto para la PUCE	Plazo de impacto
La Universidad cuenta con un sistema confiable ante amenazas cibernéticas en sus sistemas de transmisión de información	Los estudiantes no han sufrido amenazas severas en la red (pero es importante tomar en cuenta que los estudiantes no conocen aquellos sistemas)	Fortaleza	Alto	Corto
La Institución cuenta con políticas y normativas desarrolladas en base a estándares internacionales	Se implementa un buen manejo de información a nivel institucional y de Red	Fortaleza	Alto	Corto
Los estudiantes no conocen ciertas amenazas ni repercusiones de brindar su información en la Red	Los estudiantes no se protegen de manera adecuada	Debilidad	Medio	Medio
No se ha realizado difusión de información en cuanto a temas de privacidad.	No se genera el conocimiento deseado en los estudiantes.	Debilidad	Medio	Largo
La información en el contexto del país, tampoco se maneja de manera adecuada y no cuenta con métodos de recuperación, ni normativas adecuadas a la realidad ecuatoriana.	Los habitantes no exigen que se respete su derecho a la privacidad en la Internet	Debilidad	Medio	Largo

Tabla 4: Fortalezas y Debilidades.

Elaboración: Autor.

Mediante la observación del análisis FODA, se definió ciertos aspectos de la problemática, dentro del nivel más alto de la pirámide de prioridades -como la falta de conocimiento por parte de los estudiantes en cuanto a privacidad- como una oportunidad de acción de diseño dentro de la Universidad.

Mientras tanto, es importante recalcar el gran número de usuarios conectados a la red universitaria durante las horas pico de uso, especialmente, mediante teléfonos inteligentes, al ser aparatos más portables y los más utilizados para navegar en Internet dentro de la Institución. Esto fue considerado una amenaza, a pesar que dentro de la PUCE se utilice sistemas confiables de protección y transmisión de datos, debido a que una vulneración de la información privada por este medio puede impactar de igual manera en la vida personal y profesional de los estudiantes.

Finalmente, tomando en cuenta que, dentro del medio digital y el entorno de la PUCE los teléfonos celulares son las plataformas más vulnerables y de uso más recurrente, fue importante plantear un producto ideado para aquel medio, que permita cumplir, asimismo, con los otros niveles de la pirámide de prioridades. Además, se determinó a Android como el sistema operativo sobre el cual se trabajó, siendo, según Gartner, el más dominante del mercado (Costello & Cornella, 2018).

2.1.2. Definición del proyecto

Habiendo definido las prioridades del proyecto, el campo de acción y la plataforma sobre la que se iba a implementar para el contexto universitario, se pudo generar una descripción adecuada para el producto, sobre la cual posteriormente se definió una funcionalidad y recursos adecuados en base a la metodología de diseño planteada.

El producto consiste en una APP para teléfonos inteligentes con el sistema operativo Android, a la que se puede tener acceso inmediato mediante una cuenta segura y cuyo objetivo es informativo, a la vez que se presenta como una herramienta práctica de protección de información privada.

Expone las principales amenazas a las que un estudiante se encuentra expuesto en el contexto de la PUCE y los métodos de protección que puede adoptar ante ellas. Esto se realiza de manera interactiva, lúdica y gamificada, mediante una serie de mini juegos informativos, asociados a distintos temas de privacidad en Internet.

La APP y los mini juegos funcionan dentro de un solo sistema, generando un diseño de experiencia de usuario, en el que el estudiante puede apropiarse de un ‘avatar’ para cumplir los distintos objetivos dentro de los juegos y a la vez puede desbloquear, obtener y compartir logros y objetos, así como herramientas prácticas para el mundo real.

Además, integra métodos e instrumentos de protección que atienden a la necesidad de brindar mayor información y de organizar cuentas y contraseñas de manera segura y fácil. Igualmente incluye notificaciones personalizadas que brindar ‘tips’ o consejos de seguridad periódicamente. Esto cual atiende al segundo nivel de prioridades.

Finalmente y para generar un sentimiento de familiaridad y apropiación adicional en el estudiante, se utiliza recursos de la misma Universidad, como entornos reales existentes en la Institución, que se implementan en las dinámicas de los juegos y de la misma aplicación.

Este planteamiento partió de Benford et al. (2009), como se cita por Benyon, que explica el concepto de las trayectorias de interacción:

> Una trayectoria describe un viaje a través de una experiencia de usuario, enfatizando su total continuidad y coherencia. Las trayectorias pasan a través de diferentes estructuras híbridas. Múltiples espacios físicos y virtuales pueden ser adyacentes, estar conectados y sobrepuestos para crear un espacio híbrido que provea el escenario para la experiencia. (Benyon, 2013, p.101)

Por último, el proyecto se encuentra, además, entre el nivel adecuado de protección y la generación de hábitos y conciencia en el usuario, generando una introducción a los métodos de protección de la privacidad, riesgos e implicaciones, por medio del juego y la interactividad.

Fig.6: Esquema de funcionamiento del proyecto.

Elaboración: Autor.

De esta manera, la solución de diseño toma un papel más integral y se complementa por medio de distintas herramientas con cualidades diferentes que potencian distintas capacidades e interacciones, pues “el diseño de experiencia es acerca de reconocer que los productos y servicios interactivos no solamente existen en el mundo, sino afectan quienes somos. Influencian nuestra cultura e identidad” (Benyon, 2013, p. 99).

2.2. Requerimientos de usuario y de diseño

A continuación fue importante analizar los requerimientos de diseño del objeto en base a las necesidades del usuario. Éstos fueron generados para entender a detalle el funcionamiento del producto, definir su contenido y forma, así como la composición, funciones, entre otros, tomando en cuenta los objetivos planteados anteriormente. Fueron determinados y clasificados en los distintos vectores de la forma, que permiten contemplar de manera completa las facetas y etapas del producto de diseño, presentados en el libro ‘Diseño, Estrategia y Táctica’ de Luis Rodríguez Morales (2004).

Vectores de la forma		Requisitos	Herramientas sugeridas
Función	Ergonomía	Arquitectura de la información clara y simple. GUI intuitiva para navegación. Buena accesibilidad a distintas funciones. Tamaño de elementos adecuado para una buena interacción.	Mapa de interfaz, navegación y flujo de tareas. Uso de medidas adaptables y estándares ergonómicos. Pruebas de usabilidad.
	Mecanismos	GUI post-wimp Interacción táctil y sonora	Medios digitales Botones y targets amigables (considerar zona del pulgar). Google material design
Expresión	Perceptual	Generar placer psicológico e ideológico Familiar y amigable Confiable Divertido	Historia Objetivos de juego Reglas Escenarios ya existentes dentro de la universidad
	Simbólico	Informal, lúdico pero organizado y sistemático Contraste entre misterio y confianza	Ilustraciones simples (flat illustration) Iconografía simple Colores planos Colores de la Universidad Formas simples y geométricas.
Tecnología	Materiales	Medios digitales	Programas de Adobe para generar un prototipo
	Procesos	Ilustraciones digitales Programación Pruebas de usabilidad.	Bocetos, digitalización Simuladores
	Costos	Accesible para la Institución	Cálculo de costos de producción
Comercial	Expectativas del usuario	Que sea llamativo, lúdico, divertido y les ayude a protegerse mejor	Interacciones en teléfonos celulares
	Ventas / Distribución	Dentro de la universidad	Recomendación de descarga, video y afiches

Tabla 5: Requerimientos de Diseño.

Elaboración: Autor.

2.3. Concepto de diseño

Después de haber definido los requerimientos de diseño en base a las necesidades de usuario, se desarrolló un concepto que permita dar forma al proyecto y generar una secuencialidad entre las diferentes etapas y secciones de la aplicación.

> El concepto de diseño es una descripción aproximada de la forma tecnológica, funcional y estética del producto en desarrollo. Usando bocetos, maquetas y descripciones, el diseñador crea una explicación concisa de las maneras en que el producto satisfará las necesidades del comprador. (Rodgers, Milton, 2013, p.78)

El concepto de diseño funciona como una especie de vínculo que existe entre los diferentes vectores de la forma y la intención del producto para resolver un problema, tomando en cuenta el contexto y las necesidades e intereses de un usuario determinado. Se puede basar en las características del producto, sean intangibles o físicas y puede recurrir al uso de metáforas para la configuración formal.

Para el caso del concepto de diseño dentro del proyecto de protección de información privada en Internet en los estudiantes de la PUCE, se buscó la generación de metáforas y analogías para llegar a un concepto de diseño que describa al producto planteado. Éste consiste en una aplicación lúdica telefónica que sirve para prevenir, informar y brindar herramientas y técnicas de protección al usuario de la Red.

Mediante el análisis de la información recabada dentro la investigación, se analizó aspectos importantes, debilidades y fortalezas del manejo de la información por parte de los estudiantes. Así, se llegó a la conclusión que

la información puede llegar a ser frágil y transparente, verse fácilmente vulnerada, si no se es lo suficientemente cuidadoso. Por esta razón fue importante generar un producto que pueda impactar e informar de manera instantánea y entretenida al usuario y que sirva como un sistema de recompensas que motive al estudiante a entender mejor su privacidad y que esté a disposición en cualquier momento.

En vista que los jóvenes en la actualidad son individuos tecnológicos y en base a la información que se brinda en Internet, se puede crear un perfil de usuario detallado y encontrar datos acerca de la identidad de las personas, cuentas, intereses, en definitiva sombras digitales, se utilizó la metáfora de un agente que proteja la información personal sensible y la privacidad del estudiante -a manera de un representante virtual de la seguridad en medios digitales- puesto que la información que se brinda en Internet, se puede ver sujeta a amenazas similares al mundo real.

Un agente que busca proteger algo es relacionado a menudo con libros, películas, videojuegos y estereotipos de agentes secretos o especiales, que pueden llegar a ser incluso algo lúdico y novelístico. Además, en el caso de la PUCE, un agente puede ser relacionado con un representante físico de la seguridad, como es el caso de los guardias o incluso los encargados de mantener la seguridad en los sistemas de la Institución y en su manejo de información, como los profesionales en redes y oficiales de seguridad.

Por esta razón el producto es presentado como un medio de acceso a la información portable y presentado en forma de actividades lúdicas como un videojuego que cuente con una historia, personajes, escenarios y dinámicas educativas y entretenidas. Sin embargo, no solamente debe ser un espacio de interacciones de juego y ocio, pero también es importante considerar que debe ser un espacio donde encontrar y almacenar cierta información, como

guías de uso, precauciones y contraseñas, similar a las medidas que toma un agente de seguridad.

Finalmente, se llegó al concepto de diseño, mediante el cual se realizó la configuración formal de la aplicación. El producto utiliza el concepto de un agente de seguridad.

A continuación se muestra un cuadro en el que se enfrenta cada requisito de diseño, junto a la manera en la que será implementado en la aplicación por medio del concepto de diseño.

Requerimiento formal del proyecto en relación al problema identificado.	Concepto de diseño aplicado a la etapa del proyecto.	Propuesta de diseño, descripción verbal de lo que se va a desarrollar.
GUI intuitivo Adaptabilidad AI simple	AI ser un agente de seguridad, es importante no dejar cabos sueltos en la información que se brinda, por lo que se relaciona la AI hacia un personaje con herramientas como una guía extra, elementos de protección, avisos y notificaciones acerca de privacidad y manejo de contraseñas adecuado.	Desde el ingreso al sistema interactivo, será necesario entrar con doble autenticación. El personaje es customizable y tendrá consigo herramientas (aparte de las acciones que pueda realizar en los juegos), como una guía de amenazas y formas de protección y un gestor de sus cuentas y contraseñas. A parte, se podrá entrar en el sistema a distintos desafíos encontrados en forma de mini juegos, logros y una tienda por medio de un menú principal.
Usabilidad e interactividad relacionada hacia el juego mediante interacción táctil	El agente de seguridad debe realizar distintas actividades de protección en relación a las amenazas existentes y ser precavido en su manejo de la información, lo que se ve reflejado de manera interactiva mediante el juego de ser un agente y realizar esas actividades.	El agente o personaje debe pasar por distintos desafíos y retos para llegar hasta cierto objetivo que se cuenta dentro de la historia. Para llegar a ese punto, necesita aprender y completar los desafíos ganando recompensas monetarias que se podrán utilizar dentro del mismo juego para comprar objetos alternativos. Cada desafío atiende a un tema principal dentro de la seguridad de información.
El usuario debe sentirse familiarizado e identificado con la interfaz y esto se vea contrastado con lo sombrío y desconocido.	AI ser el agente el protagonista y personaje customizable se genera apropiación y confianza en el usuario. Se interviene con escenarios conocidos, manipulados de alguna manera desconocida.	En la historia que se cuenta, el personaje deberá ir avanzando por diferentes etapas o escenarios dentro de la misma Universidad, hasta llegar al nivel final. De esta manera se juega con entornos conocidos en los que desenvolverse. En cada escenario deberá realizar una actividad de protección o precaución.
Generar placer ideológico y psicológico y social por medio del juego.	A medida que el agente protege y evoluciona, va cumpliendo sus ideales y protegiendo los derechos de mejor manera.	Se genera un sistema de recompensas en los que el personaje recibe cibermonedas y beneficios para poder customizar el mismo personaje de maneras diferentes, avanzar de nivel y obtener beneficios en la vida real, incluyendo un premio final al completar los logros del personaje. Los logros y status del personaje pueden ser compartidos mediante redes sociales.
Portable como medio digital en teléfono. Retroalimentativo.	AI ser un agente de seguridad que protege la privacidad en medios digitales, debe proteger y acompañar en todo momento.	No necesita de conexión a red, excepto para realizar algunas actividades dentro de las bonificaciones, como el compartir los logros. Se envían notificaciones periódicas para proteger mejor la información privada.
Configuración formal, de maquetación, tipografía, color, iconografía adecuada para el estudiante en medio digital, tomando en cuenta el valor simbólico de lo misterioso frente a lo confiable.	Un agente se encuentra siempre expuesto a peligros, sin embargo debe brindar confianza al usuario.	Contrastes de color, en colores planos, ilustraciones simples de formas básicas. Tipografía sans-serif para apoyo en legibilidad y acorde a la línea gráfica. Iconografía que apoye a la información brindada.

Tabla 6: Concepto de Diseño.

Elaboración: Autor.

2.4. Desarrollo del diseño

En esta etapa se describe de manera detallada la generación de la propuesta de diseño, a partir de la organización de las secciones y componentes de la aplicación, describiendo la configuración formal, composición y estética del producto, así como el manejo cromático, tipográfico e iconográfico en el desarrollo de la propuesta gráfica. Es importante tomar en cuenta que la propuesta se encuentra realizada en relación a los requerimientos de diseño y a las necesidades del usuario en consonancia con el concepto.

2.4.1. Arquitectura de la información

El primer paso a realizar, fue el de organizar el contenido y las secciones de la aplicación, que debían atender a la parte informativa y las herramientas prácticas, como un solo sistema de diseño de experiencia, en el que la funcionalidad tiene una secuencia lógica.

Para esto fue necesario pensar una estructura en la que los elementos interactúen entre sí y con el usuario, mediante una navegación que facilite el acceso a los distintos componentes.

Esto se realizó por medio de la arquitectura de la información (AI), que “es la encargada de delimitar la forma que tomará la interfaz gráfica (GUI), a partir de la cual el diseñador y el programador conceptualizan la experiencia de usuario más eficaz y estética” (Wood, 2015, p. 42).

2.4.1.1. Mapa del sitio

Para organizar la información y el contenido de la aplicación, se crearon diferentes secciones de navegación, cada una con sus propios elementos y subsecciones. Para graficar el orden y las interacciones entre cada componente se utilizó un mapa del sitio, como el que se muestra en Steane:

> La elaboración de mapas de sitios es una tarea importante en la creación de sitios web y aplicaciones interactivas, dado que ofrece a los clientes y equipos de diseño y desarrollo una visión de alto nivel de la estructura del contenido, donde se incluyen los sistemas de etiquetado y navegación. (Steane, 2016, p.42)

Como menciona este autor, esta es una aplicación de tipo estático, puesto que los contenidos de cada sección son únicos y no se encuentran en constante cambio o actualización, como por ejemplo, los artículos de periódico en una plataforma digital de noticias.

A continuación se muestra el orden de contenido definido para la APP, con su respectiva numeración, de manera que se facilite el entendimiento de los pasos de navegación que se utilizan al ingresar e interactuar con la GUI.

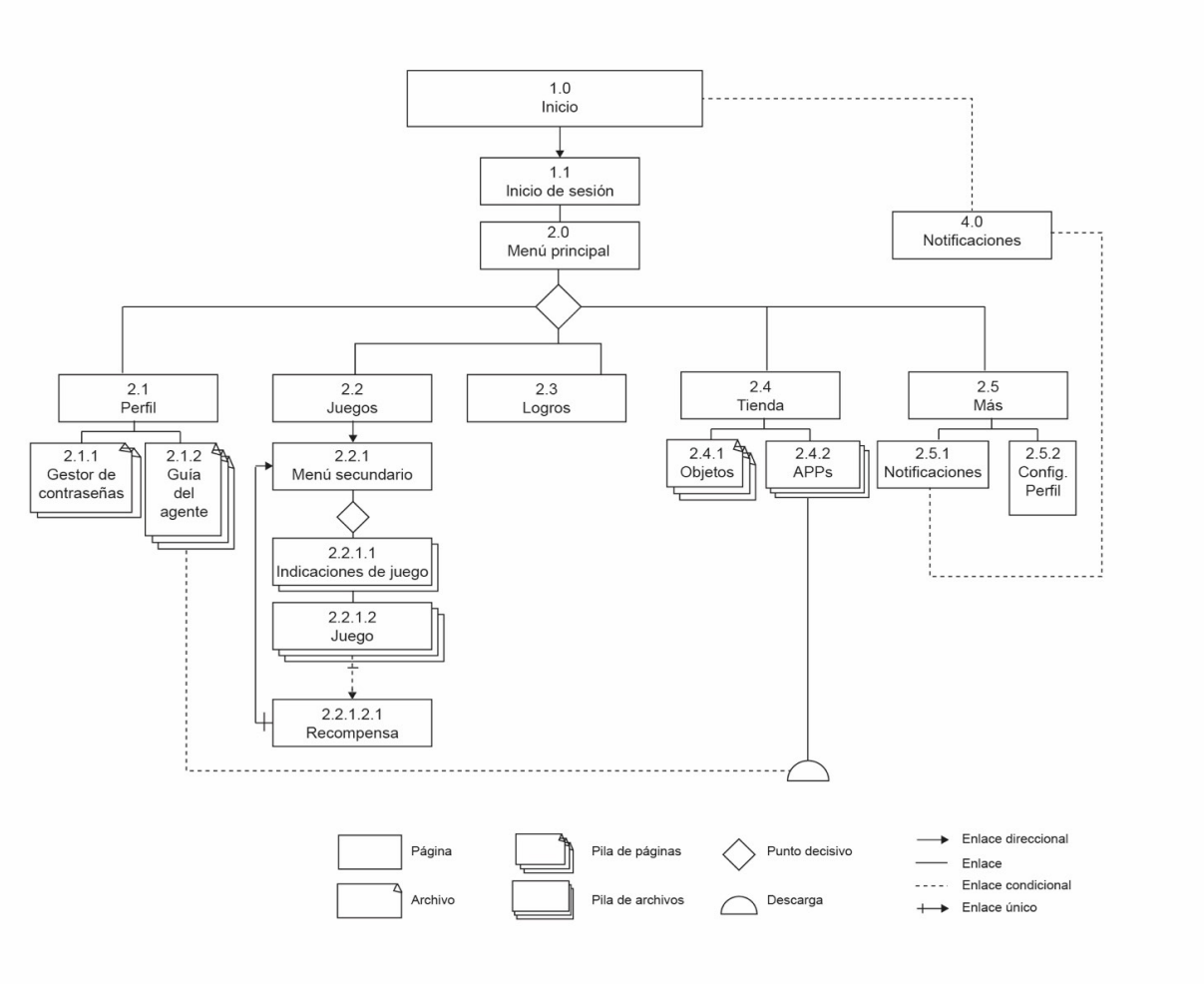


Fig. 7: Mapa de sitio

Elaboración Autor

2.4.1.2. Wireframes

En base a la estructura definida en el paso anterior, se procedió a la utilizar una herramienta muy útil para tener un indicio de la usabilidad, las prioridades de navegación e incluso los componentes estéticos, antes de realizar un prototipo más avanzado del producto. Esto se logra mediante la ubicación espacial de los componentes principales de navegación, como barras, botones, encabezados, entre otros, dentro de pantallas dibujadas a mano que simulan cómo se verán las pantallas posteriormente con los elementos necesarios para entender su funcionamiento.

Esta herramienta son los ‘wireframes’, que se encuentran bocetados a escala real y “revelan la lógica, el comportamiento y la funcionalidad subyacentes a cada pantalla de la interfaz […] se trata de un método para decidir qué elementos deben incluirse, qué parte de la AI” (Wood, 2015, p. 54).

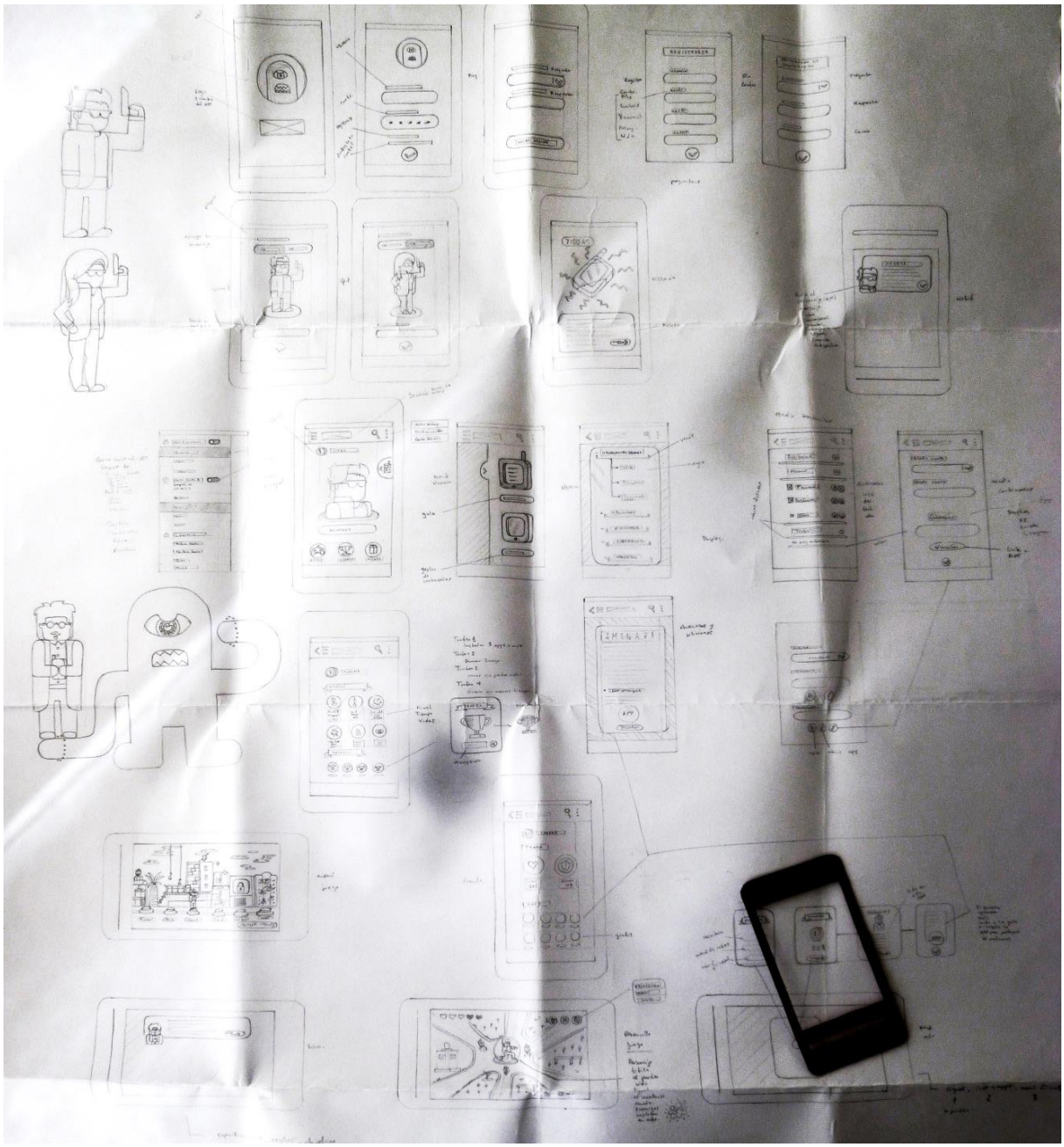


Fig. 8: Wireframes

Elaboración: Autor.

Cabe recalcar que la realización de los ‘wireframes’, fue basada en una primera propuesta del mapa de sitio dentro de la arquitectura de la información. De esta manera, el boceto en papel permitió definir interacciones más directas y optimizar la navegabilidad, que son las del mapa de sitio que se muestra anteriormente, para generar el prototipo final en base a la observación de aquellas relaciones.

La siguiente etapa tratará acerca de la definición de los elementos formales -tanto en la aplicación, como en los mini juegos- como parte del prototipo final, sobre el que finalmente se realizaron las pruebas de usabilidad.

2.5. Principios de diseño

Para entender de manera más clara las características finales del producto, se recurre a los postulados de Benyon (2013), en los que se presenta ciertos principios fundamentales para generar un diseño interactivo desde una perspectiva centrada en el usuario.

A partir de estos principios se analizará ciertos componentes del producto, como parte de una experiencia y que permitirán ir desglosando los detalles del prototipo final en las diferentes facetas de su composición.

Benyon expone doce principios clasificados en tres categorías. La primera consiste en el acceso, la facilidad de aprendizaje y la memoria en relación con la GUI. La segunda hace referencia a la facilidad de uso y la tercera, con la efectividad. Asimismo, se presenta una cuarta categoría aparte, que busca acomodar y respetar las diferencias entre las personas. (Benyon, 2013, p. 89)

A continuación se expone los doce principios, pertenecientes a cada una de las categorías, con una breve explicación de lo que se entiende por cada uno.

Categoría	Principio	Explicación
Acceso	**1. Visibilidad**	Es importante que todos los elementos sean visibles u observables con facilidad, para entender las acciones disponibles del sistema y poder recordarlas.
	2. Consistencia	Las características de diseño conceptuales y físicas deben ser consistentes entre sí y responder a un estándar y sistemas similares.
	3. Familiaridad	Es necesario recurrir a lenguajes, metáforas y símbolos que resulten familiares para el usuario.
	4. Conformidad	Cada elemento debe relacionarse adecuadamente a su función.
Facilidad de uso	**5. Navegación**	La navegación es clara y brinda soportes, como señales y símbolos que permitan al usuario moverse por las secciones del sistema sin complicación.
	6. Control	Es importante generar una percepción de control en el usuario. El control se mejora si hay un mapeo claro y lógico entre los controles y el efecto que tienen.
	7. Retroalimentación	Se debe generar un sistema que retroalimente al usuario, para saber qué efecto tuvieron sus acciones.
Efectividad	**8. Recuperación**	Es importante brindar métodos de recuperación de acciones, como equivocaciones, de forma rápida y efectiva.
	9. Restricciones	Es necesario establecer restricciones para que el usuario no intente o pueda hacer cosas inapropiadas.
Acomodación	**10. Flexibilidad**	Tomar en cuenta múltiples formas de realizar una misma acción, que permitan el manejo de usuarios con diferentes niveles de experiencia. Proporcionar opciones de personalización.
	11. Estilo	Los diseños deben presentarse de manera estética y atractiva para el usuario.
	12. Cordialidad	Es importante asegurarse de generar un sistema amable y amigable en cuanto a las interacciones. Brindar opciones para conectar a grupos de personas.

Tabla 7: Principios de diseño de interacción.

Fuente: (Benyon, Designing Interactive Systems. A comprehensive guide to HCI, Ux and interaction designe, 2013, p. 90)

Para exponer los componentes formales del producto se tomó como línea básica explicativa, los principios planteados anteriormente, sin embargo se los organizó y clasificó en un orden coherente para entender las cualidades del producto como un todo.

2.5.1. Familiaridad

Como se ha mencionado previamente, se tomó como una prioridad de diseño, en este caso, el generar apropiación de la herramienta propuesta como producto en el medio estudiantil. En ese sentido, se generó una serie de metáforas y dinámicas, con las que el usuario pueda sentirse identificado.

Una estrategia utilizada para esto fue el determinar elementos dramáticos para el desarrollo de la experiencia. Es decir, se planteó una historia que sirva como hilo conductor para la aplicación y los mini juegos.

Por otro lado, era importante que los sucesos tomen parte en un entorno conocido para el usuario y de esa manera se refuerce ese sentimiento de pertenencia. Entonces se utilizó lugares existentes dentro de la Universidad para completar los distintos desafíos presentados en los juegos.

2.5.1.1. Definición de elementos dramáticos del juego

2.5.1.1.1. Premisa

La premisa de un juego es una breve explicación de la trama del mismo y "establece la acción del juego en un contexto o metáfora. Sin una premisa dramática, muchos juegos serían demasiado abstractos para que los jugadores pudieran verse conectados emocionalmente con el resultado" (Fullerton, 2008, p. 93)

Premisa: Eres un agente de seguridad que debe luchar contra un monstruo que se alimenta de la información privada de los estudiantes de la PUCE y está aterrorizando la Universidad. Deberás enfrentarte a las diferentes amenazas que el monstruo y sus secuaces han asentado en varios lugares de la Institución, para salvar a los estudiantes de perder su privacidad.

2.5.1.1.2. Personajes

La historia cuenta principalmente con 4 personajes. Dos son 'buenos' y dos 'malos'. El protagonista es el usuario customizable. Sus enemigos son 'Monstruo Sombra' y 'Dr. Data', que parece ser bueno, sin embargo es la verdadera amenaza. Los aliados (secundarios) del protagonista son los 'Oficiales de Seguridad', que informan acerca de las reglas del juego.

> Los personajes son los agentes a través de cuyas acciones se cuenta un drama. Al identificarse con un personaje y el resultado de sus metas, la audiencia internaliza los eventos de la historia y empatiza con sus movimientos hacia la resolución. […] Los personajes también pueden ser simbólicos y luchar por ideales mayores. (Fullerton, 2008, p. 96)

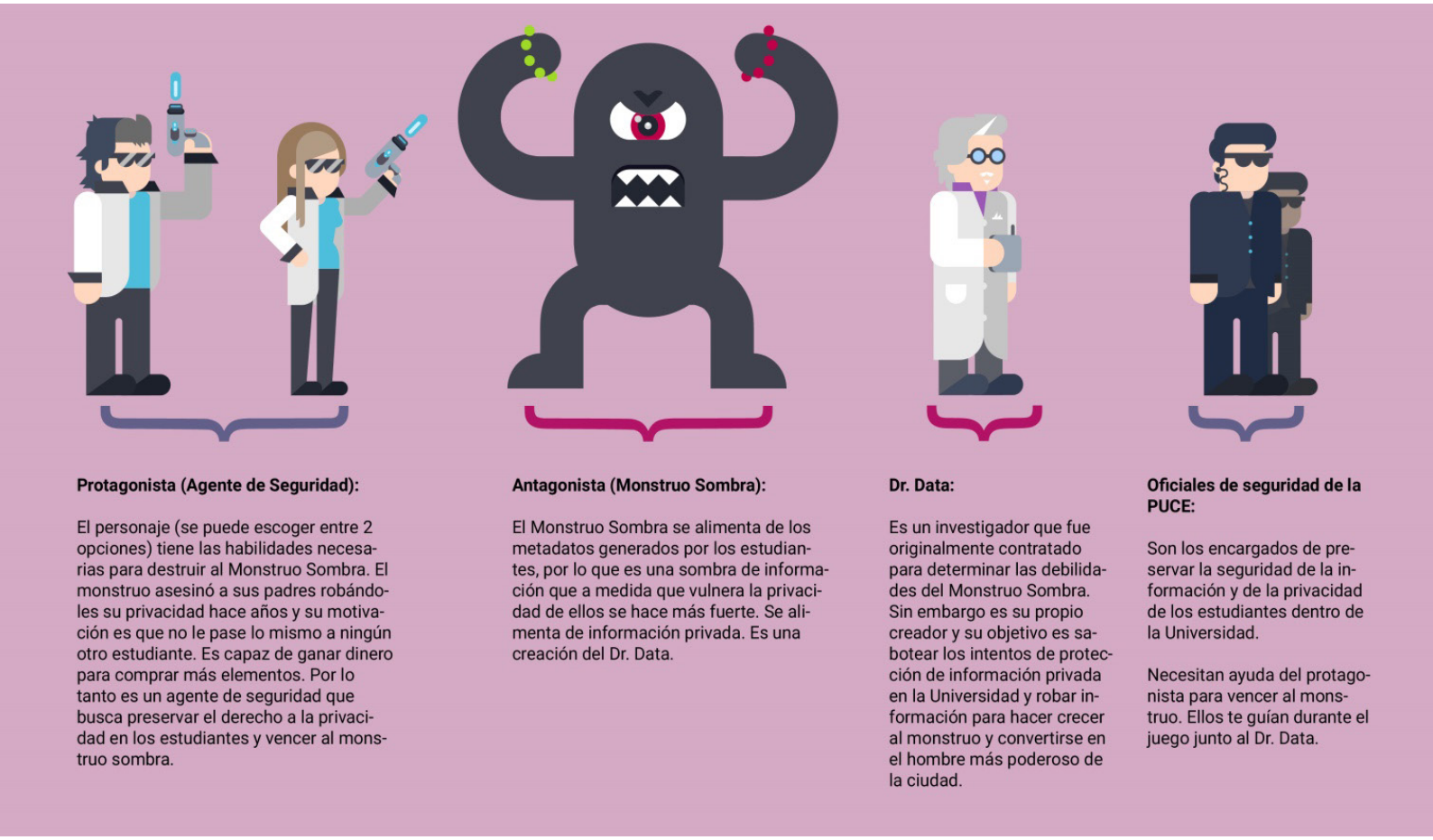


Fig. 9: Personajes.

Elaboración: Autor

2.5.1.1.3. Historia

En los videojuegos la evolución del arco argumental puede tener muchas salidas y giros inesperados y en gran cantidad de ocasiones el mismo protagonista es el que debe descubrir el cierre de la historia sin habérselo anticipado.

Sin embargo, en el caso de la historia planificada para la aplicación gamificada toma cabida otro tipo de narrativa, debido a que el objetivo del producto es más bien informativo y los objetivos son claros desde el principio.

Fullerton lo describe de la siguiente manera:

> La historia da un contexto y entorno para el conflicto del juego y puede crear motivación para los personajes, pero la progresión de un punto al siguiente no se ve afectada por la jugabilidad. Un ejemplo de esto es la tendencia de insertar capítulos de la historia en el principio de cada nivel, creando una progresión linear que sigue un arco narrativo tradicional. (2008, p.100)

Asimismo en el caso de la aplicación planteada, la historia se cuenta como una progresión linear, sobre la que el personaje principal debe seguir avanzando con cierta expectativa hasta el final (la de derrotar al antagonista). Los personajes secundarios son los mismos narradores de los hechos y los que presentan las amenazas ante las cuales el protagonista se enfrente en cada momento.

Historia: Durante la historia, el protagonista –quien ha perdido a sus padres a manos del antagonista- se entera que ha sido llamado por los Oficiales de seguridad para destruir al Monstruo Sombra que ha regresado después de varios años. Se introduce al Dr. Data, investigador contratado para determinar las debilidades del enemigo. Igualmente, se presenta al monstruo y se comenta que se alimenta de metadata y la información privada de los estudiantes. En cada nivel, el protagonista debe ir enfrentando una amenaza distinta relacionada a aquel lugar.

Después de enfrentarse con ‘malwares’, desencriptar información de los estudiantes almacenada de forma ilegal, evitar a los ‘phishers’ y desmantelar un sistema de vigilancia masiva, el Agente de Seguridad se entera que el creador del monstruo es realmente el Dr. Data, quien quiere robar la información de todos los estudiantes para convertirse en el hombre más poderoso de la ciudad. Finalmente, el protagonista enfrenta a los villanos

en su guarida y después de salir vencedor, el Dr. Data es arrestado y el Monstruo Sombra, destruido.

Fig. 10: Historia

Elaboración: Autor.

2.5.2. Estilo y visibilidad

En el diseño interactivo es importante generar un diseño atractivo y sencillo, mediante el cual el usuario pueda seleccionar funciones de manera rápida y eficaz para tomar decisiones dentro de la interfaz. Asimismo se debe encontrar los elementos cromáticos, ilustraciones, tipografías e imágenes adecuadas que permitan comunicar ideas de manera eficiente sin perder el concepto de diseño.

> Según en qué contexto se interpreten una fotografía, ilustración, ícono o composición pueden sugerir varios conceptos distintos. Los elementos visuales diseñados nunca son neutrales y, desde una perspectiva cultural, pueden implicar diferentes significados para las distintas sociedades. (Wood, 2015, p. 120)

Desde este punto de vista se planteó una línea gráfica, uso cromático y tipográfico que favorezca a una rápida transmisión de información tomando en cuenta las características del público objetivo.

2.5.2.1.Ilustraciones

En vista que el diseño consiste en una APP telefónica que busca generar interacciones simples para informar conceptos de seguridad de manera introductoria y por un medio digital, se escogió la ilustración plana o Flat Illustration, debido a que “enfatiza la facilidad de uso […], tiene su origen en los desarrolladores web, quienes trataron de dar realismo a lo que vemos en la pantalla […] y proporciona una ilustración más simplificada, donde los elementos ornamentales son vistos como innecesarios” (Amell, 2015)

Fig. 11: Ilustración plana

Elaboración: Autor.

Se utilizó este tipo de ilustración debido a su simplicidad y pregnancia, como un modo de asociación de los personajes y distintos niveles del juego, hacia diferentes amenazas y métodos de protección e identificación con el medio universitario. Para homologar la línea gráfica fue necesario partir de una malla principal de 8 dp cuadrados, como se explica de manera más detallada en la sección de ‘maquetación’ más adelante.

2.5.2.1.1. Malla de ilustración

En este caso, se tomó la grilla de 8 dp cuadrados como una base, sobre la cual se sitúan elementos más grandes y más pequeños de hasta 2 dp, sin embargo siempre manteniendo una relación numérica par entre el ocho, el cuatro y el dos. A continuación se muestra un ejemplo de esto, en la construcción del personaje principal.

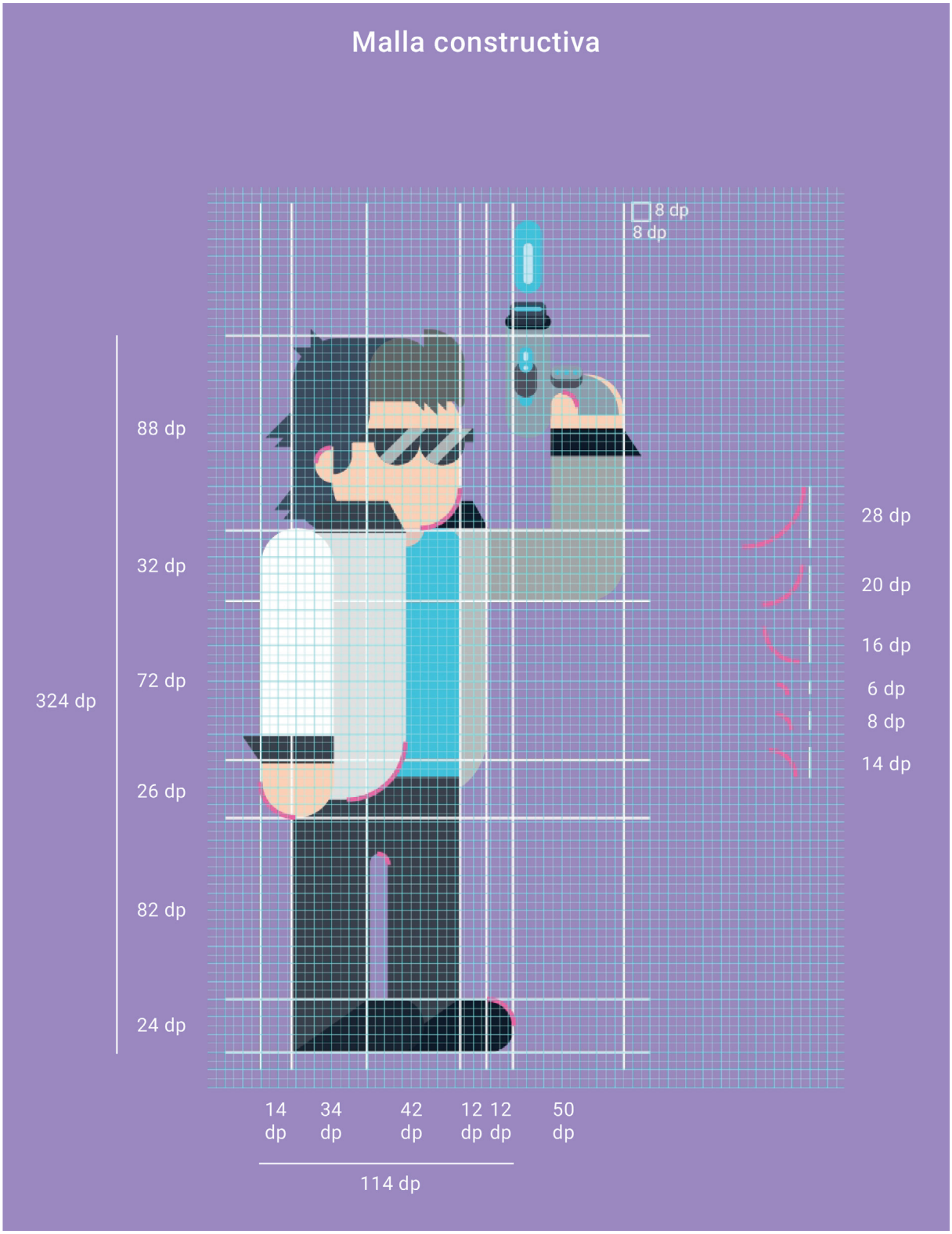


Fig. 12: Malla de ilustración para personajes

Elaboración: Autor.

De igual manera, para la construcción de los escenarios, se manejó la misma base modular. Sin embargo, para la distribución de los elementos en el espacio, incluyendo el tamaño de cada uno, se realizó una grilla de apoyo de 32 dp cuadrados, sobre la cual se hizo la colocación espacial de personajes y objetos. Para los botones y otras funciones se manejó la misma base de 8 dp, respetando un margen de 24 dp en los costados.

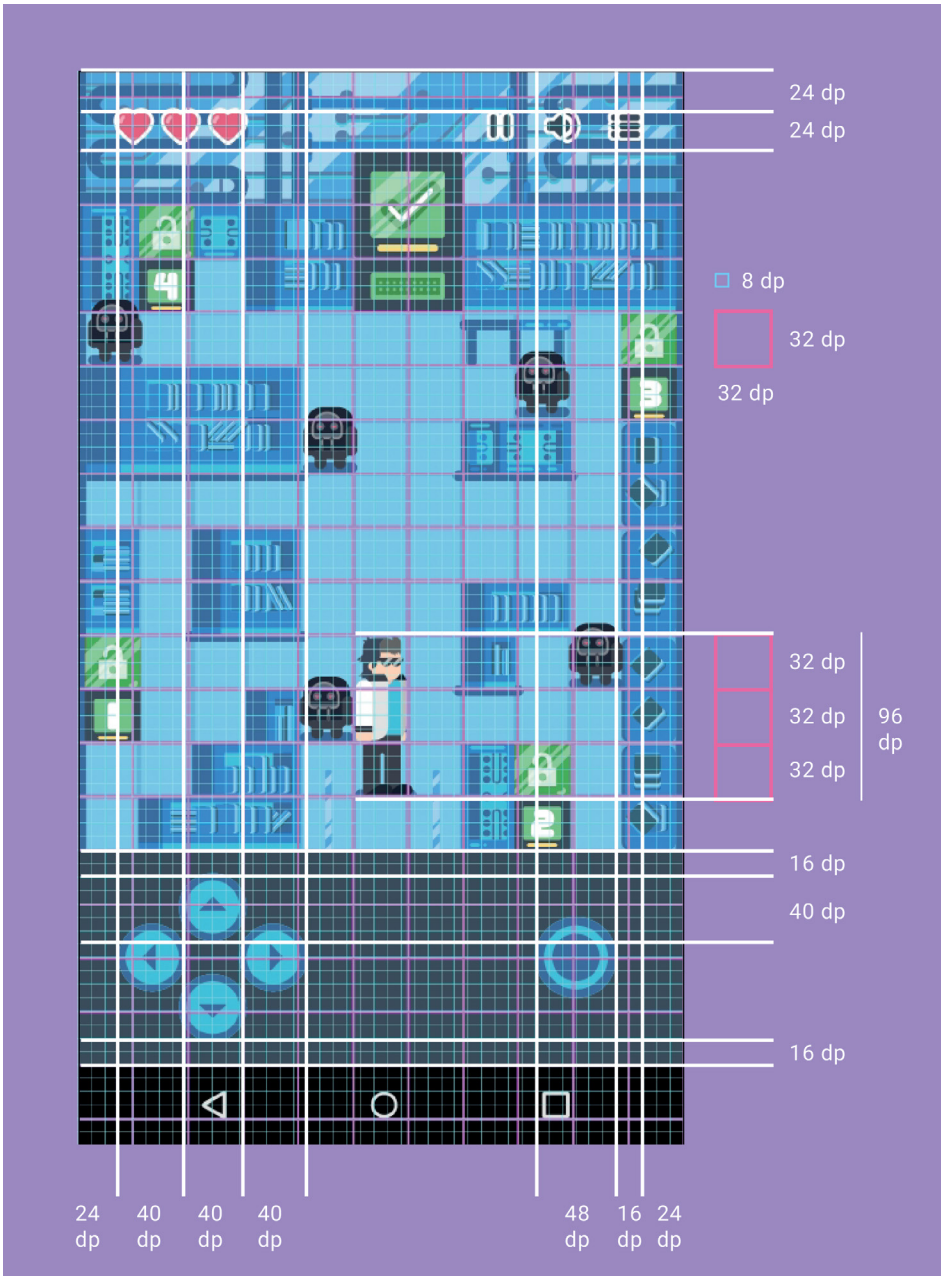


Fig. 13: Malla de ilustración para escenarios

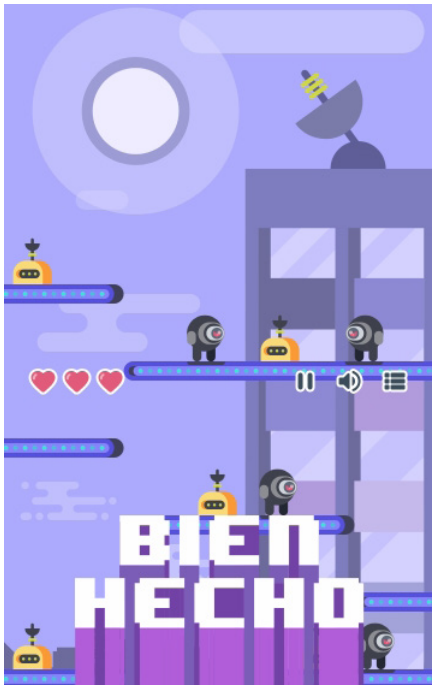
Elaboración: Autor.

2.5.2.2. Cromática

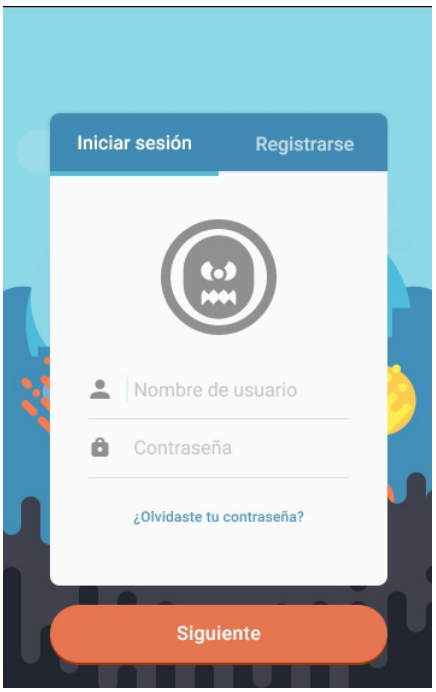
Para el manejo cromático se utilizó el modelo aditivo o RGB, debido a la plataforma sobre la cual el producto debe ser utilizado. Tomando en cuenta el contexto estudiantil sobre el cual debía implementarse el producto, se determinó que el uso de color debía corresponder al entorno. Por esta razón se utilizó una cromática basada en los colores identitarios de la PUCE.

> El efecto del color reside más allá de sus estructuras técnicas y matemáticas; es eficaz en la comunicación no verbal porque afecta a nuestras emociones en un nivel subconsciente. Desde una perspectiva jerárquica, el color atrae y dirige la vista a lo largo de la interfaz. (Wood, 2015, p. 80)

Sobre estos colores se basó una paleta cromática que consta de colores primarios, secundarios y terciarios, de manera que se pueda generar contrastes mediante el uso de combinaciones análogas y complementarias.



Combinación de análogos



Combinación de complementarios

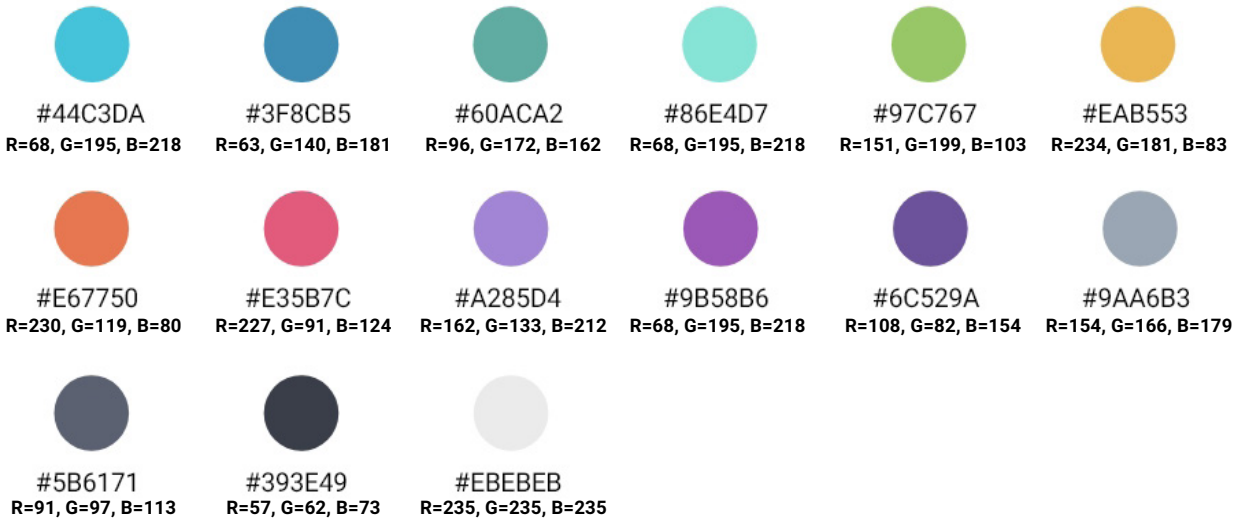


Fig. 14: Paleta cromática.

Elaboración: Autor.

2.5.2.3. Tipografía

Para el uso tipográfico fue importante considerar una versatilidad jerárquica dentro de la familia tipográfica utilizada. Wood (2015) afirma que dentro de una interfaz, el texto sirve inclusive dentro de la navegación como un elemento clave, por lo que es importante que sea adaptable y versátil. De igual manera comenta que las tipografías de palo seco funcionan de manera uniforme en distintas escalas. (p. 78)

Con el fin de generar una experiencia de usuario que resulte familiar en un entorno digital, se utilizó la tipografía estándar de Android según 'Material Design', el lenguaje visual desarrollado por Google para el desarrollo de material gráfico estandarizado en Android (Material Design, 2018).

La tipografía utilizada fue la familia Roboto, debido a su gran cantidad de aplicaciones y adaptabilidad en distintas dimensiones y jerarquías.

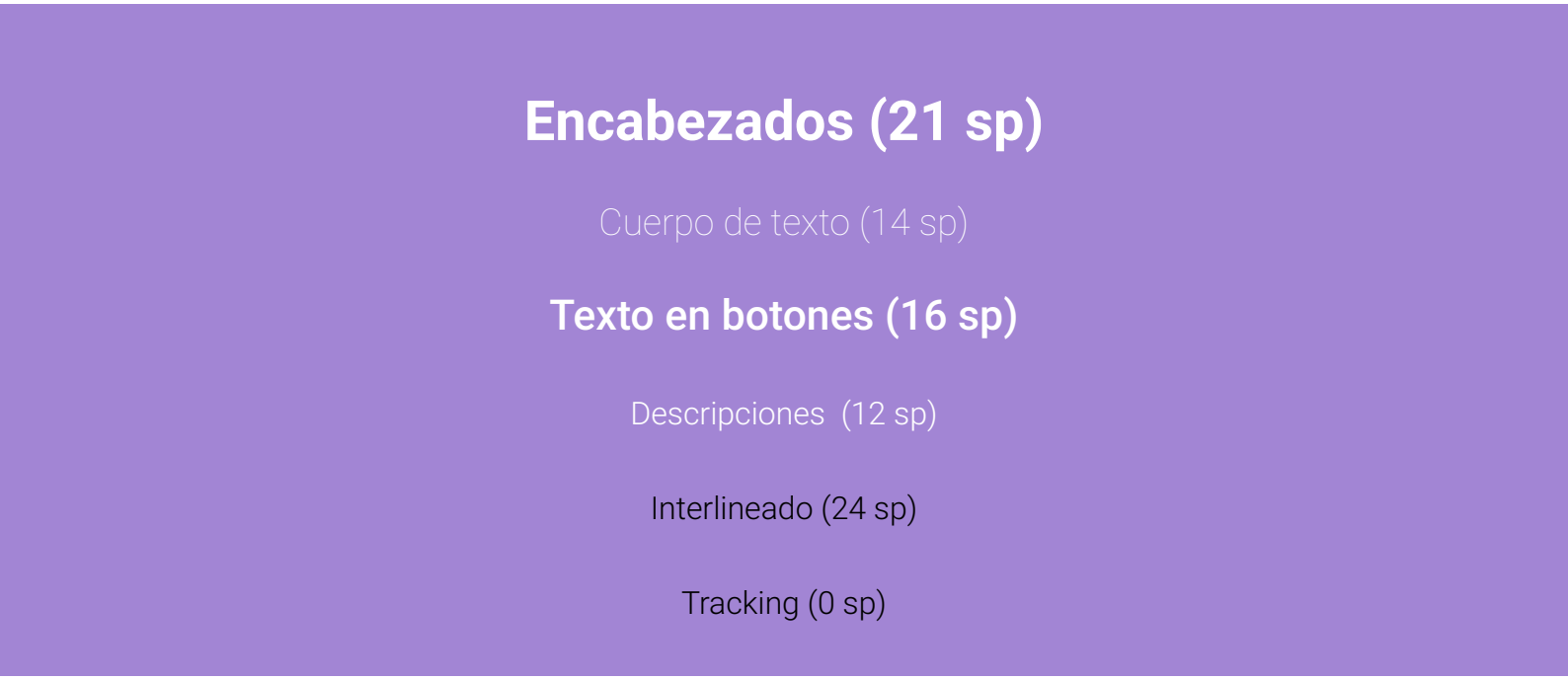


Fig. 15: Tipografía Roboto

Elaboración: Autor.

2.5.3. Consistencia

Para obtener un GUI homologado, que permita entender la experiencia de usuario como un todo, es indispensable que la organización de los elementos en términos de composición, sean consistentes. A continuación se analiza la estructura utilizada para la generación formal del producto y los detalles de construcción basados en los estándares del sistema operativo Android.

2.5.3.1. Maquetación

Para generar un soporte, sobre el cual ubicar los distintos elementos de la interfaz de usuario y distribuir de manera jerárquica los textos y mensajes visuales y prácticos, se utilizó una cuadrícula de 8dp cuadrados.

Anteriormente se habló acerca de los estándares de diseño para productos digitales de la plataforma Android, propuestas por Google. De igual manera, se propone una cuadrícula de 8dp por 8dp para distribuir la ubicación de objetos, al igual que se brinda por defecto el programa de diseño Adobe XD (Material Design, 2018).

> Las cuadrículas aportan estructura esquelética que sustenta el diseño que ofrece el contenido. Las cuadrículas diseñadas correctamente son invisibles a los usuarios finales de sitios web o aplicaciones; como mucho, se apreciará una cierta eficacia inherente y cierta satisfacción en el uso, reafirmando la decisión de visitar el sitio o descargar la aplicación en cuestión. (Steane, 2016, p. 126)

El diseñar en base a una cuadrícula permite de igual manera mantener espacios de respeto y dimensiones de manera adaptativa, lo cual facilita el uso de la interfaz en dispositivos con distintos tamaños de pantalla. Igualmente, en este caso, la retícula modular de 8dp cuadrados sirvió para estructurar y generar distintos aspectos de la aplicación, como las ilustraciones y los componentes de los mini juegos, pero también ubicar elementos de navegación e interacción, con sus medidas adecuadas y manteniendo un espacio de uso apropiado.

A continuación se presentan distintas aplicaciones de la cuadrícula para el uso dentro de la app gamificada.

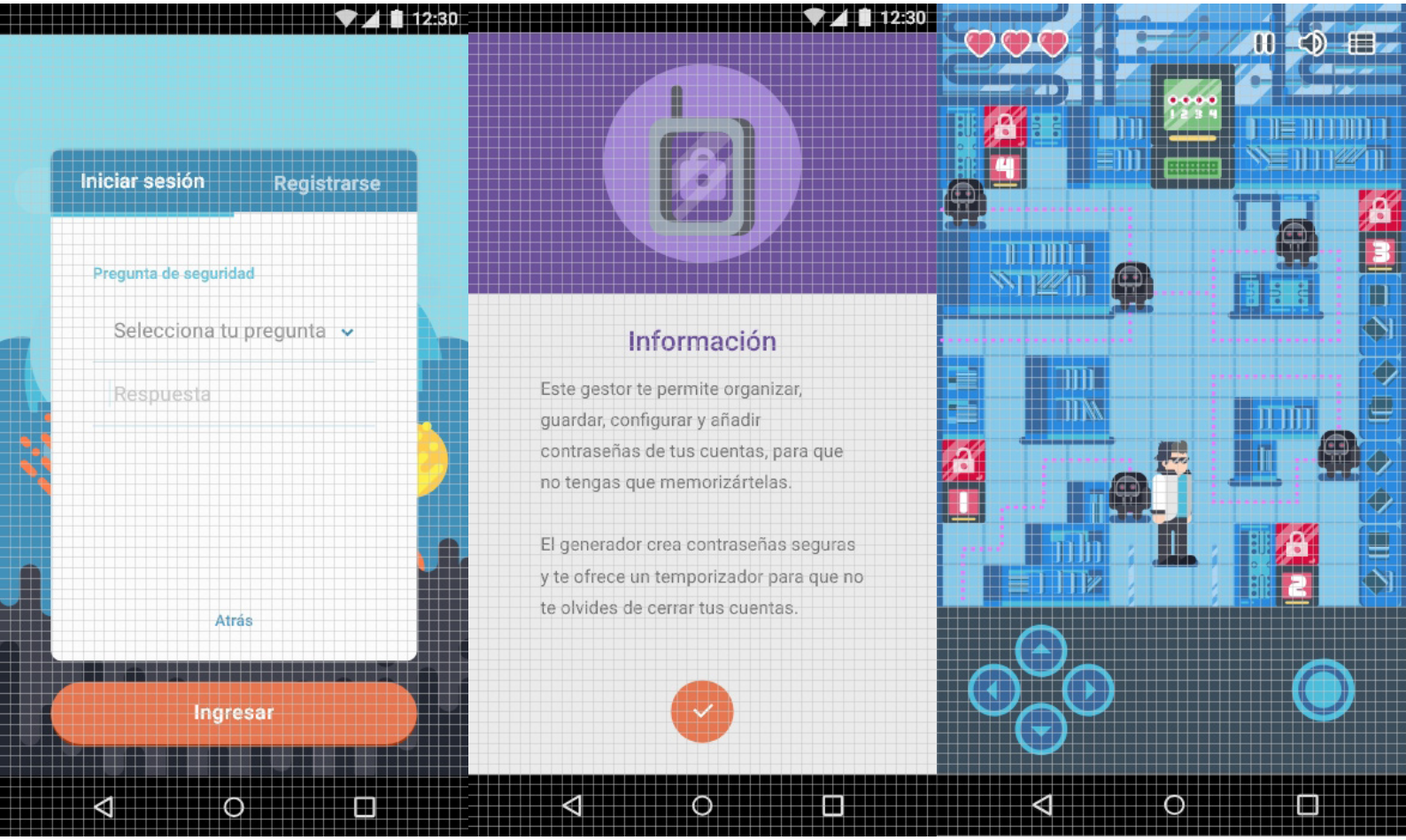


Fig. 16: Aplicación de la cuadrícula

Elaboración: Autor.

2.5.3.2. Detalles constructivos

En base a la cuadrícula utilizada para la organización de cada elemento dentro de la interfaz de usuario, se construyó elementos de funcionalidad similar, que se rigen a ciertos lineamientos de forma.

Según Ellen Lupton en su libro 'Tipografía en Pantalla' (2014), los botones deben tener un tamaño de 44 px para ser ergonómicamente funcionales en relación al tamaño del dedo que toca la pantalla.

En este caso se utilizó botones que mantengan un aspecto relativo a la cuadrícula, es decir en unidades que sean múltiplos de 8. Así, se mantuvieron botones de 48 dp de altura y 56 dp en el caso de botones de mayor tamaño que representen alguna sección en específico.

Los botones y secciones mantienen un espacio de respeto mínimo de 16 dp en relación a los márgenes o límites de la pantalla y un mínimo de 8 dp entre los mismos botones.

Fig. 17: Comportamiento de los botones.

Elaboración: Autor.

Es importante recalcar que el modelo fue realizado en las dimensiones de un teléfono Android pequeño promedio, cuya pantalla fue de 360x640 px, y como ya se mencionó anteriormente, se respetó un mínimo de 16 dp a manera de margen, antes de ubicar elementos grandes de interacción en pantalla.

Asimismo, el espacio de respeto cambió al momento de presentar una gran cantidad de texto, aumentando el margen, de manera que se pueda brindar espacios de descanso visual y aire en medio de la información.

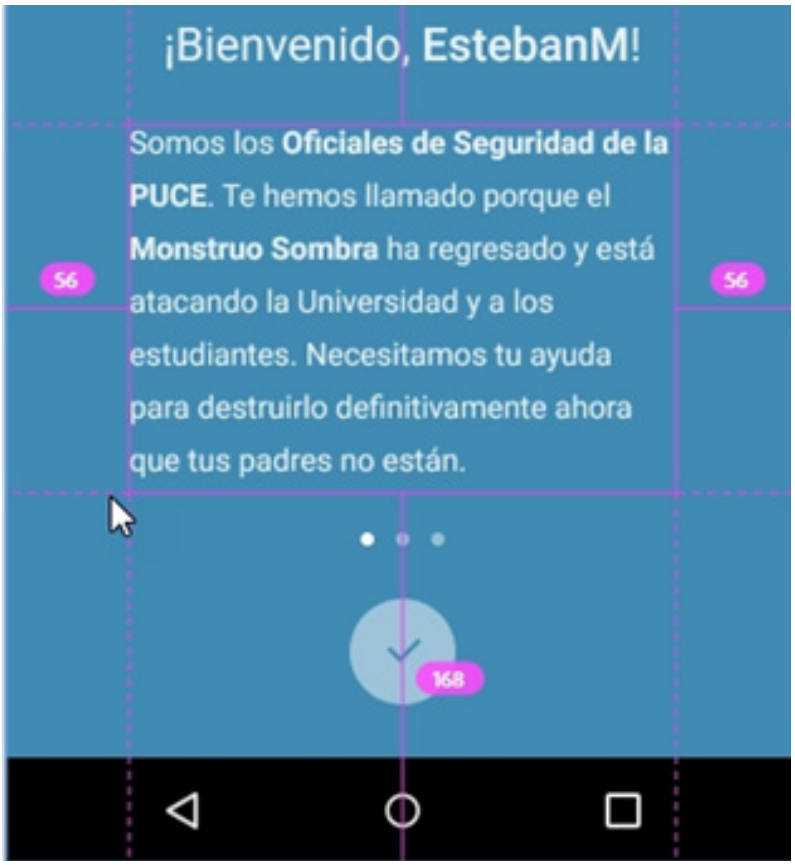


Fig. 18: Adaptabilidad de pantallas.

Elaboración: Autor.

1.5.4. Navegación

"Para mejorar la interactividad, la navegación debe ser obvia, conveniente y fácil de usar. Las etiquetas de navegación deberían usar términos sencillos que el usuario pueda entender, ya que esto facilitará que encuentren un camino lógico a través de la interfaz" (Wood, 2015, p. 52)

Se buscó generar métodos de acceso rápido a las distintas secciones y herramientas de la aplicación, por lo que se presentó una sola pantalla como menú principal, en el cual el menú es estático y muy accesible.

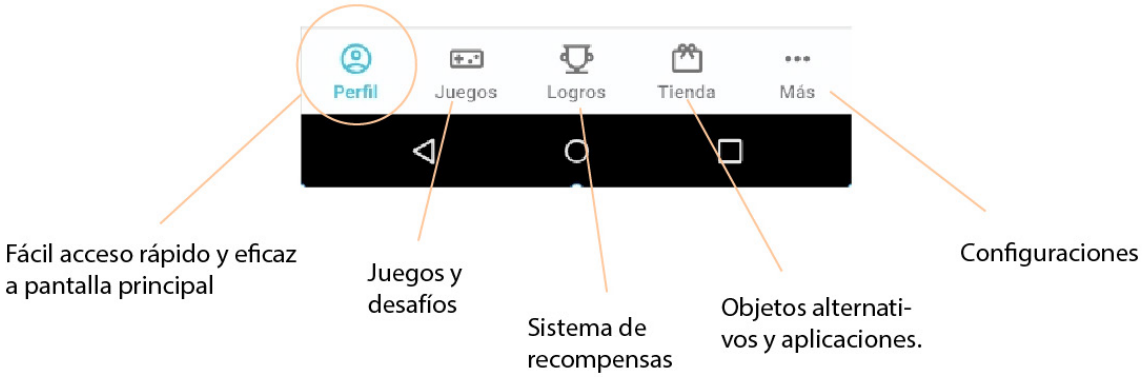


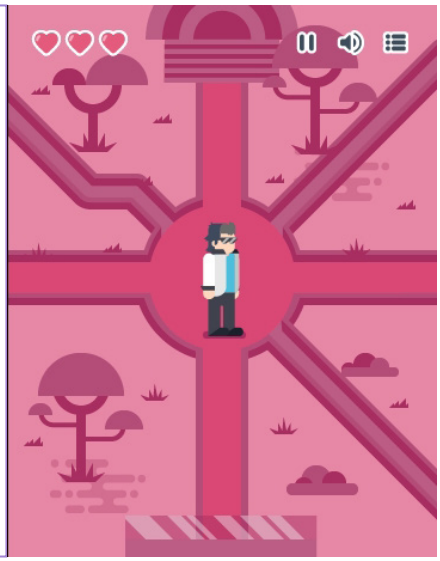
Fig. 19: Navegación en interfaz.

Elaboración: Autor.

2.5.5. Conformidad

Para culminar el análisis de diseño, en esta etapa se analizará los mini juegos dentro de la APP. Para entender mejor la relación de los objetos dentro del GUI con cada acción que les corresponde, se realizó un cuadro en el que se muestran las relaciones formales de los cinco mini juegos.

Nivel 1

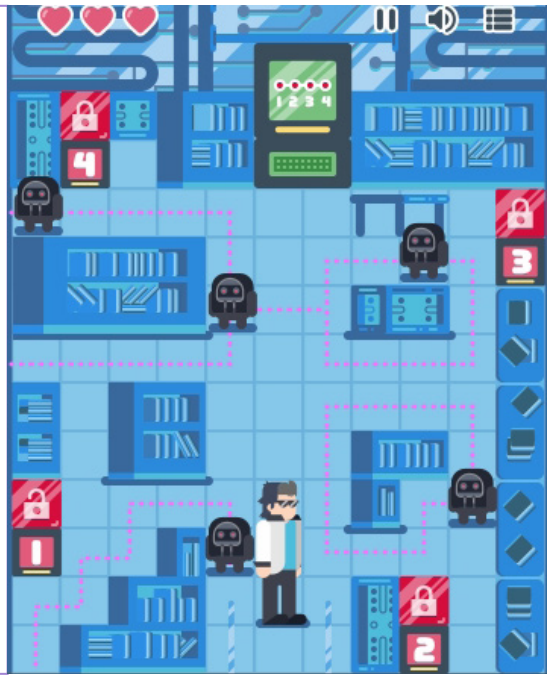


Juego	Determinantes	
1er nivel	**Objetivos:**	Eliminar a todos los enemigos malware
	Reglas:	Eliminar 30 enemigos para ganar Sólo se puede realizar el ataque dentro del rango del círculo
	Recursos:	3 vidas Vacuna antivirus
	Movimientos:	Se puede inyectar y eliminar virus El personaje permanece en su lugar pero puede mirar en las cuatro direcciones cardinales
	Unidades:	30 enemigos malware
	Escenario:	Parque central de la Universidad
	Resultado:	Ganar 200 cibermonedas

Tabla 8: Componentes del primer nivel.

Elaboración: Autor.

Nivel 2



Juego	Determinantes	
2ndo nivel	**Objetivos:**	Desencriptar la información
	Reglas:	Desbloquear cada candado en orden de menor a mayor Evadir los enemigos
	Recursos:	3 vidas Vacuna antivirus
	Movimientos:	Arriba, abajo, izquierda, derecha Poner la llave en los candados
	Unidades:	5 enemigos y 4 candados
	Escenario:	Biblioteca de la Universidad
	Resultado:	Ganar 200 cibermonedas

Tabla. 9: Componentes del segundo nivel.

Elaboración: Autor.

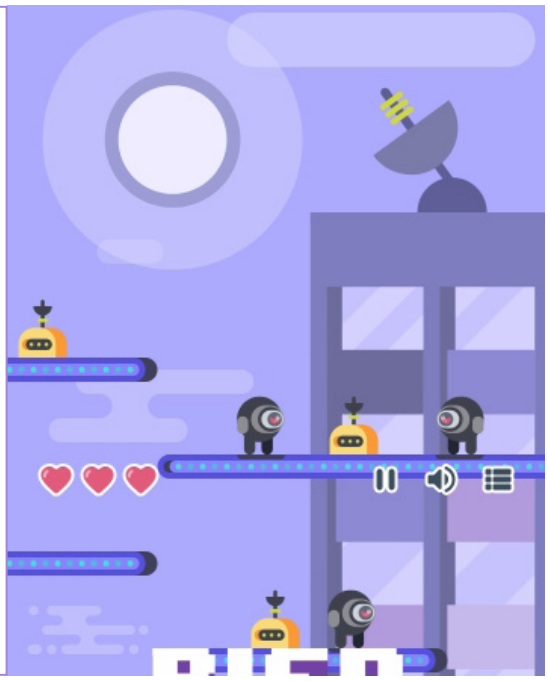
Nivel 3

Juego	Determinantes	
3er nivel	**Objetivos:**	Llegar al final del boulevard a salvo
	Reglas:	Evadir los anzuelos Se puede caer encima a los peces
	Recursos:	3 vidas Jetpack
	Movimientos:	Izquierda, derecha Doble salto
	Unidades:	3 ganchos y 2 peces
	Escenario:	Boulevard de la Universidad
	Resultado:	Ganar 200 cibermonedas

Tabla. 10: Componentes del tercer nivel.

Elaboración: Autor.

Nivel 4

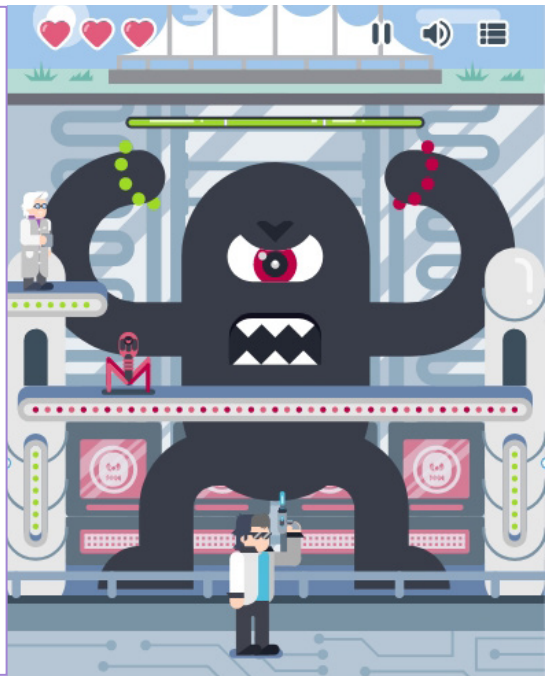


Juego	Determinantes	
4to nivel	**Objetivos:**	Desmantelar el sistema de vigilancia masiva
	Reglas:	Destruir antenas pequeñas cayéndoles encima, para destruir la antena grande Evadir los enemigos
	Recursos:	3 vidas Manto de anonimato
	Movimientos:	Arriba, abajo, izquierda, derecha Salto
	Unidades:	5 enemigos y 5 antenas
	Escenario:	Torre de la Universidad
	Resultado:	Ganar 200 cibermonedas

Tabla. 11: Componentes del cuarto nivel.

Elaboración: Autor.

Nivel 5



Juego	Determinantes	
4to nivel	**Objetivos:**	Destruir al Monstruo Sombra
	Reglas:	Destruir 3 malware para poder realizar un ataque directo al monstruo Evadir las balas
	Recursos:	3 vidas Pistola de seguridad
	Movimientos:	Izquierda, derecha Disparo
	Unidades:	9 enemigos y jefe
	Escenario:	Centro de Cómputo de Universidad
	Resultado:	Ganar el juego y 200 cibermonedas

Tabla. 12: Componentes del quinto nivel.

Elaboración: Autor.

2.6. Proceso de producción

Habiendo generado el diseño del producto mediante los principios expuestos anteriormente y determinado los detalles de construcción del mismo, el siguiente paso fue tomar en cuenta la implementación del proyecto dentro del entorno universitario dentro del cual se establece y tiene cabida.

Se generó una planificación para la publicación de la app/videojuego mediante los elementos claves que expone Fullerton (2008). Estos incluyen cuatro aspectos principales (desarrollo, licenciamiento, marketing y distribución), los cuales fueron adaptados a la implementación del producto en la PUCE y engloban el proceso de producción.

> El diseño de un videojuego es solo una pequeña parte del elaborado proceso de producción del juego. La producción también es una parte más pequeña del largo proceso para publicar un título. La publicación de un juego involucra todos los pasos necesarios para llevar a un juego desde un pequeño concepto hacia un producto pulido que se distribuye en las perchas de las tiendas. (Fullerton, 2008, p. 423)

Entonces, fue importante determinar en primer lugar, cuáles son los recursos necesarios para poder llevar al producto hacia el teléfono de los usuarios, estudiantes de la Universidad.

2.6.1. Implementación en la PUCE

Basándose en las ideas de Fullerton, fue necesario pensar en recursos que atiendan a las necesidades en cuanto al desarrollo de la app, más allá de los componentes de diseño. También fue importante pensar en estrategias de difusión y distribución, y finalmente, tomar en cuenta formas de análisis y actualización del software en base a la reacción de los estudiantes en la práctica y al uso de la aplicación.

Por esta razón se consideró que es de vital importancia el trabajo en conjunto con la misma Institución y con los departamentos encargados del desarrollo de software de y para la misma Universidad, como es el caso del Centro de Educación Virtual y Tecnológica Educativa y del Departamento de Redes de la Dirección de Informática, encargados de la plataforma virtual 'Moodle' y la 'Intranet'.

De esta manera, se puede generar apropiación mediante el desarrollo del proyecto dentro de la PUCE y se puede trabajar con programadores y desarrolladores de la Institución, que aseguren un trabajo de calidad con una postura y visión acorde a la Institución, además de llevar un control adecuado en cuanto al uso de la aplicación y a la detección de los aspectos que necesitan ser mejorados o cambiados con el paso del tiempo.

Por otro lado, se consideró igualmente relevante el presentar el proyecto a la Federación de Estudiantes de la PUCE (FEUCE), para recibir el apoyo de las autoridades máximas universitarias, con el fin de tener acceso a medios de difusión dentro del mismo campus e implementar estrategias de distribución de la aplicación hacia los estudiantes y recibir el apoyo económico y el respaldo financiero necesario para el desarrollo del proyecto.

2.6.2. Desarrollo de la APP en la PUCE

Previamente se comentó la importancia del apoyo de los desarrolladores y programadores de la PUCE, para llevar a cabo el proyecto. Se consideró adecuado que el trabajo entre diseñador y programador sea claro y manejado de manera técnica con especificaciones de composición e interacciones, para evitar confusiones en el diseño de interfaz. Sin embargo, primero es necesario que se entregue un documento de diseño a los miembros del equipo, para que todo el proyecto quede claro, desde el contexto, hasta las dinámicas del juego.

El desarrollo digital de juegos es un medio inherentemente colaborativo. Una de las partes más importantes de la administración de este proceso, es la comunicación de la visión total del juego a cada uno de los miembros del equipo […] Un buen documento de diseño es como los planos de construcción de un edificio. (Fullerton, 2008, p. 394)

Fullerton comenta que el documento de diseño debe contener ciertas áreas determinadas en las que se explique una visión general del proyecto, la audiencia hacia la que el juego se dirige, la plataforma sobre la que se desarrollará, la jugabilidad, los personajes, la historia o trama, el escenario, y finalmente, los recursos de diseño que se utilizará. La mayoría de estos elementos fueron detallados en las secciones anteriores del presente TFC, sin embargo, a continuación se especificará un poco más acerca de cómo deben entregarse los recursos de diseño a los otros miembros del equipo de trabajo.

2.6.2.1. Detalles técnicos

Wood (2015) recomienda generar un archivo de composición que conste con cada variante de página y sin capas combinadas, donde se especifique los valores de los principales colores en RGB, información acerca de tipografía y las interacciones de la interfaz, de manera clara. (p. 146)

Por esta razón se trabajó en un prototipo -cuyos links de acceso pueden encontrarse en los anexos- que demuestra las propiedades e interacciones de la interfaz, mediante el programa 'Adobe XD', el cual permitió realizar una simulación de la app, en cuanto a funcionamiento del GUI. Además, como se mencionó anteriormente durante el análisis FODA de diseño, la aplicación propuesta se maneja en la plataforma Android, por lo que el archivo final que se trabaja con los desarrolladores y programadores, es una APK.

Cabe recalcar que dentro del prototipo se puede encontrar una simulación del funcionamiento de la app, pero también sus detalles constructivos, es decir, códigos de color, tamaños, formatos, tipografía e interacciones específicas de botones, que permiten a los programadores un fácil acceso a la información necesaria para replicar la interfaz. Finalmente, también se encuentra disponible una visión detallada de todas las pantallas que forman parte de la aplicación.

Asimismo, Fullerton recomienda realizar un demo del videojuego, para entender de manera más clara la jugabilidad y los movimientos que deben realizarse durante la programación. También comenta que si esto no es posible de realizar, es recomendable por lo menos realizar un video donde se demuestre el modo de juego y los personajes. (p. 446)

Por esta razón se realizó un prototipo básico de uno de los mini juegos de la aplicación en 'Unity', un programa para desarrollar videojuegos. Asimismo,

se incluyó videos de todos los niveles para demostrar el funcionamiento de cada uno de los mini juegos. Estos recursos se encuentran igualmente disponibles en los anexos.

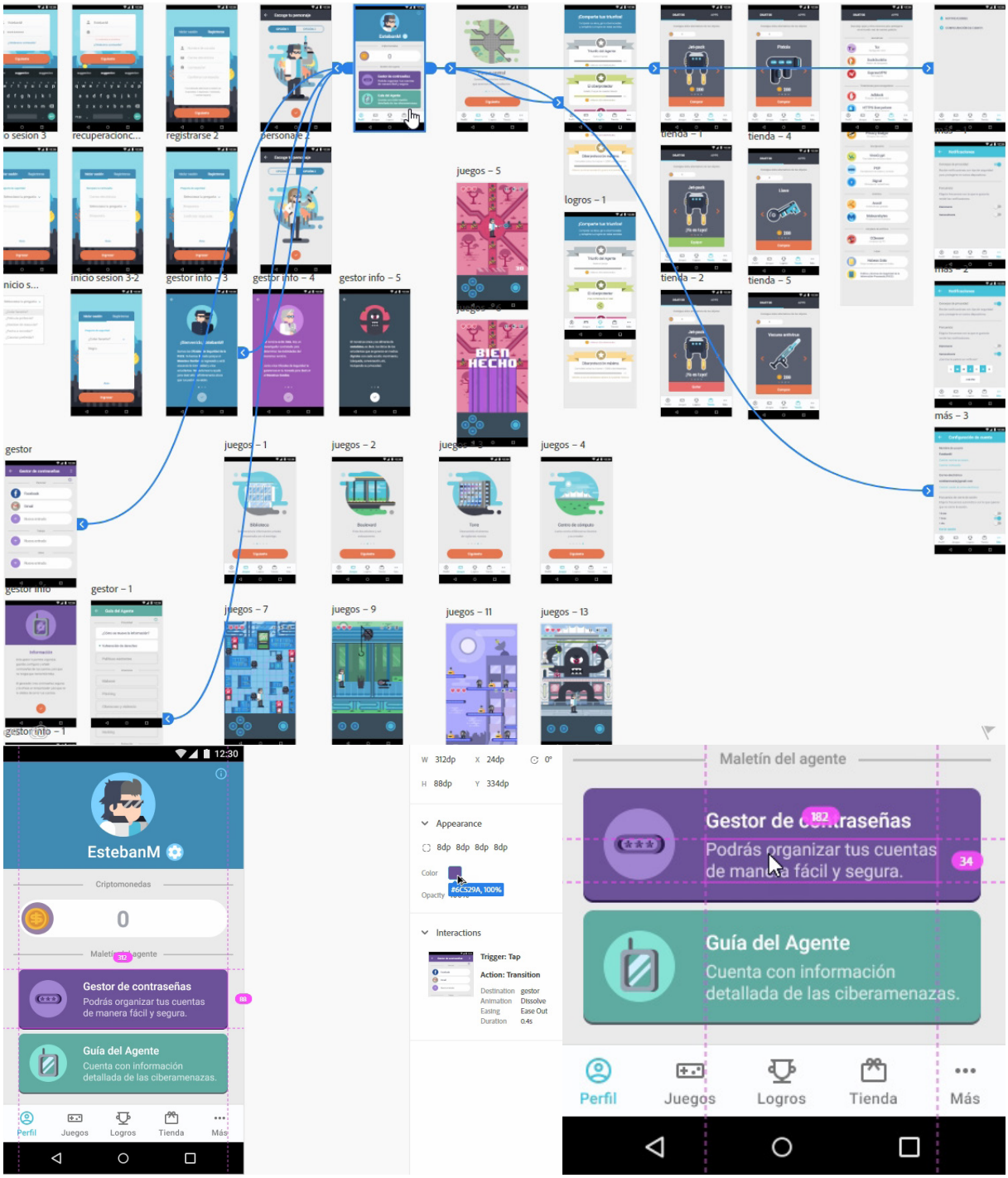


Fig. 20: Ejemplos de detalles técnicos.

Elaboración: Autor.

Por otra parte, también es necesario que el resto del equipo entienda la AI que se maneja en la aplicación. Anteriormente se comentó acerca del mapa de sitio sobre el cual se desarrolló el GUI. Sin embargo, fue igualmente necesario generar un flujo de tareas para el trabajo interdisciplinario de desarrollo de la app y mini juegos.

> El flujo de tareas difiere de los mapas de sitios porque representa las decisiones y las secuencias de tareas concretas, como la función de inicio o búsqueda, que se realizan sin abandonar la página. Para visualizar los mapas de sitios o flujos de tareas suele emplearse una sintaxis sencilla. (Steane, 2016, p. 42)

Finalmente, para facilitar el proceso de interacciones entre los personajes dentro de los juegos, además de los videos demostrativos de movimiento y jugabilidad, se realizó una hoja de ‘sprites’, que según Christensson (2012), es “un mapa de bits que está diseñado para ser parte de una escena más grande. Puede ser una imagen estática o un gráfico animado. Ejemplos de sprites incluyen objetos en 2D en videojuegos.” (párr. 1)

A continuacion se encuentran gráficos el desarrollo de cada uno de estos elementos, como recursos provistos para la programación del videojuego y el entendimiento de las interacciones dentro del mismo.

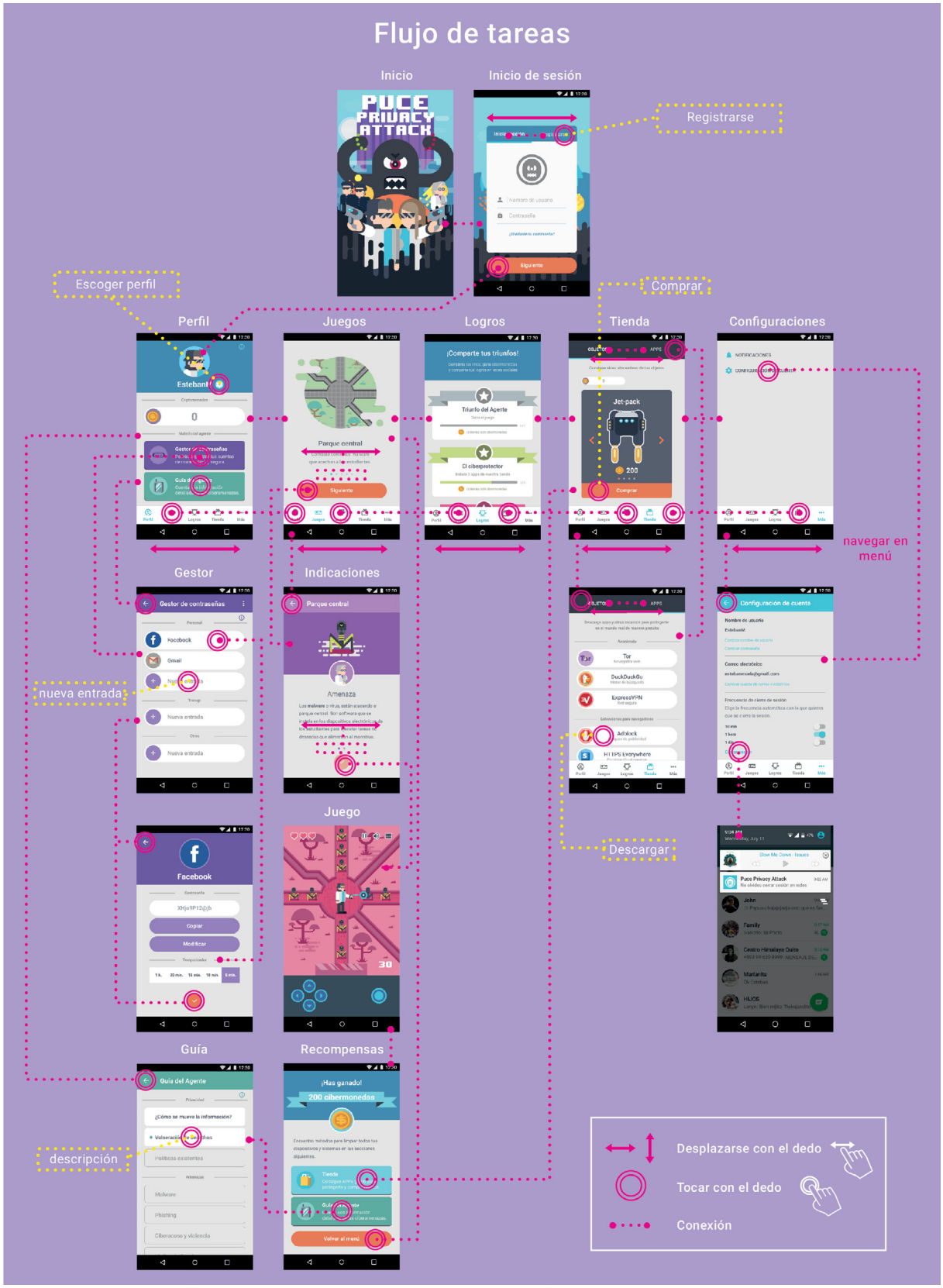


Fig. 21: Flujo de tareas.

Elaboración: Autor.

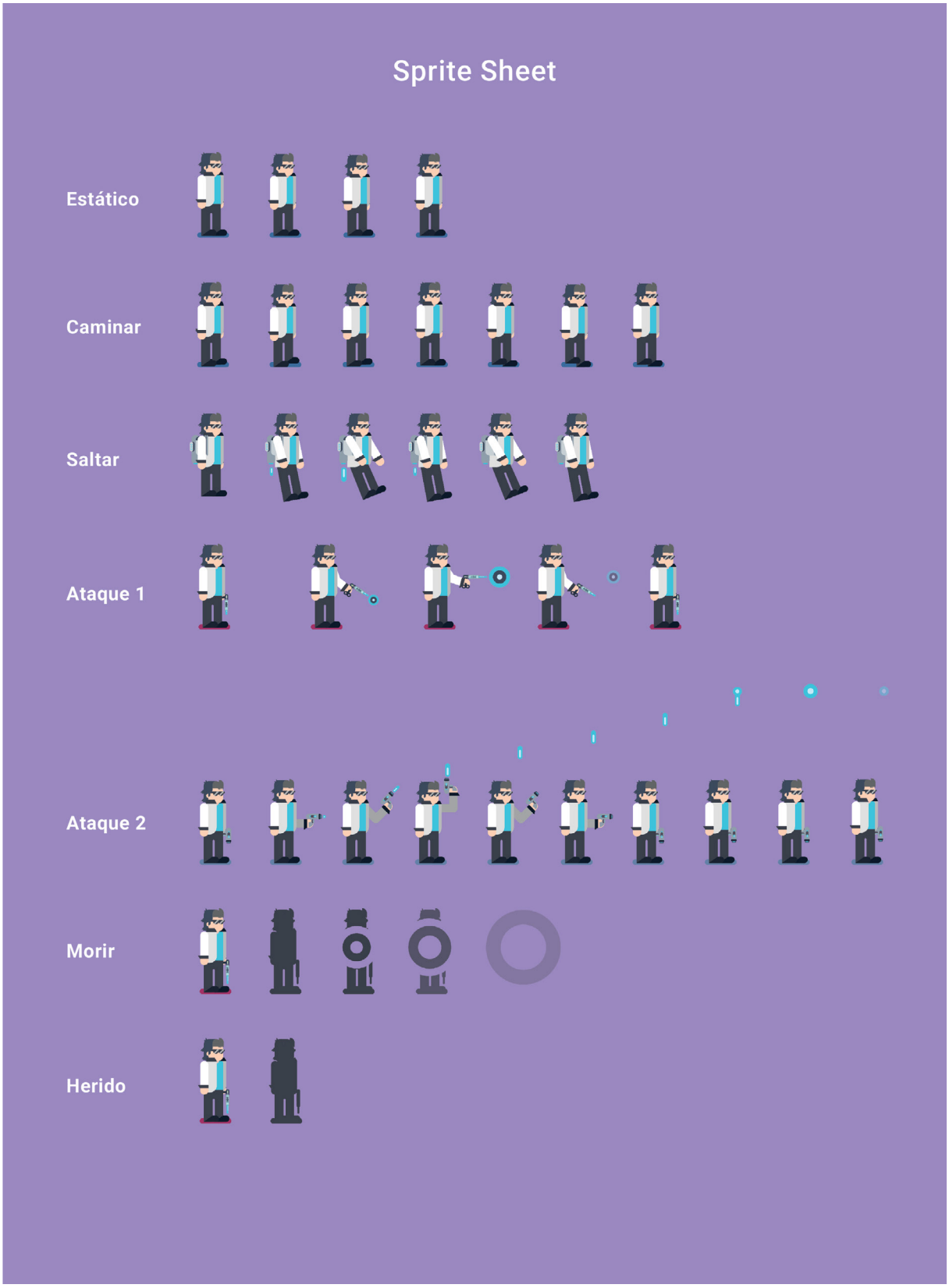


Fig. 22: Hoja de sprites del personaje principal.

Elaboración: Autor.

2.6.2.2. Plataforma de desarrollo y distribución

Considerando que la aplicación/videojuego fue diseñada para Android y pensada en su forma de lanzamiento como una APK, se trata de una app, que para una difusión y control efectivo, podría lanzarse mediante 'Play Store', la tienda de Google integrada por defecto en todos los teléfonos inteligentes que tienen determinado sistema operativo.

A continuación se detalla los requisitos para subir una APP al sistema de Google Play. Primero es necesario entrar con un perfil de Google y crear una cuenta mercantil en la plataforma Play Console, para un manejo más adecuado por parte de varias personas. (Play Console, 2018)

El tamaño máximo de la APK varía según la compatibilidad de la versión del sistema operativo Android con la aplicación. Es posible subir varios archivos con diferentes compatibilidades para los distintos dispositivos, siempre y cuando se mantengan entre los rangos de tamaño de archivo especificado por Google.

Para versiones de Android 2.3 y posteriores, los archivos pueden pesar un máximo de 100 mb, sin embargo en versiones menores, solamente pueden llegar a 50 mb. Es importante tener en cuenta que los archivos APK cuentan con un código, cuyo tamaño y peso aumenta con cada actualización de la app. El valor mayor de este código es 200000000 y si supera ese número, Play Console no permite enviar nuevos APK. Por esta razón es importante optimizar al máximo el tamaño de los archivos subidos en la plataforma.

Una vez que se obtiene el archivo APK listo para su publicación, se debe llenar ciertos campos relevantes y entregar determinados recursos gráficos que brindan las primeras impresiones de la aplicación a las personas. Adelante se indica en forma de lista, las secciones que deben ser completadas.

- Título de la app (límite de 50 caracteres)
- Descripción corta (límite de 40 caracteres)
- Descripción larga (límite de 4000 caracteres)
- De 2 a 8 pantallazos de la app (JPEG o PNG de 24 bit sin transparencia, de 320 – 3840 px)
- Ícono de la app (PNG de 32 bit con transparencia, de 512x512 px)
- Tipo de app
- Categoría
- Puntaje del contenido
- Contacto del desarrollador o compañía
- Tipo de política de privacidad

En referencia al último punto, la política de privacidad debe explicar de manera clara y detallada cómo se recopilan y usan los datos de usuario recopilados por la aplicación. Para esto es necesario el asesoramiento de un representante legal, que el caso de este proyecto podría ser un abogado de la PUCE. Sin embargo, por la naturaleza del proyecto, los datos generados en la aplicación solamente deben utilizados para la actualización de la aplicación o el mejoramiento de su funcionamiento y se rige a las leyes de protección de PII de la PUCE.

Por otra parte, la licencia que se concede a Google al subir la app a la plataforma, es libre de regalías, es decir que la organización puede utilizar el producto de manera no exclusiva, a nivel mundial y puede reproducir, analizar y utilizar el material en relación a las políticas de marketing del organismo y adecuar de acuerdo a las actualizaciones que se realice a la plataforma. Por otro lado, el desarrollador y los publicadores pueden hacerse cargo de la difusión y uso libre de la aplicación bajo las normas acordadas y la política de privacidad establecida. (Play Console, 2018)

2.6.2.3. Análisis de métricas y actualizaciones

Para asegurar una continuidad en el desarrollo del proyecto y en la eficacia del producto es necesario considerar no solamente que el Internet es un medio que se encuentra en constante actualización, sino que las necesidades de los usuarios igualmente va cambiando y consigo los medios tecnológicos van adaptándose a las tendencias y cambios sociales.

De esta manera, es necesario también que el producto propuesto continúe mejorando en base al análisis de los errores y dificultades y continúe adaptándose a medida que pasa el tiempo hacia las necesidades de los estudiantes y al movimiento tecnológico de manera iterativa y circulatoria. Es por esta razón que es importante generar métodos de análisis de la información relevante para el contínuo mejoramiento de la aplicación.

El análisis de métricas se refiere a “la colección y análisis de datos en relación a cuántas veces se accede a un sitio web, quién accede y qué hicieron una vez dentro […] De esto el diseñador web puede ganar información valiosa acerca de problemas de navegación.” (Benyon, 2013, p. 410).

Benyon explica el análisis de datos desde el punto de vista del diseño web. Sin embargo es el mismo funcionamiento y principios que se da en el uso de una aplicación. Mediante la recolección de información relativa al uso de la app, es posible determinar en qué secciones de la aplicación se encuentra dificultad en cuanto a navegación o al entendimiento de funcionalidad. A pesar que se realizó pruebas de usabilidad en el usuario, es indispensable un análisis contínuo y retroalimentativo del uso de la aplicación.

> Puedes encontrar si algo está mal con el diseño de tu juego por ejemplo o puedes encontrar un error en el código. También puedes determinar cuántos usuarios hacen click en un botón específico, cuántos son capaces de terminar el juego o cuánto tiempo pasan en un área específica del juego, etc. (Mignano, 2016)

El proyecto tiene una finalidad informativa, por lo que se puede utilizar el análisis de datos para entender y mejorar la eficacia en la comunicación y los mensajes que se busca transmitir, así como la funcionalidad de juegos y herramientas prácticas como el 'gestor de contraseñas'.

Afortunadamente, la misma plataforma de desarrollo de Google propuesta en el punto anterior, permite añadir una herramienta para el análisis de datos, denominada Play Games Player Analytics. Frenkel (2015) comenta que se trata de un "conjunto de reportes gratis que ayudan a manejar el negocio de juego y entender el comportamiento dentro de juego, en las aplicaciones subidas a Play Developer Console" (párr. 1)

Frenkel explica igualmente que es posible identificar puntos clave en las métricas de negocios, para enfocarse en realizar actualizaciones y cambios en el juego, que tengan un mayor impacto. En el caso del presente TFC, el proyecto no se centra dentro de un modelo de negocios y no tiene fines lucrativos, es decir que la app/videojuego se distribuirá de manera gratuita.

Aun así, la información recolectada puede aplicarse de igual manera en el tratamiento de puntos críticos y cambios sustanciales con la finalidad de mejorar la recepción de información, más no de ganar dinero y se sugiere realizarla cada semestre con el inicio de clases y la entrada de nuevos estudiantes, de manera que haya una retroalimentación semestral.

2.7. Estrategia de difusión de la APP

Es importante desarrollar e implementar estrategias de gestión de comunicación en distintos niveles para asegurar una difusión efectiva que motive a los estudiantes de la PUCE a instalar la aplicación en sus teléfonos inteligentes.

> Tener una estrategia consiste en estar consciente del lugar al que uno va y cómo pretende llegar allí. El propósito de tener una estrategia es asegurar que las actividades permanezcan apegados a la realidad con respecto a las restricciones de tiempo, recursos, etc. (Rodríguez, 2004, p. 83)

La PUCE como institución estudiantil maneja una gran variedad de medios por los que se notifica a los miembros de la Universidad de temas de índole diversa. La FEUCE siendo los representantes de los estudiantes, tienen acceso a varios de estos medios de igual manera. Anteriormente se mencionó la importancia de trabajar con ambas entidades en conjunto, puesto que se puede realizar un trabajo integral para aprovechar los distintos tipos de medios de comunicación, para generar apropiación y atracción hacia el producto desarrollado.

> La táctica se ocupa de los medios que serán utilizados para alcanzar los fines estratégicos. En tal sentido, serán consideradas las herramientas tácticas de comunicación: publicidad; relaciones públicas; promoción; difusión periodística; literatura; papelería; heráldica corporativa; actos; auspicios; etcétera. (Scheinsohn, 2009, p.94)

En la siguiente página se presenta una tabla con distintas propuestas y alternativas de tácticas que podrían ayudar a la difusión de la app, generar expectativa, así como apropiación que motiven a los estudiantes a descargar el producto. La tabla se parte del público objetivo, es decir los estudiantes de la PUCE y se encuentra basada en el proceso de planeación planteado por Aljure. (2015, p. 29)

Actividades estratégicas	Objetivos	Mensajes	Recursos
Lanzar el producto a inicio de semestre.	Posicionar la herramienta y generar interés en la comunidad universitaria y en los nuevos estudiantes.	Existe una nueva herramienta que permite divertirse y proteger los datos de los estudiantes mediante el aprendizaje y el juego.	Aplicación disponible para descargar en Play Store de Google.
Promocionar el juego en la página web de la PUCE e Intranet, mediante un pequeño anuncio antes del ingreso para realizar la automatrícula y mantenerlo así durante las primeras semanas de lanzamiento del videojuego.	Generar expectativas de un juego específico de la PUCE, que los estudiantes podrán jugar a principio de semestre.	Pronto llegará un juego gratuito para los estudiantes, que te permitirá aprender mientras juegas.	Pequeños anuncios digitales con tips de privacidad y otros con pantallazos de la apariencia gráfica del juego.
Utilizar la lista de mailing de la FEUCE, para promocionar y promover la aplicación como un método de protección de la información.	Brindar información acerca de los usos de la aplicación, incluyendo la descarga de la misma.	Se trata de una app/juego que también sirve como herramienta práctica para la protección cotidiana de la privacidad.	Lista de nombres y correo de la FEUCE. Informativo acerca de la app.
Promocionar la app en redes sociales de la FEUCE y brindar tips de protección. Preguntar opiniones.	Promover el uso de la aplicación mediante redes sociales y obtener retroalimentación mediante las mismas.	Los desarrolladores se encuentran atentos ante cualquier situación y mejora a realizar.	Promocionales para redes.
Añadir un folleto informativo en la agenda que se entrega a principio de semestre, explicando beneficios de descargar la app.	Realizar una breve introducción a la app, su funcionamiento y objetivos de protección en los estudiantes.	La app es útil en la cotidianidad y lúdica. Es importante descargarla. Se obtiene beneficios.	Alrededor de 10700 folletos.
Promocionar mediante la radio de la universidad y los programas periodísticos en las televisiones de la Institución.	Dar a conocer más sobre el producto y generar apropiación del mismo.	Se trata de una aplicación especializada con varios beneficios.	Realizar spots publicitarios, videos de gameplays.

Tabla. 13: Estrategias para la difusión.

Elaboración: Autor.

2.8. Costos del proyecto

Para determinar el costo total del proyecto, se tomó en cuenta 7 rubros distintos. En primer lugar está el costo de diseño por pantalla de la aplicación. En ese caso se tomó como referente el número de pantallas utilizadas en el prototipo final y se puso un valor unitario de cinco dólares a cada uno.

Después se tomó en cuenta el valor de programación de cada mini juego. En la práctica fue contratado un programador para llevar a cabo pruebas de usabilidad de uno de los juegos. Este costo fue de alrededor de 130 dólares, por lo que se toma ese mismo precio como referente, pero multiplicado por el número de juegos que tiene la aplicación en total.

En una consulta realizada a Carlos Castillo, desarrollador de medios digitales de la PUCE, se determinó que solamente el desarrollo de la aplicación, sin los videojuegos costaría alrededor de 2,500 dólares (C. Castillo, comunicación personal, 2018).

El siguiente rubro a contemplar es el de uno de los incentivos presentados en el juego, una suscripción gratuita para un antivirus pagado. Está pensado que solamente 50 estudiantes puedan acceder a este beneficio.

Posteriormente se asignó un presupuesto para los efectos de sonido y la música, estipulados en alrededor de 50 a 100 dólares por cada nivel. Por último se tomó en cuenta el valor a pagar por subir la app a la plataforma de Google, en 25 dólares.

La sumatoria de todos los rubros da el costo total del proyecto sin tomar en cuenta costos de difusión ni actualización.

Cantidad	Descripción	P. Unitario	Valor de Venta
80	Diseño de pantallas	$ 5,00	$ 400,00
5	Programación juego	$ 130,00	$ 650,00
1	Programación APP	$ 2.500,00	$ 2.500,00
1	Suscripción para 50 personas en antivirus pagado	$ 800,00	$ 500,00
5	Música y sonidos por nivel	$ 100,00	$ 500,00
1	Permiso para subir app a Play Store	$ 25,00	$ 25,00
		Subtotal:	**$ 4.575,00**
		12% IVA:	**$ 549,00**
		TOTAL:	**$ 5.124,00**

Tabla. 14: Costos.

Elaboración: Autor.

Finalmente, el costo total, dividido entre en número total de estudiantes dio un total de 0,48 ctvs de dólar por cada unidad o descarga de aplicación, con una vigencia mínima de seis meses. Como se explicó en el desarrollo del proyecto, esta cifra sería cubierta por la Institución.

Capítulo 3

TERCER COMPONENTE: VALIDACIÓN

Una vez terminado el producto, se procedió a realizar una serie de validaciones con profesionales que laboran en diferentes ámbitos: un diseñador, un experto en redes, más pruebas de usabilidad en usuarios.

Para la evaluación experta se utilizaron herramientas heurísticas con base en los principios básicos de diseño expuestos por Benyon (2013), en tanto para los usuarios se utilizó una herramienta basada en el Co-descubrimiento y en posteriores entrevistas.

Cabe recalcar que la validación al comitente fue realizada en el Centro de Educación Virtual y Tecnológica Educativa, de la PUCE, en el cual se encuentran desarrolladores y diseñadores encargados del desarrollo de software especializado para estudiantes y docentes dentro de la Universidad, como la plataforma ‘Moodle’. Por esta razón se realizó una evaluación heurística similar a la profesional de diseño, sin embargo cambiando ciertos parámetros para que sean adecuados para su evaluación.

3.1. Validación heurística

Campo: Diseño Gráfico

Nombre: Xavier Barriga

CRITERIO	PARÁMETROS	RANGO							OBSERVACIONES
		-3	-2	-1	0	1	2	3	
VISIBILIDAD	Las funciones de la app son claramente distinguibles.							X	Tener cuidado con el contexto de la tecnología
	Los textos se distinguen con facilidad. (legibilidad)					X			Tamaño, revisar contraste, sobre todo en la tienda
	Las ilustraciones tienen un grado de iconicidad adecuado.						X		Complejo pero bien logrado
	Se maneja contrastes que permiten entender los elementos importantes de forma clara.						X		Cuidar textos. Realizar pruebas de contraste, también en la tienda
	Se logra reconocer con facilidad las secciones de la app.							X	Sí
	Se proporciona un feedback adecuado y puntual.							X	
	El movimiento de los elementos es adecuado.					X			Cuidar movimiento en indicación/ amenaza
	Se utiliza otros recursos sensoriales que permiten entender mejor las acciones e interacciones.						X		Juego sí, app no

CRITERIO	PARÁMETROS	RANGO							OBSERVACIONES
		-3	-2	-1	0	1	2	3	
NAVEGACIÓN	Se brindan soportes para permitir al usuario navegar fácilmente por toda la app.							X	
	Se complementa el uso de la app con instrucciones paso a paso fáciles de encontrar y recuperar.							X	
	La disposición de los elementos de la aplicación permite una navegación efectiva.							X	
CONTROL	La aplicación permite un manejo del perfil y notificaciones de usuario adecuado.							X	Revisar notificaciones para temporizado (ubicación adecuada) y que se pueda colocar en las notificaciones.
	Hay un mapeo claro y lógico entre los controles y el efecto que éstos tienen.						X		El mapeo es claro, revisar tamaño y posición. Revisar la forma del controlador de acción. Revisar el espacio que se destinó a los controles.
	El usuario tiene control sobre sus decisiones, apropiándose de la aplicación.							X	
COMENTARIOS	Se entiende de manera rápida y eficaz los efectos de las acciones y decisiones tomadas en los juegos y app.							X	
	Se cuenta con un buen sistema de retroalimentación de usuario.							X	
RECUPERACIÓN	La recuperación de errores y equivocaciones es rápida y efectiva.				X				Revisar bien mapeo en inicio de juegos. Brindar opción de confirmación de compra.

CRITERIO	PARÁMETROS	RANGO							OBSERVACIONES
		-3	-2	-1	0	1	2	3	
RESTRICCIONES	La restricción para evitar efectuar acciones peligrosas o no adecuadas es efectiva.			X					
	Se utiliza reglas o indicaciones que facilitan el entendimiento de acciones peligrosas.			X					
FLEXIBILIDAD	Se puede acceder a la información por varios medios.			X					Revisar organización del gestor de contraseñas. Brindar opción de buscar y ordenar
	Se brinda la opción de personalizar las acciones más repetidas.		X						Cambiar en bloque o sugerir cambios en contraseña
	El sistema es adecuado para personas con distintos niveles de experiencia.						X		No está pensado en los PRO
	La aplicación permite ser accedida por diferentes medios o plataformas.				X				Está pensado sólo para Android
ESTILO	El diseño es estético e invita a que la aplicación sea utilizada.							X	
	La configuración formal de los elementos es atractiva.							X	
	Se evita información irrelevante.				X				Es un juego
CORDIALIDAD	Los mensajes y transmisión de información resultan amigables.							X	
	El lenguaje y el tono de los mensajes son adecuados para un público juvenil							X	
	Se utiliza tecnología interactiva para conectar a las personas y/o apoyarlas.							X	

CRITERIO	PARÁMETROS	RANGO							OBSERVACIONES
		-3	-2	-1	0	1	2	3	
CONSISTENCIA	El contenido encontrado en las distintas partes de la app es consistente entre sí.							X	
	La tipografía es consistente en toda la aplicación.							X	
	La cromática es consistente en toda la aplicación.					X			Rojo del botón de aceptar (√) es alarmante
	El concepto siempre se encuentra presente.							X	
FAMILIARIDAD	La experiencia de usuario se encuentra correctamente homologada. Cada componente de la app parecer formar parte de una sola experiencia.							X	
	Se utiliza un lenguaje que resulta familiar para el usuario.							X	
	La información se presenta de manera accesible y siguiendo un orden lógico.							X	Terminar el juego y pasar al siguiente. Brindar opción de pasar al próximo juego de manera directa
CONFORMIDAD	Las metáforas utilizadas son adecuadas.							X	Uso de la metáfora a la narrativa es interesante
	Se presentan las opciones de forma evidente.							X	
	Las instrucciones de uso son claras y concisas.							X	Revisar temporizado
	Los botones, señales e íconos son fácilmente reconocibles.							X	

Tabla. 15: Herramienta de validación heurística (Diseño).

Elaboración: Autor.

Dentro de la validación con un especialista en diseño, se recomienda la realización de pruebas de contraste, especialmente con los textos de menor tamaño con el fondo gris. Además es importante brindar opciones al usuario como la de avanzar directamente a otros juego, opción de confirmación de compra; y buscar, ordenar y cambiar en bloque las contraseñas dentro del gestor.

Se hace un buen uso de la metáfora en la narrativa, la accesibilidad es positiva, la línea gráfica funciona bien y es coherente con la finalidad del proyecto. Por lo tanto tiene concordancia con los objetivos establecidos.

3.2. Validación con el comitente

Campo: Seguridad en Redes

Nombre: Carlos Castillo

CRITERIO	PARÁMETROS	RANGO							OBSERVACIONES
		-3	-2	-1	0	1	2	3	
VISIBILIDAD	La información que describe la importancia de la privacidad es suficiente.						X		Aumentar ingeniería social
	La información es clara y entendible.							X	Sí
	Se diferencia claramente entre amenazas, métodos de protección.							X	Mejorar entendimiento para alguien que no sepa
	Las herramientas incluidas en la aplicación son fáciles de encontrar.							X	Sí
	Las herramientas incluidas en la aplicación son útiles.							X	La suscripción está muy bien y las herramientas son útiles

CRITERIO	PARÁMETROS	RANGO							OBSERVACIONES
		-3	-2	-1	0	1	2	3	
CONSISTENCIA	El contenido encontrado en las herramientas incluidas, la información brindada, las dinámicas de los juegos y el sistema interactivo, son consistentes entre sí.							X	Sí
	La aplicación ataca a los principales conflictos identificados.							X	Sí
FAMILIARIDAD	Los términos técnicos utilizados son explicados, de manera que sean entendibles para cualquier usuario estudiante.						X		Es necesario mejorar la claridad para quien no conoce las amenazas
	Se identifica la amenaza asociada a cada nivel.							X	Sí
	Las metáforas utilizadas son adecuadas.							X	Sí
	Se ajusta a los requerimientos de la Universidad.							X	El tema y el diseño es pertinente para público joven e incluso para los profesores
CONFORMIDAD	Se distingue claramente el uso de las herramientas expuestas.							X	Sí
	La propuesta responde a las necesidades de la Institución.							X	Sí y es muy necesaria
	Ayuda a solventar las necesidades comunicacionales de la Universidad.						X		Sí sobre el tema, sin embargo tomar en consideración la ingeniería social, especialmente por el manejo de los PIN.
NAVEGACIÓN	Las instrucciones brindadas en cada nivel, permiten entender las interacciones a continuación.							X	Sí

CRITERIO	PARÁMETROS	RANGO							OBSERVACIONES
		-3	-2	-1	0	1	2	3	
CONTROL	La aplicación permite un fácil manejo del perfil de usuario							X	Cambiar el nombre de perfil por el de inicio
RETROALIMENTACIÓN	Se entiende de manera rápida y eficaz los efectos de las acciones y decisiones tomadas en los juegos y app.							X	Sí
RECUPERACIÓN	La recuperación de errores y equivocaciones es rápida y efectiva.							X	Sí
RESTRICCIONES	La restricción para evitar efectuar acciones peligrosas o no adecuadas es efectiva.						X		Es mejor no mostrar las contraseñas en el gestor
FLEXIBILIDAD	Se puede acceder a la información por varios medios.							X	Sí
ESTILO	El diseño invita a que la aplicación sea utilizada.							X	Sí
CORDIALIDAD	Los mensajes y transmisión de información resultan amigables.							X	Sí

Tabla. 16: Herramienta de validación heurística (Comitemte).

Elaboración: Autor.

El especialista remarcó la importancia de incluir el tema de la ingeniería social dentro de la herramienta de diseño. Es importante mejorar también el entendimiento de términos técnicos que pueden causar confusión en un usuario que tiene desconocimiento del tema. Además se considera sustancial el no mostrar las contraseñas dentro del gestor de forma abierta. Menciona de igual manera que la herramienta es muy útil para el contexto, inclusive pudiendo beneficiar a profesores y es necesaria para implementarse dentro de la Universidad.

3.3. Validación de usuario

Carrera: Diseño gráfico y Artes

Edad: 23.6

Gamer: Sí 3; **No** 2

TAREA	TIEMPO	ERRORES	OBSERVACIONES
Completar un juego	3min, 13 seg	Tres de los cinco evaluados no leyeron la historia completa. En uno de los casos la vacuna fue confundida con una pistola, sin embargo, no afectó en la jugabilidad.	Una de las personas percibió el juego como para niños, sin embargo lea grada el hecho de informar. Otros, a pesar de no leer las instrucciones completas entendieron el objetivo del juego. Una persona tuvo problema para entender el juego 1 (no leyó las instrucciones) pero al jugar captó enseguida. En promedio se eliminó entre 20 y 30 enemigos en los primeros intentos del juego 1.
Descargar una APP de seguridad	2min, 44 seg	Ingresaron en otras secciones	La mayor parte de los usuarios se confundieron en encontrar la sección donde se brindan las apps. A pesar que varios entraron en la tienda, les costó encontrar la sección.

TAREA	TIEMPO	ERRORES	OBSERVACIONES
Comprar un objeto	20 seg		Aunque en la mayor parte de los casos no hubo problema en encontrar la sección, hubo dificultar al identificar el uso de los objetos.
Compartir un triunfo	41 seg		En la mayoría no hubo problema. En un par de ocasiones y al inicio no lograron encontrar la función de compartir.
Cambiar la configuración de notificaciones	15 seg	Un usuario de IPhone se confundió al ingresar en el botón correcto, pensando que todo se concentraba en un solo apartado.	En la mayoría de casos no hubo problema.
Generar una contraseña	1min, 12 seg	Ingresaron muchas veces en otras secciones, buscando el acceso a la herramienta.	Esta fue la actividad que mayor dificultad ocasionó en los usuarios. Se demoraron mucho en encontrar la herramienta y, al ingresar en ella, la funcionalidad no estaba clara.
Informarse más acerca de privacidad	30 seg		No hubo ninguna dificultad. La mayoría ocupó entre 5 y 10 segundo y solo una persona se demoró casi 120 segundos porque ingresó a jugar otro juego, por eso el promedio no es muy demostrativo.
Observaciones generales: A los usuarios los juegos les parecieron atractivos y entretenidos, inclusive generando gratas emociones. Es necesario encontrar otras alternativas para narrar la historia y brindar las indicaciones de los juegos. Hay dificultad en encontrar la herramienta de contraseña y la sección de apps en la tienda. Es necesario brindar explicaciones previas para algunas funciones de interacción.			

Tabla. 17: Prueba de usabilidad (Usuario).

Elaboración: Autor.

Entrevista

1.- ¿Cuáles fueron tus mayores dificultades?

No saber para qué sirve lo compra.- No saber para qué sirve el generador de contraseña.- No entender por haber demasiado texto para leer.- No se entendía que había la función de descargar un app.- Al ser un usuario de IPhone está acostumbrada a otro tipo de interfaz.

2.- ¿Tuviste algún problema al entender el funcionamiento de los juegos?

Varios usuarios no tuvieron problema para entender el funcionamiento.- Un usuario no entendió bien el primer juego.-

3.- ¿Tuviste algún problema al entender la información que se te proporcionó?

Los usuarios que no leyeron el texto (historia e indicaciones) tuvieron dificultad en asimilar la información

4.- ¿Qué opinas del uso del color?

Opinan que ayuda a entender bien los elementos, que la cromática atrae y que utiliza colores institucionales en varias ocasiones.

5.- ¿Qué opinas de la apariencia de la app?

Se tiene la sensación que es para jóvenes y genera curiosidad. Los que ingresan a la Universidad pueden sentirse identificados con la Institución. Se maneja una línea homologada. A una persona no le llamó la atención.

6.- ¿Cuál fue tu expectativa de la aplicación?

En unos casos se opina que la expectativa era la de enfrentarse al jefe final. Causa curiosidad el gestor de contraseña. Pensaba que sería simple para pasar el rato.

7.- ¿Para ti, cuál es el propósito de la app?

Enseñar cómo funciona la app en Internet.- Demostrar de forma interactiva cómo proteger tus cuentas.- Entender las amenazas cibernéticas.- Otro usuario tenía la expectativa de informarse con el plus de poder entretenerse (es importante cómo se lo venda, cómo se lo presente).- Fue el de entretenimiento

8.- ¿Qué fue lo mejor/peor del prototipo?

Mejor:

El reto de ganar un juego.- No había visto algo como el gestor de contraseña.- Le gustó la parte interactiva como una forma de aprendizaje.- La información sintetizada.- La simpleza que le recordó a su infancia.

Peor:

Los juegos están sueltos.- Problemas al encontrar el gestor.- Que exista mucho texto.- Estética que no le llama la atención.- Que sea de Android y que la información se encuentre en forma de texto.

9.- ¿Qué tan fáciles fueron las tareas?

No tuvo idea qué hacer en las contraseñas.- Dificultad en el gestor de contraseñas.- Dificultad en descargar una app.- Fácil lo de los logros y le costó el gestor de contraseña.

10.- ¿Qué aspectos cambiarías de la aplicación?

Añadir descripción en los elementos de la tienda.- No le gusta leer indicaciones, cambiarlo.- Disminuir los textos o buscar una forma alternativa de transmitir la información.- La estética.- Que no exista botones redundantes.

En general el propósito de la aplicación se logró entender de manera clara como una herramienta informática para la mayoría de los usuarios, sin embargo, se determinó que el método de transmisión de la información como parte de una historia mostrada de forma textual, no fue del todo efectiva.

Es necesario generar nuevos métodos de presentar las amenazas y objetivos dentro de los juegos.

Uno de los aspectos clave que generó mayor confusión fue el gestor de contraseñas, cuyo propósito no se presentó de manera clara causando conflicto en el entendimiento de la herramienta.

Cierre del documento

Conclusiones

a. En el contexto universitario, las herramientas propuestas en el producto de diseño son consideradas útiles para entender cómo hay que mejorar hábitos y formas de protección general de la información privada.

b. Los estudiantes de la PUCE, cuentan con una conciencia de protección de su privacidad en Internet, aún así se genera desconocimiento y confusión en cuanto a los métodos de protección y las amenazas a los que se encuentran expuestos.

c. La sociedad Ecuatoriana no facilita medios de recuperación ni concientización de la importancia del derecho a la privacidad a pesar de contar con algunas normativas para este fin. Las políticas no van acorde ni son aplicables al contexto.

d. El producto tuvo tres objetivos principales, el de informar, brindar herramientas prácticas para la protección y generar un sentimiento de pertenencia de la herramienta en los estudiantes. Esto se realizó mediante la gamificación de un sistema interactivo para generar una experiencia de usuario.

e. Fue importante tomar en cuenta el concepto de la privacidad por defecto en la implementación de herramientas digitales para la protección de información privada. Además tomando en cuenta principios de diseño interactivo para su implementación y la generación de una interfaz amigable con el usuario.

f. Los actores involucrados mostraron satisfacción y conformidad con los resultados y el funcionamiento del producto, remarcando que es una herramienta que debe seguir en constante evolución.

Recomendaciones

a. Es importante generar adicionalmente al aplicativo, ampliar los métodos para transmitir los conocimientos técnicos asociados a la informática sobre protección de información

b. La forma de comunicación de la información presentada podría mejorarse mediante el uso de técnicas audiovisuales que complementen las dinámicas propuestas.

c. Es indispensable mantener un proceso de retroalimentación constante entre el usuario y el sistema gamificado para asegurar un funcionamiento más efectivo.

d. Se puede mejorar las indicaciones dentro de la interfaz, que permitan identificar rápidamente para que sirve cada componente.

e. Expandir e implementar más versatilidad dentro de los personajes para generar mayor identificación del usuario y el sistema de logros y recompensas.

f. Se recomienda implementar distintos niveles de dificultad en las interacciones para gente con mayor o menor experiencia.

Referentes bibliográficos

Libros:

Amell, C. (2015). Flat ILLUSTRATION. (J. Minguet, Ed.). Barcelona, España: Instituto Monsa de Ediciones.

Aranda, D., Gómez, S. y Navarro, V. (2015). Game & Play. Diseño y análisis del juego, el jugador y el sistema lúdico. España: Editorial UOC, S.L.

Aljure, A. (2014). Plan estratégico de comunicación: método y recomendaciones prácticas para su elaboración. Colombia: UOC.

Ballesteros, L. (2006). La Privacidad Electrónica. Valencia, España: Editorial TIRANT LO BLANCH.

Bennet, A., Vulpinari, O. (2011). Icograda Design Education Manifesto 2011. (p. 158). Italia: Grafiche Tintoretto.

Benyon David. (2013). Designing Interactive Systems. A comprehensive guide to HCI, Ux and interaction designe (3erd New E). Harlow, United Kingdom: Person Education Limited.

Coates, K., Ellison, A. (2014). Introducción al Diseño de Información. (p. 23-24). Buenos Aires, Argentina: Editorial Parramón.

Consejo Nacional de Planificación. (2017). Plan Nacional de Desarrollo 2017-2021-Toda una Vida. Quito, Ecuador: Senplades.

Costello, K., & Cornella, S. (2018). Gartner Says Worldwide Sales of Smartphones Returned to Growth in First Quarter of 2018. Recuperado 28 de julio de 2018, de https://www.gartner.com/

newsroom/id/3876865

Frascara, J. (2012). El diseño de comunicación. Buenos Aires, Argentina: Ediciones Infinito.

Ferran, T. (2015) Gamificación: Motivar jugando. Barcelona, España: Editorial UOC

Fullerton, T. (2008). Game Design Workshop: A Playcentric Approach to Creating Innovative Games. Technology. https://doi.org/10.1007/s13398-014-0173-7.2

Gobierno Nacional de la República del Ecuador. (2008). Constitución de la República del Ecuador. Ecuador: Publicada en el Registro Oficial No. 449.

Hernández, R., Fernández, C. y Baptista, P. (2006). Metodología de la investigación. MacGraw-Hill / Interamericana.

Lupton, E. (2014). Tipografía e pantalla. Ed. Gustavo Gili

Milton, A. y Rodgers, P. (2013). Métodos de investigación para el diseño de productos. Barcelona: BLUME.

Morin, E., 1981. La méthode, tome 1: La Nature de la nature. SEUIL.

Muñoz, S. (2000). La regulación de la red. Poder y derecho en Internet. Madrid, España: Taurus.

Nielsen, J., Budiu, R. (2013) Usabilidad en dispositivos móviles. Madrid, España: Ediciones Anaya Multimedia

Oficina de seguridad de la información (OSI-PUCE), (2012), POLÍTICA DETALLADA Y NORMAS DE SEGURIDAD LÓGICA DE LA

INFORMACIÓN PROCESADA CON SISTEMAS INFORMÁTICOS. Pontificia Universidad Católica del Ecuador.

Pérez de Acha, G. (2016). Hacking Team, Malware para la vigilancia en América Latina. ONG. Derechos Digitales

Pratt, A., Nunes, J. (2013). Diseño Interactivo Teoría y aplicación del DCU. Barcelona, España: Editorial Océano.

Preece Jennifer, Rogers Yvonne, & Sharp Helen. (2002). Interaction Design, beyond human-computer interaction. (Santor Ken, Ed.). New York USA: John Wiley & Sons, Inc.

Sheinsohn, D. (2009) La comunicación Estratégica, Edit. GRANICA, BUENOS AIRES.

Steane, J. (2016). Fundamentos del diseño interactivo. Principios y procesos que todo diseñador debe conocer (1ra. Edici). Barcelona, España: Promopress.

Tomeo, F. (2014). Redes sociales y tecnologías 2.0. Buenos Aires, Argentina: Editorial Astrea SRL.

Wood, D. (2015). Diseño de interfaces. Barcelona, España: Parramón Arts & Design.

En Internet:

Access Now. “Statement for online Freedom of Expression, Anonymity, and Privacy in Ecuador”. Access Now. Recuperado el 27 de enero del 2017 de https://www.accessnow.org/ecuador-free-expression-letter/.

Association for Progressive Communications (2017). Digital Security Fist Aid Kid Human Rights Defenders (Second Edition). Association for progressive Communications. Recuperado de https://www.apc.org/en/irhr/digital-security-first-aid-kit

Bogado David. “Hacking Team y Ecuador: Pronunciamiento En Defensa De La Privacidad”. Electronic Frontier Foundation. Recuperado el 13 de julio de 2017 de https://www.eff.org/node/86861.

Bravo, D. “Ecuador se muestra vulnerable a ciberataques”. El Comercio. Recuperado el 26 de julio del 2016 de http://www.elcomercio.com/actualidad/ecuador-muestra-vulnerable-ciberataques.html.

Cavoukian, A. (2015). “Privacy by Design The 7 Foundational Principles ”. Information and privacy commissioner of Ontario. Recuperado el 13 de julio de 2017 de https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf.

Consejo de Europa, “CONVENIO Nº 108 DEL CONSEJO DE EUROPA, de 28 de Enero de 1981, PARA LA PROTECCION DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARACTER PERSONAL”. Recuperado el 27 de enero del 2017 en: http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf.

Consejo de Derechos Humanos (2016). “El derecho a la privacidad en la era digital”. Asamblea General de las Naciones Unidas. Recuperado de http://www.acnur.org/fileadmin/Documentos/BDL/2017/10904.pdf

Computerworld (2007). “Internet es un reflejo de la sociedad” según Cerf. Recuperado de http://www.computerworld.es/archive/internet-es-un-reflejo-de-la-sociedad-actual-segun-cerf#.

Christensson, P. (2012). “Sprite Definition”. TechTerms. Recuperado el 25 de septiembre de 2018 de https://techterms.com/definition/sprite.

Digiteen. (2008). “Digital Security and Safety”. Digiteen. Recuperado el 14 de julio de 2017 de https://digiteen.wikispaces.com/page/code/Digital+Security+and+Safety.

Bestuzhev, Dmitry. (2015). Twitter. [Tweet], Recuperado el 14 de julio de 2017 de https://twitter.com/AperturaRadical/timelines/714329431288913920.

DHS. (2012). DHS Handbook for Safeguarding Sensitive Personally Identifiable Information. Homeland Security. Recuperado de https://www.dhs.gov/publication/dhs-handbook-safeguarding-sensitive-pii

EFF. (2015). “Why Metadata Matters”.EFF. Recuperado el 15 de julio de 2017 de https://ssd.eff.org/en/module/why-metadata-matters.

EFF. (2015). “Keeping Your Data Safe”. EFF. Recuperado el 27 de enero del 2017 de https://ssd.eff.org/en/module/keeping-your-data-safe.

Encyclopedia. (2010). “What is phishing?”. Encyclopedia by Kaspesky lab. Recuperado de https://encyclopedia.kaspersky.com/knowledge/what-is-phishing/

Frenkel, B. (2015). “Power Great Gaming with New Analytics from Play Games”. Google. Recuperado el 25 de septiembre de 2018 de https://android-developers.googleblog.com/2015/03/power-great-gaming-with-new-analytics.html.

Garay, V. (2013). ” El anonimato en Internet también es un derecho”. Derechos Digitales. Recuperado el 15 de julio de 2017 de https://derechosdigitales.org/6173/el-anonimato-es-un-derecho/.

Kaye, D. (2015). “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye”. OHCHR. Recuperado el 27 de enero de 2017 de http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx.

El Economista. (2015). “Ciberataques a Ecuador”. Ecuador. El Economista. Recuperado el 17 de agosto de 2017 de “¿Qué hacen twitter y Facebook con sus datos personales?”. 21/05/15. México. Internet. http://eleconomista.com.mx/finanzas-personales/2015/05/21/que-hacen-twitter-facebook-sus-datos-personales.

Material Design (2018). Typography - Style - Material Design. Recuperado 30 de julio de 2018, de https://material.io/archive/guidelines/style/typography.html#typography-language-categorization

Mignano, M. (2016). “Game Analytics: Analyze And Improve Your Game With Analytics”Recuperado el 25 de septiembre de 2018 de http://gamedevelopertips.com/game-analytics-analyze-games/

Nyst, C. (2013). “MULTIMEDIA TRAINING KIT INTERNET RIGHTS ARE HUMAN RIGHTS: THE RIGHT TO PRIVACY HANDOUT”. Association for progressive communications. Recuperado el 14 de julio de 2017 de http://www.itrainonline.org/itrainonline/mmtk/APC_IRHRCurriculum_Privacy_Handout.pdf

ONG Derechos Digitales (2016). “¿Quién necesita anonimato?”. [Actualización de estado de facebook] Recuperado el 17 de agosto de 2017 de https://www.facebook.com/permalink.php?story_fbid=1012912762119700.

Naciones Unidas (1948). “Declaración Universal de Derechos Humanos” Naciones Unidas. Recuperado de http://www.un.org/es/documents/

udhr/.

Play Console (2018). Sube una app. Recuperado 25 de septiembre de 2018, de https://support.google.com/googleplay/android-developer/answer/113469?hl=es-419

Privacy International. (2014). “What is privacy?”. Privacy International. Recuperado el 17 de agosto de 2017 de Internet. https://www.privacyinternational.org/node/54.

Privacy International. (2014). “Data Protection”. 12/11/2014 Internet. https://www.privacyinternational.org/node/44.

SecureList. (2016). “Kaspersky Security Bulletin. El spam en 2015”. Secure list. Recuoerado de https://securelist.lat/analysis/boletin-de-seguridad-de-kaspersky/82540/kaspersky-security-bulletin-spam-and-phishing-in-2015/.

Security in a Box. (2009). “Tácticas”. Security in a box. Recuperado el 17 de agosto de 2017 de https://securityinabox.org/es/tactics/legacy.

Tactical Tech. (2016). “¿Qué son los rastros digitales?”. Me and my Shadow. Recuperado el 17 de agosto de 2017 de https://myshadow.org/es/digital-traces-content-and-metadata.

Trend Micro Incorporated. (2015). “¿Qué constituye un ataque cibernético?”. NEC. Recuperado el 27 de enero de 2017 de http://mex.nec.com/es_MX/solutions/security/safety/info_management/cyberattack.html.