PROCESO DE DISEÑO EN SEGURIDAD USABLE Y AUTENTICACIÓN MEDIANTE UN ENFOQUE CENTRADO EN EL USUARIO

PAULO CÉSAR REALPE MUÑOZ

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Popayan, Colombia
2017

PAULO CÉSAR REALPE MUÑOZ

PROCESO DE DISEÑO EN SEGURIDAD USABLE Y AUTENTICACIÓN MEDIANTE UN ENFOQUE CENTRADO EN EL USUARIO

Tesis grado presentada a la Facultad de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca para la obtención del título de:

Doctor en:
CIENCIAS DE LA ELECTRÓNICA

Director:
Ph.D. César Alberto Collazos
Codirector:
Ph.D. Julio Ariel Hurtado
Asesor Externo:
Ph.D. Jaime Velasco Medina

Comisión Evaluadora
Ph.D. Jaime Muñoz Arteaga
Ph.D. Andrés Solano Alegría
Ph.D. Juan Manuel González
Ph.D. Luis Merchán Paredes

Universidad del Cauca
Facultad en Electrónica y Telecomunicaciones
Departamento de Sistema
Popayán, Colombia
2017

A mis padres por acompañarme en este recorrer tras una meta. En especial a mi amada esposa y mi querido hijo.

Agradecimientos

A Dios que es mi guía y mi soporte en los momentos más difíciles de mi vida.

A mi mi bella y amada familia por apoyarme incondicionalmente para alcanzar una nueva meta. A mis padres Ignacio Realpe y Olga Muñoz por su amor, paciencia, tiempo y fortaleza para alcanzar mis sueños.

A mi esposa Martha Isabel por su amor y apoyo en este proceso y a mi querido y amado hijo Juan Andres Realpe por ser mi mas grande bendición.

Al profesor César Collazos, por darme esta oportunidad, por guiarme, por levantarme y estar ahí siempre, espero la vida me de la oportunidad de retribuir toda su dedicación y apoyo.

Al profesor Jaime Velasco Medina, por su apoyo incondicional en la realización de este trabajo y abrirme las puertas para este proceso.

Al profesor Toni Granollers, por su conocimiento, aportes y su colaborado desinteresa en la realización de esta tesis.

Al profesor Julio Hurtado, por su tiempo, paciencia, apoyo y por darme momentos de tranquilidad y ánimo.

Al profesor Eduardo Fernández de la Universidad Atlántica de la Florida (FAU) por sus aportes y permitirme realizar mi estancia en tan importante universidad.

A las personas del grupo IDIS y GRIHO que me colaboraron de alguna u otra forma en la realización de este trabajo.

Al comité del Doctorado por su gran apoyo en cada una de las actividades. A la Universidad del Cauca y a COLCIENCIAS, por el soporte económico brindado que hicieron posible el desarrollo de mis estudios.

Resumen

Actualmente, la seguridad informática es una de las tareas mas importantes y más cuando día tras día, complejas computadoras se desarrollan los cuales permiten procesar una mayor cantidad de información en un tiempo mas corto, esto hace a la seguridad informática un factor clave para las organizaciones. Sin embargo, es habitual encontrar en la literatura que los usuarios encuentran la seguridad y la privacidad difíciles de comprender. Es por esto que la seguridad representa un objetivo secundario para la mayoría de personas que utilizan sistemas informáticos. Como consecuencia de lo anterior, los usuarios tienen a ignorar las características de seguridad del sistema generando con esto decisiones equivocadas y poniendo en riesgo la información privada que pueda tener. El campo de la Seguridad Usable (del inglés *Usable Security* o USec) es el área que investiga este tipo de problemas, cuyo principal objetivo es el diseño de características de seguridad y privacidad que puedan ser fáciles de usar y entender por parte de los usuarios. De lo anterior podemos decir que la Seguridad Usable permite encontrar un equilibrio o *trade-off* entre las características de seguridad y usabilidad. Sin embargo, encontrar este balance es un reto debido a que estos dos atributos en ocasiones son contrarios.

Este proyecto de investigación esta enfocada a encontrar principios para seguridad usable y autenticación de usuario junto con un mecanismo de evaluación cualitativo y cuantitativo el cual permita que el *trade-off* entre seguridad y usabilidad se pueda llevar a cabo. Para encontrar estos principios, un proceso de desarrollo es propuesto el cual consta de tres etapas: desarrollo, revisión y aplicación. Este proceso permite tener análisis cualitativo y cuantitativo en la aplicación de estudio teniendo en cuenta los aspectos de la seguridad usable. Desde nuestro conocimiento, no existe en la literatura un proceso cualitativo y cuantitativo que describa como aplicar una evaluación heurística en el campo de la seguridad usable. Como parte del análisis cuantitativo, el mecanismo de evaluación propuesto presenta un nivel del grado de seguridad usable y otros atributos donde la seguridad es parte esencial. Para lograr esto se establecen niveles de importancia, de severidad y de impacto para los principios de diseño encontrados. Con base en lo anterior y teniendo en cuenta las posibles vulnerabilidades que pueda tener el sistema, se presenta la primera propuesta del nivel de riesgo utilizando los principios como pieza clave.

A partir de los principios encontrados para seguridad usable y autenticación de usuario junto con su evaluación, en esta investigación se propone incluir estos dos elementos en un modelo de diseño centrado en el usuario muy conocido por la comunidad académica

y empresarial, el modelo MPIu+a. Debido a que este modelo esta orientado al diseño de sistemas interactivos altamente usables y accesibles, consideramos que hace falta incluir la seguridad como elemento fundamental. Aunque la integración que se propone entre el modelo MPIu+a y las guías de diseño junto con la evaluación es una version preliminar, mas estudio es necesario para establecer un modelo adecuado. Sin embargo, consideramos que puede ser un punto de partida para constituir futuras mejoras.

Palabras clave: Usabilidad, Seguridad, Seguridad Usable, Autenticación, Heurística, Evaluación.

Abstract

Today, computer security is one of the most important tasks, and when day after day, complex computers are developed which allow to process more information in a shorter time, this makes computer security a key factor for organizations . However, it is common to find in the literature that users find security and privacy difficult to understand. This is because security is a secondary goal for most people using computer systems. As consequence of the above, users have ignore the security features of the system generating with this, mistaken decisions and putting at risk the private information that they may have. The field of Usable Security (Usable Security or USec) is the area that investigates these types of problems, whose main objective is the design of security and privacy features that can be easy to use and understand for users. From the above, we can say that the Usable Security allows to find a balance or *trade-off* between the characteristics of security and usability. However, finding this balance is a challenge because these two attributes are sometimes inversely proportional.

This research project is focused on finding principles for usable security and user authentication, together with a qualitative and quantitative evaluation mechanism which allows the *trade-off* between security and usability can be carried out. To find these principles, a development process is proposed which consists of three stages: development, review and application. This process allows to have qualitative and quantitative analysis in the study application taking into account elements of usable security. From our knowledge, there is no qualitative and quantitative process in the literature describing how to apply a heuristic evaluation in the field of usable security. As part of the quantitative analysis, the proposed evaluation mechanism presents a nivel of the degree of usable security and other attributes where security is an essential part. To achieve this we establish levels of importance, severity and impact for the design principles found. Based on the above and taking into account the possible vulnerabilities that the system may have, the first proposal of the risk level is presented using the principles as a key piece.

From the principles found for usable security and user authentication along with its evaluation, this research proposes to include these two elements in a user-centered design model well known by the academic and business community, model MPIu+a. Because this model is oriented to the design of highly usable and accessible interactive systems, we consider that it is necessary to include security as a fundamental element. Although the proposed integration between the MPIu+a model and the design guides together with

the evaluation is a preliminary version, more study is necessary to establish an adequate model. However, we believe that it can be a starting point for future improvements..

Keywords: Usability, Security, Usable Security, Authentication, Heuristic, Evaluation

Contenido

1. Introducción **1**
- 1.1. Planteamiento del Problema . . . 3
- 1.2. Objetivos . . . 5
  - 1.2.1. Objetivo General . . . 5
  - 1.2.2. Objetivos Específicos . . . 5
- 1.3. Hipótesis . . . 6
  - 1.3.1. Hipótesis Alternativa . . . 6
  - 1.3.2. Hipótesis Nula . . . 6
- 1.4. Principales contribuciones . . . 6
- 1.5. Organización del documento . . . 7

2. Base conceptual **9**
- 2.1. Introducción . . . 9
- 2.2. Interacción Humano-Computador . . . 9
- 2.3. Diseño Centrado en el Usuario . . . 12
- 2.4. Usabilidad . . . 14
  - 2.4.1. Evaluación de la Usabilidad . . . 15
- 2.5. Seguridad . . . 20
  - 2.5.1. Propiedades de Seguridad . . . 21
  - 2.5.2. Privacidad . . . 23
  - 2.5.3. Evaluación de Seguridad . . . 24
- 2.6. Seguridad Usable . . . 25
  - 2.6.1. Integrando Seguridad y Usabilidad . . . 27
  - 2.6.2. Evaluación de Seguridad Usable . . . 28
  - 2.6.3. Principios de Seguridad Usable . . . 29
- 2.7. Integrando Usabilidad y Seguridad en el Proceso de Desarrollo . . . 34
  - 2.7.1. Ingeniería de la Seguridad . . . 35
  - 2.7.2. Procesos de Diseño para Seguridad Usable . . . 39
  - 2.7.3. Metodología MPIu+a . . . 42
- 2.8. Métodos de Autenticación . . . 45
  - 2.8.1. Elementos de Autenticación . . . 45
  - 2.8.2. Factores y Métodos de Autenticación . . . 46
  - 2.8.3. Criterios de Calidad . . . 52
  - 2.8.4. Evaluación de Autenticación . . . 53

3. Proceso de Desarrollo Heurístico **56**
3.1. Introducción . . . 56
3.2. Justificación de la Propuesta de Desarrollo Heurístico . . . 57
3.3. Proceso de Desarrollo Heurístico y Evaluación . . . 58
3.3.1. Etapa 1: Desarrollo Heurístico . . . 63
3.3.2. Etapa 2: Revisión con Expertos . . . 64
3.3.3. Etapa 3: Aplicación con Expertos/Usuarios . . . 65
3.4. Integrado el Proceso de Desarrollo al DCU . . . 66
3.5. Etapa 1: Desarrollo Heurístico . . . 68
3.5.1. Planificar el Proceso Heurístico . . . 68
3.5.2. Revisión de la literatura . . . 69
3.5.3. Identificar y Nombrar las reglas heurísticas de acuerdo a la Literatura 70
3.5.4. Identificar y Adaptar las sub-heurísticas de acuerdo a la Literatura 76
3.5.5. Modificar o Mejorar el Conjunto . . . 78
3.6. Especificación de USec a través de Atributos de Calidad . . . 78
3.7. Discusión . . . 81
3.8. Conjunto Heurístico Preliminar para USec y Autenticación . . . 82
3.8.1. Usabilidad . . . 82
3.8.2. Seguridad y Privacidad . . . 90
3.8.3. Accesibilidad . . . 94
3.8.4. Operabilidad . . . 95
3.8.5. Fiabilidad . . . 96
3.8.6. Desempeño . . . 97

4. Revisión Heurística del Proceso de Desarrollo **99**
4.1. Grado de Importancia . . . 99
4.2. Revisión Heurística . . . 101
4.2.1. Etapa de Planeación . . . 101
4.2.2. Etapa de Ejecución . . . 103
4.2.3. Etapa de Análisis de resultados . . . 104
4.3. Discusión . . . 115
4.4. La CaixaBank . . . 117
4.5. Conjunto Final para USec y Autenticación . . . 117
4.5.1. Usabilidad . . . 118
4.5.2. Seguridad y Privacidad . . . 127
4.5.3. Accesibilidad . . . 131
4.5.4. Operabilidad . . . 132
4.5.5. Fiabilidad . . . 133
4.5.6. Desempeño . . . 135

5. Aplicación con Expertos y Usuarios **137**
5.1. Introducción . . . 137
5.2. Formulación Cuantitativa de Evaluación . . . 137
5.2.1. Justificación de la necesidad de una métrica cuantitativa . . . 138

5.2.2. Grado de Severidad e Impacto . . . 138
5.2.3. Formulación Matemática para la Evaluación . . . 140
5.2.4. Análisis de Riesgo . . . 144
5.3. Objeto de estudio: Red social Facebook . . . 145
5.3.1. Justificación en la selección del sitio web . . . 145
5.3.2. La red social Facebook . . . 146
5.4. Evaluación con Expertos: Caso Facebook . . . 147
5.4.1. Participantes de la evaluación . . . 147
5.4.2. Etapa de Planeación . . . 147
5.4.3. Etapa de Ejecución . . . 149
5.4.4. Etapa de Análisis de Resultados. . . . 150
5.4.5. Discusión . . . 155
5.5. Evaluación con Usuarios: Caso Facebook . . . 156
5.5.1. Justificación en la selección del sitio web . . . 156
5.5.2. Justificación de selección del método de evaluación. . . . 157
5.5.3. Etapa de Planeación . . . 157
5.5.4. Etapa de Ejecución . . . 160
5.5.5. Etapa de Análisis de resultados . . . 161
5.5.6. Discusión . . . 168
5.6. Evaluación con Expertos: Caso E-Banking . . . 169
5.6.1. Justificación para la Evaluación . . . 169
5.6.2. Desarrollo . . . 169
5.6.3. Resultados . . . 172
5.6.4. Discusión . . . 174
5.7. Voto Electrónico basado en Eye Tracking . . . 174
5.7.1. Tecnología de *Eye tracking* . . . 174
5.7.2. Participantes de la evaluación . . . 175
5.7.3. Etapa de Planeación . . . 176
5.7.4. Etapa de Ejecución . . . 179
5.7.5. Etapa de Análisis de Resultados . . . 180
5.7.6. Discusión . . . 189

6. Proceso de Diseño para Seguridad Usable 192
6.1. Introducción . . . 192
6.2. Justificación de un proceso de diseño para USec . . . 193
6.3. La Seguridad y la Ingeniería del Software . . . 194
6.4. Análisis comparativos de trabajos relacionadados . . . 195
6.5. ¿Por qué MPIu+a? . . . 198
6.6. Proceso de diseño para USec y Autenticación . . . 199
6.6.1. Análisis de Requisitos . . . 201
6.6.2. Diseño . . . 206
6.6.3. Evaluación . . . 206
6.7. Discusión . . . 209

7. Conclusiones y Trabajo Futuro **210**
7.1. Conclusiones . . . 210
7.2. Limitaciones . . . 215
7.3. Trabajo Futuro . . . 215
7.4. Publicaciones . . . 216
7.4.1. Publicaciones en Revistas . . . 216
7.4.2. Publicaciones en Eventos . . . 217
7.5. Trabajos de Grado Dirigidos . . . 217

A. Análisis comparativo de los métodos de Autenticación **218**

B. Invitación para Socios de AIPO **221**

C. Documento guía para la revisión **222**

D. Recomendaciones para Seguridad Usable y Autenticación **224**
D.1. Usabilidad . . . 224
D.2. Seguridad y Privacidad . . . 227
D.3. Accesibilidad . . . 229
D.4. Operabilidad . . . 230
D.5. Fiabilidad . . . 230
D.6. Desempeño . . . 231

E. Encuesta de Clasificación Adjetiva **232**

F. Documento Guía para las sub-heurísticas de grado de importancia S **237**

G. Documento Guía para las sub-heurísticas de grado de importancia SS y SSS **244**

H. Acuerdo de confidencialidad **251**

I. Información proporcionada a los usuarios para la aplicación de Facebook **253**

J. Documentos para la Prueba de *Eye tracking* **260**

Bibliografía **269**

Lista de Figuras

2.1. Estructura del Capítulo 2 . . . 10
2.2. Principales disciplinas relacionadas con el HCI . . . 11
2.3. Interdependencias de las actividades del Diseño Centrado en el Humano . . . 12
2.4. Marco de trabajo de usabilidad . . . 15
2.5. *Honeycomb* de las propiedades de seguridad . . . 22
2.6. Atributos de privacidad . . . 23
2.7. Una definición sobre la relación entre privacidad y seguridad . . . 24
2.8. Área de la seguridad usable . . . 25
2.9. Fases del proceso de desarrollo de la ingeniería de la seguridad . . . 35
2.10. Marco de trabajo para desarrollar productos seguros . . . 37
2.11. Modelo de ciclo de vida de desarrollo para seguridad por Microsoft . . . 38
2.12. Marco de integración de Desarrollo de la Seguridad . . . 39
2.13. Proceso de diseño seguro AEGIS . . . 40
2.14. Ingeniería de la seguridad centrada en el usuario . . . 41
2.15. Modelo propuesto para equilibrar los requerimientos de seguridad y usabilidad 42
2.16. Metodología MPIu+a . . . 43
2.17. Elementos del proceso de autenticación . . . 46

3.1. Estructura del Capítulo 3 . . . 56
3.2. Proceso de tres fases para desarrollar heurísticas para USec y Autenticación 61
3.3. Proceso de desarrollo y evaluación heurística resumido . . . 61
3.4. Proceso de desarrollo y evaluación heurística . . . 62
3.5. Actividades para la etapa de desarrollo heurístico para USec y autenticación 63
3.6. Actividades para la etapa de validación con expertos . . . 64
3.7. Actividades para la etapa de aplicación con expertos/usuarios . . . 65
3.8. Integración del proceso de desarrollo y la ISO 9241-210 . . . 67
3.9. Componentes del conjunto heurístico para USec . . . 77
3.10. Estandard ISO 25010:2011 . . . 79
3.11. Atributos para USec y Autenticación de usuario . . . 80

4.1. Estructura del Capítulo 4 . . . 99
4.2. Herramienta de MS Excel para la revisión heurística. . . . 102
4.3. Categorización para todos los atributos. . . . 107
4.4. Grado de importancia para todos los atributos. . . . 110

5.1. Estructura del Capítulo 5 . . . 137
5.2. Matriz de riesgo para USec . . . 145
5.3. Planilla de las sub-heurísticas USec para evaluar. . . . 150
5.4. Promedios para USec y el impacto. . . . 151
5.5. Matriz de riesgo para Facebook. . . . 152
5.6. Distribución de éxito. . . . 162
5.7. Tiempo para realizar las tareas. . . . 163
5.8. Tiempo total para realizar las tareas por cada usuario. . . . 164
5.9. Ejemplo de AoI para el censo. . . . 181
5.10. Las barras de error representan el error estándard de la media. . . . 183
5.11. Diagrama de cajas y bigotes para las tareas. . . . 183
5.12. Barras de error del promedio y diagrama de cajas para autenticación. . . . 184
5.13. Tendencia SUS para cada participante. . . . 186
5.14. Mapa de mirada y calor para el censo UdL. . . . 187
5.15. Mapa de mirada y calor para autenticación usando Helios. . . . 188
5.16. Mapa de mirada para votación usando UdL y Helios. . . . 188
5.17. Mapa de calor para confirmar voto usando UdL y Helios. . . . 189

6.1. Estructura del Capítulo 6 . . . 192
6.2. Aproximación gráfica del MPIu+a con los resultados del trabajo (MPIu+a+s) 201

Lista de Tablas

2.1. Ventajas y desventajas de cada método de evaluación de usabilidad 17
2.2. Ventajas y desventajas de la evaluación heurística 19
2.3. Clasificación de los factores de autenticación 47

3.1. Actividades de metodologías para el desarrollo de heurísticas USec. 60
3.2. Análisis comparativo heurístico para usabilidad 71
3.3. Análisis comparativo de atributos 71
3.4. Artículos encontrados en bases de datos. 78
3.5. Número de sub-heurísticas por cada Atributo 80
3.6. Número de sub-heurísticas para usabilidad 81
3.7. Sub-heurísticas para Usabilidad. 82
3.8. Sub-heurísticas para seguridad y privacidad. 90
3.9. Sub-heurísticas para accesibilidad. 94
3.10. Sub-heurísticas para operabilidad. 95
3.11. Sub-heurísticas para fiabilidad. 96
3.12. Sub-heurísticas para desempeño. 97

4.1. Grado de importancia 100
4.2. Expertos participantes de la revisión heurística. 103
4.3. Categorización 105
4.4. Peso por área de conocimiento. 105
4.5. Categorización para Usabilidad 106
4.6. Categorización para Atributos 107
4.7. Valor cuantitativo para el grado de importancia 108
4.8. Grado de importancia para Usabilidad 109
4.9. Grado de importancia para Atributos 109
4.10. Comentarios de los expertos de las sub-heurísticas eliminadas. 111
4.11. Resumen con base en los comentarios de los expertos para Usabilidad. . . . 113
4.12. Resumen con base en los comentarios de los expertos para los atributos. . . 114
4.13. Número de sub-heurísticas por cada Atributo 115
4.14. Número de sub-heurísticas para usabilidad 116
4.15. Sub-heurísticas para Usabilidad (después de la revisión). 118
4.16. Sub-heurísticas de Seguridad y privacidad (después de la revisión). 127
4.17. Sub-heurísticas de Accesibilidad (después de la revisión). 131

4.18. Sub-heurísticas de Operabilidad (después de la revisión). 132
4.19. Sub-heurísticas de Fiabilidad (después de la revisión). 133
4.20. Sub-heurísticas de Desempeño (después de la revisión). 135

5.1. Nivel de Severidad para USec. 139
5.2. Nivel de Impacto para USec. 140
5.3. Perfil de los encuestados. 142
5.4. Clasificación adjetiva para el nivel de USec. 143
5.5. Clasificación adjetiva para el nivel de impacto. 144
5.6. Clasificación adjetiva para vulnerabilidad. 145
5.7. Expertos participantes de la evaluación heurística. 148
5.8. Resultados para el índice USec y el impacto. 151
5.9. Clasificación adjetiva para el índice USec y el impacto. 151
5.10. Clasificación adjetiva para la vulnerabilidad y el impacto. 152
5.11. Demografía de los participantes. 158
5.12. Tareas a realizar en el sitio web Facebook.com 159
5.13. Nivel de dificultad de las tareas. 164
5.14. Promedio de respuestas de los cuestionarios. 166
5.15. Escala USec (Tomado de [150]) 172
5.16. Resultado final, USec general (Tomado de [150]) 173
5.17. Perfil de los participantes (Total n=18) 177
5.18. Tareas a realizar para cada aplicación. 178
5.19. Promedio en las áreas de interés para UdL 182
5.20. Promedio en las áreas de interés para Helios 182
5.21. Promedio del número de fijaciones y duración en AoI para la autenticación 184
5.22. Análisis de promedios usando *t-test* 185
5.23. System Usability Scale (SUS) 186

6.1. La seguridad dentro del desarrollo del software. 195
6.2. Comparación con los trabajos de investigación relacionados. 197
6.3. Comparación MPIu+a y trabajos relacionados USec. 200
6.4. Actividades USec para las fases del modelo MPIu+a. 202

7.1. Relación entre los objetivos y resultados de la investigación. 214

A.1. Análisis comparativo resumido de los métodos de autenticación 218

C.1. Grado de importancia 223
C.2. Categorización 223

D.1. Requerimientos para Usabilidad. 227
D.2. Requerimientos para seguridad y privacidad. 229
D.3. Requerimientos para Accesibilidad. 229
D.4. Requerimientos para Operabilidad. 230
D.5. Requerimientos para Fiabilidad 231
D.6. Recomendaciones para desempeño. 231

Capítulo 1

Introducción

Uno de los mayores desafíos que enfrentan muchas organizaciones, sean públicas o privadas, está en proporcionar acceso a la información útil y segura a las personas. Este acceso puede ser provisto por métodos de autenticación los cuales verifican la identidad de las personas. El conocimiento de estos métodos es importante para organizaciones que necesitan de métodos de identificación fuertes, métodos que sean importantes en la estrategia de seguridad de la información, con el fin de evitar que terceros o entidades no autorizadas tengan acceso a esta información, especialmente para organizaciones cuyo bien más preciado son sus datos [1].

La verificación de la identidad de una persona es un tema trascendental, teniendo en cuenta la posibilidad de fraude o robo de identidad. Si la seguridad se ve comprometida, la privacidad es probable que también se vea comprometida. En los sistemas de información con respecto a las transacciones de dinero y la información personal, es fundamental disponer de métodos de identificación robusto con el fin de asegurar la protección contra el fraude o fuga de información. La pregunta es si el nivel de seguridad afecta la usabilidad del sistema en general [2].

Braz & Robert [3] afirman que aunque la seguridad y la usabilidad son esenciales en el proceso de autenticación, los requisitos para tener un alto nivel de seguridad manteniendo la usabilidad, puede generar conflictos entre si. Estos conflictos entre la seguridad y la usabilidad pueden ser minimizados mediante el uso de algunos criterios de diseño tales como: minimizar las acciones del usuario, entender qué acciones de seguridad son requeridas, ofrecer realimentación para prevenir errores, la carga mental y física de las acciones de seguridad debe ser tolerable y los conceptos de seguridad deben ser intuitivos para los usuarios [4][5].

Un enfoque en la integración de usabilidad y seguridad es el desarrollo de aplicaciones de seguridad centrada en el usuario [6]. Este enfoque tiene en cuenta las necesidades de los usuarios como objeto principal para definir el modelo de seguridad, interfaz o características de un sistema. La seguridad centrada en el usuario se ha identificado como un aspecto importante en la seguridad informática, además, influye en el ciclo de vida del

desarrollo software. Zurko [7] define el concepto de seguridad centrada en el usuario como "*modelos de seguridad, mecanismos, sistemas y software que tienen en la usabilidad su principal objetivo*". Además, identifica tres desafíos para la comunidad investigadora: aplicar los principios de diseño de la interacción humano-computador HCI (por sus siglas en inglés *Human-Computer Interaction*) y sus métodos de evaluación a sistemas seguros, proporcionar mecanismos y modelos de seguridad para software colaborativo, y diseñar características de seguridad directamente por los usuarios.

Los criterios de usabilidad (también denominados a veces como principios, normas, directrices o heurísticas) representan el manual de un diseñador de HCI [8]. A menudo forman parte de un conjunto de directrices o metas generales que un producto de software determinado o el diseño debería cumplir. Mientras que algunos investigadores de usabilidad trabajan en la producción de resultados teóricos que pueden ser utilizados con éxito para guiar el diseño inicial de la interfaz de usuario, muy pocos principios de usabilidad para seguridad son lo suficientemente robustos como para ser de aplicación general y lo suficientemente específico como para influir directamente en las decisiones de ingeniería, como es en el caso de los métodos de autenticación [6].

Aunque la investigacion en el campo de la seguridad y usabilidad ha ido icrementándose, encontrar un equilibrio entre la usabilidad y seguridad es una tarea complicada. Esto es debe principalmente a que es necesario combinar métodos y resultados del HCI con métodos y resultados muy diferentes en seguridad haciéndolo un área del conocimiento muy complejo. Algunos estudios donde se intenta aborar este equilibio se encuentran la evaluación de autenticación de documentos mediante firmas digitales [9], barras de herramientas de seguridad [10], estudios de usuarios sobre seguridad [11], principios de diseño y patrones para los sistemas informáticos que sean seguros y usables [12].

Aunque los investigadores en seguridad han estado aplicando principios de usabilidad en aplicaciones de seguridad de una forma parcial, algunos de estos principios tienen problemas para ser adaptados a un proceso de diseño un poco más completa, en particular al diseño y desarrollo adecuado de los servicios de autenticación. Otro aspecto muy importante es obtener una herramienta de evaluación cuantitativa que permita validar el nivel de seguridad usable para aplicaciones donde la usabildad y seguridad están presentes. En ese sentido, este trabajo de investigación propone identificar un conjunto de principios que permita un balance adecuado entre seguridad y usabilidad y proponer una herramienta de evaluación cuantitativa que pueda contribuir en el diseño de sistemas seguros y usables, especialmente para sistemas de autenticación.

En general, y teniendo en cuenta lo anterior, esta investigación intenta establecer un proceso de diseño centrado en el usuario en el campo de la seguridad usable y autenticación de usuario a través de principios y un método de evaluación específico mediante una secuencia de actividades bien definidas, especificación de entregables, descripción de los diferentes participantes del proceso de evaluación y especificación del proceso de comunicación entre los participantes.

1.1. Planteamiento del Problema

El proceso de autenticación es uno de los aspectos más importantes en temas de seguridad informática ya que permite proteger la privacidad e integridad de los usuarios. Khateeb [13] define la autenticación como "*el proceso de confirmar la identidad de una entidad*". Hay muchos esquemas de autenticación aplicados actualmente. Algunos de ellos se basan en propiedades físicas (e.g. biométricos), comportamientos de los usuarios (e.g. dinámica de tecleo), aspectos cognitivos del usuario (e.g. capacidad de recordar contraseñas de usuario) y otros se basan en lo que tiene el usuario (e.g. token o smart cards) [14].

Actualmente, el método de autenticación más común para acceder a las redes y sistemas informáticos se basa en el uso de nombres de usuario y contraseñas alfanuméricas. Sin embargo, este tipo de autenticación ha mostrado tener inconvenientes significativos tales como problemas de olvido de claves y ataques informáticos por parte de terceras personas [15]. Por otra parte, publicaciones de prensa[1] publican en sus ediciones, el fin de esta forma de autenticación debido a que las empresas de tecnología e información reportan anualmente pérdidas de más de 200 billones de dólares debido a la vulnerabilidad de las contraseñas. No obstante, estas publicaciones señalan que la investigación en señales biométricas, está abriendo camino a una nueva forma de autenticación con el fin de evitar por completo el uso de contraseñas.

Sin autenticación, un sistema informático no tendría ninguna base para determinar si un usuario tiene derecho de acceder a información privada [3]. No es sorprendente que la investigación sobre la autenticación ha logrado una gran cantidad de métodos durante las últimas tres décadas, sin embargo, debido a que las organizaciones desconfían de estas nuevas estrategias por falta de una investigación adecuada sobre el funcionamiento de estos servicios, se han producido pocos resultados aplicados y prefieren continuar trabajando con los métodos tradicionales (*login/password*) [12]. Por ejemplo, a pesar del esfuerzo invertido en desarrollar sistemas de autenticación basados en certificación digital, la mayoría de los sitios que operan en los sitios web se basan en métodos tradicionales de autenticación.

La mayoría de estos sistemas de autenticación son interactivos y la interacción se produce generalmente a través de una interfaz gráfica de usuario. La seguridad en HCI (comunmente llamada Seguridad Usable, HCISec o USec por sus siglas en inglés *Usable Security*) considera cómo las características de seguridad de la interfaz de usuario puedan ser fáciles de usar, con el fin de que los usuarios comprendan estas características, evitando por lo tanto errores en su uso [16][17]. Aunque existe trabajos de investigación en el diseño de métodos de autenticación seguros y usables [18][19], y puesto que estos son desarrollados, aplicados y hasta vulnerados, los factores humanos también deben tenerse en cuenta en su diseño (e.g. factores humanos como la accesibilidad y la memorabilidad para autenticación propuestos por Renaud [20]). Lo anterior se convierte en una cuestión estratégica de diseño

[1] Disponible en: http://www.semana.com/tecnologia/articulo/llego-el-fin-de-las-contrasenas\-en-internet/396867-3. Consultado en Agosto del 2016

para este tipo de sistemas [3].

Las reglas de Schneiderman [21] para el diseño de interfaces de usuario se aplican a casi todos los tipos de diseño de software y son vistas como objetivos para el diseñador durante el desarrollo de la aplicación, sin embargo, en el diseño de software para seguridad tienen problemas con respecto a las necesidades que esta posee (e.g. para métodos de autenticación, solo las reglas de coherencia y cuadros de dialogo para proporcionar cierre, sobreviven) [8]. Los trabajos de Yee [22], Markotten [23], Chiasson [24], Garfinkel [12] y Whitten et al. [9] proporcionan principios semejantes entre sí para el desarrollo de sistemas usables y seguros pero hasta ahora, no muchos de ellos han estado en uso activo. Sin embargo, estos factores no son suficientes para encontrar un equilibrio adecuado entre usabilidad y seguridad. Además, todavía no existe un acuerdo entre la comunidad científica sobre qué principios son útiles para el diseño de interacción segura, con el fin de proporcionar herramientas a los desarrolladores de software que permitan mejorar sus productos.

Según lo anterior, hay una necesidad de estudiar y analizar los principios existentes para el diseño y desarrollo de aplicaciones seguras y usables especialmente al diseño de servicios de autenticación. De lo anterior surge la primera pregunta de investigación: **¿Cómo integrar los principios de seguridad usable existentes para ayudar al diseñador de software a obtener un balance adecuado entre usabilidad y seguridad, y aplicados también a métodos de autenticación?**.

Otro aspecto importante de la usabilidad en aplicaciones de seguridad es tener un valor cuantitativo y evaluar el proceso de desarrollo del producto software. La percepción de la seguridad también tienen un importante impacto en la forma en que se utiliza la tecnología y la medida en la que se adopta. La incapacidad de los usuarios para evaluar las propiedades de seguridad complica el diseño experimental. Además, mientras que los estudios de usuarios que tradicionalmente se basan en informes u observaciones con el fin de inferir en problemas de usabilidad en los sistemas, los usuarios generalmente no son capaces de describir con precisión los problemas de seguridad que han experimentado [12].

En otras palabras, es necesario proporcionar algun método de evaluación con el fin de probar qué tan bien desarrollada está la aplicación en relación con los principios de seguridad usable. Aunque autores como Kaiser y Reichenbach[25], Straub [26] y Braz [3] proponen métodos de evaluación de usabilidad para aplicaciones de seguridad, la falta de principios adecuados para el diseño de software que emplea características de seguridad, hace que los métodos de evaluación existentes no se encuentran en una forma más completa.

Con base en lo expuesto anteriormente, existe la necesidad de establecer algún método de evaluación en seguridad usable con base en los principios previamente establecidos. De lo anterior surge la segunda pregunta de investigación: **¿Cómo evaluar los principios de seguridad usable teniendo en cuenta las necesidades del usuario y sean aplicados también a métodos de autenticación?**.

Jøsang & Patton [27][28] y Flinn [29] establecen sugerencias a la interfaz de usuario que pueden contribuir a una mayor facilidad de uso, claridad y de forma segura, pero en su mayoría son extensiones y complementos a aplicaciones existentes, no para el desarrollo de aplicaciones. Actualmente existen procesos de desarrollo de aplicaciones software enfocados a aspectos de seguridad [30][23][31][32][33][34][35]. Sin embargo, estos procesos presentan soluciones incompletas teniendo en cuenta los principios de seguridad usable, debido a que no existe una clasificación en profundidad del usuario y tampoco proporciona medios para medir y evaluar la usabilidad en aplicaciones de seguridad.

La falta de principios claros y un método de evaluación adecuado, representa un obstáculo en el camino hacia el desarrollo de un proceso o técnica de diseño más completo. Los procesos disponibles están incompletos o se centran en alguna fase del proceso de desarrollo. Esto hace que sea complejo para los desarrolladores de software adoptar modelos independientes. A partir de la necesidades y oportunidades expresadas anteriormente, se plantea la pregunta general de investigación alrededor de la cual se orienta el desarrollo de esta tesis: **¿Qué proceso ayuda en el diseño de sistemas seguros y usables mediante un enfoque centrado en el usuario, a partir de principios y métodos de evaluación?**.

Es importante destacar que las necesidades de los usuarios toman la mayor importancia en este trabajo de investigación y alrededor de ellos gira el proceso de diseño de sistemas seguros y usables, ya que finalmente son ellos quienes utilizan los sistemas para alcanzar sus objetivos. Lo buscado es que ellos alcancen dichos objetivos de manera fácil y eficiente, lo que contribuye directamente a su satisfacción.

1.2. Objetivos

1.2.1. Objetivo General

Presentar un proceso que ayude en el diseño de sistemas seguros y usables mediante un enfoque centrado en el usuario, a partir de principios y métodos de evaluación del área de la seguridad usable y aplicados también a métodos de autenticación.

1.2.2. Objetivos Específicos

- Identificar posibles principios de seguridad usable que permita un balance adecuado entre seguridad y usabilidad particularmente para autenticación de usuario.
- Proponer un método de evaluación para los principios de seguridad usable y que pueda contribuir en el diseño de servicios de autenticación.
- Validar los principios y el método de evaluación en aplicaciones reales.
- Presentar un proceso de diseño para seguridad usable y autenticación mediante un enfoque centrado en el usuario, a partir de los principios de seguridad usable y su evaluación.

1.3. Hipótesis

Tomando en cuenta el planteamiento del problema y la revisión de la literatura presentada en el próximo capítulo, se determinaron una serie de hipótesis con el objeto de guiar el estudio las cuales pueden servir como respuestas provisionales a las preguntas de investigación.

1.3.1. Hipótesis Alternativa

Atendiendo a lo anterior, se presenta a continuación el conjunto de hipótesis formuladas para este trabajo de investigación:

1. Es posible obtener principios de seguridad usable y de métodos de autenticación que permita un balance entre seguridad y usabilidad.

2. Establecer algún método de evaluación de seguridad usable, puede contribuir en el diseño de estas aplicaciones desde sus primeras fases de desarrollo.

3. Es posible establecer un proceso de diseño el cual involucra principios de seguridad usable y su evaluación a partir de un enfoque centrado en el usuario.

1.3.2. Hipótesis Nula

La imposibilidad de obtener principios de seguridad usable junto con algún método de evaluación, no permite establecer un proceso de diseño mediante un enfoque centrado en el usuario.

1.4. Principales contribuciones

Teniendo en cuenta los objetivos de la investigación, las principales contribuciones son:

1. **Un conjunto más amplio de principios para seguridad usable y métodos autenticación** el cual permite al desarrollador, una herramienta más completa con el fin de influir en el diseño de sistemas de autenticación y aplicaciones donde la seguridad y usabilidad son factores trascendentales. Lo anterior es importante porque permite evaluar el sistema en cualquier fase del desarrollo y mejorar su diseño.

2. **Un nivel de importancia** para los principios de seguridad usable. Los principios de seguridad usable y autenticacion junto con su grado de importancia podrían ayudar a los desarrolladores a tener en cuenta aquellos principios más relevantes para el desarrollo de las aplicaciones, ahorrando tiempo y recursos ya sean humanos o económicos.

3. **La adaptación del método de evaluación para examinar más conceptos aparte de seguridad y usabilidad** con el fin de adaptarse a las nuevas tendencias en la comunidad de seguridad usable. En esta adaptación se presenta un conjunto de atributos y características basados en el estándar ISO 25010:2011 que son complemento a la seguridad y usabilidad tales como accesibilidad, fiabilidad, desempeño y operabilidad.

4. **Resultados cuantitativos para seguridad usable en la presentación de resultados de la evaluación de los principios**. Por lo general, la evaluación de principios en el área de la seguridad usable (e.g. evaluación heurística) proporciona datos cualitativos. Sin embargo, en este trabajo de investigación se proponen diferentes medidas cuantitativas con el fin de superar la subjetividad de la evaluación.

5. **Una matriz de evaluación de riesgo para seguridad usable y autenticación** con el fin de reconocer y entender las principales amenazas de seguridad con base en los principios y su impacto.

6. **Validación con expertos y usuarios** en aplicaciones reales cuyo propósito es comprobar que la propuesta está acorde con la situación real que presenta cada una de las aplicaciones en cuestión.

7. **La integración de los resultados en proceso de diseño centrado en el usuario para seguridad usable** el cual podría alcanzar un equilibrio entre seguridad y usabilidad usando las recomendaciones de diseño y su respectiva evaluación. El proceso propuesto es el resultado de integrar el modelo del proceso de la usabilidad y la accesibilidad MPIu+a, y los principios de seguridad usable junto con el método de evaluación presentados en esta tesis.

8. **Una amplia revisión sistemática de la literatura** con el fin de obtener principios para seguridad usable y métodos de autenticación proponiendo con lo anterior un método de evaluación. Además, esta revisión permite presentar un proceso de desarrollo de sistemas seguros y usables mediante el enfoque de diseño centrado en el usuario.

1.5. Organización del documento

La organización del presente documento está dividida en 6 capítulos, los cuales se describen brévemente a continuación:

El **Capítulo 1**, se presenta la introducción del trabajo, el cual esta dividido en el planteamiento del problema, los objetivos, la hipótesis de solución, las principales contribuciones de la investigación y la estructura del documento.

El **Capítulo 2**, presenta los referentes teóricos necesarios para comprender la información presentada en el documento. Los referentes teóricos se dividen en los grupos: usabilidad, seguridad, seguridad usable, aplicación de la seguridad usable y métodos de autenticación de usuario.

El **Capítulo 3** presenta el proceso de desarrollo heurístico con el fin de obtener principios en seguridad usable y métodos de autenticación.

El **Capítulo 4** se discute las revisiones realizadas por los expertos del conjunto heurístico propuesto, quienes utilizan una herramienta de validación para revisar los principios de seguridad usable y autenticación.

El **Capítulo 5** se analiza aplicaciones donde intervienen expertos y usuarios con el fin de validar los principios de diseño, el método de evaluación propuesto y el comportamiento de los usuarios cuando existen características de seguridad en las aplicaciones.

El **Capítulo 6** se presenta la adaptación del proceso de diseño centrado en el usuario MPIu+a junto con los principios y el método de evaluación cuantitativo para seguridad usable y autenticación.

Finalmente, el **Capítulo 7** presenta las conclusiones de los resultados obtenidos y su articulación con los objetivos planteados. Adicionalmente, son presentadas las limitaciones y actividades futuras para fortalecer el presente trabajo.

Capítulo 2

Base conceptual

2.1. Introducción

En este capítulo se presentan los contenidos considerados como base teórica para el desarrollo de la investigación.

En la primera sección se introduce la disciplina de Interacción Humano-Computador (HCI, por sus siglas en inglés *Human Computer Interaction*), seguidamente se introduce el concepto diseño centrado en el usuario, usabilidad y la evaluación heurística para la usabilidad de sistemas interactivos. Posteriormente, se presenta información sobre la seguridad informática, sus propiedades, el concepto de privaciad y evaluación. Luego es presentado el área de seguridad usable o USec (por sus siglas en inglés *Usable Security*), sus principios de diseño y evaluación. Seguidamente se presenta la sección sobre el diseño de sistemas seguros y usables donde se tiene en cuenta la ingeniería de la seguridad y procesos desarrollados de la literatura. Finalmente, es presentado la autenticación de usuario junto con sus criterios, métodos y evaluación. En la Figura 2.1 se presenta el esquema general del contenido que se presentará en este capítulo.

2.2. Interacción Humano-Computador

Actualmente no existe una definición única y formal sobre la Interacción Humano-Computador HCI. Sin embargo, la SIGCHI[1] (por sus siglas en inglés de *Special Group in Computer Human Interaction*) ofrece una definición para profesionales, académicos e investigadores interesados en la Interacción-Humano Computador:

"La disciplina relacionada con el diseño, evaluación e implementación de sistemas informáticos interactivos para el uso de seres humanos, y con el estudio de los fenómenos más importantes con los que está relacionado".

[1]Disponible en: http://sigchi.org/cdg/cdg2.html Consultado: Agosto del 2016

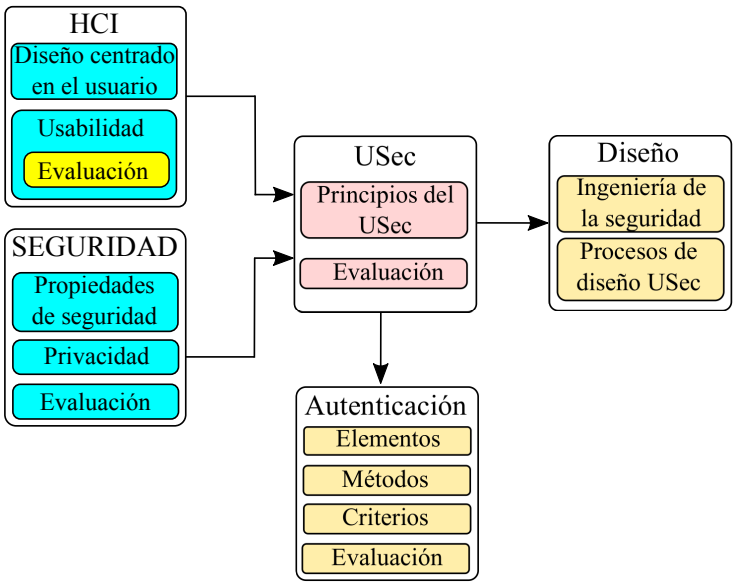


Figura 2.1: Estructura del Capítulo 2 (creación propia).

La Interacción-Humano Computador representa un campo de investigación que es el resultado de la creciente incorporación de dispositivos computacionales en los lugares de trabajo [36]. Anteriormente, los computadores estaban limitados para personas que previamente habían sido entrenadas para su uso y tenían un amplio conocimiento sobre el manejo.

Los diseñadores mantenían la idea de que los usuarios tenían un alto conocimiento técnico y que estarían familiarizados con su uso, además que tenían la habilidad para entender claramente los términos técnicos y podrían resolver los problemas técnicos que se presentaran. Sin embargo, la realidad fue distinta ya que los "usuarios comunes"generalmente se sentían frustrados mientras usaban los sistemas computacionales, debido a que estos eran difíciles de usar y con mucha frecuencia no eran usables [37].

Los principales objetivos del HCI consiste en desarrollar o mejorar los siguientes aspectos en un sistema interactivo [38]:

1. **Utilidad y efectividad**: La utilidad se relaciona con los servicios que proporciona un sistema, y la efectividad, con la habilidad de los usuarios para lograr sus objetivos a través del sistema.

2. **La eficiencia**: Es la medida de cuán rápido los usuarios pueden lograr sus objetivos al hacer uso de un sistema.

3. **La usabilidad**: Se relaciona con el grado de facilidad de uso e interpretación de una tecnología determinada (ver Sección 2.4). Un sistema "usable" puede describirse

como: fácil de aprender y recordar, eficiente en cuanto a su uso, producir pocos errores y satisfacer las necesidades del usuario.

4. **La atracción**: Se refiere a que tanto le agrada al usuario, el sistema interactivo que está utilizando, tomando en cuenta sus primeras impresiones y su satisfacción.

Para lograr los objetivos anteriores, el HCI requiere de teorías propias de otras áreas, tales como: las ciencias de la computación, factores humanos y ergonómicos, diseño gráfico, psicología cognitiva, sociología y atropología [38]. Lo anterior, ha tenido un crecimiento positivo en el diseño de sistemas así como también en los métodos de evaluación para asegurar que las tecnologías sean más fáciles de usar y aprender [39].

No solamente se enfoca en la facilidad de uso, sino también en nuevas técnicas de interacción para soportar las tareas de los usuarios, buscando mejores formas de acceso a la información y creando más poderosas formas de comunicación. Se estudian dispositivos de entrada y de salida y las respectivas técnicas de interacción; formas de presentar y solicitar información; formas para ayudar, documentar y entrenar; herramientas para el diseño, construcción, pruebas y evaluación de interfaces de usuario y los procesos que los desarrolladores siguen cuando crean las interfaces [40].

El HCI permite diseñar sistemas computacionales que ayuden a las personas a realizar sus actividades de una manera productiva y segura. Para producir sistemas con una buena usabilidad, los diseñadores tratan de entender diferentes factores tales como: psicológico, ergonómico, educativo, cultural y social. Estos factores ayudan a determinar cómo las personas operan y usan efectivamente la tecnología. Por tal razón, hay que pensar en trabajar en equipos interdisciplinarios que trabajen conjuntamente para desarrollar estos sistemas. Entre las disciplinas más importantes se destacan: programación, psicología, sociología, ergonomía, inteligencia artificial, ingeniería de software, etnografía, documentación y diseño gráfico, ver Figura 2.2 [41].

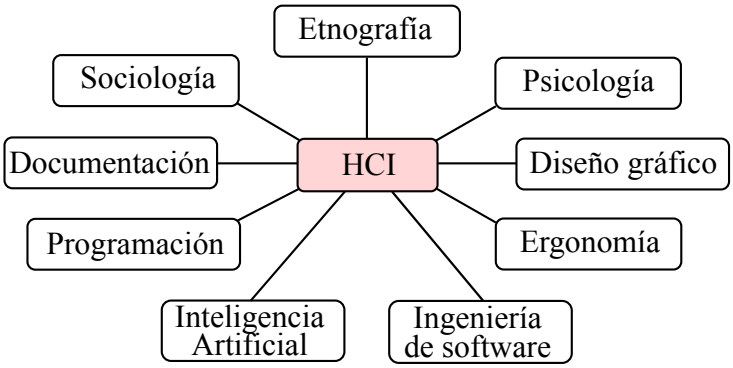


Figura 2.2: Principales disciplinas relacionadas con la Interacción Humano-Computador (Tomado de [41]).

2.3. Diseño Centrado en el Usuario

El proposito del diseño centrado en el usuario (DCU) es el desarrollo de sistemas interactivos que tiene como objetivo hacer que los sistemas sean utilizables y útiles teniendo en cuenta al usuario, sus necesidades y requerimientos, y mediante la aplicación de técnicas y conocimiento en usabilidad. Las necesidades y las tareas de los usuarios también deben estar en línea con lo que se indica en los documentos de los requisitos [42].

La importancia de la HCI queda incluso reflejada en un apartado de las normas ISO, el estándar ISO 13407:1999 (*Human-Centred Design Processes for Interactive Systems*). Ese estándar es una guía para el desarrollo de sistemas interactivos usables incorporando el diseño centrado en el usuario. Sin embargo, esta norma fue cancelada y reemplazada por la norma ISO 9241-210 [43]. En esta norma, el término – Diseño Centrado en el Usuario – fue sustituido por Diseño Centrado en el Humano (DCH), porque se dirige tanto a desarrolladores como a usuarios [44].

El estándar ISO 9241-210:2010 proporciona un marco que integra diferentes procesos de diseño y desarrollo apropiado en un determinado contexto; complementando diferentes metodologías de diseño. La Figura 2.3 muestra las actividades y su interdependencia definida por la norma.

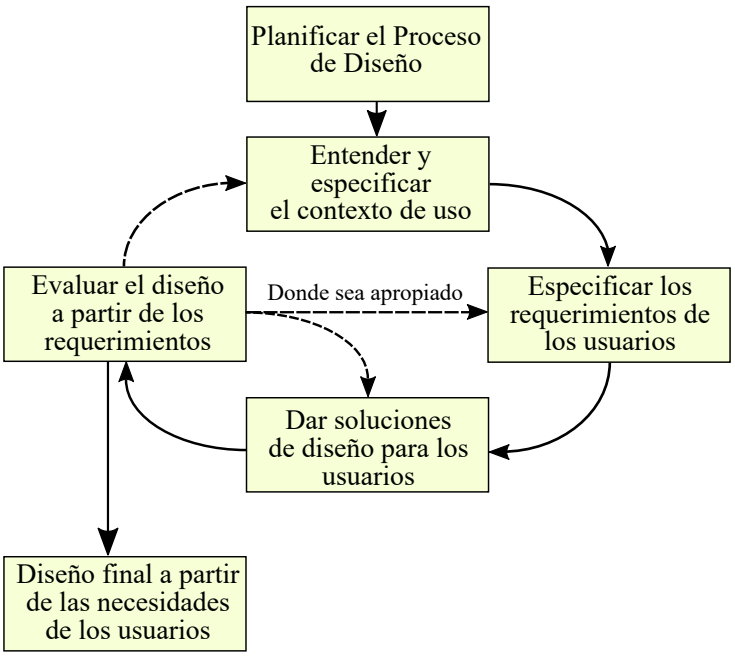


Figura 2.3: Interdependencias de las actividades del Diseño Centrado en el Humano (Tomado de [43]).

Desarrollar un sistema interactivo implica que ciertas normas y procedimientos son seguidos por el equipo de desarrollo. El proceso general definido por la norma ISO 9241-210

proporciona varias interacciones hasta conseguir todos los objetivos o requisitos, estos se indican mediante las respectivas líneas punteadas.

El desarrollo de sistemas centrado en el usuario, tiene varias etapas las cuales se describen a continuación [45][43][44]:

1. **Planificar el proceso de diseño**: En esta etapa se resume el propósito del sistema interactivo que se está desarrollando (e.g. sitio web, video juego, etc.). Se determina también, el tipo de personas para las cuales será desarrollado dicho sistema, así como los beneficios que proporcionará a sus usuarios.

2. **Entender y especificar el contexto de uso**: Esta actividad corresponde al contexto en el cual se utilizará el sistema. Para definirlo, se consideran las características de los usuarios, tareas y el ambiente organizacional, técnico y físico. En cuanto al análisis de las tareas, se busca establecer lo que los usuarios harán, es decir, cuáles son sus objetivos (lo que ellos quieren lograr), y las tareas o actividades que tienen que realizar para alcanzar dichos objetivos

3. **Especificar requerimientos de los usuarios**: En esta actividad se identifica lo que el usuario tiene que lograr a través del sistema. De la misma forma, se especifica cualquier limitación impuesta por el contexto de uso.

4. **Soluciones de diseño**: Las soluciones se basan en la descripción del contexto de uso, de los resultados de evaluaciones preliminares y del estado del arte en el dominio de aplicación. En el diseño es fundamental las directrices de usabilidad, la experiencia y el conocimiento del equipo de diseño multidisciplinar. La iteracción es esencial en este punto y puede dar lugar a requisitos de usuario adicionales.

5. **Evaluación**: Se realizan pruebas de usabilidad a la interfaz desarrollada. Una prueba básica y simple consiste en proporcionar el sistema interactivo a un grupo de usuarios y pedirles su opinión del mismo después de utilizarlo (evaluación basada en usuarios).

Con base en lo anterior, el rol del HCI dentro del proceso de diseño de sistemas interactivos, consiste en mejorar la calidad de la interacción entre humanos y computadores. Para lo cual es necesario aplicar de manera sistemática el conocimiento sobre las metas, capacidades, y limitaciones de los humanos que utilizarán un sistema interactivo determinado, junto con el conocimiento sobre las capacidades y limitaciones de dicha tecnología. El reto para los desarrolladores de sistemas interactivos consiste en saber cómo realizar la transición de lo que se puede hacer (funcionalidad), a cómo debe hacerse para cubrir los requerimientos del usuario (usabilidad) dentro de su ambiente de trabajo [45].

Por otro lado, el estándar ISO 9241-210 involucra seis principios claves que caracterizan un diseño centrado en el usuario.

1. El diseño está basado en una comprensión explícita de usuarios, tareas y entornos.

2. Los usuarios están involucrados durante el diseño y el desarrollo.
3. El diseño está dirigido y refinado por evaluaciones centradas en usuarios.
4. El proceso es iterativo.
5. El diseño está dirigido a toda la experiencia del usuario.
6. El equipo de diseño incluye habilidades y perspectivas multidisciplinarias.

Por último, es importante tener en cuenta que centrarse en el usuario significa centrarse en todos los usuarios, sin que ello indique que debamos incorporar a todos los posibles usuarios de un determinado sistema, sino que debemos contemplar todos los rasgos diferenciales entre ellos, pensando incluso en aquellos que adolecen de alguna discapacidad [46].

2.4. Usabilidad

El término usabilidad coloquialmente es definido como "facilidad de uso" ya sea de una página web, una aplicación informática o cualquier otro sistema que interactúe con un usuario [47]. Se trata de una propiedad que no es tan solo aplicable a los sistemas de software, sino que es aplicable a elementos de la vida cotidiana. Aunque esta definición es correcta, no deja de ser incompleta ya que el término engloba muchas más connotaciones [46]. En la actualidad existe una serie de definiciones formales, aunque no existe una definición exacta de este término. Por esta razón, serán presentadas una serie de definiciones formales y dadas por autores prominentes del área de la usabilidad con el objetivo de establecer la idea general del concepto.

Carroll [48], en su libro *Human Computer Interaction in the New Millennium*, relaciona el HCI y la usabilidad afirmando que:

"El HCI es el estudio y la práctica de la usabilidad y a su vez interpreta la usabilidad como la relación entre el conocimiento y la creación de software y otras tecnologías que las personas quieran usar, que sean capaces de usar y que las encuentran efectivas cuando las utilizan".

Según la norma ISO 9241 [43], "*la usabilidad es el grado en el que un producto software puede ser utilizado por usuarios específicos para alcanzar objetivos específicos con efectividad, eficiencia y satisfacción en un contexto de uso específico*". Es una definición centrada en el concepto de calidad en uso, es decir, se refiere a cómo el usuario realiza tareas específicas en escenarios específicos con efectividad. La efectividad se refiere al nivel de exactitud con que el usuario cumple los objetivos; la eficiencia se refiere a los recursos usados para la concreción de estos objetivos por parte del usuario, mientras que la satisfacción está relacionada con la comodidad y postura del usuario durante la interacción con el producto.

La definición de usabilidad dada por Bevan [49] es: *"la facilidad de uso y aceptabilidad de un sistema o producto para una clase particular de usuarios que llevan a cabo tareas específicas en un ambiente específico, donde la facilidad de uso afecta el rendimiento y satisfacción del usuario y la aceptabilidad afecta si el producto es utilizado o no"*. Esta definición es bastante completa y pretende integrar las dos definiciones dadas por el estándar ISO 9241.

Jacob Nielsen [50] define la usabilidad como un *"atributo de calidad que evalúa que tan fácil de usar es una interface de usuario"*. Además, menciona que el término usabilidad está definida por cinco componentes de calidad: facilidad de aprendizaje, eficiencia, memorabilidad, errores y satisfacción.

En este trabajo de investigación la definición propuesta por la norma ISO 9241 se utiliza cuando el término usabilidad es presentada, puesto que es ámpliamente conocida y representa completamente el sentido del término en cuestión [51]. La Figura 2.4 describe la relación entre los diferentes componentes de la definición de usabilidad, un sistema que consiste en usuarios, equipos, tareas y un entorno físico y social, con el propósito de alcanzar objetivos particulares [43]. En efecto, un usuario está llevando a cabo tareas, que son colecciones de actividades, para lograr sus objetivos.

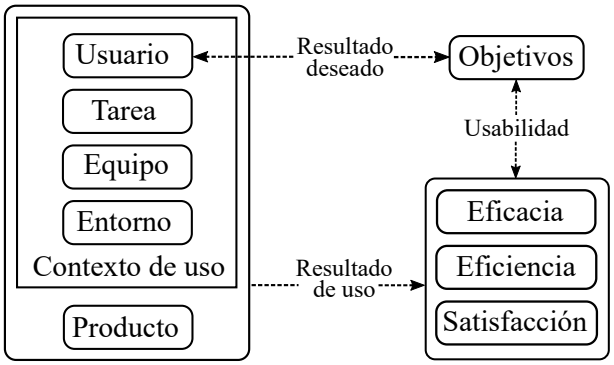


Figura 2.4: Marco de trabajo de usabilidad (Tomado de [43]).

2.4.1. Evaluación de la Usabilidad

La evaluación de la usabilidad se compone de metodologías para la medición de aspectos de usabilidad en la interfaz de usuario de un sistema interactivo y la identificación de problemas específicos. Esta evaluación es una parte importante del proceso de diseño de la interfaz en general, que idealmente se compone de ciclos iterativos de diseño, prototipado y evaluación. La evaluación de la usabilidad es en sí mismo un proceso que implica varias actividades en función del método empleado [50][52].

Este proceso puede ser llevado a cabo por personas con diferentes habilidades y conocimientos, involucrando usuarios potenciales y actuales, expertos en usabilidad, diseñadores

de sistemas, entre otros. Es necesario realizar la evaluación de usabilidad para validar que el producto final cumple con los requerimientos y es usable [46].

La evaluación de usabilidad es una parte fundamental en el desarrollo del software, porque las actividades de evaluación pueden producir soluciones de diseño para su aplicación en el próximo ciclo de desarrollo o, al menos, un mayor conocimiento sobre la naturaleza del problema de interacción detectado. Por tanto, la evaluación de usabilidad es parte inherente del proceso de desarrollo [53].

Para Mayhew [54], la evaluación de la usabilidad es un estudio empírico con usuarios reales del sistema propuesto, con el propósito de proporcionar realimentación en el desarrollo de software durante el ciclo de vida de desarrollo iterativo. Se trata de un proceso para producir una medida de la facilidad de uso en el que intervienen el objeto a evaluar y un proceso a través del que se juzgan uno o más atributos [55]. En cualquier caso, el propósito de evaluación de la usabilidad se podría resumir como un proceso con los siguientes objetivos:

1. Proporcionar realimentación para mejorar el diseño.

2. Valorar en qué medida se están consiguiendo cumplir los objetivos marcados frente a los usuarios y a la propia organización.

3. Monitorizar el uso a largo plazo de productos o sistemas.

Existen muchas propuestas de métodos para la evaluación de la usabilidad y se han establecido varias clasificaciones de los mismos atendiendo a diversos criterios. Algunos de estos métodos requieren grandes medios materiales, como un completo laboratorio de usabilidad con espacios independientes para el desarrollo de las pruebas y tecnología específica como cámaras de vídeo y equipos de *eye tracking*[2], y otros pueden llevarse a cabo con poco más que una interacción semi-formal entre el grupo de desarrollo y los usuarios finales.

2.4.1.1. Métodos de Evaluación de Usabilidad

La evaluación de la usabilidad de una aplicación es una de las etapas más importantes dentro del diseño centrado en el usuario, ya que permite obtener las características de usabilidad de un sistema y la medida en que los atributos, paradigmas y principios de usabilidad se están aplicando en éste [57]. Es por esto que existen métodos de evaluación de usabilidad los cuales se han convertido en una fuente interesante de estudio por parte de los investigadores de la usabilidad, sus características de aplicación, la variedad de métodos existentes y los resultados que generan [51].

[2]La técnica *Eye Traking* determina dónde está mirando alguien con el fin de medir las características de los movimientos oculares y el propio ojo. Es ampliamente utilizado en la investigación en los sistemas visuales, en psicología, en lingüística cognitiva y en diseño de productos [56].

Los métodos de evaluación de usabilidad se pueden dividir en tres categorías: de prueba, de inspección y de indagación. Cada categoría se puede aplicar a una o más fases del ciclo de vida de diseño de la siguiente manera [52][58].

1. **Métodos de prueba**: Los usuarios trabajan en tareas típicas utilizando el sistema (o el prototipo) y los evaluadores utilizan los resultados para ver cómo la interfaz de usuario es compatible con los usuarios en la ejecución de sus tareas.
2. **Métodos de inspección**: En la metodología de inspección, los expertos en usabilidad examinan aspectos de usabilidad de una interfaz de usuario. Este trabajo de investigación se centra en uno de los métodos de evaluación de usabilidad por inspección; la evaluación heurística por su facilidad y bajo costo.
3. **Métodos de indagación**: Los evaluadores de usabilidad obtienen información sobre los gustos de los usuarios, disgustos, necesidades y comprensión del sistema mientras los observa y habla con ellos durante la ejecución del sistema. Además, respondan a preguntas de forma oral o escrita.

Tabla 2.1: Ventajas y desventajas de cada método de evaluación de usabilidad (Tomado de [59]).

Método de evaluación	Ventajas	Desventajas
Métodos de prueba	Estimación real de la usabilidad en su mayor parte. Puede dar un registro claro de los problemas importantes	Consumo de tiempo. Costoso para una muestra grande de usuarios. Requiere de prototipos.
Métodos de inspección	Rápido y económico	Variabilidad de los expertos afecta indebidamente los resultados. Puede sobre valorar cierto número de problemas.
Métodos de indagación	Proporciona estimación rigurosa de los principios de usabilidad. Se puede realizar en la especificación de la interfaz	Mide sólo un componente de la usabilidad. Aplicabilidad de tarea limitada.

Las ventajas y desventajas de cada método se resumen en la Tabla 2.1. Se podría decir que el mejor enfoque para la evaluación de la usabilidad es la combinación de métodos, por ejemplo, métodos de inspección y de prueba, ya que los resultados de un metodo de prueba normalmente no cubre la mayor parte de la interfaz como un método basado en indagación. Obviamente, la evaluación de la usabilidad ocurre durante todo el proceso de diseño, el despliegue de varios métodos en diferentes etapas es a la vez útil y que puede llevar a una mayor facilidad de uso en el producto final [59].

2.4.1.2. Evaluación Heurística

La evaluación heurística es considerado como un método de evaluación por inspección para evaluar la usabilidad de sistemas interactivos, el cual es realizado por un grupo de expertos en usabilidad. Los expertos aplican un conjunto específico de heurísticas o principios para evaluar la usabilidad de una aplicación en particular. Esto proporciona un análisis del producto, que ayuda a corregir elementos confusos en el diseño actual. Es ampliamente utilizado porque es un excelente método de diagnóstico y análisis para identificar problemas de usabilidad en un corto período de tiempo. Específicamente, su propósito es identificar problemas que están asociados con el diseño de interfaces de usuario [47][52].

En esta técnica, varios expertos inspeccionan y analizan el diseño. Por lo que, debe existir un número de expertos que participen en la evaluación, alrededor entre 3 y 5. Cada uno de los evaluadores examinará el diseño de forma independiente, documentando los problemas identificados. Tal y como demuestra Nielsen [60][61], en donde se presentan evaluaciones heurísticas conducidas por profesionales relacionados con las ciencias de la computación, como programadores y estudiantes de informática, los evaluadores no tienen que ser expertos en usabilidad.

La evaluación heurística es una de las metodologías más utilizadas debido a su rapidez y costo (en comparación con otros métodos como los test del usuario). Se puede aplicar en todas las diferentes etapas del proceso de desarrollo [60], no necesita una planificación exhaustiva y el proceso de evaluación es muy intuitivo. Además, se cree que detecta el 42 % de los problemas graves y el 32 % de los problemas menores [60]. Por todas estas razones, a menudo se considera como una de las técnicas de evaluación más usadas de usabilidad [52].

Una evaluación heurística no debe reemplazar los métodos de prueba de usabilidad. Aunque las heurísticas se refieren a criterios que afectan la usabilidad de su sitio, los problemas identificados en una evaluación heurística son diferentes a los encontrados en una prueba de usabilidad. Aunque la evaluación heurística es un buen método de evaluación de usabilidad, también tiene algunas desventajas [62]. La Tabla 2.2 resume las ventajas y desventajas del método de evaluación heurística.

Debido a que la evaluación heurística es el "corazón" de este trabajo de investigación, debido a sus ventajas y que desde un principio fue elegido como método de evaluación usando los principios de seguridad usable y autenticación propuestos, proponiendo con esto una métrica cuatitativa para USec, es necesario considerar ciertos aspectos. Masip [63] en su tesis doctoral presenta trabajos relacionados donde diferentes términos como principios, directrices, recomendaciones, reglas de diseño, pautas, entre otras, están ámpliamente disponibles, pero en muchos formatos diferentes. Sin embargo, detalla que el término principio de diseño es más general.

Pero lo anterior no significa que se descarten otras opciones. En cualquier caso en que se utilice el término heurístico, también se pueden considerar otros términos como directriz,

Tabla 2.2: Ventajas y desventajas de la evaluación heurística (Tomado de [62]).

Ventajas	Desventajas
Puede proporcionar algunos comentarios rápidos y relativamente asequible a los diseñadores.	Requiere conocimientos y experiencia para aplicar eficazmente la heurística.
Puede obtener realimentación en las primeras etapas del proceso de diseño.	Los expertos en usabilidad capacitados son a veces difíciles de encontrar y pueden ser costosos.
Asignar la heurística correcta puede ayudar a los diseñadores a tomar medidas correctivas.	Debe utilizar varios expertos y agregar sus resultados.
Puede realizar pruebas de usabilidad para examinar más a fondo posibles problemas.	La evaluación puede identificar más problemas menores y menos problemas importantes.

principio, recomendación, regla de diseño, guía de estilo entre otros [63]. Ya que esta investigación se centra en evaluación heurística, los términos heurístico, principio o principio de diseño serán utilizado.

2.4.1.3. Métricas para la Evaluación de la Usabilidad

Las métricas de usabilidad proporcionan herramientas y resultados para determinar en el diseño la eficacia del desarrollo, su seguimiento, proporcionando ideas para decisiones de posibles mejoras. Las métricas reemplazan las intuiciones y sentimientos con hechos. Las métricas de usabilidad y su medición pueden mostrar una mejora, una disminución o una indiferencia en la experiencia del usuario con un producto mejorado o modificado [64]. Albert & Tullis [64] presentan algunas métricas básicas de usabilidad para desempeño.

1. **Éxito de la tarea**: es quizás la métrica de rendimiento más ampliamente utilizada. Mide la eficacia con la que los usuarios pueden completar un conjunto de tareas determinado.

2. **Tiempo de tarea**: es una métrica de rendimiento común que mide cuánto tiempo se requiere para completar una tarea.

3. **Los errores**: reflejan los errores cometidos durante una tarea.

4. **La eficiencia**: se puede evaluar examinando la cantidad de esfuerzo que un usuario gasta para completar una tarea.

5. **El aprendizaje**: es una forma de medir cómo el rendimiento cambia con el tiempo.

Nielsen [65][66] propone la utilización de cinco métricas para la evaluación de la usabilidad en las interfaces de un sitio web generadas durante el proceso de desarrollo del mismo.

1. **Tiempo de tarea**: número de segundos que le toma al usuario encontrar respuesta a preguntas específicas sobre el contenido de la aplicación.
2. **Errores**: porcentaje basado en el número de respuestas incorrectas dadas por los usuarios a preguntas cuya respuesta correcta es conocida.
3. **Memoria**: comprende la memoria de reconocimiento el cual consiste en un porcentaje basado en el número de respuestas correctas menos el número de respuestas incorrectas dadas por los usuarios a cinco preguntas de opción múltiple, y la memoria de retención que consiste en un porcentaje basado en el número de objetos correctamente recordados menos el número de elementos incorrectamente recordados por los usuarios.
4. **Tiempo de memorización de la estructura de la aplicación**: El número de segundos que le lleva al usuario dibujar un mapa de la aplicación.
5. **Satisfacción subjetiva**: puede ser determinada mediante las respuestas dadas por los usuarios a un cuestionario específico.

El conjunto de métricas de Nielsen responde al "cómo" trabaja la aplicacion desde el punto de vista de los usuarios, y no el desempeño de los usuarios, es decir, puede haber usuarios que tarden mucho tiempo en contestar las preguntas sobre el contenido de la aplicación y aun así pensar que le resultó muy fácil encontrar información requerida [45].

2.5. Seguridad

El término seguridad tiene diferentes definiciones en la literatura. El estándar ISO/IEC 25010:2011 [67] lo define como "*el grado en que un producto o sistema protege la información y los datos para que las personas u otros productos o sistemas tengan acceso a datos apropiados de acuerdo a tipos y niveles de autorización*".

Morrie [68] define la seguridad como "*la protección de los sistemas de información de daños en el hardware, software y el robo de información sobre ellos, así como la alteración o mala dirección de los servicios que ellos proveen*".

La seguridad de un sistema comprende un conjunto de métodos y técnicas que trabajan en conjunto para obtener mecanismos de seguridad. Los mecanismos de seguridad se utilizan para prevenir debilidades de los sistemas mediante la aplicación de tres propiedades de seguridad: 1) *confidencialidad*, 2) *integridad*, y 3) *disponibilidad* [68]. El estandar ISO/IEC

25010 incluye tres propiedades adicionales: no repudio, responsabilidad y autenticidad [67].

La seguridad está relacionada con el software de dos maneras. Software de seguridad y seguridad del software son términos donde la seguridad y el software trabajan juntos para garantizar la seguridad, sin embargo, los dos términos no son los mismos. Seguridad del software es un proceso llevado a cabo durante el ciclo de vida del desarrollo de software para aplicar prácticas de seguridad con el fin de producir productos software seguros. Por el contrario, el software de seguridad es un producto de software desarrollado para proteger la información y evitar ataques informáticos [69].

2.5.1. Propiedades de Seguridad

La confidencialidad, integridad, disponibilidad, responsabilidad, no repudio y autenticidad deben ser aplicadas con el fin de proporcionar sistemas informáticos seguros. A continuación se presenta una breve definición de los seis objetivos de los sistemas informáticos de seguridad [67][70].

1. **Confidencialidad**: grado en el que un producto o sistema garantiza que los datos sólo sean accesibles a los autorizados.
2. **Integridad**: grado en que un sistema, producto o componente impide el acceso no autorizado o la modificación de programas de computadora o datos.
3. **Disponibilidad**: capacidad para garantizar que los sistemas informáticos estén disponibles para clientes autorizados en cualquier momento.
4. **Responsabilidad**: capacidad para monitorear y analizar los registros de los usuarios para descubrir y prevenir cualquier incidente de violación.
5. **No repudio**: grado en el cual se puede demostrar que las acciones o eventos han tenido lugar, de modo que los eventos o acciones no pueden ser repudiados más tarde.
6. **Autenticidad**: grado en que se puede demostrar que la identidad de un sujeto o recurso es la solicitada.

Estos mecanismos de seguridad están presentes en los sistemas informáticos porque la mayoría de ellos se ocupan de información sensible y privada de diversas maneras. El objetivo de cualquier mecanismo de seguridad es cumplir y lograr las tres propiedades principales de seguridad (confidencialidad, integridad y disponibilidad). Cuando los mecanismos anteriores se aplican a sistemas computacionales y de información de una forma adecuada, se cumple con la seguridad del sistema. La Figura 2.5 explica la interacción de las propiedades para lograr seguridad [71].

Por otro lado, existe un gran número de estrategias para tratar de reducir los riesgos asociados con el intercambio de información en linea. De acuerdo con Sanz et al. [72], la mejor manera de evitar riesgos, es la reducción de las vulnerabilidades del sistema en línea. Esto

Figura 2.5: *Honeycomb* de las propiedades de seguridad (creación propia).

es posible usando tecnologías como: mecanismos para el control de acceso, la autenticación de identidades, herramientas para la detección de intrusos, aproximaciones criptográficas mediante el uso de llaves públicas y privadas, entre otras. Sin embargo, es bien sabido que el concepto de "seguridad total" es inalcanzable. La meta es lograr que un sistema sea lo suficientemente confiable al garantizar el cumplimiento de los requerimientos de seguridad específicos de una organización determinada [45].

De la misma manera, D'Hertefelt [73] presenta cuatro factores importantes (comprensible, predecible, flexible y adaptable), mediante los cuales es posible transmitir confianza al usuario en un ambiente donde la seguridad es pieza clave.

1. **Comprensible**: proporciona una respuesta a el usuario sobre el estado actual del sistema, cómo alcanzar sus objetivos, si el sistema proporciona suficiente realimentación y cambiar el estado actual del sistema.

2. **Predecible**: indica el grado razonable de certeza cuando realiza una acción.

3. **Flexible y Adaptable**: no todos los usuarios ejecutarán una tarea de la misma manera. Un usuario se sentirá en control de un sistema interactivo si el usuario puede elegir la forma en que se ejecuta una tarea en lugar de tener que averiguar cómo el sistema requiere que se haga.

Los factores de D'Hertefelt [73] están orientados hacia la facilidad de uso y aprendizaje de la interfaz mediante un diseño minimalista de la misma, y hacia la apropiada notificación de las características del sistema al usuario. Así, al trasladar dichos conceptos a un ambiente de seguridad mediante la aplicación de los criterios de diseño de la seguridad usable, es posible lograr que el usuario confíe en la seguridad del sistema [74].

2.5.2. Privacidad

La privacidad es otro aspecto fundamental que motiva a los investigadores de seguridad en crear métodos y técnicas para proteger la información privada. Desde la revolución de la tecnología de la información, la privacidad digital ha sido altamente relacionada con la tecnología de la información [71].

La privacidad tiene un conjunto de cinco atributos: conceder acceso, propiedad, alteración, publicación y aprobación. Estos atributos son presentados en la Figura 2.6 y se describe cada uno como [71]:

1. **Conceder Acceso**: el derecho a otorgar privilegios para acceder a la información privada.
2. **Propiedad**: el derecho a tener información privada.
3. **Alteración**: el derecho a modificar o actualizar información privada.
4. **Publicación**: el derecho a publicar información privada al público.
5. **Aprobación**: el derecho de transmitir información privada a una parte en particular.

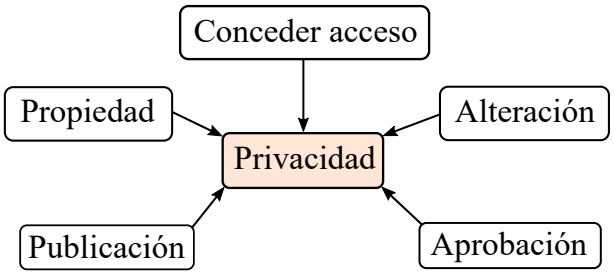


Figura 2.6: Atributos de privacidad (creación propia).

La relación entre la privacidad y la seguridad ha sido examinado desde varios puntos de vista [75], sin embargo, no existe una relación plenamente aceptada y justificada. Algunos investigadores creen que la privacidad y la seguridad son idénticos; otros creen que son completamente diferentes, otro grupo creen que la privacidad es parte de la seguridad tal como se presenta en la Figura 2.7, mientras que otros autores como Herold [76] afirman que la privacidad esta enfocada a un conjunto de leyes que determinan el derecho a poseer información y permitir el acceso, actualizar, publicar y transmitir información, mientras que la seguridad es un conjunto de estrategias, métodos y técnicas que se utilizan para hacer la información inaccesible, sin alteraciones a terceros no autorizados.
Administrar la configuración de seguridad o privacidad casi no representa el objetivo principal de un sitio web, ya que los usuarios están interesados principalmente en los servicios que ofrece la aplicación. Aunque la seguridad y la privacidad son funciones secundarias a los usuarios, estas deben ser transparentes, intuitivas y bien diseñadas.

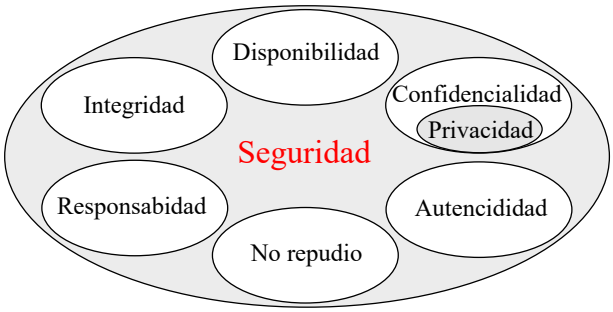


Figura 2.7: Una definición sobre la relación entre privacidad y seguridad (creación propia)

2.5.3. Evaluación de Seguridad

El proyecto OWASP (por sus siglas en inglés *Open Web-Application Security*) [77] desarrolló una metodología subjetiva de evaluación de seguridad para estimar los riesgos relacionados con la seguridad. El proyecto OWASP es un proyecto de seguridad de aplicaciones de código abierto. La comunidad de OWASP está formada por corporaciones, organizaciones educativas y una variedad de expertos en seguridad de todo el mundo que comparten su conocimiento de vulnerabilidades, amenazas, ataques y defensa. Por estas razones, esta tesis ha adoptado OWASP como la fuente primaria para identificar el nivel de riesgo de las aplicaciones tomando como base los principios de USec encontrados.

El modelo estándar se basa en factores de cálculo de probabilidad e impacto con el fin de estimar la gravedad del riesgo como se presenta la Ecuación 2.1.

$$Riesgo = probabilidad * impacto \tag{2.1}$$

De acuerdo a la ecuación anterior, la probabilidad esta integrada por un conjunto de amenazas y de vulnerabilidades. El objetivo aquí es estimar la probabilidad de un ataque exitoso por este conjunto de agentes. Por lo tanto, expandiendo la ecuación 2.1, la evaluación de riesgo esta dada por:

$$Riesgo = (amenaza * vulnerabilidad) * impacto \tag{2.2}$$

La metodología de evaluación de riesgo del OWASP está relacionado con nuestro trabajo porque evalúa el riesgo de seguridad a partir de los principios de seguridad usable y su impacto. Es simple y fácil de aplicar. Sin embargo, los factores de amenaza según la Ecuación 2.2 no se tienen en cuenta en esta tesis debido al alcance del trabajo de investigación, pero esta evaluación de riesgo podría representar una aproximación real del riesgo de la aplicación. La metodología de evaluación de riesgo en esta tesis es subjetiva y sólo proporciona cuatro niveles de gravedad (baja, media, alta y crítica).

A diferencia de la propuesta de Hausawi y Allen [71] sobre la evaluación del riesgo donde tiene en cuenta la seguridad y usabilidad por separado, en este trabajo sí se considera estos dos atributos de calidad de forma unida y además, presenta una interrelación del factor impacto de la seguridad con los principios de seguridad usable.

2.6. Seguridad Usable

El objetivo de la seguridad usable (USec) es el de mejorar la usabilidad y las características de seguridad y privacidad en sitios web y aplicaciones para los usuarios. Este es un campo de investigación relativamente nuevo, que requiere una comprensión de los campos de la seguridad informática y el HCI [78]. Comúnmente a la seguridad usable también se la encuentra en la literatura como Interacción-Humano Computador de la Seguridad o HCISec [79]. La Figura 2.8 ilustra la integración entre la usabilidad y la seguridad donde su resultado es la interrrelacionada área de la seguridad usable.

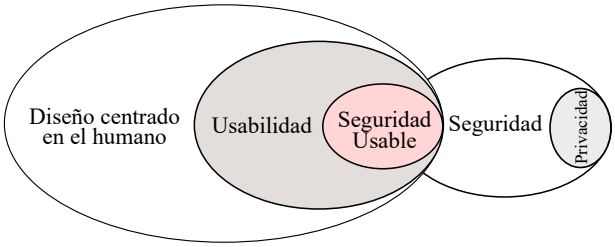


Figura 2.8: Área de la seguridad usable (Tomado de [71]).

Hay tres enfoques importantes iniciales para el diseño de sistemas seguros y usables [80][81]:

1. Construir sistemas que funcionen sin considerar la usabilidad durante el diseño, a continuación, tener en cuenta la usabilidad mediante la aplicación de los usuarios para obtener el uso de los mecanismos de seguridad.

2. Desarrollar sistemas con diseños que aliente a los usuarios a utilizar los mecanismos de seguridad de forma inventiva y correcta, ya que la usabilidad se aplica mediante el estímulo.

3. Construir sistemas teniendo en cuenta el aprendizaje. La usabilidad se aplica enseñando y capacitando a los usuarios sobre lo que necesitan saber para interactuar con los mecanismos de seguridad de manera adecuada y efectiva.

Entre los tres enfoques, el segundo parece ser el mejor, ya que proporciona una solución real de equilibrio entre usabilidad y seguridad. Este enfoque considera la usabilidad y la seguridad desde las etapas iniciales del desarrollo del software. Los otros dos enfoques no son soluciones apropiadas, sino que son elementos adicionales que cubren el problema sin resolverlo [82].

Para que una aplicación o sitio web pueda utilizarse desde una perspectiva de seguridad y privacidad, se espera de los usuarios lo siguiente [83]:

1. Los usuarios deben estar informados de manera consistente y confiable de las tareas relacionadas con la seguridad que necesitan para realizar.

2. Los usuarios deben ser capaces de determinar fácilmente cómo realizar las tareas necesarias con éxito.

3. Los usuarios no deben ser propensos a cometer errores que ponga en peligro la seguridad del sistema.

4. Los usuarios deben estar cómodos con la interfaz de usuario para que puedan seguir usándola.

Las propiedades de seguridad usable indican que la aplicación debe ser segura y que los usuarios deben ser capaces de reconocer las vulnerabilidades de seguridad y privacidad que existen. Por lo tanto, pueden protegerse mediante la utilización de las características de seguridad y privacidad de la aplicación de manera correcta y eficaz, ya que son fáciles de usar, aprender, entender y aplicar [78].

Existen diferentes definiciones de la seguridad usable de importantes investigadores: Whitten y Tygar [9] definen la seguridad usable como: "*el software de seguridad es usable si los usuarios confían en las tareas de seguridad que deben realizar, son capaces de averiguar cómo realizar con éxito esas tareas, no cometen errores peligrosos y están lo suficientemente cómodos con la interfaz para seguir usándola*".

Por otro lado, Jøsang y Patton [84] detallan que la seguridad usable "*trata de como debe manejarse la información de seguridad en una interfaz de usuario*". Johnston et al. [74] definen la seguridad usable como "*la parte de una interfaz de usuario que es responsable de establecer el terreno común entre un usuario y las características de seguridad de un sistema. Es decir, es la interacción humano-computador aplicada al área de la seguridad informática*".

El campo de la USec abarca el hecho de que la mayoría de las aplicaciones tienen características de seguridad que los usuarios finales tienen que interactuar. Estas interacciones incluyen la configuración y la toma de decisiones relacionadas con la seguridad. Sin embargo, la forma en que se presentan los aspectos de seguridad, en términos de su usabilidad, lo convierte en un proceso complicado, que los usuarios prefieren evitar y en la mayoría de los casos ignoran [85].

Varios estudios identifican al error humano como una de las causas más comunes de los problemas de tareas de seguridad. La razón de esto se debe principalmente al pobre diseño de la interfaz [85][9]. Los investigadores han señalado que el uso de sistemas de seguridad que carecen de usabilidad permite a los usuarios cometer errores debilitando la seguridad del sistema [79]. En consecuencia, la investigación en el campo de la seguridad usable se ha convertido en una necesidad.

Un obstáculo importante que impide que los usuarios entiendan las opciones de seguridad en la interfaz es el lenguaje y la terminología utilizada. Este es un problema que puede ser superado fácilmente con una investigación adecuada, permitiendo a los desarrolladores

optar por estrategias de diseño con respecto al lenguaje de seguridad. Es necesario implementar funcionalidades adicionales de ayuda, así como capacitar a los usuarios en cómo abordar las decisiones relacionadas con la seguridad de la aplicación [85].

2.6.1. Integrando Seguridad y Usabilidad

La necesidad de mejorar la usabilidad de las características de seguridad es indiscutible [9][85]. Sin embargo, existe una paradoja entre seguridad y usabilidad. Esta paradoja ha dado lugar a un debate dentro de la comunidad científica acerca de si estos dos atributos pueden ser fusionados. Algunos trabajos indican que la usabilidad funciona en contra de la seguridad. Asimismo, la seguridad trabaja contra la usabilidad. Este concepto se ha extendido entre la mayoría de los investigadores de la seguridad usable [80][81]. Sin embargo, otros investigadores tomaron la dirección opuesta, creyendo que la usabilidad y la seguridad no son conceptos contradictorios [83].

Yee [83] afirma que si es posible integrar la usabilidad y la seguridad de la siguiente manera: "*un sistema que es más seguro es más controlable, más fiable y por lo tanto más usable; un sistema más usable reduce la confusión y, por lo tanto, es más probable que sea seguro*".

Whitten y Tygar [9] indican que cuanto más utilizable sea el sistema informático, menos seguridad posee. Lampson [86] afirma que una de las principales razones para que los sistemas de seguridad fracasen en la práctica, es el problema semántico conceptual. A los usuarios y administradores no les gustan los mecanismos de seguridad porque creen que estos mecanismos debilitan la usabilidad de los sistemas.

Gutmann y Grigg [87] afirmaron que hay varias opciones a considerar cuando se trata de alinear la seguridad y la usabilidad. En general, a través de la igualdad entre seguridad y usabilidad, o priorizando uno sobre el otro.

La igualdad se produce cuando la usabilidad y la seguridad se combinan en un concepto y se consideran desde el momento inicial de los sistemas informáticos en desarrollo. La usabilidad y la seguridad están mejor alineados cuando van juntos desde el inicio del desarrollo del sistema informático [88]. En este trabajo de investigación, esta opción es la que se tiene en cuenta.

La priorización ocurre cuando uno de los dos términos de usabilidad o seguridad se utiliza para trabajar en beneficio de la otra. Obviamente, la seguridad no puede funcionar en beneficio de la usabilidad, porque es más complicado generar "mecanismos de usabilidad seguros". Más bien, es más fácil obtener "mecanismos de seguridad usable". El enfoque anterior ha sido apoyado y demostrado por varios investigadores [79][89][90].

Idealmente, las herramientas de seguridad (e.g., contraseñas) deberían diseñarse con un porcentaje de 100 % en términos de seguridad y un porcentaje de 100 % en términos de usabilidad. Sin embargo, esto es imposible de lograr. Lo importante es reconocer qué tanto

la seguridad como la usabilidad son igualmente críticas en el diseño y que la integración entre ellos pueda ser superada.

2.6.2. Evaluación de Seguridad Usable

Se ha determinado que es necesario establecer nuevos métodos de evaluación con el fin de desarrollar interfaces de usuario para USec. Esto se determina sobre la base de tres características humanas que han sido identificadas entre los usuarios finales [78]. La primera es la apertura donde los usuarios continúan o abandonan el uso del sistemas por voluntad propia. La segunda es la adaptación donde los usuarios tienen sus propios requisitos, tecnologías y necesidades especiales. Y la tercera es la aparición donde se relaciona con la adaptación, lo que conduce a nuevos comportamientos que no se han visto antes.

Herzog y Shahmehri [91] han investigado el área de USec desde una perspectiva diferente, pero igualmente importante. Reconocen la necesidad de nuevos métodos y herramientas de evaluación para USec, sin embargo, afirman que poco se ha hecho realmente con respecto a cómo las aplicaciones pueden ayudar a los usuarios en las decisiones de seguridad y sus tareas. Por esa razón, investigan las diversas técnicas de ayuda que mejor se adapten a los usuarios con sus tareas relacionadas con la seguridad. Estas técnicas de ayuda incluyen documentación en línea, ayuda contextual, asistentes, puesta en escena segura, navegación social y seguridad ocultada incorporada.

Kaiser & Reichenbach [25] proponen una taxonomía para clasificar los errores de usabilidad con respecto a la seguridad. El primer nivel de la taxonomía es dividir los errores en problemas de usabilidad y relacionados con la seguridad. La intersección de estos dos conjuntos es la importante: los problemas de usabilidad críticos de la seguridad. Este grupo de problemas se divide nuevamente en problemas que ocurren a pesar de que el usuario tiene suficientes omisiones dentro de la seguridad y lo que ocurre debido a la falta de conocimiento. El último nivel está dividido en categorías, *decaer* (la secuencia correcta de acciones no produjo los resultados esperados) y *errores* (una secuencia factible de acciones originadas de un plan defectuoso). Los autores siguen estableciendo desigualdades para medir la criticidad de los diferentes tipos de errores, y recomiendan el uso de evaluación heurística para descubrir los errores.

Braz et al. [4] propone un nuevo diseño de inspección de usabilidad basado en métricas para diseñar, inspeccionar y evaluar la usabilidad de los sistemas de seguridad. El modelo es denominado *Security Usability Symmetry* (SUS). El SUS tiene un conjunto de pasos a seguir que al final identifica problemas que están relacionados con la usabilidad y la seguridad juntos durante la fase de diseño.

La investigación anterior está directamente relacionada con nuestra investigación en dos puntos. En primer lugar, se tienen en cuenta algunos principios para métodos de autenticación que consideramos son los mas relevantes para nuestro trabajo. A diferencia del modelo de Braz et al. [4], en esta tesis sí se tiene en cuenta una integración más completa

entre la usabilidad y seguridad haciendo su evaluación menos subjetiva. En segundo lugar, el modelo de Braz et al. [4] descubre los problemas de seguridad usable durante la fase de implementación. En esta propuesta, los problemas de seguridad usable pueden ser evitados porque se tiene en cuenta recomendaciones de diseño en la fase de requisitos.

2.6.3. Principios de Seguridad Usable

A pesar de que la USec es un área de amplio interés, hay principios limitados que explican cómo se puede lograr. Un argumento interesante planteado es que los usuarios no son los únicos que requieren seguridad usable. Los desarrolladores también han sido identificados como un grupo objetivo que requiere preparación y herramientas adecuadas para sus diseños [92].

La falta de orientación para los desarrolladores ha dado lugar a los primeros intentos de proporcionar un estándar para USec. El primer esfuerzo en esta área fue proporcionado por un grupo de trabajo del consorcio W3C[3] (por sus siglas en inglés *World Wide Web Consortium*) llamado *Web Security Context Working Group* donde se definen directrices y requisitos para la presentación y comunicación de información de contexto de seguridad web a los usuarios finales. El objetivo del estándar es hacer que la seguridad sea útil y especificar las acciones del usuario para la seguridad [93].

Varios investigadores han propuesto principios para la seguridad usable. Los trabajos de investigación de Whitten & Tygar [17][9], se consideran pioneros en este aspecto. Los principios más reconocidos y referenciados en la literatura incluyen los de Whitten & Tygar [9], Yee [83], Johnston et al. [74], Katsabas et al. (2005), Saltzer & Schroeder [94], Chiasson et al. [95] y Garfinkel [12] . Los trabajos de estos investigadores proporcionan una base sobre la cual se pueden diseñar más métodos de evaluación para USec.

El trabajo de investigación de Whitten & Tygar [9] sobre la usabilidad de una aplicación de cifrado (PKI[4] por sus siglas en inglés *Public Key Infrastructure*) considera que tiene una buena interfaz gráfica de usuario, pero los resultados mostraron que no era adecuado en la parte de usabilidad para proporcionar seguridad eficaz para la mayoría de los usuarios. Diseñar estrategias para la creación de la seguridad usable necesitarán tomar en cuenta explícitamente estas propiedades. Cinco propiedades se describen a continuación:

1. **Usuario sin motivación**: la seguridad es usualmente un objetivo secundario para las personas. Los diseñadores de interfaces de usuario no deben asumir que los usuarios estarán motivados a leer políticas de seguridad. Por otra parte, si la seguridad es demasiado difícil, los usuarios pueden renunciar a ella por completo.

[3]Disponible en: https://www.w3.org/. Consultado Enero del 2017

[4]Una infraestructura de clave pública PKI, es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

2. **Abstracción**: la gestión de la seguridad a menudo implica políticas de seguridad, que son sistemas de reglas abstractas que deciden si conceden acceso a los recursos.

3. **Realimentación**: los sistemas deben proporcionar información adecuada a fin de evitar errores y apoyar las tareas del usuario, que son a veces un tanto confusa para los desarrolladores.

4. **Puerta del establo**: una vez que un *password* se ha dejado accidentalmente sin protección, aunque sea por poco tiempo, no hay manera de asegúrese de que ya no ha leído por un atacante.

5. **Enlace más débil**: los usuarios (vistos como el eslabón más débil) deben estar motivados para manejar la configuración de seguridad a fin de evitar que esta esté comprometida.

Yee [83] ha desarrollado un modelo de actor-capacidad describiendo el aparente conflicto entre la forma en que los usuarios esperan que el computador funcione y la manera de que realmente puede funcionar, elaborado una lista de diez principios básicos para el diseño de interacción segura.

1. **Camino de la menor resistencia**: la forma más natural de hacer cualquier tarea también debe ser la forma más segura.

2. **Límites apropiados**: la interfaz debe exponer, y el sistema debe hacer cumplir, las diferencias entre los objetos y acciones que le importan al usuario.

3. **Autorización explícita**: las autoridades de los usuarios sólo deben ser proporcionados a otros actores como resultado de una acción explícita del usuario.

4. **Visibilidad**: la interfaz debe permitir al usuario revisar fácilmente los actores activos y las relaciones de autoridad que afectarían las decisiones relevantes para la seguridad.

5. **Revocabilidad**: la interfaz debe permitir al usuario revocar fácilmente autoridades que el usuario ha concedido, siempre que la revocación sea posible.

6. **Capacidad esperada**: la interfaz no debe dar al usuario la impresión de que es posible hacer algo que no se pueda hacer realidad.

7. **Ruta de confianza**: la interfaz debe proporcionar un canal de comunicación infalsificable y fiel entre el usuario y cualquier entidad de confianza para manipular las autoridades en nombre del usuario.

8. **Identificabilidad**: la interfaz debe hacer cumplir que los distintos objetos y distintas acciones tienen representaciones identificables y diferenciables infalsificables.

9. **Expresividad**: la interfaz debe proporcionar suficiente poder expresivo para describir una política de seguridad segura y sin excesiva dificultad y permitir que los usuarios expresan las políticas de seguridad en términos de que se ajusten a sus metas.

10. **Claridad**: el efecto de cualquier acción relevante para la seguridad debe ser claramente evidente para el usuario antes de que se adopte la medida.

Los principios Johnston et al. [74] ayudan a crear una relación de confianza entre el usuario y la interfaz. Desde la perspectiva del usuario, una aplicación sólo se utilizará a su máximo potencial si el usuario puede confiar en ella.

1. **Transmitir características**: la interfaz debe transmitir las características de seguridad disponibles al usuario.

2. **Visibilidad del estado del sistema**: los usuarios deben ser capaces de observar el estado de seguridad de las operaciones internas.

3. **Aprendizaje**: la interfaz no debe trasmitir temor y ser fácil de aprender.

4. **Diseño estético y minimalista**: sólo se mostrará la información de seguridad relevante.

5. **Errores**: los mensajes de error deben ser detallados y, si es necesario, explicar dónde obtener ayuda.

6. **Satisfacción**: la interfaz debe ayudar al usuario a tener una experiencia satisfactoria con el sistema.

Katsabas et al. [96] ha identificado diez principios, que asegurarán a los desarrolladores seguir métodos eficaces y utilizables para la funcionalidad de la seguridad en las aplicaciones.

1. **Estado visible del sistema y funciones de seguridad**: las aplicaciones no deben esperar que los usuarios busquen para encontrar las herramientas de seguridad o que tengan funciones ocultas dentro de la aplicación. La información de estado debe actualizarse periódicamente y debe ser fácilmente accesible.

2. **La seguridad debe ser fácilmente utilizada**: la interfaz debe ser cuidadosamente diseñada y requiere un mínimo esfuerzo para hacer uso de las características de seguridad.

3. **Conveniente para usuarios avanzados como principiantes**: mostrar información suficiente para un usuario por primera vez, mientras que no demasiada información para un usuario experimentado.

4. **Evitar el uso intensivo de vocabulario técnico o términos avanzados**: a usuarios principiantes les resultará difícil utilizar las características de seguridad en su aplicación si se usan vocabulario técnico y términos avanzados.

5. **Manejar los errores apropiadamente**: diseñar la aplicación cuidadosamente para evitar errores y minimizar el máximo posible los errores causados por el uso de las características de seguridad.

6. **Permitir la personalización sin riesgo**: las opciones de salida deben ser proporcionadas en caso de que algunas funciones sean elegidas por error y los valores por defecto se deben restaurar fácilmente.

7. **Configuración de seguridad fácil de configurar**: de esta manera el usuario se sentirá más seguro de cambiar y configurar la aplicación de acuerdo a sus necesidades.

8. **Ayuda y documentación**: se debe proporcionar ayuda y documentación apropiada que ayude a los usuarios en las dificultades que puedan enfrentar.

9. **Proteger al usuario**: la aplicación deben proporcionar al usuario las últimas características de seguridad para sentirse protegido.

10. **La seguridad no debe reducir el rendimiento**: al diseñar la aplicación con cuidado y utilizando algoritmos eficientes, debería ser posible utilizar las características de seguridad con el mínimo impacto en la eficiencia de la aplicación.

El trabajo de Saltzer & Schroeder [94] presenta la base necesaria para el diseño e implementación de sistemas de software de seguridad. Sus principios describen prácticas útiles que son apropiados principalmente para las decisiones de software a nivel de arquitectura, independientemente de la plataforma o el lenguaje del software.

1. **Mantener el diseño tan simple y pequeño como sea posible**: la forma más natural de hacer cualquier tarea también debe ser la forma más segura.

2. **Defectos a prueba de fallos**: significa que la situación por defecto es la falta de acceso, y el esquema de protección identifica condiciones en las que se permite el acceso.

3. **Diseño abierto**: el diseño no debe ser secreto. Los mecanismos no deben depender de el desconocimiento de los posibles atacantes, sino más bien sobre un control especifico (*passwords* o teclas protegidas).

4. **La separación de privilegio**: cuando sea posible, un mecanismo de protección que requiere dos llaves para desbloquear es más robusta y flexible que el que permite el acceso con una única clave.

5. **Menor privilegios**: cada programa software y usuario deben funcionar con el menor número de privilegios necesarios para completar el trabajo.

6. **Menos mecanismos comunes**: cada mecanismo compartido (especialmente la de las variables compartidas) representa una ruta potencial de información entre usuarios, y debe ser diseñado cuidadosamente para asegurarse de no poner en peligro la seguridad.

7. **Aceptabilidad psicológica**: es esencial que la interfaz humana esté diseñado para facilitar su uso, por lo que los usuarios que lo usan de forma rutinaria y automática, apliquen los mecanismos de protección correctamente.

Aunque los usuarios finales son la principal preocupación en el campo de la seguridad usable, las interfaces para profesionales en seguridad son igualmente importantes, ya que las consecuencias de los problemas de usabilidad pueden potencialmente ser vulnerables a ataques. Chiasson et al. [95] desarrollaron un conjunto preliminar de directrices de diseño para las interfaces de gestión de seguridad de la siguiente manera:

1. Los administradores debe ser consciente de forma fiable sobre las tareas de seguridad que deben realizar.

2. Los administradores deben ser capaces de averiguar cómo llevar a cabo con éxito estas tareas.

3. Los administradores deben ser capaces de decir cuando se han completado sus tareas.

4. Los administradores deben tener realimentación suficiente para determinar con precisión el estado actual del sistema y las consecuencias de sus acciones.

5. Los administradores deben ser capaces de volver a un estado anterior si una decisión de seguridad tiene consecuencias imprevistas.

6. Los administradores deben ser capaces de formar un modelo mental preciso y significativo del sistema que están protegiendo.

7. Los administradores deben ser capaces de examinar fácilmente el sistema en diferentes niveles de encapsulación con el fin de obtener una perspectiva general y ser capaz de diagnosticar con eficacia los problemas específicos.

8. La interfaz debe facilitar la interpretación y diagnóstico de posibles amenazas de seguridad.

9. Los administradores deben ser capaces de buscar asesoramiento y aprovechar el conocimiento de la comunidad para tomar decisiones de seguridad.

10. La interfaz debe alentar a los administradores a abordar temas críticos en el momento oportuno.

En su estudio de usabilidad con respecto a dos gestores de contraseña, Chiasson et al. [24] propusieron dos criterios adicionales que apoyan realmente los puntos 2 y 3 de Whitten & Tygar [9] sobre:

1. **Ser capaz de decir cuando se haya completado su tarea**: los usuarios no podían decir si su tarea había sido completado con éxito, y a veces asume incorrectamente el éxito.

2. **Realimentación para determinar con precisión el estado actual del sistema**: es especialmente importante para apoyar los modelos mentales en interfaces de seguridad.

Simson Garfinkel [12] desarrolló un conjunto de principios de diseño para la creación y evaluación de los sistemas de seguridad y evalúa el trabajo de Yee con la intención de construir principios de diseño con base en lo propuesto por Yee.

1. **El principio de la menor sorpresa**: sostiene que el computador no debe sorprender al usuario cuando espera que el equipo se comporte de una manera que sea segura.

2. **El principio de buena seguridad**: sostiene que es un error no instalar un buen sistema que actualmente se disponen. Si buenos sistemas no se instalan, los usuarios finales que no están capacitados en seguridad, crearán sus propias soluciones de seguridad propia con características deficientes.

3. **Proporcionar políticas de seguridad estandarizadas**: actualmente los sistemas de seguridad ofrecen demasiadas opciones de configuración que son relevantes para la seguridad. Estas opciones son con frecuencia molestas para los usuarios finales. Lo que se necesita es una serie de políticas bien estructuradas, comprensibles y fáciles de enseñar.

4. **Vocabulario consistente**: la usabilidad se promueve cuando la información se presenta con un vocabulario consistente y significativo.

5. **Control y ubicación consistente**: además de la estandarización de vocabulario, es importante que los controles relacionados con la seguridad en interfaces gráficas de usuario pueden ser igualmente estandarizados.

6. **Sin carga externa**: las herramientas de seguridad no deben suponer una carga para los no usuarios que no se benefician de su uso.

2.7. Integrando Usabilidad y Seguridad en el Proceso de Desarrollo

La seguridad es un complejo e importante requisito no funcional de los sistemas de software. Según Anderson [97], "*muchos sistemas fallan porque sus diseñadores protegen las cosas equivocadas, o protegen las cosas correctas en el camino equivocado*". Algunos enfoques recientes han dirigido la seguridad desde la perspectiva tecnológica, otros desde el ángulo de Interacción Humano-Computador, ofreciendo mejores interfaces de usuario para mejorar

la usabilidad de los mecanismos de seguridad [79]. Sin embargo, los métodos de diseño actuales para desarrollar aplicaciones usables y seguras están incompletos o se centran en cierta fase en el proceso de desarrollo. Esto hace que sea difícil para los desarrolladores debido a que deben hacer uso de modelos independientes.

2.7.1. Ingeniería de la Seguridad

La ingeniería de seguridad incluyen entre muchas cosas, las actividades necesarias para diseñar una solución segura. Entre estos se incluyen la obtención y definición de requisitos de seguridad, principios de diseño para la seguridad, uso de herramientas de análisis estático, revisiones e inspecciones seguras y métodos de prueba seguros [98].

Como la seguridad es un atributo de calidad fundamental para la mayoría de los productos de software actuales, la importancia de incorporar actividades relacionadas con la seguridad entre los desarrolladores de software se está incrementando rápidamente [99]. Como resultado, ha habido trabajos en la integración de la seguridad en el ciclo de vida del desarrollo del software. Es importante mencionar que la privacidad está implícitamente integrada en la seguridad (ver Figura 2.7), y a su vez en el desarrollo del software, ya que la seguridad considera a la privacidad durante la fase de requisitos.

Eckert [100] propone un método para la construcción de sistemas seguros en términos de ingeniería de seguridad sistemática. La autora utiliza un método iterativo descendente como en el desarrollo del software y ajusta su método con respecto a problemas especiales de ingeniería de seguridad. En la Figura 2.9 se muestran las fases de desarrollo para la construcción de sistemas de seguridad.

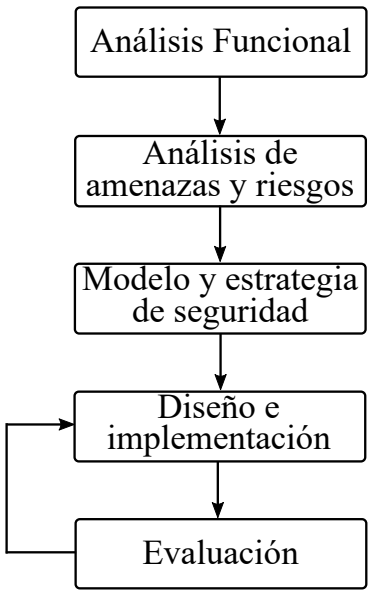


Figura 2.9: Fases del proceso de desarrollo de la ingeniería de la seguridad (Tomado de [100])

1. *Análisis funcional*: definir las características funcionales, el entorno y el propósito del sistema. Posteriormente, se describen y unen los componentes y servicios necesarios del sistema con su funcionalidad.

2. *Análisis de amenazas y riesgos*: se realiza un análisis de la amenaza en el sistema. El análisis considera diferentes tipos de ataques y define a posibles atacantes, como programadores, usuarios y código móvil. Posteriormente, en el análisis de riesgo las amenazas encontradas deben ser clasificadas en relación con la probabilidad de ocurrencia y el daño potencial que puede causar.

3. *Modelo y estrategia de seguridad*: con los resultados de la fase anterior, los requisitos del sistema se pueden deducir. Además, debe construirse un modelo de seguridad abstracto para comprobar las características de seguridad.

4. *Diseño e implementación*: en primer lugar, se debe definir todos los componentes del sistema, interfaces y dependencias. Y además, deben elegirse algoritmos y mecanismos de seguridad adecuados para los componentes con funcionalidad de seguridad.

5. *Evaluación*: el sistema implementado tiene que ser probado en varias etapas (prueba de módulo, prueba de integración, inspección de código) con especial énfasis en la funcionalidad de seguridad y las interfaces del sistema. Con los resultados de la evaluación, es posible que el sistema sufra algunos cambios.

Grupta et al. [31] desarrollaron un enfoque para integrar la seguridad en el ciclo de vida del desarrollo del producto. La construcción de este enfoque apoya el objetivo de realizar productos seguros. El enfoque de seguridad se puede aplicar a cualquier dominio para facilitar el análisis de requisitos de seguridad y el desarrollo de herramientas usables como listas de comprobación, principios y políticas de seguridad. El enfoque propuesto hace uso del marco de seguridad desarrollado por Bell Labs[5], el cual permite ayudar a los operadores de red entender las necesidades para diseñar, implementar y mantener una red segura. Este marco es ahora el fundamento de las normas internacionales de seguridad de redes conocidas como ISO/IEC 18028-2:2005 y ITU-T X.805 [101][102].

La Figura 2.10 ilustra el enfoque propuesto para asegurar el proceso de desarrollo del producto. Garantizar que los objetivos y compromisos de seguridad se integran en los procesos de realización del producto es un factor clave para integrar la seguridad en el ciclo de vida general del desarrollo. Algunos atributos deben incluirse en el proceso de desarrollo para el lanzamiento seguro del producto tales como capacitación, documentación, entorno operativo y usabilidad.

1. *Fase de requerimientos y diseño*: en esta fase, los requisitos de seguridad se definen para satisfacer los objetivos de seguridad de la organización y las necesidades del usuario. Algunas consideraciones de seguridad para características generales, así como requisitos de seguridad son los principales resultados de la fase de requisitos.

[5]Disponible en: https://www.bell-labs.com/. Consultado en Septiembre del 2016

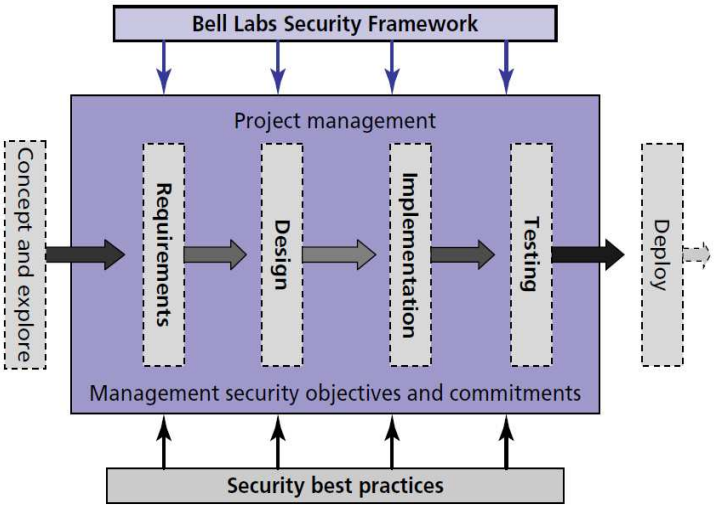


Figura 2.10: Marco de trabajo para desarrollar productos seguros (Tomado de [31])

2. *Fase de implementación*: la fase de implementación simplemente es una instancia de las recomendaciones propuestas en la fase de diseño y requisitos. Una de las áreas clave en la fase de implementación es la ingeniería del software de tal manera que la seguridad está incorporada.

3. *Fase de evaluación*: La evaluación de seguridad debe ser parte integral de cualquier estrategia de seguridad de productos y servicios. Debe incorporarse en procesos que permitan una adecuada planificación y apoyo para garantizar que los usuarios reciban la calidad que se espera. Las pruebas deben centrarse en los activos adecuados y las vías de los ataques.

Microsoft Corporation [103] ha desarrollado un modelo de ciclo de vida de desarrollo para seguridad compuesto por siete fases y basado en el ciclo de vida de desarrollo de software tradicional. Este modelo es una colección de 17 actividades de seguridad aplicadas al proceso de desarrollo de software para obtener software seguro. Cada fase tiene un conjunto de acciones que deben ser tenidas en cuenta. La Figura 2.11 muestra las fases desarrollado por Microsoft junto con sus actividades.

Mohammeda et al. [104] identifican enfoques existentes de seguridad de software utilizados en el ciclo de vida del desarrollo de software. Con el fin de cumplir con el objetivo, llevaron a cabo un estudio sistemático para identificar los estudios preliminares sobre el uso de técnicas de seguridad en el desarrollo del software. En total, seleccionaron y categorizaron 118 estudios primarios. Después de analizar los estudios seleccionados, identificaron 52 enfoques de seguridad y los clasificaron en cinco categorías principales: modelado de requisitos, identificación de vulnerabilidades, adaptación y mitigación, proceso centrado en seguridad de software, perfiles de modelado seguros y no-modelado seguro basado en UML.

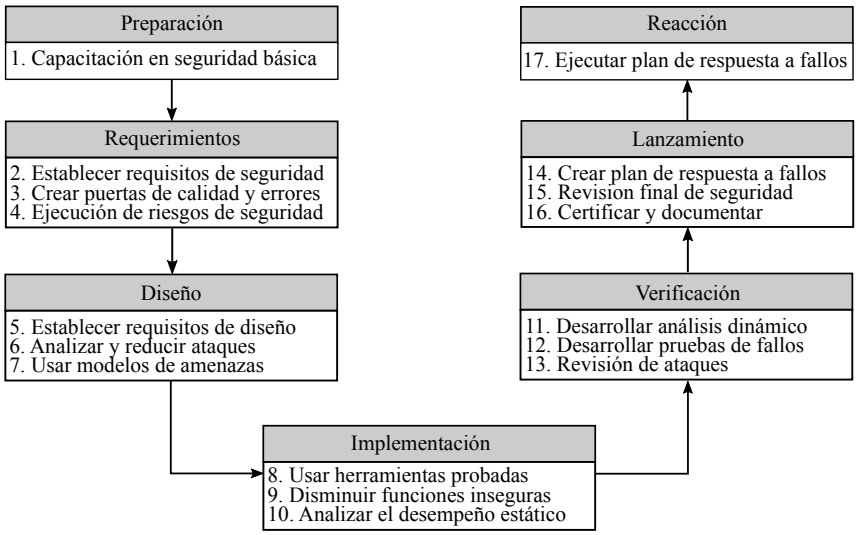


Figura 2.11: Modelo de ciclo de vida de desarrollo para seguridad por Microsoft (Adaptado de [103])

Los resultados muestran que los enfoques más utilizados son el análisis estático y el análisis dinámico que proporcionan controles de seguridad en la fase de codificación. Además, muestran que muchos estudios en esta revisión consideraron los controles de seguridad alrededor de la etapa de codificación del desarrollo de software. Este trabajo ayudará a las organizaciones de desarrollo de software a comprender mejor los enfoques de seguridad de software existentes utilizados en el ciclo de vida del desarrollo de software. También puede proporcionar a los investigadores una base firme sobre la que desarrollar nuevos enfoques de seguridad de software.

Alkussayer & Allen [99] desarrollaron un *framework* para integrar patrones de seguridad y prácticas de seguridad en el ciclo de vida del desarrollo de software. El *framework* tiene dos conjuntos de componentes, uno de ellos representa un proceso de desarrollo en seis etapas sobre prácticas de seguridad, y el otro representa un proceso de utilización en cuatro etapas de patrones de seguridad. Según los autores, la relación entre las prácticas de seguridad y los patrones es bidireccional. Los autores afirman que el marco de integración relaciona fuertemente los patrones de seguridad con las prácticas de seguridad apropiadas, lo que conduce a un desarrollo claro y sencillo para el software seguro. La Figura 2.12 muestra el marco .

A pesar de la continua investigación sobre seguridad, esta no ha sido investigado más a fondo como otros atributos de calidad. Tal vez esto se deba a que la seguridad se considera como un requisito cualitativo no funcional que suele considerarse como un complemento después de que el desarrollo del producto de software se ha completado o en las últimas etapas. En consecuencia, otros atributos de calidad, como la usabilidad, se han vuelto más maduros que la seguridad [71].

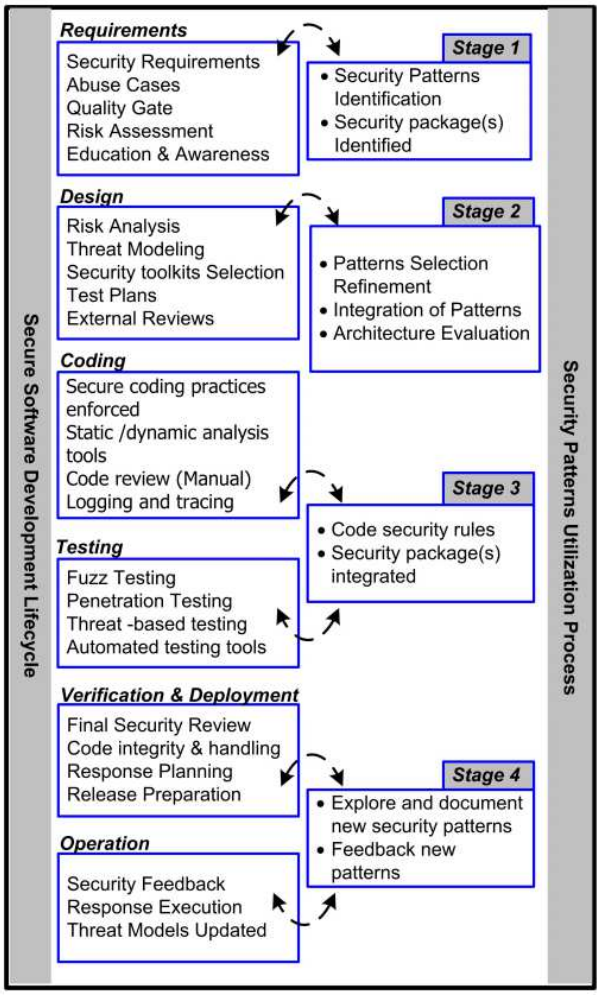


Figura 2.12: Marco de integración de desarrollo de la seguridad (Tomado de [99]).

A partir de lo anterior surge una pregunta, ¿qué tiene que ver la ingeniería de la seguridad con la seguridad usable?. Y la respuesta es simple, mucho. Como se vió en los apartados anteriores, trabajos tales como [31] y [100] enfatizan en la componente de usabilidad en sus diseños de seguridad. Además, como lo sostiene Markotten [23] donde afirma que los enfoques actuales de la ingeniería de seguridad se centran principalmente en modelos de ataques, mecanismos seguros y pruebas de código para garantizar un estándar de seguridad de alto nivel. Sin embargo, estos enfoques no enfatizan suficientemente la usabilidad del sistema y surge el riesgo de que los mecanismos implementados creen sobrecargas para los usuarios o requieran un comportamiento del usuario que no sea factible.

2.7.2. Procesos de Diseño para Seguridad Usable

Los atributos de calidad del software en general, y la seguridad y usabilidad en particular, son requisitos importantes no funcionales para la mayoría de los sistemas informáticos. Para ello, se han realizado varios estudios y se han propuesto métodos, marcos o procesos

para hacer que tales atributos sean aplicables a las actividades de desarrollo de software [105]. Con base en lo anterior, la integración de la usabilidad y la seguridad es un reto. Este hecho es declarado por la mayoría de los investigadores de la seguridad usable en trabajos anteriores.

Flechais et al. [79] describe AEGIS (por sus siglas en inglés *Appropriate and Effective Guidance for Information Security*)para ayudar a los desarrolladores a identificar desafíos de seguridad en el proceso de desarrollo y suministrar métodos para tratarlos sistemáticamente. AEGIS es útil en el diseño de sistemas de seguridad usable porque la usabilidad se considera desde el inicio del ciclo de vida del desarrollo. El punto clave de los autores es que la usabilidad debe considerarse como uno de los requisitos de seguridad, y los requisitos de seguridad deben aplicarse a los mecanismos de seguridad para revelar los problemas de seguridad relacionados con la usabilidad. En la Figura 2.13 es presentado el modelo AEGIS.

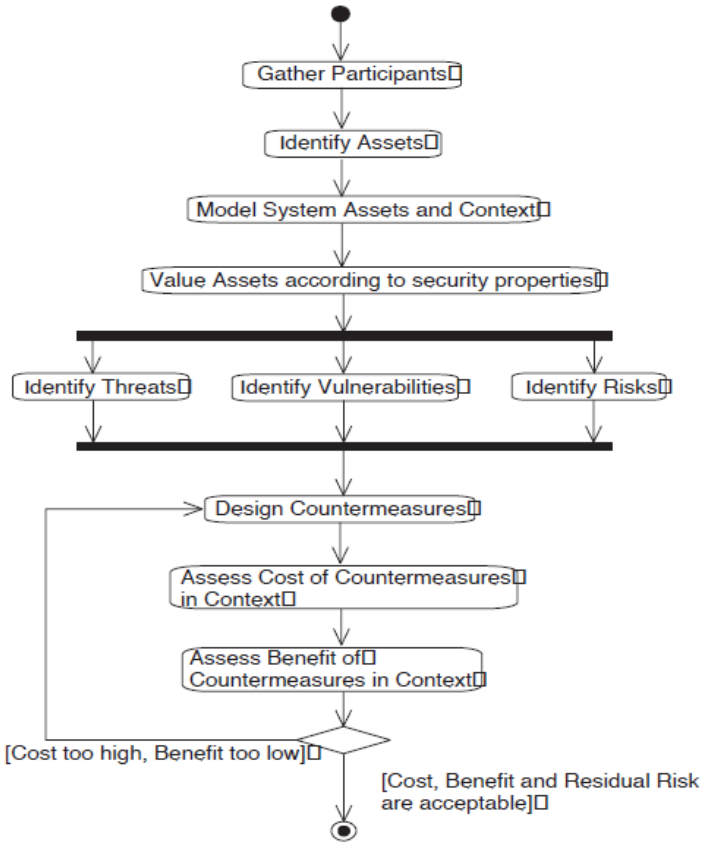


Figura 2.13: Proceso de diseño seguro AEGIS (Tomado de [79]).

Un enfoque similar pero más general es presentado por Markotten [23]. Este proceso se basa en la ingeniería de la usabilidad de Nielsen [50] y el modelo de la ingeniería de seguridad de Eckert [100]. Aunque estos modelos son muy bien conocidos por los desarrolladores del HCI y la comunidad de seguridad, estos por lo general están separados en el desarrollo

del software. Markotten propone un modelo nuevo combinando los modelos anteriores en un proceso donde la seguridad y la usabilidad convivan, ver Figura 2.14.

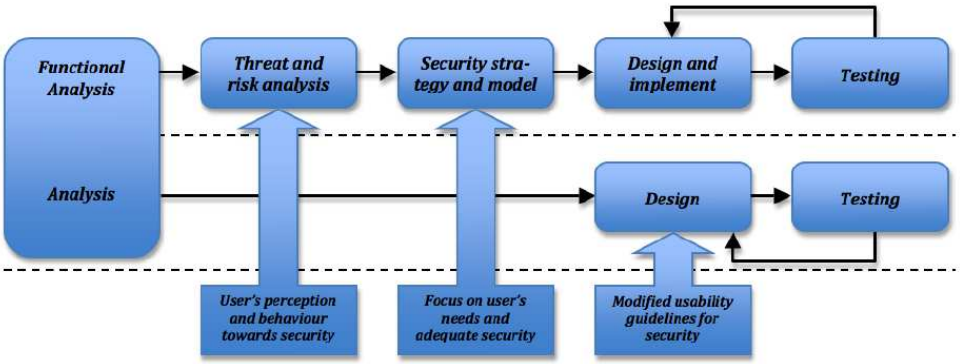


Figura 2.14: Ingeniería de la seguridad centrada en el usuario (Adaptada de [23]).

Khalid et al. [106] introduce un modelo que pueda ayudar a equilibrar los requisitos de seguridad y usabilidad para desarrollar sistemas con un nivel adecuado, ver Figura 2.15. El objetivo se logra mediante la identificación de los requisitos de seguridad y usabilidad, analizando la relación entre estos requisitos y finalmente diseñando el modelo propuesto. El modelo propuesto ayuda a identificar y especificar los requisitos de usabilidad de cada requisito de seguridad especificado. Este modelo no se limita a manejar los requisitos de usabilidad que se requieren para ser equilibrados con los requisitos de seguridad, sino que también implica la identificación y evaluación de los requisitos de usabilidad que no se requiere para ser equilibrado con los requisitos de seguridad.

Un producto software diseñado con elementos de seguridad es mucho más confiable que aquellos en los que la seguridad se considera posterior. Tradicionalmente, las características de seguridad se consideran durante la fase de diseño y su usabilidad se ha encontrado después de la fase de implementación del proceso de desarrollo del software. Parven et al. [32] presenta un diagrama de flujo para el proceso de especificación de requisitos seguros y usables que describe los pasos principales con el fin de identificar requisitos funcionales y no funcionales para seguridad (amenazas, vulnerabilidades y casos de riesgo y abuso) y usabilidad (aprendizaje fácil, la eficiencia de la tarea, la capacidad de recordar y la comprensión y la satisfacción del usuario).

Kainda et al. [34] propone un modelo de amenaza para realizar análisis de seguridad y usabilidad. Emplea escenarios de uso y de amenazas para comprender e identificar los elementos del sistema que son amenazas para la usabilidad, seguridad o ambos de un sistema. Los escenarios de uso se utilizan para identificar áreas que pueden dificultar la usabilidad de un sistema, mientras que los escenarios de amenazas se utilizan para identificar áreas que pueden ayudar a usuarios no malintencionados a romper la seguridad del sistema. Cuando los escenarios de amenaza de un sistema son más utilizables en comparación con los escenarios de uso, es más probable que los usuarios realicen los primeros.

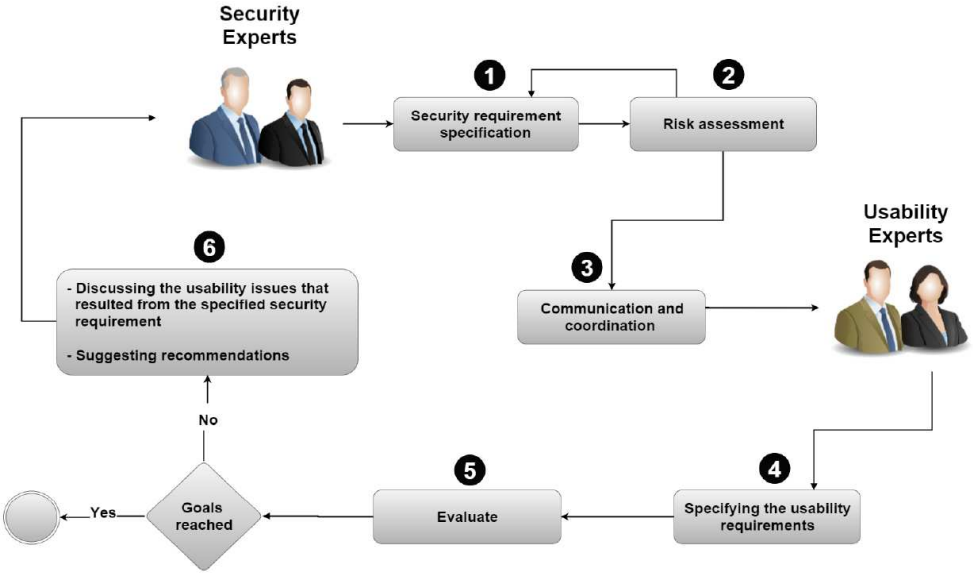


Figura 2.15: Modelo propuesto para equilibrar los requerimientos de seguridad y usabilidad (Tomada de [106]).

Faily et al. [35] describen un estudio en el que se utilizaron técnicas de seguridad y usabilidad en un proyecto de investigación y desarrollo llamado *Webinos* – un entorno seguro y multiplataforma para aplicaciones web. Describen las dificultades con que se enfrentan para aplicar estas técnicas de seguridad y usabilidad, los enfoques adoptados para superarlas y las lecciones que pueden ser aprendidas por otros que tratan de construir usabilidad y seguridad en los sistemas de software.

Hausawi & Allen [71] proponen directrices para mejorar la selección de las herramientas de diseño adecuadas para la seguridad, usabilidad y seguridad usable con el fin de garantizar que el proceso de diseño satisfaga las necesidades de los requisitos. Por otra parte, estas directrices ayudan a identificar adecuadamente la selección de herramientas de diseño, descubriendo los conflictos y ayudando a superar las contradicciones en las decisiones de diseño.

Finalmente, Ursula Holmström [107] presenta un enfoque centrado en el usuario para el diseño de software de seguridad. Aplica el diseño centrado en el usuario al desarrollo de un concepto de gestor de seguridad para un dispositivo portátil y de comunicación. El objetivo principal está en el desarrollo de los conceptos de seguridad relevantes para un usuario no técnico de servicios en red.

2.7.3. Metodología MPIu+a

La metodología MPIu+a propuesta por Granollers [41], está orientada hacia el diseño de sistemas interactivos centrados en el usuario. El modelo propuesto tiene las siguientes

fases como se presenta en la Figura 2.16: análisis de requisitos, diseño, implementación, Uno de los aspectos importantes de la propuesta es integrar la ingeniería de software con los principios de ingeniería de usabilidad y accesibilidad, proporcionando una metodología capaz de guiar a los equipos de desarrollo durante el proceso de implementación de un determinado sistema interactivo.

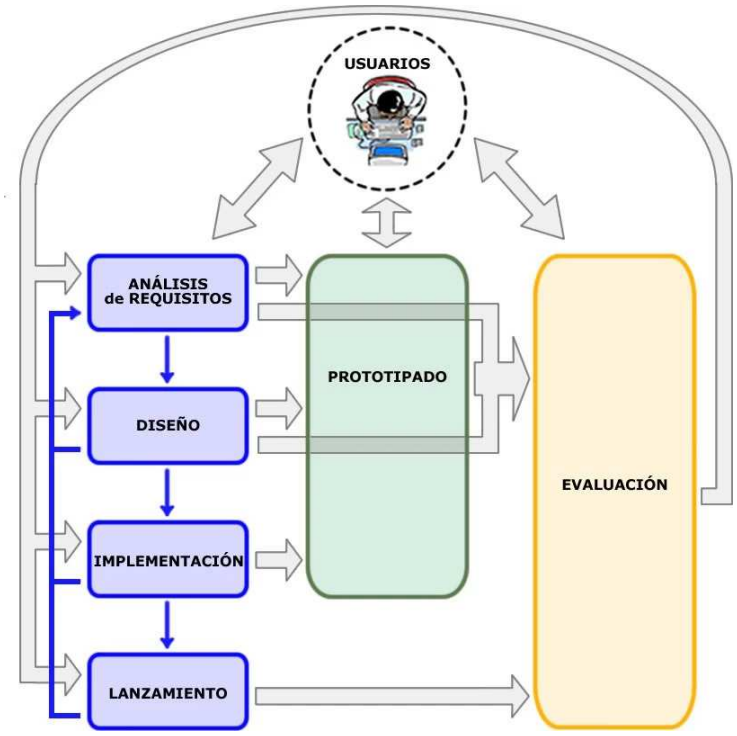


Figura 2.16: Metodología MPIu+a (Tomado de [41])

La metodología tiene una codificación de colores orientados a la ingeniería de software identificado con el color azul, el prototipado engloba técnicas que permitirán la posterior fase de evaluación y se encuentra identificado con el color verde y la evaluación con color amarillo, quién engloba e incluye métodos de evaluación.

Esta metodología da mucha importancia al usuario final, por lo que sigue la filosofía de diseño centrado en el usuario, donde involucra la participación de diferentes disciplinas durante el proceso de desarrollo de sistemas interactivos y la participación de cada disciplina en el proceso de desarrollo software. A continuación se da una breve descripción de las fases:

1. **Análisis de requisitos**: la comunicación con los usuarios es un aspecto prioritario para las empresas que desarrollan sistemas de software, además las necesidades y las experiencias de los usuarios pueden cambiar. En esta fase toma en cuenta los siguientes factores: análisis etnográfico, Implicados (Stakeholders), clasificación de los usuarios, objetivos, plataforma y reflexión acerca de la información recolectada.

2. **Diseño**: se cubren diferentes dos funcionalidades, el diseño de la actividad y diseño de la información como principales actividades que conforman el proceso global de diseño de la interacción.

3. **Implementación**: hace relación actividades de la implementación. También conocida como la fase de codificación, ya que es donde se debe escribir el código software necesario que hará posible que el sistema finalmente implementado cumpla con las especificaciones establecidas en la fase de análisis de requisitos y responda al diseño del sistema. También involucra la accesibilidad, ya que es un factor importante en la codificación y validación de sitios web aplicando los estándares de la W3C.

4. **Lanzamiento**: en esta fase deberá comprobarse que se ha conseguido la aceptabilidad del sistema, mediante una correcta combinación de aceptabilidad social y practica. En esta fase es importante tener una retroalimentación del usuario a través de pruebas.

5. **Prototipado**: esta fase se involucra desde la fase inicial de metodología, ya que desde que se empieza el desarrollo de un sistema se necesita probar partes el mismo con multitud de objetivos para: Verificar funcionalidades, averiguar aspectos relacionados con la interfaz del sistema, validar la navegación, probar nuevas posibilidades de técnicas, entre otros.

6. **Evaluación**: esta fase se involucra desde la fase inicial, ya que consiste en probar algo. Tanto para saber si funciona correctamente o no, si cumple con las expectativas o no, o simplemente para conocer como funciona una determinada herramienta. La evaluación es un punto clave para la obtención de sistemas interactivos usables y accesibles. En esta fase se aplican técnicas necesarias para recibir la realimentación por parte de los usuarios. También hace relación a las métricas de usabilidad y métodos de evaluación.

Entre algunos de los beneficios que presenta este modelo podemos rescatar los siguientes.

1. Es tecnológicamente independiente, adecuándose a cualquier cambio, tanto tecnológico como de paradigma.

2. Es aplicable a todo tipo de proyectos, independientemente de su clase y envergadura.

3. Se adapta a los diferentes modelos mentales de los equipos multidisciplinares.

4. Es lo más simple posible.

5. Esta conforme a los principios del Diseño Centrado en el Usuario.

6. Evidencia la usabilidad del sistema cómo objetivo prioritario.

7. Es consistente con los estándares de calidad relacionados.

2.8. Métodos de Autenticación

La usabilidad se convierte en un problema estratégico en la implementación de métodos de autenticación para las organizaciones. La seguridad usable está relacionada con el estudio de cómo debe manejarse la información de seguridad y la facilidad de uso en la interfaz de usuario [3].

La autenticación es el proceso de establecer si alguien es quien declara ser. En redes de computadoras privadas y públicas, la autenticación se hace por lo general mediante el uso de contraseñas de inicio de sesión. Las propiedades de seguridad (confidencialidad, integridad y disponibilidad) dependen de la diferenciación entre usuarios autorizados y no autorizados, para poder diferenciarlos, la autenticación debe estar presente [108].

El proceso de autenticación se basa en criterios de riesgo. Los sistemas y aplicaciones con alto nivel de riesgo requieren distintas formas de autenticación con el fin de comprobar con mayor precisión la identidad del usuario, a diferencia de una aplicación de bajo nivel de riesgo, donde la confirmación de la identidad no es tan significativa desde el punto de vista del riesgo. Esto se denomina normalmente *autenticación multi-factor*. Aunque la autenticación multi-factor mejora seguramente la seguridad, no hay garantías de que los usuarios finales lo acepten como un método conveniente y utilizable.

¿Por qué centrarse en la autenticación? La autenticación es un importante factor debido al colapso de los perímetros de seguridad de la red, la expansión del número de dispositivos que desean acceder a las redes y el creciente número de usuarios remotos y dispositivos inalámbricos. Los usuarios que necesitan acceder se ha ampliado para abarcar todos los aspectos tanto personales como empresariales, incluyendo correo electrónico, un mayor rango de aplicaciones y diversos tipos de datos. En particular, se ha producido un aumento impresionante en la necesidad de los usuarios de acceder a los recursos de la red, exponiendo a las organizaciones a riesgos significativos a menos que adopten medidas de protección [109].

2.8.1. Elementos de Autenticación

En un proceso de autenticación, Smith [110] proporciona algunos elementos que siempre deben de estar presentes como puede ser visto en la Figura 2.17:

1. Un *usuario* para ser autenticado. El usuario es la entidad que solicita la autorización. Generalmente es una combinación de usuario, dispositivo y/o servicio.

2. Una *credencial* que es poseído por el usuario que lo presenta como prueba de identidad. Los principales tipos de credenciales son la contraseña, contraseña de una sola vez (OTP por sus siglas en inglés *One-Time Password*), certificado digital y credencial biométrica.

3. Una *característica* que distingue a ese usuario en particular.

4. Un *propietario* que es responsable del sistema en uso.

5. Un *mecanismo de autenticación* para verificar la existencia de la característica distintiva.

6. Un *servidor* que es el almacenamiento de clave de autenticación.

7. Un privilegio cuando la autenticación es exitosa empleando un *mecanismo de control de acceso* que rechaza el privilegio si la autenticación no tiene éxito.

8. *Información contextual* de la solicitud de autenticación que abarca la red, la ubicación física de la solicitud y el nivel de amenaza de seguridad.

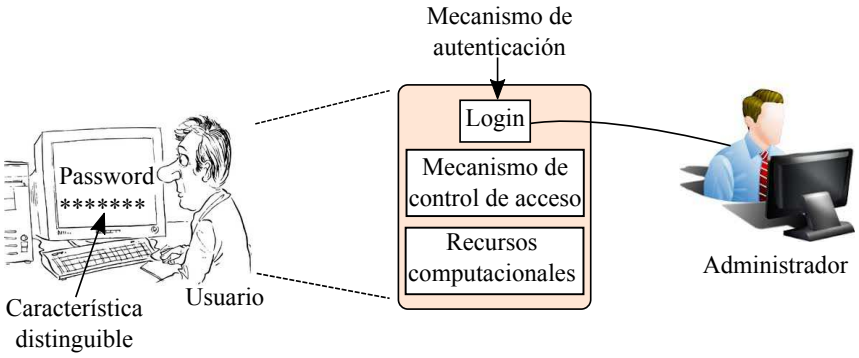


Figura 2.17: Elementos del proceso de autenticación (Tomado de [110])

2.8.2. Factores y Métodos de Autenticación

En algunas aplicaciones, no es necesario que los usuarios sean autenticados por el sistema, como es el caso de buscar información por Internet usando un navegador. Por lo tanto, si los datos son públicos, no hay necesidad de limitar el acceso a los usuarios. Sin embargo, cuando los recursos están protegidos, por ejemplo en un sitio web de banca en línea, el usuario debe ser autenticado para tener acceso a los servicios. El propósito fundamental de la autenticación es controlar quién tiene acceso a la información, ya sea física o digital.

2.8.2.1. Factores de Autenticación

Un factor de autenticación es una información utilizada para autenticar o verificar la identidad de una persona. Hay cinco factores de autenticación de usuario que pueden emplearse o en combinación para aumentar el nivel de seguridad de la identidad de un usuario como se presenta en la Tabla 2.3. Algo que se tiene (e.g. una tarjeta inteligente), algo que sabe (e.g. contraseña o PIN), algo que eres (e.g. huella dactilar), donde estas (e.g. posicionamiento global) y comportamiento de los usuarios (e.g. habla). El uso de cualquier factor de autenticación solo proporciona autenticación de un solo factor. Se pueden combinar varios de estos factores para proporcionar autenticación multi-factor.

Tabla 2.3: Clasificación de los factores de autenticación (Creación propia).

Clasificación	Factor	Ejemplo
Autenticación por conocimiento	Algo que sabe	PIN (*Personal identification Number*) *Passwords*
Autenticación por posesión	Algo que tiene	Llave Física Tarjeta con chip
Autenticación por característica	Algo que eres	Huella dactilar Reconocimiento facial
Autenticación por posición espacial	Donde esta	Localización por GPS (Global Posición System)
Autenticación por comportamiento	Algo que haces	Firma Habla
O combinación de los anteriores		

2.8.2.2. Métodos de Autenticación

Esta sección se describen los métodos de autenticación de usuario más representativos actualmente disponibles para las tecnologías de la información. Un análisis comparativo sobre estos métodos en términos de sus ventajas, desventajas, usabilidad y seguridad es presentado en el Apéndice A. La información que se presenta a continuación se basa en [111][108][112]:

2.8.2.2.1. Contraseña y PIN

Probablemente, la forma más básica de autenticación de usuario es a partir de un nombre de usuario y una contraseña o *password*. Sin embargo, es el tipo de autenticación más inseguro. Un nombre de usuario es un identificador único que puede ser definido por el sistema o por el usuario. Normalmente, los nombres de usuario se construyen con texto para que los usuarios puedan recordarlo fácilmente.

Por otra parte, las contraseñas deben ser fáciles de recordar y ser sencillas para proporcionar una autenticación rápida. Por otro lado, en términos de seguridad, la contraseña debe ser difícil de adivinar, cambiada con alguna frecuencia y única para cada cuenta [113]. Sin embargo, con base en los adelantos tecnológicos, los ataques dirigidos a contraseñas se están poniendo más fáciles de implementar. Las computadoras de alta potencia lo hacen bastante eficiente junto con ataques de fuerza bruta para obtener contraseña difíciles de obtener.

Dado que las contraseñas todavía están ampliamente implementadas en sistemas informáticos, existen algunas prácticas recomendadas para su creación. Las contraseñas deben ser alfanuméricas, lo que significa que requieren que tanto las letras como los números sean válidos. También deben tener una longitud mínima. Seis caracteres parecen ser un mínimo generalmente recomendado pero más sistemas están exigiendo 8 caracteres como mínimo.

Para mayor seguridad, las contraseñas también deben incluir caracteres especiales como el asterisco (*), punto y coma (;) o signo de dólar ($). Sin embargo, muchos sistemas no permiten este tipo de caracteres especiales en las contraseñas. Esto se ha mantenido con las aplicaciones de banca electrónica.

A su vez, un número de identificación personal PIN (por sus siglas en inglés *Personal Identification Number*) es una cadena de caracteres personales única que se utiliza como contraseña, generalmente con un número de cuatro dígitos, que debe ser introducido por el usuario. Los PIN se emplean a menudo con una tarjeta de banda magnética o tarjetas inteligentes en un cajero automático para autenticarse, por ejemplo, un cliente del banco.

Ahora bien, si un atacante está tratando de adivinar un PIN, por cálculos estadísticos le puede tomar algún tiempo, pero si lo realiza un sistema computacional puede hacerlo en milisegundos. Esta es la razón por la cual la mayoría de los sistemas que implementan un PIN tienen una característica de bloqueo. Si el usuario o cualquier otra fuente introduce un PIN incorrecto más de un número predeterminado de veces, la cuenta de usuario se bloqueará hasta que el administrador del sistema reactive la cuenta. Lo anterior es un serio problema de usabilidad.

2.8.2.2.2. Contraseñas gráficas

En este método, los usuarios deben recordar una serie de imágenes en vez de recordar una contraseña. Esto permite al sistema mostrar varias imágenes y permitir al usuario reconocer la imagen o las imágenes correctas que proporcionará acceso al usuario. Los estudios han demostrado que este método de autenticación puede reducir la capacidad de un atacante para adivinar la clave de autenticación correcta y reducir la capacidad para registrar la clave correcta (ya que es una imagen) [114]. Algunos sitios web de banca electrónica están comenzando a integrar las imágenes como parte de sus sistemas de autenticación.

2.8.2.2.3. Frases de contraseña

Las frases de contraseña (*passphrases*) son más seguras que las contraseñas, y son más fáciles de recordar. La clave que hace que las frases de contraseña sean mejores tanto para la seguridad como para la usabilidad, es que las personas son mucho más propensas a recordar una frase que contiene palabras normales y humanas que una contraseña difícil de entender. Por lo tanto, no necesitamos escribir nuestras contraseñas, y no necesitamos usar la misma contraseña para todo.

Para usar las frases de contraseña, solo necesitamos sugerir la frase al usuario y eliminar las reglas de las contraseñas. El usuario que quieren usar contraseñas tradicionales pueden hacerlo si así lo desean, pero la mayoría de las personas intentarán una frase sobre una contraseña a propósito ilegible. Es una buena idea para mejorar la usabilidad de cualquier manera.

2.8.2.2.4. Contraseñas de un solo uso OTP

La contraseña de un solo uso o OTP (del inglés *One-Time Password*) es una contraseña dinámica que tiene validez una sola vez. Los sistemas que usan este tipo de método, son más resistente frente ataques de fuerza bruta, ya que cada vez que cambia la contraseña ,los intentos realizados anteriormente para romper la contraseña anterior son inútiles y hay que empezar de nuevo. Sin embargo, las OTPs son difíciles de utilizar para las personas, debido a que el usuario no puede memorizar todas las contraseñas.

2.8.2.2.5. Autenticación sin contraseña

Los usuarios sólo tiene que recordar su nombre de usuario, correo electrónico o número de teléfono, y reciben un código único (al celular o al correo electrónico) para completar el inicio de sesión. Nunca crean ni introducen una contraseña. Mediante el uso de vínculos o un token único en la URL, un enlace en un mensaje de correo electrónico o texto puede abrirse directamente e iniciar sesión en una aplicación.

Por razones de seguridad, los códigos o vínculos caducan poco después de que se envíen o después de que se utilicen. Esto es lo que hace que la autenticación sin contraseña sea mejor que la autenticación de contraseña. El acceso se concede exactamente cuando alguien lo necesita y está restringido en cualquier otro momento, pero no hay contraseña para realizar un seguimiento.

2.8.2.2.6. Autenticación de acceso resumido

La autenticación de acceso resumido es uno de los métodos usados en servidores web para negociar credenciales, tal como nombre de usuario y contraseña, desde el navegador web. El método es usado para confirmar la identidad de un usuario antes de proporcionar información sensible, como el historial de transacciones de un banco. Se aplica una función de cifrado a la contraseña antes de ser enviada sobre la red, lo que resulta más seguro que enviarla en texto plano como en la autenticación básica.

2.8.2.2.7. Tarjeta electrónica

Es un elemento hardware programado dado a usuarios específicos para probar sus identidades. Contienen componentes avanzados como un microprocesador y memoria, soportando sofisticados protocolos de autenticación que proporcionan un alto nivel de seguridad. Para verificar la identidad del usuario, el sistema realiza su protocolo de autenticación utilizando datos codificados en chip que se encuentra en la tarjeta.

Este tipo de autenticación se puede utilizar junto con otros métodos de autenticación, como un PIN para transacciones en cajeros automáticos. La tarjeta por sí misma no es un medio suficiente de autenticación ya que es propensa a pérdida o robo. Los datos de la

tarjeta se pueden duplicar mediante equipos especializados. Esto significa que un tercero podría crear una tarjeta con la misma información o simplemente utilizar la información en un método diferente.

2.8.2.2.8. Tarjeta sin contacto

La tarjeta sin contacto no requieren contacto eléctrico o físico con algún dispositivo para su lectura. El usuario aproxima la tarjeta cerca del lector de tarjetas y la información se intercambia inalámbricamente. La tarjeta sin contacto comparte los mismos problemas que las tarjetas electrónicas, es decir, con un equipo adecuado, la tarjeta puede ser duplicada y la información puede ser robada.

2.8.2.2.9. *Token* USB

El *token* USB es muy similar a las tarjetas electrónicas o sin contacto. Contiene información sobre la identidad de un usuario y sirve para que el usuario acceda a la información protegida. El *token* debe estar conectado a un puerto USB del dispositivo para que el equipo tenga acceso a la información. Al igual que con otros elementos de autenticación que poseen los usuarios, el *token* USB pueden ser perdido, robado o duplicado.

2.8.2.2.10. Autenticación por voz humana

La autenticación de voz es un enfoque moderno de autenticación. Hace mucho tiempo que la gente quería simplemente decirle a su computadora qué hacer. Esto se está convirtiendo en una realidad. Una combinación de hardware y software de autenticación por voz puede permitir a una organización verificar la identidad de los usuarios por teléfono, celular o Internet. La autenticación de voz, captura la voz de una persona (características físicas del tracto vocal, sus frecuencias armónicas y resonantes) y lo compara con una huella de voz almacenada durante el proceso de inscripción. Un inconveniente de este método de autenticación es que si un usuario tiene una enfermedad que afecten el sonido producido por las cuerdas vocales, el sistema no podría reconocer la voz del usuario.

2.8.2.2.11. Autenticación por firma

Los usuarios deben registrar su firma antes de usar el sistema o utilizarlo activamente para dejar que el sistema "aprenda" la firma con el tiempo. La autenticación por firma también requiere generalmente una tableta en la que el usuario pueda firmar. Este tipo de autenticación permite ahorrar tiempo y verificar rápidamente la identidad de las personas.

2.8.2.2.12. Reconocimiento por pulsación de tecla

Muchos trabajos hoy requieren el uso de un teclado. A partir de lo anterior, la autenticación por teclado puede integrarse fácilmente en el lugar de trabajo. La autenticación puede

lograrse mediante la medición de varias características distintas relativas a las técnicas de escritura de una persona. La latencia entre las pulsaciones de teclas, las duraciones de pulsaciones de teclas, las posiciones de los dedos y la cantidad de presión aplicada a las teclas se pueden combinar para establecer una identidad única para el usuario. El único hardware necesario necesario para que el usuario autentique es un teclado estándar conectado en red al sistema de autenticación. Este método de autenticación puede tener profundas ventajas en futuras aplicaciones.

2.8.2.2.13. Huella dactilar

El reconocimiento de huella dactilar es la forma más común de autenticación por biometría. Uno de los esquemas de identificación biométrica más conocidos y comúnmente utilizados es la huella digital. Este método compara las huellas dactilares de los usuarios con una plantilla previamente almacenada y determina la validez y autenticidad basándose en esta comparación.

Una ventaja es que todas las huellas dactilares son únicas, no existe en este mundo dos huellas dactilares idénticas a menos de que sean gemelos idénticos. Las huellas dactilares son imposibles de falsificar o recrear. Inclusive usando residuo de aceite de una huella digital toma una gran cantidad de esfuerzo para transferir al dispositivo biométrico. Algunos inconvenientes de la tecnología son que algunas personas no tienen huellas dactilares. Las víctimas de quemaduras pueden no tener huellas dactilares en absoluto. Pueden producirse falsos negativos si el usuario no orienta su dedo correctamente en el dispositivo para su escaneo. Los cortes o ampollas también pueden causar falsos negativos.

2.8.2.2.14. Reconocimiento óptico

Existen dos tipos comunes de biometría óptica: la retina y el iris. Los dispositivos de escaneo de la retina y del iris permiten a los individuos ser escaneados incluso a través de anteojos y lentes de contacto. Los escáneres de iris y retina diferencian a los usuarios midiendo sus características en el ojo. Medir estas características y sus relaciones espaciales entre sí proporciona otros parámetros cuantificables útiles para el proceso de identificación.

Al igual que otras técnicas biométricas, el usuario debe primero tener su iris y retina escaneado en el sistema. El sistema funciona de la misma manera que otros datos biométricos, ya que calcula estadísticas de las diferencias físicas del cuerpo humano. Puesto que hay tantas diferencias entre el iris y retina de una persona a otra, el sistema puede autenticar con precisión a las personas.

2.8.2.2.15. Geometría de mano

Los escáneres biométricos de geometría de mano son dispositivos que miden las propiedades de la mano humana en la que se basa la autorización. Al igual que las huellas dactilares,

cada mano tiene diferencias en la longitud, el ancho y el grosor del dedo. La geometría de la mano para adultos rara vez cambia. Lesiones en las manos podrían causar falsos negativos.

2.8.2.2.16. Autenticación basada en localización

La autenticación basada en localización no se utiliza mucho actualmente, salvo por ejemplo limitando el acceso a servicios tales como cajeros automáticos. Para encontrar la ubicación de los usuarios, algunos métodos sugeridos implican el uso de dispositivos con capacidad de GPS, por ejemplo un teléfono celular con este tipo de tecnología.

2.8.3. Criterios de Calidad

Hay una comprensión creciente del papel del usuario en la seguridad de cualquier sistema. Una forma de fortalecer el vínculo de usuario es considerar factores o criterios esenciales tales como la necesidad, inclinaciones y habilidades del usuario en la formulación de mecanismos y políticas de seguridad. Para apoyar la comparación significativa de mecanismos de autenticación, Karen Renaud [20] propone un conjunto de criterios de calidad que pueden ser utilizados para una evaluación cuantitativa y pueden ser aplicados a varios tipos de mecanismos de autenticación. Cada una de estas criterios tiene varias dimensiones y que ayudan a entender la necesidad de que estos criterios estén presentes en estos tipos de métodos de autenticación.

2.8.3.1. Accesibilidad

La accesibilidad asegura que todos, independientemente de las capacidades cognitivas, de movilidad y sensorial, puedan utilizar un mecanismo de autenticación. Esto incluye discapacidades tales como audición, vista, movilidad, aprendizaje y color, que son pertinentes en un contexto de autenticación.

La accesibilidad también se aplica a los niveles de conocimientos técnicos y de alfabetización, así como a la calidad del equipo del usuario. Por lo tanto, los sistemas de autenticación que requieren hardware, software o conocimientos técnicos especiales también pueden excluir a los usuarios por falta de una adecuada accesibilidad. A continuación se presentan las dimensiones de este criterio.

1. **Requisitos hardware/software**: este aspecto se refiere al hardware, software o conocimientos técnicos mínimos necesarios para soportar el mecanismo de autenticación.

2. **Conveniencia**: hay tres aspectos de conveniencia que deben considerarse: tiempo de registro, tiempo de autenticación y tiempo de reemplazo clave.

3. **Inclusividad**: este aspecto aborda la cuestión de la exclusión de los usuarios. Tres clases de discapacidad son consideradas; cognitivas, físicas y sensoriales.

2.8.3.2. Memoria

La mayoría de los mecanismos de autenticación están basados en el conocimiento, por lo que este criterio es importante. Las dimensiones refleja diferentes características de la facilidad con la que los usuarios podrán memorizar y recuperar su credencial.

1. **Estrategia de recuperación**: los usuarios encuentran más fácil reconocer que recordar. Por lo tanto, un sistema que requiere sólo reconocimiento o un sistema que no requiere que el usuario recuerde en absoluto no tiene déficit.

2. **Significado**: los humanos recuerdan mejor las cosas si son deducibles y muy bien, si son significativos.

3. **Profundidad de procesamiento**: los seres humanos recuerdan mejor las cosas si, en la etapa de codificación, hay alguna actividad cognitiva asociada con el proceso.

2.8.3.3. Seguridad

Este criterio describe los diversos aspectos de la dimensión de la seguridad, que están relacionados y son interdependientes, pero que deben considerarse por separado debido a sus diferentes características.

1. **Previsibilidad**: hace referencia a la probabilidad de obtener las credenciales de los usuarios.

2. **Abundancia**: el usuario debe ser capaz de elegir, o serle asignado, un amplio número de posibles claves o credenciales.

3. **Divulgación**: la credencial no debe ser divulgado a otro usuario; De lo contrario, la autenticación fallará.

4. **Confidencialidad**: la autenticación requiere que el usuario y el sistema intercambien una clave previamente acordada.

5. **Privacidad**: la privacidad mide la cantidad de detalles privados requeridos por el mecanismo de autenticación. Una clave comprometida viola la privacidad de la persona y podría resultar en robo de identidad.

6. **Ataque**: hace referencia al esfuerzo y tiempo que un atacante tendría que gastar para obtener una credencial. Cuanto más alto sea el tiempo y esfuerzo, menos vulnerable será un mecanismo de autenticación.

2.8.4. Evaluación de Autenticación

Los métodos de evaluación de usabilidad no son totalmente apropiados para evaluar sistemas basados en seguridad. Algunos trabajos de investigación se han centrado en el desarrollo de métodos adecuados para la evaluación de la seguridad y la usabilidad en

los mecanismos de autenticación [115][116][117]. En consecuencia, estos métodos no pueden generalizarse para todos los tipos de mecanismos de autenticación. Para realizar un análisis de los mecanismos de autenticación de usuarios, inicialmente se requiere un marco adecuado para la evaluación [118].

Mihajlov et al. [118] presentan un enfoque de cuantificación para evaluar la seguridad y usabilidad que puedan utilizarse en métodos de autenticación. El propósito de este enfoque es guiar el proceso de evaluación de los métodos de autenticación en un entorno específico, permitiendo un equilibrio entre usabilidad y la seguridad a partir de definiciones de criterios de calidad cuantificables.

1. Evaluación de Usabilidad: los métodos de autenticación requieren actividad cognitiva en algún nivel; por lo tanto es importante considerar las características de procesamiento de información de usuario que determinan directamente el éxito de estos métodos.

    a) *Profundidad del proceso*: mide la actividad cognitiva implicada en el proceso de codificación de autenticación. La profundidad de procesamiento en tiempo de codificación se determina por la cantidad de atención que se presta a la actividad.

    b) *Recuperación significativa*: mide el esfuerzo mental del usuario para recuperar y deducir la clave de autenticación.

    c) *Requisitos*: miden los recursos necesarios para el software, el hardware y el apoyo técnico del método.

    d) *Conveniencia*: mide el tiempo de registro, inicio de sesión y cambio de datos.

    e) *Inclusión*: asegura que todas las personas puedan utilizar estos métodos, sin importar la parte cognitiva, movilidad o habilidades sensoriales. Esto incluye discapacidades como el oído, la vista, la movilidad, el aprendizaje y el color.

2. Evaluacion de Seguridad: los criterios de calidad de seguridad presentan características dispares a los de la usabilidad; Por lo tanto, se tratan como entidades separadas.

    a) *Secreto*: mide la aleatoriedad de las claves generadas por los usuarios.

    b) *Cantidad*: mide el numero de claves disponibles contra el numero de claves usadas en la práctica.

    c) *Confidencial*: mide el nivel de divulgación de la clave desde la perspectiva del usuario y el sistema.

    d) *Privacidad*: mide la cantidad de detalles privados requeridos por el método.

    e) *Fragilidad*: mide el esfuerzo necesario para romper el algoritmo de seguridad y acceder al sistema.

Los autores argumentan que este marco de evaluación tiene muchos aspectos adicionales que pueden ser exploradas y desarrolladas. Algunos criterios son interdependientes que

requiere un enfoque de cuantificación diferente. Las dependencias entre los criterios específicos pueden ser investigados a fin de mejorar el enfoque de cuantificación.

Basado en el análisis y clasificación de los factores de identidad en los sistemas (por posesion, conocimiento, caracteristica y comportamiento), Xia et al. [119] diseña un método para cuantificar múltiples factores y propone una aritmética de evaluación para métodos de autenticación. También adopta en la evaluación una forma de intensidad de autenticación (autenticación fuerte o débil) y su coste.

El método propuesto por los autores puede proporcionar referencias de cuantificación en la selección del mecanismo de autenticación. Sin embargo, todavía existen algunos factores que deben influir en la intensidad y el costo de la autenticación, por ejemplo, la longitud de la contraseña, el método de creación de la contraseña y los tiempos de los intentos de inicio de sesión, etc.

Eliasson et al. [120] propone un marco de criterios para la evaluación de esquemas de autenticación en servicios de multimedia. Los criterios primarios son seguridad, facilidad de uso y sencillez. Entre estos criterios, se pueden encontrar criterios secundarios tales como conciencia, usabilidad y algoritmos. Cada criterio, tanto primario como secundario, se divide también en uno o varios sub-criterios. La discusión de los criterios es seguida por una descripción de la metodología de evaluación, la cual comprende evaluaciones tanto cualitativas como cuantitativas, el uso de las estándares ISO, las reacciones de los usuario y mediciones de tiempos de autenticación.

Capítulo 3

Proceso de Desarrollo Heurístico en Seguridad Usable y Autenticación

3.1. Introducción

Tendiendo en cuenta uno de los objetivos particulares de esta investigación, "*identificar principios de seguridad usable que permita un balance adecuado entre seguridad y usabilidad particularmente para autenticación de usuario*", en este capítulo es presentado una propuesta para obtener un conjunto de principios de seguridad usable y autenticación de usuario los cuales podrían ser evaluados por expertos en usabilidad, seguridad o seguridad usable. Es por esto, que este capítulo representa uno de los apartados claves de esta investigación. En la Figura 3.1 se presenta el esquema general del contenido que se presentará en este capítulo.

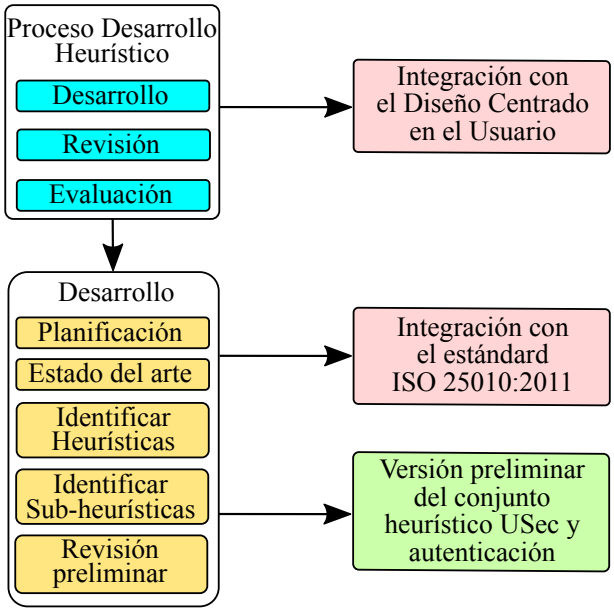


Figura 3.1: Estructura del Capítulo 3 (creación propia).

3.2. Justificación de la Propuesta de Desarrollo Heurístico

Algunos trabajos han propuesto procesos que permiten el desarrollo de principios para propósitos particulares o generales. Además, con relación a la seguridad usable hay muy pocos trabajos de investigación que presentan propuestas para el desarrollo de principios donde la seguridad y la usabilidad estén presentes y unidas.

Sim et al. [121] propone un enfoque de diseño basado en evidencia para el desarrollo de heurísticas específicas. Mujinga et al. [122] define un modelo de desarrollo heurístico para e-banking teniendo en cuenta la seguridad y usabilidad. Este modelo tiene el inconveniente de no tener validación real por expertos y usuarios. Hausawi & Allen [71] proponen principios para seleccionar las herramientas de diseño adecuadas con el fin de apoyar la integración de los requisitos de usabilidad y seguridad en la fase de diseño y resolver conflictos entre seguridad y usablilidad, sin embargo, esta propuesta es puramente cuantitativa analizando la seguridad y usablilidad como atributos independientes.

Leavit & Shneiderman [123] presentan una serie de etapas para obtener un conjunto de guías de diseño a partir de una revisión exhaustiva externa e interna. Este conjunto posee un grado de importancia a partir de encuestas a expertos de sitios web donde se califica con base en una escala similar a la de Likert. Wilson [124] describe un proceso de como crear heurísticas útiles y usables, enfocándose principalmente al diseño centrado en el usuario. Yeratziotis [78] propone un método para desarrollar principios de seguridad usable principalmente a redes sociales en linea particularmente en el dominio de la salud, sin embargo, este enfoque no tiene en cuenta ningún aspecto cuantitativo.

A partir de la revisión de literatura, se analizó e identificó diferentes inconvenientes en el desarrollo de principios y evaluación para aplicaciones seguras y usables. En las propuestas existen aspectos incompletos, es decir, mientras en unos se desarrollan principios para ser evaluados de forma cualitativa, en otros esta evaluación es solo cuantitativa. Además, de los trabajos encontrados, ninguno de ellos evidencia una evaluación heurística real donde expertos en seguridad y usabilidad estén presentes con el fin de realizar evaluaciones exhaustivas a aplicaciones con base en principios USec. Por esta razón, se hace necesario proporcionar un proceso más completo, que involucre expertos y usuarios, y que su análisis de resultados sea tanto cuantitativo como cualitativo.

Entre las mejoras mas importantes para nuestra propuesta teniendo en cuenta lo anterior, podemos resaltar las siguientes:

1. Utiliza un mayor conjunto de metodologías que permite desarrollar heurísticas para diferentes aplicaciones donde la seguridad y la usabilidad estén presentes.

2. Algunos atributos y características del estándar ISO 25010:2011 se encuentran integradas en los resultados del conjunto heurístico.

3. Establece métricas y niveles de importancia para cada principio con el fin de tener no solamente un análisis cuantitativo, sino también una herramienta para que los desarrolladores tengan presente los principios más importantes para el diseño de sistemas seguros y usables.

4. Evaluación heurística de aplicaciones con parámetros cuantitativos y cualitativos.

5. Evaluación de aplicaciones con el componente de seguridad teniendo en cuenta a los usuarios, definiendo métricas con el fin de realizar un análisis cuantitativo y cualitativo.

3.3. Proceso de Desarrollo Heurístico y Evaluación

En esta sección es presentado la propuesta de un proceso que permite obtener principios de seguridad usable para aplicaciones, principalmente para sistemas de autenticación de usuario. Debido a que en esta propuesta existe una integración entre los estándares ISO 9241:2010 – *Diseño Centrado en el Humano* y el ISO/IEC 25010:2010 – *Calidad del software*, hay cuatro razones principales por las que el nuevo proceso se basa en esta integración:

1. El proceso debe proporcionar atributos y características de calidad para producir aplicaciones de la mejor calidad posible y cumplan con las expectativas de los usuarios.

2. Los principios deben proporcional niveles de importancia con el fin de decidir los aspectos más relevantes que deben existir en un sistema que permite alta usabilidad y seguridad.

3. Los usuarios pueden contribuir en la evaluación de aplicaciones con base en sus tareas, preocupaciones y satisfacción.

4. El proceso se basa en una serie de actividades que permita desarrollar un nuevo conjunto heurístico para seguridad usable y autenticación, teniendo en cuenta el elemento humano (e.g. usuarios y desarrolladores).

El conjunto de principios introducido se basa en el análisis de varias metodologías, algunas de estas metodologías presentan pautas o requisitos para seguridad usable. Para desarrollar el conjunto heurístico, se utilizaron cinco tipos de metodologías. Estas metodologías fueron elegidas teniendo en cuenta su nivel de complejidad y consumo de tiempo en el análisis de resultados.

1. La metodología de Ling & Salvendy [125] se basa en estudios previos, modificando la heurística existente y evaluando los resultados. Esta metodología se ha utilizado con éxito en el desarrollo de heurísticas para pantallas ambientales y aplicaciones

de grupo de trabajo colectivo. Pierotti [126] y Braz et al. [127] son algunos de los trabajos previos identificados y algunas de sus heurísticas han sido analizadas y modificadas utilizando la metodología de Ling & Salvendy [125].

2. La metodología de Bonastre & Granollers [128] permiten obtener heurísticas a partir de una recolección de recomendaciones dadas por investigaciones relacionadas. Luego, cada recomendación se reescribe formulando una oración interrogativa añadiéndose comentarios a cada principio.

3. La metodologia de Paddison & Englefield [129] incluye un análisis exhaustivo de la literatura y el análisis de datos de trabajos relacionados. Esta metodología es similar a una revisión sistemática de la literatura, en la que se lleva a cabo un estudio y análisis en seguridad utilizable y autenticación de usuario para encontrar principios en estos campos.

4. La metodología de Rusu et al. [130] proponen un método para desarrollar heurísticas de usabilidad para aplicaciones emergentes. En este caso, las etapas 1 a 6 de la metodología propuesta se realizaron para USec y autenticación de usuario. Es importante destacar que la etapa 4 de esta metodología, no se realiza la plantilla como propone los autores ya que se encuentra por fuera del enfoque de esta investigación. Sin embargo, si se realiza una explicación de cada heurística incluyendo algunos ejemplos.

5. Finalmente, la última metodología se basa en Yeratziotis [78] el cual presenta un proceso cualitativo de desarrollo y validación de principios de seguridad usable para redes sociales en linea, principalmente aplicado al dominio de la salud.

Con base en las metodologías presentadas y aplicadas en este trabajo, en la Tabla 3.1 se resume las características más importantes para cada metodología.

A partir del estudio de estos trabajos, se propone un modelo de desarrollo heurístico y evaluación para seguridad usable que podría ser usado en un espectro más amplio de aplicaciones. Además, a partir de este modelo se desarrolla el primer conjunto de principios para los principales métodos de autenticación (e.g. conocimiento, característica y posesión), actualmente usados por la mayoría de las personas donde la seguridad y usabilidad están estrechamente unidas.

El proceso de desarrollo heurístico y evaluación propuesto integrado por tres etapas usando las metodologías anteriormente presentadas se presenta en la Figura 3.2. En esta se destaca la incorporación de las actividades desarrolladas por los estudios de las metodologías presentados en la Tabla 3.1 en cada fase del nuevo proceso. Se presenta cada uno de los estudios con sus respectivas actividades. Cada actividad presenta un color el cual corresponde a la etapa del nuevo proceso. Todas las actividades de los trabajos se incorporan el en nuevo proceso excepto la activiadad 6 de Yeratziotis et al. [78] ya que los usuarios no realizan la evaluación heurística para seguridad usable, debido a que no todos ellos tienen la suficiente experiencia en este tema.

Tabla 3.1: Actividades de metodologías para el desarrollo de heurísticas USec.

Trabajo	Actividades
Padisson & Englefield [129]	1. Revisión de la literatura. 2. Análisis de estudios previos.
Ling & Salvendy [125]	1. Revisión de la literatura. 2. Modificar heurísticas. 3. Análisis de resultados.
Bonastre & Granollers [128]	1. Revisión de la literatura. 2. Obtener recomendaciones de los trabajos. 3. Reescribir en forma de pregunta e incluir comentarios.
Rusu et al. [130]	1. Revisión de la literatura. 2. Análisis de estudios previos. 3. Etapa de correlación. 4. Etapa explicativa del conjunto propuesto. 5. Comprobar las heurísticas con expertos y complementadas por pruebas de usuario. 6. Realimentación.
Yeratziotis et al. [78]	1. Revisión de la literatura. 2. Modificar heurísticas existentes. 3. Revisión por expertos. 4. Análisis de resultados de los expertos. 5. Identificar aplicación a evaluar. 6. Comprobar las heurísticas por los usuarios. 7. Análisis de resultados. 8. Realimentación.

El proceso se inicia en la **Etapa 1**, donde se centra en el desarrollo de principios para USec y autenticación. Una vez completado este paso, el proceso continúa a la **Etapa 2**, en este paso, se proporcionará a los expertos en usabilidad, seguridad y seguridad usable una herramienta de validación para revisar los principios propuestos. Una vez que esta fase esté completa, el proceso continúa a la **Etapa 3** donde se centra a la aplicación a evaluar a través de una evaluación heurística por parte de expertos y pruebas de usuario para la aplicación escogida. Para ello, se identifican y elige el sitio web/aplicación de acuerdo con el conjunto de principios, desarrollado en la **Fase 1** y revisado en la **Fase 2**.

Los principios se organizan sobre la base de determinar qué atributo o característica representa mejor al principio. Como se explica en la Sección 3.5.3, los principios se organizan en seis atributos: usabilidad, seguridad, operabilidad, accesibilidad, fiabilidad y rendimiento. Esta organización tiene la intención de facilitar la comprensión de los expertos durante la evaluación para una aplicación dada, incluyendo métodos de autenticación.

En la mayoría de las investigaciones sobre evaluación heurística para seguridad usable, el

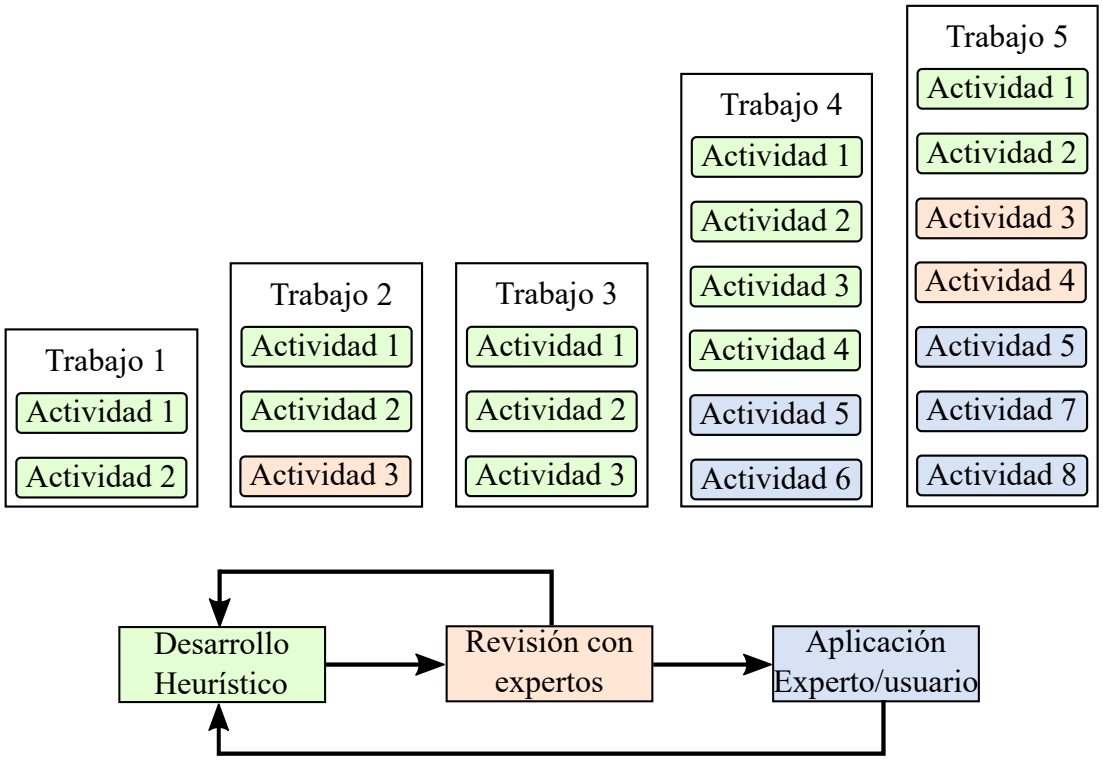


Figura 3.2: Proceso de tres fases para desarrollar heurísticas para USec y Autenticación (creación propia).

proceso de evaluación se centra principalmente de forma cualitativa. En esta investigación, el modelo propuesto tiene en cuenta una evaluación cuantitativa y cualitativa para USec y autenticación como se verá en el Capítulo 5. En la Figura 3.3 es presentado el proceso resumido a partir del estudio de los trabajos presentados anteriormente.

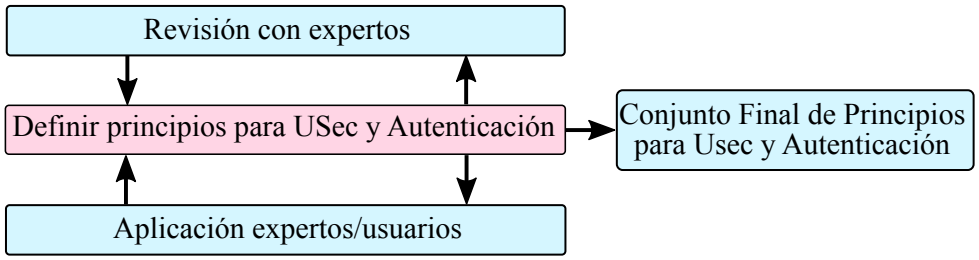


Figura 3.3: Proceso de desarrollo y evaluación heurística resumido (creación propia).

El proceso propuesto, está divido inicialmente en tres etapas: desarrollo heurístico, revisión con expertos y aplicación con expertos/usuarios. La primera etapa desarrolla un conjunto heurístico para USec y autenticación teniendo en cuenta principalmente la revisión del estado del arte. En la segunda etapa los principios encontrados son revisados por expertos teniendo en cuenta un un grado de importancia que se verá en Capítulo 4. La tercera y

última etapa, los expertos evalúan los principios a partir de una aplicación previamente escogida y los usuarios son tenidos en cuenta con el fin de que desarrollen pruebas para obtener resultados cuantitativos y cualitativos.

De acuerdo con el análisis de resultados de las etapas 2 y 3, es posible realiza iteraciones con la etapa 1. El propósito de estas iteraciones es modificar o mejorar los principios con base en las recomendaciones y observaciones de los expertos y usuarios. En este punto, las recomendaciones de los expertos tienen prioridad ya que ellos tienen el conocimiento y la experiencia para determinar si los principios cumplen o no con las objetivos necesarias. Una vez finalizado este paso, se obtiene el conjunto heurístico final para USec y autenticación de usuario. En la Figura 3.4 se presenta una representación más completa del proceso. En la próxima sección se explicará en detalle cada etapa de este proceso.

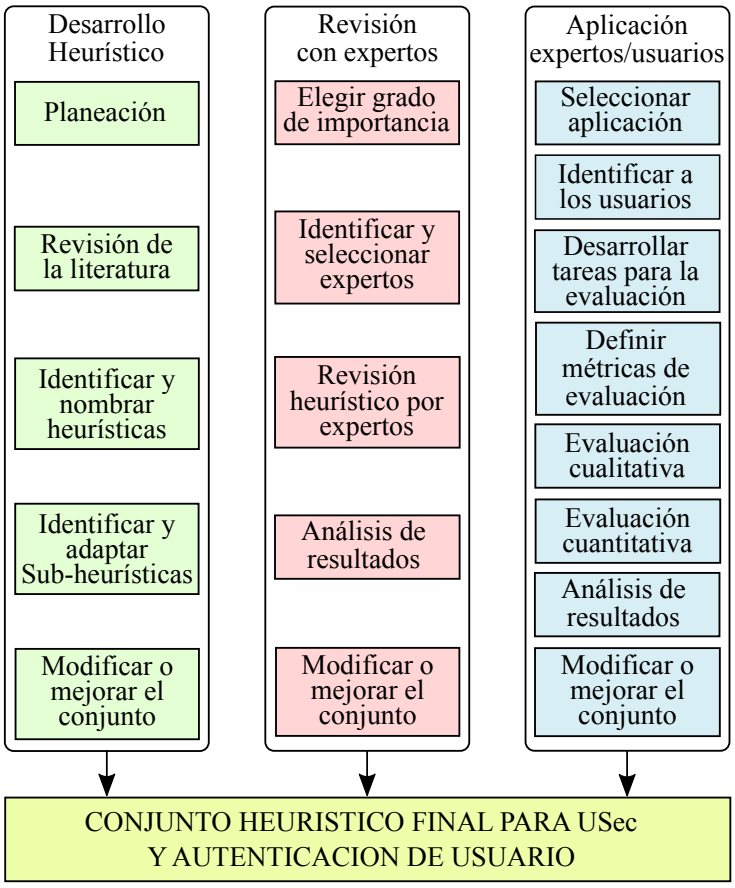


Figura 3.4: Proceso de desarrollo y evaluación heurística (Adecuación de [78]) (creación propia).

Por último, es importante que los expertos confirmen la relevancia de los principios para USec y autenticación obtenidos. Al reconocer esto, se está asegurando a los desarrolladores de software poder utilizar este conjunto heurístico para desarrollar interfaces de usuario más seguras y usables. Como resultado, los usuarios que utilicen estas interfaces

serán los beneficiarios, ya que la aplicación se verá mejorada en términos de usabilidad de las características de seguridad. Además, los desarrolladores de software también se verán beneficiados porque la probabilidad de que los usuarios acepten sus diseños podría aumentar.

3.3.1. Etapa 1: Desarrollo Heurístico

Esta etapa consiste de 5 actividades que permite obtener un conjunto de principios preliminar, las actividades de esta etapa son presentas en la Figura 3.5. Se inicia con una fuerte investigación de la literatura (e.g. artículos, eventos, tesis doctorales, etc.) con respecto a principios en USec y autenticación. Es importante tener en cuenta que los autores de estas investigaciones son personas reconocidas en el campo del HCI, USec y autenticación, por lo tanto la credibilidad y validez de la información es aceptable. En la Sección 3.5 explicará en mas detalle el procedimiento para llevar a cabo la Etapa 1.

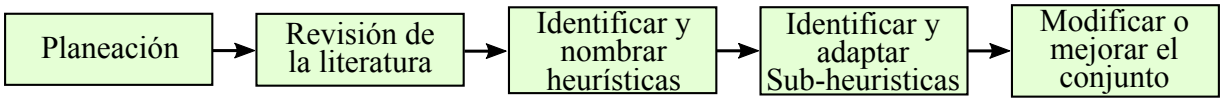


Figura 3.5: Actividades para la etapa de desarrollo heurístico para USec y autenticación (creación propia).

1. **Planeación**: Es importante tener claro una planificación adecuada incluyendo los objetivos para el desarrollo de principios y su evaluación con expertos y usuarios. El plan debe incluir una lista de requisitos de usuario. Revisar la documentación adecuada puede ser un valioso para aprender de los errores y trabajos futuros anteriores. Sin embargo, la implementación y el mantenimiento no se consideran en la planeación debido al alcance del trabajo de investigación. Entre estos objetivos se puede tener en cuenta: evaluar un sistema en busca de fallos de usabilidad y seguridad usando el conjunto heurístico, adecuar los principios a algunas normas de calidad del software, realizar tareas y cuestionarios a los usuarios en la evaluación, entre otros.

2. **Revisión de la literatura**: Se realiza una exhaustiva revisión sistemática de la literatura sobre principios o guías de diseño en usabilidad, seguridad, privacidad, autenticación, seguridad usable y atributos de calidad de software. El estudio de la literatura es un requisito esencial ya que permite determinar los requerimientos de cada área anterior.

3. **Identificar y nombrar las reglas heurísticas de acuerdo a la literatura**: A partir de la revisión sistemática de la literatura y un análisis de estos datos, se identifican los principios que podrían ser parte del conjunto general (principios para USec y autenticación de usuario). Para llevar este paso a cabo se realiza una correlación de las heurísticas existentes, se obtuvo recomendaciones de trabajos y se modificaron heurísticas relevantes todo esto en el contexto de USec y autenticación.

Cada heurística identificada presenta una definición de acuerdo a las referencias con la finalidad de comprender su uso.

4. **Identificar y adaptar las sub-heurísticas de acuerdo a la literatura**: Las sub-heurísticas o principios propuestas teniendo en cuenta el paso anterior son identificadas y adaptadas al atributo o heurística correspondiente. Cada una de estas sub-heuristicas son reescritas en forma de pregunta. Además, presentan una descripción donde se explica brevemente su uso. Otro tipo de sub-heurísticas pueden ser identificadas a partir de los requerimientos presentados en la literatura.

5. **Modificar o mejorar el conjunto**: La revisión de las sub-heurísticas permite ubicar, si es el caso, en la heurística adecuada. Además, se revisa su redacción con el fin de que los expertos comprendan adecuadamente la pregunta y la descripción en cuestión.

3.3.2. Etapa 2: Revisión con Expertos

Esta etapa consiste de 4 actividades donde un grupo de expertos en temas de usabilidad, seguridad informática, USec y HCI revisan el conjunto de principios obtenido de la etapa anterior con el fin de realizar recomendaciones y mejorar este conjunto. Las tareas de esta etapa es presenta en la Figura 3.6.

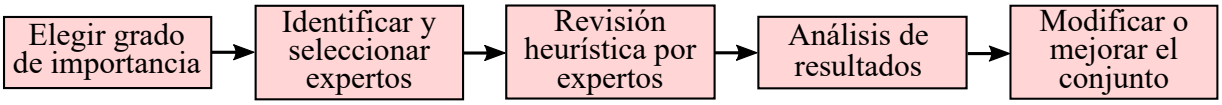


Figura 3.6: Actividades para la etapa de validación con expertos (creación propia).

1. **Elegir el grado de validación**: El grado de validación representa la importancia de cada sub-heurística. Para elegir este grado de validación, se propone un conjunto de niveles de importancia teniendo en cuenta las recomendaciones de Masip [63] para UX y de la accesibilidad de la W3C [1].

2. **Identificar y seleccionar a los expertos**: Es fundamental que los expertos más idóneos lleven a cabo la revisión. Los expertos seleccionados deben tener conocimiento y experiencia preferiblemente en las áreas de usabilidad, seguridad informática, USec y HCI. Esto asegura que el conjunto de principios propuesto tengan credibilidad y validez.

3. **Revisión heurística por expertos**: Los expertos revisan el conjunto de principios a través de una herramienta (e.g. MS Excel) previamente realizada, asignando un nivel de importancia para cada sub-heurística y una categorización usando la escala de Likert donde se determina si cada sub-heurística representa o hace parte de la

[1]Disponible en: http://www.w3.org/TR/WAI-WEBCONTENT/. Consultado en: Septiembre del 2016

heurística o atributo general. Además, presenta un espacio para que los evaluadores incluyan comentarios u opiniones sobre el conjunto propuesto.

4. **Análisis de resultados**: A partir de los resultados encontrados, se realiza el análisis de resultados con el fin de obtener un mayor grado de credibilidad en las mejoras que pueda tener.

5. **Modificar o mejorar las sub-heurísticas**: A partir del análisis anterior, el conjunto de principios puede ser modificado o mejorado. Si el análisis de resultados demuestra que los expertos no están convencidos con el conjunto propuesto, el proceso tendrá que volver a la **Etapa 1**.

3.3.3. Etapa 3: Aplicación con Expertos/Usuarios

En esta última etapa, el conjunto heurístico debe aplicarse en un contexto adecuado. Esta etapa consiste de 8 actividades en el cual un grupo de expertos evalúan una aplicación donde se validan los principios propuestos y un grupo de usuarios desarrollan diferentes taras para la misma aplicación. Es importante señalar que las modificaciones o mejoras de acuerdo al análisis de la Etapa 2 deben haberse realizado en este punto. Las actividades de esta etapa es presenta en la Figura 3.7.

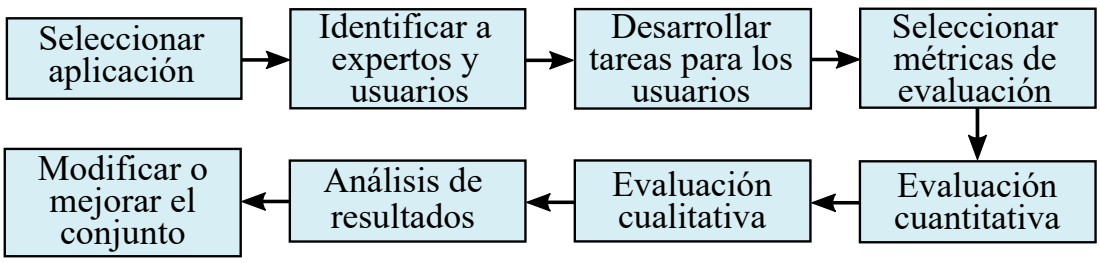


Figura 3.7: Actividades para la etapa de aplicación con expertos/usuarios (creación propia).

1. **Identificar y seleccionar la aplicación a evaluar**: En esta actividad es necesario establecer criterios como el dominio de la aplicación, alcance real de funcionalidad, tipo de usuarios que usan la aplicación, entre otros, con el fin determinar la aplicabilidad de los principios para su evaluación y las tareas que desarrollarán los usuarios. Esto implica determinar si los principios cumplen con su objetivo de detectar problemas de seguridad usable de la aplicación.

2. **Identificar a los expertos y usuarios**: En esta actividad es necesario identificar a los expertos y usuarios que realizarán la evaluación y las tareas para la aplicación. Por el momento no hay criterios para seleccionar a los usuarios, pero preferiblemente son los que utilizarán el sitio web o la aplicación. La selección de los expertos fue presentada en la anterior etapa.

3. **Desarrollar las tareas para los usuarios**: Debido a que la evaluación heurística se complementa con pruebas de usuario. En esta actividad se describen los objetivos de la prueba y se desarrollan las tareas que los usuarios experimentarán durante su interacción con la aplicación.

4. **Determinar métricas de evaluación**: En este caso se determina cuales son las métricas que se tendrá en cuenta en la realización de las tareas por parte de los usuarios. En este caso puede ser tiempo de la tarea, porcentaje de tareas realizadas, número y duración de fijaciones, satisfacción subjetiva, entre otros.

5. **Evaluación cuantitativa**: Los expertos evalúan la aplicación teniendo en cuenta dos criterios: severidad e impacto de la sub-heuristica de forma numérica. Con lo anterior se permitirá encontrar el nivel de riesgo (con respecto a la seguridad) de la aplicación. Con base en los usuarios se podrán encontrar resultados de acuerdo a las métricas escogidas para cada tarea. Al terminar esto, los usuarios completarán un cuestionario de satisfacción de usuario usando una escala tipo Likert.

6. **Evaluación cualitativa**: Los expertos evalúan cualitativamente la aplicación con base en comentarios para luego proceder con su interpretación. Para el caso de los usuarios, una serie de preguntas abiertas son formuladas con respecto a la usabilidad y seguridad de la aplicación.

7. **Análisis de resultados**: Los resultados obtenidos son analizados. De acuerdo con el análisis, es posible obtener algunas recomendaciones para mejorar el conjunto de principios por parte de los expertos.

8. **Modificar o mejorar el conjunto heurístico**: A partir del análisis y las recomendaciones, los principios pueden ser modificados o mejorados.

3.4. Integrando el Proceso de Desarrollo Heurístico al Diseño Centrado en el Usuario

El estandard ISO 9241-210 [43] constituye un marco de trabajo para el diseño centrado en el usuario al integrar diferentes procesos de diseño y desarrollo apropiados a un contexto en particular; complementando las metodologías de diseño existentes. En esta parte, el término diseño centrado en el usuario se sustituyó por diseño centrado en las personas, debido a que aborda tanto a los *stakeholders* como a los usuarios [44].

Es posible integrar el marco de referencia presentado en la Figura 2.3 al proceso propuesto presentado en la Figura 3.4, con el fin de asegurar que el enfoque propuesto para el desarrollo y evaluación heurístico para USec y métodos de autenticación pueda ser adaptado a expertos y usuarios [78]. Lo anterior tiene una importante contribución al desarrollo de un conjunto de principios para nuevas aplicaciones, además, los usuarios podrían realizar recomendaciones de acuerdo a sus experiencias personales con el fin de mejorar estos principios.

Es importante indicar que el propósito de tener en cuenta el marco de referencia de la ISO 9241-210 es identificar las actividades importantes que deben ser incorporadas al proceso propuesto presentado en la Figura 3.4 para asegurar el diseño centrado en el usuario presentado en la Sección 2.3, el cual es uno de nuestros objetivos. En la Figura 3.8 se presenta la integración entre la propuesta de desarrollo heurístico y el diseño centrado en el usuario de la ISO 9241-210.

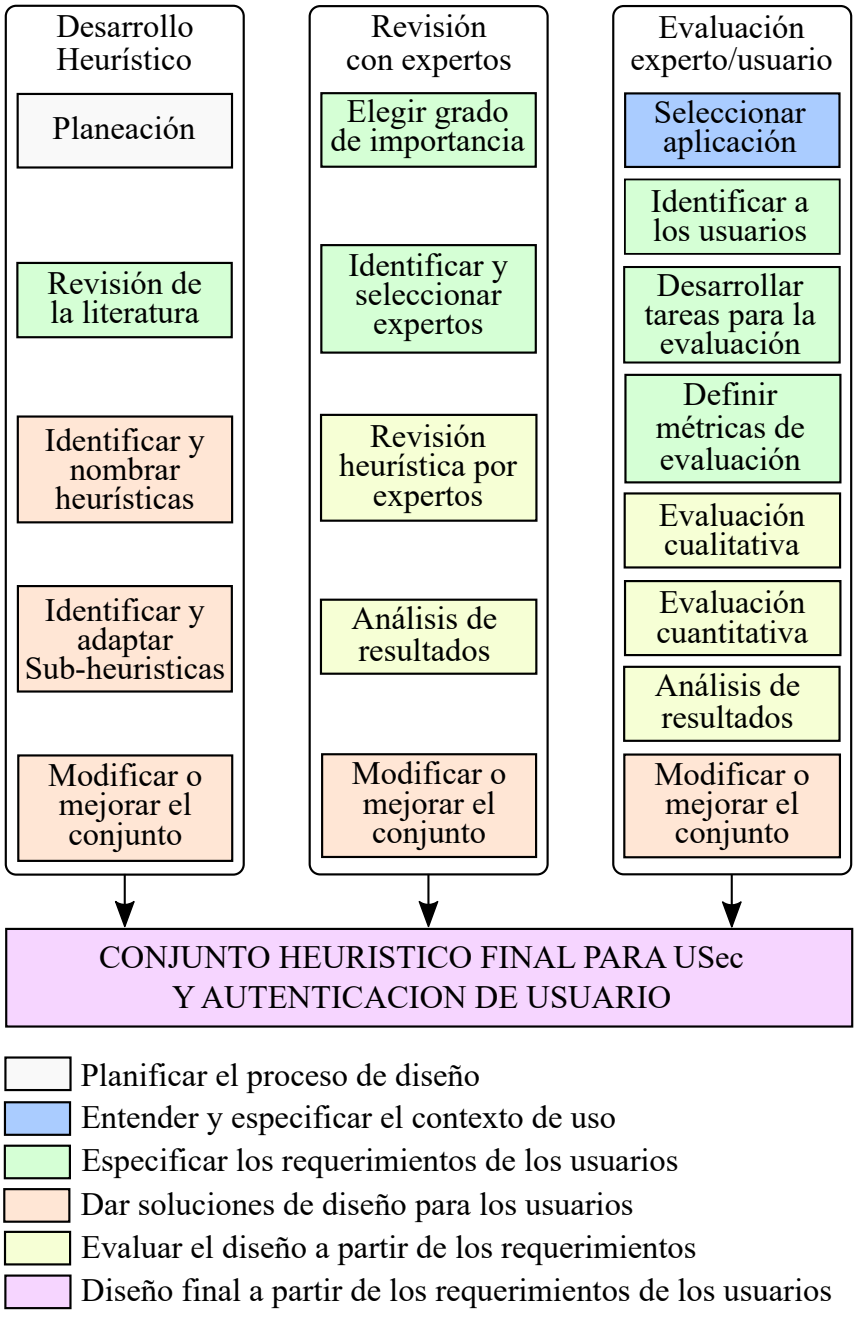


Figura 3.8: Integración del proceso de desarrollo y la ISO 9241-210 (creación propia).

Por otro lado es importante destacar en la Figura 3.8, que una actividad del DCU puede ser incorporada a una o varias actividades para cada etapa del proceso propuesto. La integración entre el DCU y el proceso propuesto puede ser brevemente resumido a partir de lo siguiente:

1. *Desarrollo Heurístico* – En la etapa 1 hay eventualidades con las actividades del DCU – *planificar el proceso de diseño*, *especificar los requerimientos de los usuarios* y *dar soluciones de diseño para los usuarios*.

2. *Revisión con Expertos* – En la etapa 2 hay eventualidades con las actividades del DCU – *especificar los requerimientos de los usuarios*, *evaluar el diseño a partir de los requerimientos* y *dar soluciones de diseño para los usuarios*.

3. *Aplicación con Expertos/Usuarios* – En la etapa 3 hay eventualidades con las actividades del DCU – *entender y especificar el contexto de uso*, *especificar los requerimientos de los usuarios*, *dar soluciones de diseño para los usuarios* y *evaluar el diseño a partir de requerimientos*.

3.5. Etapa 1: Desarrollo Heurístico

En esta sección se discute el desarrollo de los principios para USec y autenticación de usuario, es decir la etapa 1 de la Figura 3.4 y discutido en la Sección 3.3.1. Las actividades que se llevan a cabo en las etapas 2 y 3 del proceso se analizarán con más detalle en los Capítulos 4 y 5. A continuación se discute cada una de las 5 actividades que tiene esta etapa para el desarrollo del conjunto heurístico.

3.5.1. Planificar el Proceso Heurístico

El primer paso es planificar que métodos se espera utilizar en las diferentes etapas del desarrollo heurístico. Un requisito en la planificación para el diseño centrado en el usuario es definir en detalle el contexto de uso del producto. Las personas utilizan los productos para incrementar su propia productividad. Así pues, un producto se considera fácil de aprender y de usar en términos del tiempo que toma el usuario para llevar a cabo su objetivo, el número de pasos que tiene que realizar para ello y el éxito que tiene en predecir la acción apropiada para llevar a cabo [46]. Para desarrollar aplicaciones seguras y usables hay que entender el contexto de uso y los objetivos del usuario, y conocer las tareas que deben realizar para alcanzar sus objetivos.

Algunos de los elementos en la etapa de planificación para seguridad usable se presentan a continuación:

1. **Objetivos**: se debe tener una declaración de los objetivos que refleje el propósito y compromiso con los usuarios en los aspectos de usabiliad y seguridad.

2. **Facilitar el trabajo multidisciplinario**: el desarrollo heurístico para USec es multidisciplinario. En estas están involucrados diferentes disciplinas: expertos en usabilidad, seguridad informática, seguridad usable y HCI.

3. **Administrar las etapas del desarrollo**: La naturaleza iterativa del UDC es una condición previa para asegurar que el conjunto heurístico para USec esté orientado a las necesidades del usuario. Para lograr esto, se debe tener un plan que contenga las fases o etapas del desarrollo heurístico.

Además de lo anterior, se presentan los objetivos en el desarrollo de heurísticas para USec y autenticación de usuario.

1. Ampliar los principios de seguridad usable que puedan ser aplicados a una espectro más amplio de aplicaciones (e.g. e-commerce, e-banking, autenticación y redes sociales).

2. Proponer un primer conjunto de principios para autenticación de usuario que incluya los tres métodos mas aplicados en la actualidad (e.g. por conocimiento, posesión y característica).

3. Incluir los principios encontradas dentro de algunos atributos que se encuentran en la ISO/IEC 25010:2011 permitiendo con esto un nivel de calidad del sistema y que puedan ser consideradas como requisito mínimo para el diseño o evaluación de sistemas que tengan en cuenta seguridad y usabilidad.

3.5.2. Revisión de la literatura

Investigadores importantes han contribuido en el campo del HCI especialmente a la usabilidad de sistemas interactivos. Las ocho reglas de oro de Shneiderman [21] permiten diseñar buenas interfaces. Las heurísticas de Nielsen [65] permiten el éxito en la Interacción Humano-Computador. Dix et al. [52] y Preece et al. [131] presentan una teoría muy amplia sobre HCI y diseño de interfaces de usuario. Sin embargo, los autores anteriores no presentan en sus trabajos aspectos que involucren temas de usabilidad y seguridad de forma conjunta.

Investigadores reconocidos y referenciados en la literatura han propuesto principios en el campo de la seguridad usable (ver Sección 2.6.3), entre los más importantes se encuentran: Los diez principios de Yee [83] permiten el diseño de sistemas seguros. Los criterios de Johnston et al. [74] permite el éxito en la relación entre HCI y seguridad. Los 5 principios de Whitten [9] permiten establecer cuando es usable un sitema de seguridad. Los seis principios generales de Garfinkel [82] permiten alinear seguridad y usabilidad. Finalmente, las directrices de Herzog [91] permiten diseñar aplicaciones que establecen políticas de seguridad.

En este trabajo de investigaciónn también se tienen en cuenta los trabajos de Chiasson [95], Saltzer [89], Ibrahim et al. [132], Nurse et al. [133], Katsabas et al. [96], Yeratziotis [78], Bonastre et al. [128], Mijinga et al. [122], Masip [63] y Jaferian et al. [134]. Para métodos de autenticacion se tienen en cuenta investigadores como Braz [127], Bonastre et al. [128], Masip [63], Cranor et al. [108] y Renauld [20].

En esta sección no se va a discutir los principios que hacen los autores en el campo de la seguridad usable y autenticación ya que abarcaría mucho espacio en el documento. La literatura seleccionada para el análisis puede plantear preocupaciones con respecto a su relevancia. Esto se refiere a si los trabajos seleccionados fueron seleccionados correctamente y por qué otros fueron excluidos de la selección.

Sin embargo, a partir de un análisis minucioso de la literatura escogida, podemos decir que los trabajos seleccionados cumplen con los objetivos planteados ya que ellos corresponden a campos de investigación en USec y autenticación de usuario siendo los más referenciados. Estos estudios no cubren todos los requerimientos para las aplicaciones actuales, pero es un buen punto de partida para una eventual estandarización.

3.5.3. Identificar y Nombrar las reglas heurísticas de acuerdo a la Literatura

A partir de un exhaustivo análisis literatura y según los trabajos presentados en la sección anterior, se identifica que los principios encontrados pueden ser adaptado a 6 atributos de calidad que son parte del estandar ISO/IEC 25010:2011 [67], entre ellos están: usabilidad, seguridad, accesibilidad, fiabilidad, desempeño y operabilidad.

Para el caso de la usabilidad y usando la etapa de correlación de la metodología de Rusu et al. [130] se observó que la mayoría de los trabajos relacionados con seguridad usable tienen en cuenta las diez reglas heurísticas de Nielsen [65]. Debido a que estas reglas son sin duda, las más reconocidas y utilizadas en el mundo empresarial y académico por su simplicidad y prestigio, se decidió tomar como base estas reglas con el fin de proponer un conjunto heurístico en el contexto de usabilidad donde se tenga en cuenta la seguridad, es decir seguridad usable.

Adicional a lo anterior, otra regla heurística que aparece con frecuencia es el de “transmitir características” de Johnston et al. [74], esta heurística informa al usuario de las características de seguridad disponibles, mientras que el criterio de visibilidad del estado del sistema permite al usuario “ver” si estas características están activas y se utilizan . En la Tabla 3.2 se presenta un análisis comparativo de los trabajos relacionados con las heurísticas de Nielsen y el principio de transmitir características.

Una característica importante de la Tabla 3.2 es que estas heurísticas cumplen con los principios de seguridad usable el cual es uno de nuestros principales objetivos. Lo anterior significa que cada heurística, mantiene los reguisitos de usabilidad y seguridad de forma

Tabla 3.2: Análisis comparativo heurístico para usabilidad (Creación propia).

Heurística	[83]	[74]	[78]	[132]	[133]	[96]	[122]	[95]	[82]	[128]
Visibilidad	✓	✓	✓	✓	✓	✓	✓	✓	-	✓
Estética y mínimo diseño	✓	✓	✓	✓	✓	✓	✓	-	-	-
Control y libertad	✓	-	✓	-	-	-	✓	✓	-	-
Lenguaje de los usuarios	-	-	✓	✓	✓	✓	✓	-	-	-
Carga de memoria	-	✓	✓	✓	✓	-	✓	-	-	-
Reconocer errores	-	✓	✓	✓	-	✓	✓	✓	-	-
Flexibilidad y eficiencia	-	✓	-	✓	✓	✓	-	-	-	-
Prevención de errores	✓	-	✓	-	-	✓	✓	-	-	-
Consistencia y estándares	-	-	-	✓	-	-	✓	-	✓	-
Ayuda y documentación	-	-	✓	✓	✓	✓	✓	✓	-	✓
Transmitir características	-	✓	✓	✓	✓	-	-	-	✓	-

conjunta y no independiente. Además, en estas heurísticas la característica de privacidad también esta presente. A diferencia de Braz [127] donde la usabilidad y la seguridad para métodos de autenticación se evalúa de forma separada, estas heurísticas donde estos métodos están presentes, los dos atributos se encuentran unificados. Lo anterior representa desde nuestro punto de vista una contribución importante en el campo de la seguridad usable y autenticación.

Igual que en el caso anterior, en la Tabla 3.3 se presenta un análisis comparativo de los atributos que hacen parte en la seguridad usable y autenticación teniendo en cuenta la ISO 25010:2011.

Tabla 3.3: Análisis comparativo de atributos (Creación propia).

Atributo	[78]	[63]	[127]	[135]	[128]	[91]	[136]	[20]	[74]
Seguridad	✓	✓	✓	✓	✓	✓	-	-	-
Accesibilidad	-	-	✓	-	-	-	✓	✓	-
Operabilidad	-	-	✓	-	✓	-	-	-	-
Fiabiliadad	✓	✓	✓	-	✓	-	-	✓	✓
Desempeño	-	-	✓	✓	✓	-	-	-	-

En la Tabla 3.3 se puede observar que el trabajo de Braz et al. [127] abarca todos los atributos, esto se debe a que este trabajo esta enfocado principalmente a métodos de autenticación y en cada uno de estos atributos existen principios para autenticación.

3.5.3.1. Usabilidad

Los conceptos y avances de la usabilidad son esenciales en la investigación de la seguridad usable. La literatura seleccionada y muy amplia por cierto, intenta integrar los conceptos

de usabilidad y la seguridad para formar un solo conjunto, la USec. Con base en el concepto de la usabilidad presentado en el Capítulo 2 y de la seguridad usable, la usabilidad necesita cerciorarse de que los usuarios desarrollen las tareas de seguridad y privacidad de una forma efectiva, eficiente y que proporcione una sensación de satisfacción de manera que no haya frustración de por medio. Como se dijo anteriormente, las heurísticas de Nielsen [65] ampliamente aceptados y usados, han sido el pilar para llevar a cabo esta integración entre usabilidad y seguridad, junto con el criterio de transmitir características el cual presenta alguna similitud con la heurística de visibilidad de Nielsen.

A continuación se presenta la definición de cada una de estas heurísticas desde el contexto de la seguridad usable. **NOTA**: Es importante aclarar que la definición propuesta para cada heurística es propia del autor y es desarrollada con base en la literatura seleccionada.

1. **Visibilidad del estado del sistema**: El sistema debe mantener informado al usuario sobre el estado de seguridad del sistema y de las acciones que pueda estar haciendo. Lo anterior puede generar confianza en el uso de una aplicación, sin embargo, esta visibilidad debe ser moderada y no se debe atacar al usuario con sistemas de alerta todo el tiempo. Algunos ejemplos de esta categoría podrían estar: visibilidad del nombre de la alerta, establecer colores de seguridad estándar (rojo, amarillo y verde) e iconos como indicadores visuales (semáforo como icono de seguridad y con los colores anteriores propuesto por Arteaga et al. [45] como patrón de interfaz de usuario) [83, 74, 91, 132, 133].

2. **Estética y mínimo diseño**: El sistema debe aplicar apropiadamente representación visual de elementos de seguridad identificable y diferenciable. Únicamente información de seguridad relevante debe ser desplegada evitando información irrelevante, por ejemplo, evitar información técnica [21, 83, 74, 132, 133, 96, 65, 78].

3. **Control y libertad para el usuario**: El sistema debe permitir a los usuarios deshacer fácilmente cualquiera de sus acciones de seguridad, siempre que sea posible. Lo anterior conlleva a volver a un estado anterior si una acción de seguridad pueda tener consecuencias imprevistas [83, 21, 95, 91, 78].

4. **Utilización del lenguaje de los usuarios**: El sistema debe utilizar un lenguaje consistente y significativo en materia de seguridad para que los usuarios puedan entenderlo fácilmente. Es importante evitar el uso de términos técnicos avanzados que resultan incomprensibles para el usuario [65, 132, 82, 91, 133, 96, 78].

5. **Minimizar la carga de memoria**: El sistema debe asegurar que las acciones de seguridad sean fáciles de aprender y recordar. El uso de metáforas del mundo real ayuda a recordar fácilmente estas acciones a los usuarios (e.g. llaves o cerraduras como metáforas) [21, 133, 65, 74, 78].

6. **Reconocer, Diagnosticar y Recuperarse de Errores**: El sistema debe proporcionar a los usuarios con mensajes de error de seguridad detalladas que puedan comprender y actuar. Es importante que el mensaje sea significativo e indicar

donde obtener ayuda, además, hay que tener en cuenta que los mensajes de error en situaciones de seguridad son críticos en comparación con los errores comunes [133, 65, 96, 74, 78].

7. **Flexibilidad y Eficiencia de Uso**: El sistema debe ofrecer opciones para los usuarios (expertos y novatos) con diversos niveles de habilidad y experiencia en materia de seguridad. El sistema debe mostrar suficiente información para usuarios por primera vez mientras no demasiada información para usuarios experimentados. Usar atajos a tareas frecuentes de seguridad permite eficiencia [133, 65, 78].

8. **Prevención de Errores**: El efecto de cualquier acción relevante para la seguridad debe ser comprensible para el usuario. El sistema debe informar a los usuarios con antelación sobre las consecuencias de las acciones de seguridad. A partir de mensajes, los usuarios serán informados sobre cualquier acción que afecte la seguridad del sistema [83, 65, 78, 96].

9. **Consistencia y Estándares**: Los controles relacionados con la seguridad en la interfaz de usuario pueden ser estandarizados, el uso de estándares en la interfaz facilita el aprendizaje. Los usuarios deben ser capaces de encontrar los elementos de seguridad que necesiten en un lugar adecuado y en un tiempo razonable [82, 132, 65, 126].

10. **Ayuda y Documentación**: Es necesario que el sistema disponga de ayuda y documentación con respecto a la seguridad para los usuarios. El usuario debe ser capaz de encontrar ayuda fácilmente a sus preguntas, centrada en las tareas del usuario y no ser muy extensa [133, 65, 78].

11. **Transmitir características**: La interfaz debe proporcionar al usuario de una manera clara las características de seguridad disponibles. Además, proporciona interés en los usuarios para encontrar políticas de seguridad sin excesiva dificultad, permitiendo que expresen estas políticas en términos de que se ajusten a sus objetivos [83, 74, 132].

3.5.3.2. Seguridad y Privacidad

Como se discutió en la Sección 2.5.2, el cual la privacidad es un sub-conjunto de la seguridad, la privacidad junto con las características de la seguridad lo trataremos como un único conjunto llamado Seguridad y Privacidad. Esto se debe a que la relación entre seguridad y privacidad tienen puntos en común como se afirmó anteriormente. La integración entre las características de la seguridad junto con la privacidad para desarrollar principios es necesaria con el fin de ayudar a los desarrolladores de software a mejorar sus diseños para la seguridad y privacidad de los usuarios. Por lo tanto, no tiene sentido práctico separar estas propiedades, sino más bien combinarlas.

Con el fin de obtener principios de seguridad y privacidad, se ha seleccionado la literatura adecuada donde los requisitos de seguridad de los usuarios y las preocupaciones de

privacidad estén presentes. Lo anterior puede resultar complicado ya que estos requisitos pueden estar enfocado a condiciones muy técnicas o a una perspectiva comercial. Por lo tanto es necesario enforcar la seguridad y privacidad dentro de los requerimientos USec. En este trabajo se intenta integrar la seguridad y la privacidad desde el punto de vista del usuario y no de intereses particulares.

Este conjunto también esta enfocado a autenticación el cual es uno de nuestros principales objetivos donde la seguridad y privacidad estén presentes. Aunque existe muchos más requisitos de seguridad y privacidad donde el usuario es pieza fundamental, en este trabajo se obtuvo los principios más importantes e influyentes dentro del campo de la seguridad usable y autenticación.

A continuación se presenta las 5 características importantes de la seguridad y privacidad y que son parte importante en esta investigación. La definición de estos aspectos son tomados de [67][137].

1. **Integridad**: Grado en que un sistema, producto o componente impide la modificación de los datos, tomando las medidas para asegurar que los datos no pueden ser alterados por personas no autorizadas.

2. **Autenticidad**: La identidad de una persona o recurso puede ser demostrado y ser quien dice ser.

3. **Confidencialidad**:Grado en que un producto o sistema asegura que los datos sean accesibles a aquellos usuarios autorizados a tener acceso.

4. **Privacidad**: La relación entre la tecnología y las cuestiones legales que lo rodean, o la expectativa pública de la intimidad en la recopilación e intercambio de datos sobre la persona.

5. **No repudio**: Una autentificación que con un alto aseguramiento pueda ser reafirmado como genuino.

3.5.3.3. Accesibilidad

La accesibilidad significa proporcionar flexibilidad para acomodarse a las necesidades de cada usuario y a sus preferencias y/o limitaciones. Además de lo anterior, es importante destacar que la accesibilidad se proporciona mediante una combinación de hardware y software: el primero proporciona los mecanismos físicos que permiten salvar ciertas discapacidades y el segundo proporciona la manera eficaz de acceder a las funcionalidades e informaciones para estos dispositivos y a otros programas (e.g. un navegador web) [41].

Según lo anterior, para los sistemas de autenticación que requieren hardware y software, o conocimientos especiales, también pueden excluir a los usuarios y abandonar los aspectos de accesibilidad en un entorno incontrolado. En esta investigación se tienen en cuenta estos dos aspectos (hardware y software) ya que los dos son importantes para realizar una

autenticacion exitosa.

Karen Renaud [20] una respetable investigadora en el campo de la USec afirma que la tendencia general actual es hacia la inclusión. La tecnología ya no es un elemento opcional, sino algo que todo las personas tiene que ser capaces de utilizar. De ahí que la cuestión de la accesibilidad también es importante cuando se tiene en cuenta la seguridad. Así, el mecanismo de autenticación debe ser capaz de acomodarse a los cambios de las capacidades del usuario a través del tiempo.

Finalmente, la conveniencia del mecanismo de autenticación es un factor muy importante en la usabilidad de los mismos. Los usuarios pueden ser demasiado sensibles a los sistemas que pierden su tiempo especialmente cuando consideran que el contenido del sistema es menor de lo esencial. Tienden a acceder a las solicitudes de seguridad sólo hasta un punto y se molestan si estos demoran demasiado tiempo. Esto también se convierte en un problema de accesibilidad, especialmente para los usuarios que acceden a un sistema a través de la red [20].

En el caso de la accesibilidad en la autenticacion de usuario, se tiene en cuenta 3 aspectos importantes.

1. **Requerimientos de hardware y software**: Este aspecto se refiere a los requerimientos mínimos necesario de hardware y software para apoyar el método de autenticación.

2. **Conveniencia**: Hay tres aspectos de conveniencia que se debe tener en cuenta: el tiempo de registro, el tiempo de autenticación, y el tiempo de reemplazo de clave. El tiempo de autenticación es el más relevante, por lo que es en este punto donde se verifica el desempeño del método de autenticación.

3. **Inclusión**: Este aspecto aborda la cuestión de la exclusión de los usuarios. Tres tipos de discapacidad se podrían considerar: cognitiva, física y sensorial.

3.5.3.4. Operabilidad

La operabilidad en el contexto del software se refiere a las cualidades de un sistema que lo hacen funcionar bien durante su vida útil. Se puede decir que un sistema ofrece operabilidad no solo en su aspecto de funcionabilidad, sino también para generar confianza y seguridad en los usuarios. Los sistemas que presentan buena operabilidad tienden a ser fáciles de operar, mantener (servicio), tener alta disponibilidad y confiabilidad [138].

Con base en la definición del estandard ISO 25010:2011 [67], la operabilidad es el grado que un producto o sistema tiene características que lo hacen fácil de operar y controlar. A partir de lo anterior, y enfocándonos en nuestro objetivo, la operabilidad hace referencia a la cantidad de esfuerzo necesario para operar o controlar un método de autenticación [127].

3.5.3.5. Fiabilidad

El estandard ISO 25010:2011 [67] define la disponibilidad como el grado en que un sistema, producto o componente realiza funciones específicas bajo condiciones específicas durante un período de tiempo específico. Las características de la fiabilidad incluyen también la disponibilidad (incluyendo tolerancia a fallas y recuperabilidad), seguridad (incluyendo confidencialidad e integridad), mantenimiento y soporte. La fiabilidad en nuestro caso y con base el estándar ISO 25010:2011 indica la capacidad de realizar funciones específicas que permitan llevar a cabo una autenticación satisfactoria.

3.5.3.6. Desempeño

El desempeño representa la cantidad de recursos utilizados en las condiciones establecidas. Estos recursos pueden incluir también la configuración de software y hardware (e.g. medios de almacenamiento) [67]. En cuestión al desempeño para un sistema de autenticación, el sistema presenta dos características importantes: mínima acción y tiempo de carga.

1. **Mínima acción**: Capacidad de la aplicación para ayudar a los usuarios a alcanzar sus tareas en el menor numero de pasos (e.g. cantidad de pasos en transacciones o procedimientos) [127].

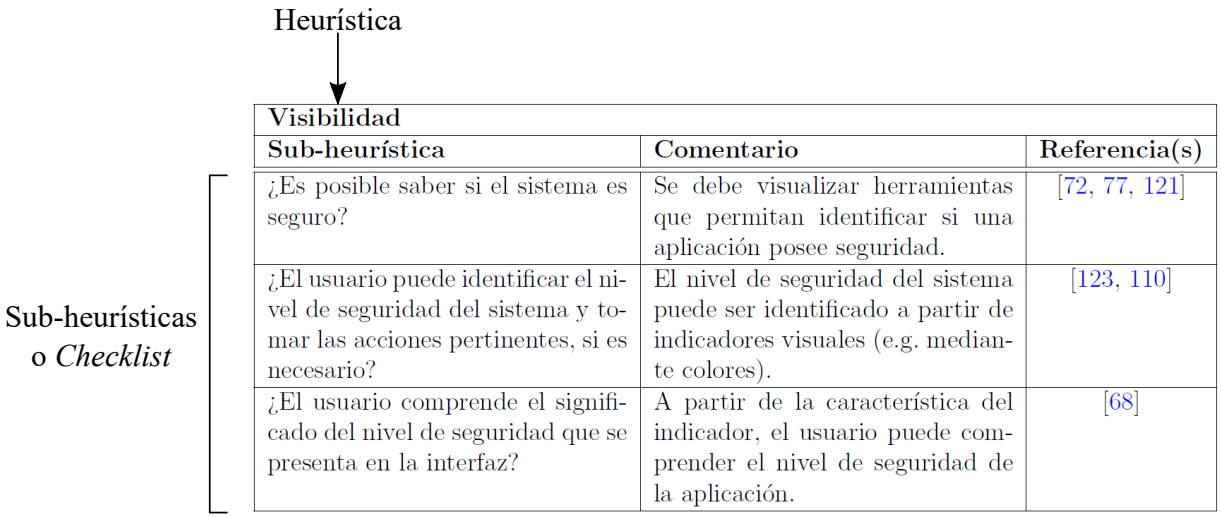
2. **Comportamiento en el tiempo**: Representa el tiempo requerido por la aplicación para cargar, es decir, que tan rápido responde el sistema a las instrucciones del usuario [67].

3.5.4. Identificar y Adaptar las sub-heurísticas de acuerdo a la Literatura

En la Figura 3.9 se presenta un ejemplo de la heurística y sub-heurísticas para usabilidad con sus respectivos componentes como resultado preliminar usando las metodologías durante la etapa 1 del proceso de desarrollo heurístico. En primer lugar se presenta el nombre heurístico (visibilidad del estado del sistema) donde se podría escribir su respectiva definición para el campo de la USec pero no se presenta debido al espacio que genera en el documento, en segundo lugar se presenta las sub-heurísticas o lista de chequeo (*checklist*) donde cada una de estas tiene su respectiva descripción para un mejor entendimiento y por último, la fuente o fuentes donde se obtuvo dichas sub-heurísticas.

El conjunto heurístico obtenido se basa en el análisis de varios trabajos anteriormente presentados (ver Sección 3.5.2), estos trabajos representan directrices o requisitos actuales para seguridad usable y métodos de autenticación. Aunque estos trabajos no cubren todos los aspectos de la calidad del software, uno de los objetivos de este trabajo es proponer una estandarización de estas heurísticas como se dijo anteriormente.

La metodología de Ling & Salvendy [125] se basa en modificar heurísticas existentes para que se adapten a los a los requerimientos del sistema, en este caso seguridad y usabilidad.



Visibilidad		
Sub-heurística	**Comentario**	**Referencia(s)**
¿Es posible saber si el sistema es seguro?	Se debe visualizar herramientas que permitan identificar si una aplicación posee seguridad.	[72, 77, 121]
¿El usuario puede identificar el nivel de seguridad del sistema y tomar las acciones pertinentes, si es necesario?	El nivel de seguridad del sistema puede ser identificado a partir de indicadores visuales (e.g. mediante colores).	[123, 110]
¿El usuario comprende el significado del nivel de seguridad que se presenta en la interfaz?	A partir de la característica del indicador, el usuario puede comprender el nivel de seguridad de la aplicación.	[68]

Figura 3.9: Componentes del conjunto heurístico para USec (creación propia).

A partir de las sub-heurísticas de Pierotti [126], el cual presenta un conjunto muy completo, se identificaron algunas de estas que podrían satisfacer los requisitos de seguridad y usabilidad.

La metodología presentada por Bonastre & Granollers [128] permite obtener heurísticas a partir de recomendaciones dadas en los trabajos citados sobre seguridad usable y autenticación de usuario. Las recomendaciones son reescritas para formar una oración interrogativa.

La metodología de Paddison & Englefield [129] sobre una búsqueda sistemática de la literatura y su respectivo análisis. A partir de bases de datos existentes en la web (e.g. ACM, IEEE, ScienceDirect, Springer, Scopus y *web of knowledge*) y a partir de palabras claves, es posible obtener recomendaciones en el área de interés, en nuestro caso, seguridad usable y autenticacion de ususario. El proceso de búsqueda exhaustiva abarca desde el año 1995 hasta el 2015 [139].

- "seguridad usable" AND "principios de diseño".
- "principios de seguridad usable" AND "principios de autenticación".
- "evaluación seguridad usable" AND "evaluación autenticación".
- "proceso de diseño autenticación" AND "principios seguridad".
- "seguridad centrada en el usuario" AND "autenticación centrada en el usuario"

Los artículos encontrados fueron filtrados según su título, palabras clave y fue llevado a cabo un análisis del resumen, introducción y conclusión para seleccionar las referencias más importantes. La Tabla 3.4 presenta las bases de datos en línea, la cantidad de documentos

encontrados y los documentos relevantes de acuerdo con las palabras claves, necesarias para nuestra investigación.

Tabla 3.4: Artículos encontrados en bases de datos.

Base de Dato	Artículos Encontrados	Artículos Relevantes
IEEE	18	3
Springer	7	3
ACM	14	4
Science Direct	11	2
Scopus	13	10
Web of Knowledge	10	3
TOTAL	**73**	**25**

Las sub-heurísticas identificadas se analizan y se se ubican lo más adecuadamente posible en cada uno de los atributos anteriormente presentados. Para realizar esta ubicación se tuvo en cuenta principalmente la descripción de la sub-heurística y la ubicación que se hacia de los trabajos de la literatura.

3.5.5. Modificar o Mejorar el Conjunto

En este caso se realiza una revisión exhaustiva de los principios obtenidos. En este punto se considera la revisión de definiciones, referencias, reubicación de sub-heurísticas y redacción con el fin de modificar o mejorar el conjunto de principios general.

3.6. Especificación de USec y Autenticación a través de Atributos de Calidad

Los sistemas computacionales son fundamentales en casi todos los ámbitos de la vida de las personas y su correcto funcionamiento es crucial para el éxito de negocios, de la comunicación entre las personas y para la seguridad de las mismas, por tanto, desarrollar o escoger sistemas software de alto nivel cualitativo constituye un aspecto imprescindible [41].

La ISO (del inglés *International Organization for Standardization*) definió en 2011 la ISO/IEC 25010:2011 SQuaRE (del inglés *Systems and Software Quality Requirements and Evaluation*) [67] el cual es un norma que define el sistema y software de calidad. Esta norma internacional se deriva de la ISO/IEC 9126:1991 – Ingeniería de software – Calidad del producto, que fue desarrollada para soportar estas necesidades.

El concepto de la calidad se define en la ISO/IEC 25010 como "*el conjunto total de características de una entidad (producto, proceso o servicio) que le confieren la capacidad de satisfacer las necesidades establecidas y las necesidades implícitas* [67]. La real academia española[2] define la calidad como "*adecuación de un producto o servicio a las características especificadas*". Debido a la importancia del estándar ISO/IEC 25010, la definición con respecto a la calidad del software será el que presenta este estándar.

El estándar ISO 25010:2011 define un **modelo de calidad de uso** compuesto de cinco características (eficiencia, eficacia, satisfacción, libre de riesgo y cobertura del contexto) que se relacionan con el resultado de la interacción cuando un producto se utiliza en un contexto particular de uso y un **modelo de calidad del producto** compuesto de ocho características (adecuación funcional, eficiencia de desempeño, compatibilidad, usabilidad, fiabilidad, seguridad, mantenabilidad y portabilidad) que se relacionan con las propiedades estáticas del software y las propiedades dinámicas del sistema informático. Los atributos de la norma y sus características son presentados en la Figura 3.10.

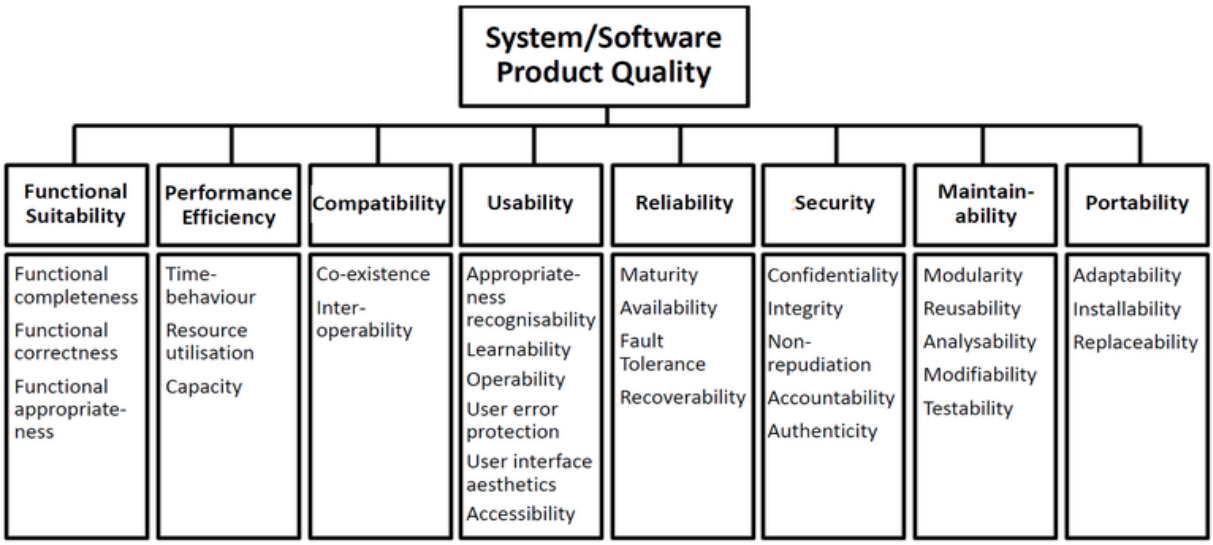


Figura 3.10: Estandard ISO 25010:2011 (Tomado de [67]).

Sin embargo, y con respecto a nuestro estudio, no existe en la literatura una relación entre los atributos de este estándar que la comunidad pueda utilizar para evaluar USec y autenticación de usuario. Para lograr esto, en este trabajo se propone algunos atributos que considera la literatura y que están incluidos con el estándard ISO/IEC 25010:2011 [140].

De acuerdo con nuestra investigación llevada a cabo sobre seguridad usable y autenticacion, los atributos tenidos en cuenta según la norma ISO/IEC 25010:2011 son la usabilidad, seguridad, accesibilidad, fiabilidad, operabilidad y desempeño tal y como se presenta en la Figura 3.11. Es importante aclarar que en estos atributos se consideran solo algunas de

[2]Disponible en: www.rae.es. Consultado en Septiembre de 2016.

características importantes que están implícitamente incluidos en la norma. Para el atributo de seguridad las características incluidas son confidencialidad, integridad, privacidad, autenticidad y disponibilidad.

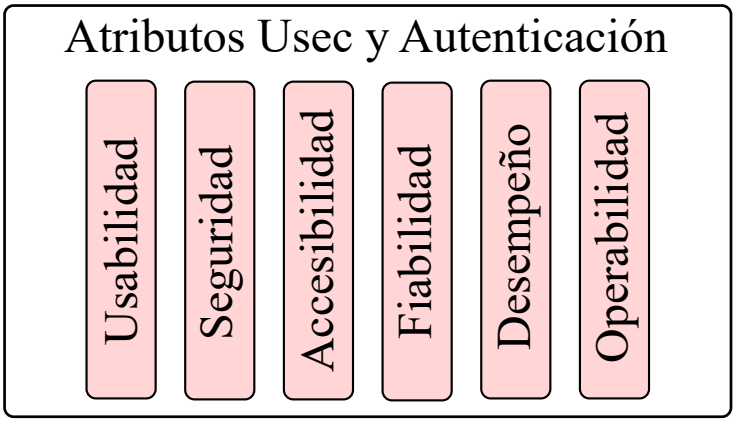


Figura 3.11: Atributos para USec y Autenticación de usuario basado en la ISO 25010 (Creación propia).

Debido a que la usabilidad posee el mayor número de sub-heurísticas de acuerdo a la literatura, esta tendencia numérica seguía creciendo a medida de que se analizaban los trabajos de investigación proporcionados por el estado del arte. Cada sub-heurística encontrada fue analizada y ubicada en el atributo adecuado de acuerdo a la actividad 4 de la Etapa 1 del desarrollo heurístico. Un total de 152 sub-heurísticas distribuidos en cada atributo fueron encontrados tal y como se muestra en la Tabla 3.4. Observamos que la usabilidad, con 75 sub-heurísticas, presenta el número más alto debido a que nuestra investigación se centra en la seguriad usable y además, es la mas utilizada a la hora de diseñar y evaluar un sistema interactivo seguro y usable, la seguridad abarca 34 sub-heurísticas, la accesibilidad con 8, desempeño 11, operabilidad 9 y finalmente fiabilidad con 15 sub-heurísticas respectivamente, ver Tabla 3.5.

Tabla 3.5: Número de sub-heurísticas por cada Atributo (Creación propia).

Atributo	**Número de sub-heurísticas**
Usabilidad	75
Seguridad	34
Accesibilidad	8
Desempeño	11
Operabilidad	9
Fiabilidad	15
TOTAL	**152**

Con respecto a la usabilidad, en la Tabla 3.6 se presenta el número de sub-heurísticas para

cada heurística.

Tabla 3.6: Número de sub-heurísticas para usabilidad (Creación propia).

Heurística	Número de sub-heurísticas
Visibilidad del estado del sistema	11
Estética y mínimo diseño	5
Control y libertad de usuario	7
Utilización del lenguaje del usuario	5
Minimizar carga de memoria	9
Reconocer, diagnosticar y recuperarse de los errores	7
Flexibilidad y eficiencia de uso	7
Prevención de errores	5
Consistencia y estándares	6
Ayuda y documentación	6
Transmitir características	7
TOTAL	**75**

3.7. Discusión

La seguridad es un área problemática para el diseño de interfaces de usuario. En consecuencia, los desarrolladores necesitan herramientas que les ayuden a mejorar sus diseños en términos de seguridad utilizable para aplicaciones, por ejemplo, la autenticación de usuario. Por lo tanto, los problemas de diseño de seguridad y privacidad se pueden reducir usando principios de USec presentados en esta investigación. Consideramos que esto es una contribución importante al campo USec.

Las actividades presentadas en el proceso de desarrollo heurístico consisten en comprender y especificar el contexto de uso, especificar los requisitos del usuario y del dominio de aplicación, investigar qué atributos pueden ser importantes en el área de la seguridad usable y qué sub-heurísticas hacen parte de estos atributos con el fin de ser evaluados por expertos. El objetivo de este proceso es asegurar que el conjunto principios satisfaga los requisitos para los usuarios de aplicaciones específicas donde las características de seguridad sean parte del sistema.

En este capítulo se propuso una integración entre la norma ISO 9241-210 y un proceso de desarrollo con el fin de obtener un conjunto de principios para USec, teniendo en cuenta algunos atributos y características de la norma ISO/IEC 25010:2011. Muchos usuarios no son capaces de percibir los problemas de seguridad correctamente, generando una amenaza a la seguridad debido a malentendidos y evitando tácticas para proteger el sistema. Aunque existen diferentes métodos para evaluar la usabilidad de los sistemas de seguridad, algunos métodos como la evaluación heurística, no son convenientes para su evaluación

debido a la falta de principios USec adecuados.

Con base en lo anterior y mediante actividades ordenadas, se encontraron principios que podrían ser pieza clave en el diseño de aplicaciones más seguras y usables para desarrolladores que necesitan ciertas recomendaciones básicas cuando están comenzando a desarrollar aplicaciones para sus usuarios.

Con base en el primer objetivo de esta tesis "*identificar posibles principios de seguridad usable que permita un balance adecuado entre seguridad y usabilidad particularmente para autenticación de usuario*", creemos que ha sido completado casi en su totalidad, pues es necesario que estos principios sean revisados uno a uno por expertos en el área de la usabilidad, seguridad y seguridad usable. Estos principios han sido adaptados para seguridad usable y que sean evaluados usando uno de los métodos de inspección de usabilidad, la evaluación heurística. La validez y aplicabilidad de estos principios para USec se abordarán en los Capítulos 4 y 5 donde ratificaremos o no, el posible potencial que podrían tener estos principios en aplicaciones reales.

3.8. Conjunto Heurístico Preliminar para USec y Autenticación

A continuación se presenta los atributos y principios, producto de la primera etapa del desarrollo heurístico. En las Tablas presentadas a continuación, se puede observar los tres elementos importantes, la sub-heurística obtenida a través de las metodologías presentadas anteriormente, un comentario donde se explica brevemente la sub-heurística y las referencias de donde se obtuvo.

3.8.1. Usabilidad

Tabla 3.7: Sub-heurísticas para Usabilidad.

Sub-heurística	Descripción	Fuente(s)
1. Visibilidad del estado del sistema		
¿Es posible saber si el sistema es seguro?	Se debe visualizar herramientas que permitan identificar si una aplicación posee seguridad.	[78][83][133]
¿El usuario puede identificar el nivel de seguridad del sistema y tomar las acciones pertinentes, si es necesario?	El nivel de seguridad del sistema puede ser identificado a partir de indicadores visuales (e.g. colores).	[134][122]
¿El usuario comprende el significado del nivel de seguridad que se presenta en la interfaz?	A partir de la característica del indicador, el usuario puede comprender el nivel de seguridad de la aplicación.	[74]

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Fuente(s)**
¿Se ha utilizado el color específicamente para llamar la atención e indicar los cambios relacionados con la seguridad?	El tipo de color presentado puede indicar cambio del nivel de seguridad o riesgo del sistema.	[74]
Si hay retrasos observables en el tiempo de respuesta del sistema a una acción relacionada con la seguridad, ¿está el usuario informado de los avances del sistema?	Usualmente, un indicador de progreso podría visualizar el estado del sistema.	[78][128]
Después de que el usuario complete una acción de seguridad, ¿la realimentación indica que el siguiente grupo de acciones puede ser iniciada?	A partir de mensajes que visualicen el inicio para el desarrollo de acciones posteriores (e.g. el sistema presenta un mensaje de "inicio de sesión").	[78][134]
¿Hay alguna forma de realimentación para cada acción relacionada con la seguridad?	Diferentes sistemas y niveles de seguridad deben ser visualizado de acuerdo al riesgo.	[78][96][133]
En las interfaces de alerta, ¿el sistema provee el nombre de las herramientas de seguridad?	Cuando se presenta una interfaz de alerta, el usuario identifica herramientas de seguridad que se están ejecutando (e.g. firewall).	[132] [91]
¿El estado del usuario es visible en el sistema?	A partir de palabras o colores, es posible identificar el estado del usuario.	[78][96]
Al observar el estado de seguridad del sistema, ¿el usuario puede decir las alternativas para las acciones relacionadas con la seguridad, si es necesario?	A partir del nivel de seguridad del sistema, el usuario debe conocer alternativas necesarias con el fin de no poner en riesgo las acciones que se están llevando a cabo.	[78][83]
¿El sistema mantiene informado al usuario sobre el estado de conexión del sistema?	La interfaz debe informar al usuario el tipo de protocolo de seguridad cuando existen conexiones con entidades que podrían no ser confiables.	[122]
2. Estética y mínimo diseño		
¿La información de seguridad presentada en pantalla es relevante?	Es necesario presentar en pantalla información de seguridad relevante y no aspectos técnicos.	[128, 78, 74, 132, 133, 96]
¿Los íconos de seguridad son identificables y diferenciables?	Los iconos de seguridad deben ser fácilmente visualizados y distinguibles.	[83][78]
¿Las etiquetas de seguridad son sencillas, fáciles de entender y representativas?	Las etiquetas de seguridad no deben tener términos técnicos abstractos y ser visualizados adecuadamente.	[78]

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Fuente(s)**
¿Las indicaciones de seguridad son expresadas en sentido de confirmación?	A partir de mensajes que confirmen la acción que desea realizar (e.g. ¿le gustaría revisar sus configuraciones predeterminadas?).	[78, 132, 63]
¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?	El sistema puede tener elementos visuales que permitan al usuario conocer políticas de privacidad sobre el uso del sistema.	[78, 132, 135, 128]
3. Control y libertad de usuario		
¿Los usuarios pueden revertir fácilmente sus acciones de seguridad?	El sistema tiene la capacidad de volver al estado anterior fácilmente si el usuario lo desea.	[83, 78, 91, 95]
¿Los usuarios pueden cancelar las operaciones de seguridad en curso?	Los botones de cierre permite a los usuarios cancelar las acciones que se estén ejecutando.	[78, 91]
¿Hay una función "desistir o deshacer" para una simple acción o grupo completo de acciones de seguridad?	Una función puede revertir una o varias acciones de seguridad en ejecución.	[83, 95]
¿El sistema esta diseñado de manera que los botones con nombres similares, no desarrollen acciones de seguridad opuesto?	Si los botones tienen etiquetas similares, estos deben cumplir funciones de seguridad adecuado sin ejecutar procedimientos opuestos.	[78]
Cuando las indicaciones implican una acción de seguridad necesaria, ¿las palabras del mensaje son coherente con la acción?	Los avisos de seguridad que aparecen en los mensajes desplegados deben coincidir con la acción de seguridad necesaria.	[78]
¿Las opciones de seguridad en el menú hace evidente si la selección de la opción es posible?	Las opciones del menú son fácilmente seleccionadas o revocadas.	[78]
¿El usuario es capaz de confirmar cualquier acción que tenga consecuencias drásticas, negativas o destructivas?	El usuario debe conocer que clase de acción esta ejecutando el sistema, esto evitaría riesgos de seguridad.	[63]
4. Utilización del lenguaje del usuario		
¿Los mensajes de seguridad están nombrados coherentemente en todo sistema?	Los mensajes de seguridad expresados en un lenguaje coherente y adecuado permite al usuario utilizar el sistema con menor riesgo.	[78]
¿Las sentencias de alerta son simples, cortas y comprensibles?	Toda la información de seguridad que es presentada por el sistema debe ser concisa y sencilla de entender.	[132]

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Fuente(s)**
¿Las preguntas de seguridad son expresadas en un lenguaje claro y sencillo?	Las preguntas de seguridad que permiten mitigar amenazas, son comprensibles por el usuario.	[78]
¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?	Los términos técnicos o avanzados relacionados con el manejo de las políticas de seguridad y privacidad deben ser evitados.	[91, 132, 133, 96, 135]
¿El sistema evita el uso de palabras diferentes para transmitir la misma idea o concepto?	Usar diferentes palabras para transmitir la misma idea puede confundir a los usuarios, pues esto crea explicaciones incorrectas y generan ambigüedad.	[82]
5. Minimizar carga de memoria		
¿Las relaciones entre los controles de seguridad y las acciones de seguridad son claras para el usuario?	Las acciones de seguridad identificadas a partir de controles, deben tener relación para una mejor comprensión.	[78]
¿Las tareas de seguridad son fáciles de aprender y recordar?	Es necesario que las operaciones de seguridad realizadas por los usuarios no tengan procedimientos complejos.	[74, 133, 132]
¿Existen situaciones predeterminadas de selección de seguridad?	El sistema informa al usuario opciones predeterminadas de selección de seguridad específicas (si existen) durante su interacción.	[78, 133]
¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	Los elementos de seguridad de los menús en la interfaz son claros para el usuario.	[78]
¿La información relacionada con la seguridad es presentada de una manera coherente y estandarizada?	Información coherente y basado en estándares es mas fácil de aprender y recordar.	[78, 74]
En un proceso de autenticación por conocimiento, ¿la carga de memoria para los usuarios es minimizada?	Sin memorizar datos extensos, complicados procedimientos o realizar actividades cognitivas complejas.	[127]
¿El sistema evita usar más de 4 dígitos para autenticación por PIN?	El uso de más de 4 dígitos para PIN hace más difícil recordarlo.	[127]
Si se utiliza el reconocimiento visual para autenticación, ¿los usuarios pueden asociar una frase o palabra a una imagen como contraseña?	Una imagen permite al usuario recordar palabras o frases con facilidad.	[127]

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Fuente(s)**
Para PINs de más de 7 caracteres, ¿el sistema hace uso de herramientas nemotécnicos?	La mente humana tiene la posibilidad de recordar fácilmente hasta 8 caracteres, la facilidad de recordar se mejora mediante el uso de herramientas mnemotécnias.	[127]
6. Reconocer, Diagnosticar y Recuperarse de Errores		
¿Los mensajes relacionados con la seguridad son declarados de forma constructiva?	Los mensajes de error relacionados con la seguridad debe guiar a solucionar la dificultad sin criticar al usuario.	[78]
¿Los mensajes de error relacionados con la seguridad informan al usuario de la gravedad del error?	Conocer el nivel de seriedad del error ayuda a tomar acciones adecuadas.	[78]
¿El sistema facilita la posibilidad de diagnostico a posibles errores?	Cuando existe una amenaza de seguridad el sistema puede presentar fallas (e.g. bloqueo), por lo tanto es necesario realizar un diagnostico de los errores que dejo la amenaza.	[95]
¿Los mensajes de error relacionados con la seguridad son significativos y sensibles al problema?	En algunos casos los mensaje de error debe proporcionar la causa del error de seguridad y de una forma que el usuario pueda entenderlo.	[78, 96]
¿Los mensajes de error relacionados con la seguridad indican la acción que el usuario debe tomar para corregir el error?	Es necesario que el sistema recomiende acciones de acuerdo a errores de seguridad específicos.	[78, 132]
¿Los mensajes de error relacionados con la seguridad son adecuados al lenguaje del usuario?	Los mensajes de error deben tener un lenguaje sencillo que los usuarios puedan entender y tomar decisiones.	[74]
¿Los mensajes de error relacionados con la seguridad indican al usuario dónde obtener ayuda?	Si el usuario no comprende el mensaje de error, este debe proporcionar ayuda para solucionarlo.	[74]
7. Flexibilidad y Eficiencia de Uso		
¿Los usuarios pueden cambiar fácilmente entre los niveles de principiante y experto?	El sistema tiene la posibilidad de presentar información y acciones adecuadas para principiantes y expertos.	[78, 132]
Si el sistema es compatible con usuarios principiantes y expertos, ¿los niveles de los mensajes de error con respecto a la seguridad están disponibles en detalle?	La información de los mensajes de error de seguridad se adecuan a usuarios principiantes y expertos.	[78, 132]

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Fuente(s)**
¿Los usuarios pueden elegir entre información de seguridad de texto o gráfico (ícono), según sea el caso?	El usuario puede visualizar (a partir de texto o gráfico) información de seguridad según se adecue a sus preferencias.	[78]
¿El sistema permite configurar fácilmente las propiedades de seguridad?	La facilidad de configuración de seguridad permite al usuario realizar tareas adecuadas de acuerdo a sus necesidades.	[96]
Si el sistema es compatible con usuarios principiantes y expertos, ¿Los niveles de seguridad están disponibles en detalle?	El nivel de seguridad de una aplicación puede ser cambiada según las habilidades y preferencias del usuario.	[78, 133]
¿Los usuarios pueden personalizar fácilmente las opciones seguridad y privacidad para satisfacer sus preferencias individuales?	El sistema posee características propias de seguridad y privacidad de acuerdo a una aplicación en particular.	[78, 96, 135]
¿El sistema posee atajos a tareas de seguridad frecuente?	El usuario puede usar atajos de teclado o comandos a tareas de seguridad frecuente.	[133]
8. Prevención de Errores		
¿El sistema permite a los usuarios confirmar acciones de seguridad que pueda tener consecuencias severas?	Es necesario que el sistema informe de una manera adecuada y agradable al usuario las posibles consecuencias a la seguridad a partir de sus acciones.	[83, 78]
¿La información necesaria para tomar una buena decisión de seguridad, es adecuada y esta disponible antes de que se adopte la medida?	La información y las consecuencias de cualquier decisión relevante para la seguridad, (e.g. revelar información sensible) deben ser claras.	[83]
¿El sistema advierte a los usuarios si están a punto de cometer un error de seguridad potencialmente grave?	Por desconocimiento, los usuarios pueden realizan tareas sin darse cuenta de las consecuencias que pueden tener.	[78]
¿El sistema impide a los usuarios cometer errores de seguridad siempre que sea posible?	El sistema puede adelantarse impidiendo ejecutar acciones del usuario si detecta posibles errores a la seguridad.	[78, 96]
¿Las funciones importantes que pueden causar resultados serios de seguridad, están en posiciones difíciles de alcanzar?	Las funciones que puedan comprometer la seguridad del sistema no deben ser accesible a los usuarios novatos.	[78]
9. Consistencia y estándares		
¿Los iconos de seguridad poseen etiqueta?	La etiqueta en los iconos de seguridad permite al usuario conocer su función.	[126, 65]

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Fuente(s)**
¿Los títulos de las opciones de seguridad están centrados o justificados a la izquierda?	Los títulos de los menús de seguridad deben estar centrados o justificados a la izquierda.	[126, 65]
¿Los controles de seguridad son consistentes y están ubicados en lugares específicos?	Con un conjunto consistente de controles de seguridad y ubicación adecuada, existirá más oportunidades para el aprendizaje pasivo y su coste de esfuerzo disminuye.	[82, 132, 122]
Para interfaces de preguntas y respuestas sobre seguridad, ¿las entradas válidas para una cuestión están listadas?	Las posibles respuestas con relación a una pregunta de seguridad realizada por el usuario, son presentadas en forma de lista.	[126, 65]
¿Los nombres de las opciones de seguridad en los menús, son consistentes con relación a los demás nombres en cuanto a términos técnicos?	Las opciones de seguridad deben tener semejante terminología técnica en cuanto a la seguridad del sistema.	[122]
¿Las abreviaturas para palabras de seguridad poseen una longitud predeterminada y fácil de identificar?	La longitud de las palabras abreviadas poseen un promedio en su longitud y ser identificada.	[126, 65]
10. Ayuda y Documentación		
¿Hay una función de ayuda de seguridad visible?	La función de ayuda debe ser visible e identificable por el usuario.	[78, 128, 122, 132, 96, 133],
¿La información proporcionada por la ayuda es relevante?	La información de seguridad debe ser significativo con respecto a las necesidades del usuario.	[78, 96]
¿Los usuarios pueden cambiar fácilmente entre la ayuda de seguridad y sus tareas?	El usuario puede obtener ayuda mientras realiza tareas y viceversa.	[78]
¿Las instrucciones de la ayuda siguen la secuencia de acciones de seguridad del usuario?	Las instrucciones de ayuda para una situación especifica debe seguir unos pasos ordenados para solucionar el inconveniente.	[78]
¿El sistema provee actualizaciones oportunas a documentación relacionada con la seguridad y privacidad?	La documentación de seguridad y privacidad debe actualizarse periódicamente con el fin de proporcionar nuevas herramientas para los usuarios.	[127, 135]
¿El sistema provee soporte técnico en linea para solucionar problemas de seguridad?	Es importante que exista ayuda técnica en linea a situaciones complejas de seguridad.	[95, 128, 132]

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Fuente(s)**
11. Transmitir características		
¿Hay una clara comprensión de las capacidades de seguridad del sistema?	Los usuarios pueden observar en el sistema características y capacidades en seguridad, y actuar en caso de ser necesario.	[83, 133, 91]
¿El sistema anticipa adecuadamente y pronto la próxima actividad probable relacionada con seguridad?	El sistema tiene la capacidad de proponer la próxima acción de seguridad que permita una solución mas efectiva para los usuarios.	[127]
¿El sistema notifica a los usuarios si está interactuando con fuentes no confiables?	La fuente no confiable representa algo que no tiene información sobre su identidad, si esto llega a presentarse, el sistema notifica al usuario que puede existir algún tipo de vulnerabilidad.	[74]
¿El sistema muestra logos de seguridad?	Debe mostrarles especialmente para transmitir confianza (e.g. SSL).	[128, 74]
¿El sistema tiene certificados de seguridad otorgado por entidades externas reconocidas?	Es importante conseguir que los usuarios conozcan sus funciones (e.g., VeriSign, ControlScan o SSL).	[128, 74]
¿Los datos que los usuarios no pueden modificar están desactivados?	Los datos que son propios de la seguridad del sistema sistema no pueden ser editados.	[63]
¿El sistema proporciona un número limitado de configuraciones de seguridad estandarizados que pueden ser auditados, documentados, y fácilmente aprendido por los usuarios?	Los sistemas informáticos actuales tienen un gran número de políticas de seguridad que son complejos y desconocidos. Es mejor dar una cantidad limitada de políticas estandarizadas que por lo general no necesitan ser personalizadas.	[82, 132]

3.8.2. Seguridad y Privacidad

Tabla 3.8: Sub-heurísticas para seguridad y privacidad.

Sub-heurística	Descripción	Fuente(s)
¿Las áreas protegidas son completamente inaccesibles?	Las áreas críticas del sistema, no deben tener acceso para usuarios comunes sino solo para los administradores del sistema.	[78, 63]
¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?	Para información sensitiva, siempre debe accederse usando algún tipo de credencial.	[127]
¿El sistema emplea mecanismos critográficos para la transmisión segura de la información?	Es necesario implementar protocolos seguros para la transmisión de datos.	[78, 63]
Si el sistema utiliza *cookies* informáticos, ¿la información sobre la privacidad del sistema describe con precisión el uso de estas cookies?	La informacion de privacidad debe describir si las cookies llevan el control de los usuarios (e.g. almacenamiento de información, passwords) o conseguir información sobre los hábitos de navegación del usuario.	[135]
¿Los caracteres de la clave de acceso están ocultos directamente en el campo?	Los caracteres de la clave de acceso (passwords o PIN) aparecen en forma de puntos o asteriscos mientras se digitan.	[63]
¿El proceso de autenticación hace cumplir un límite de intentos de acceso no válidos consecutivos por un usuario?	El sistema se bloquea si el número de intentos posibles consecutivos en un tiempo determinado, no certifican la identidad del usuario.	[78, 63, 127]
Si el sistema necesita más de una clave de acceso, ¿el sistema utiliza técnicas fáciles para reducir la carga cognitiva de los usuarios?	El sistema puede usar caracteres alfanuméricos (para passwords) y gráficos (para graphical passwords). Es mas fácil recordar una imagen que una palabra.	[63, 127]
En un método de autenticación por conocimiento, ¿el sistema permite al usuario modificar su clave de acceso?	El sistema facilita el cambio de claves de acceso fácilmente en cualquier momento.	[63, 128]
¿El sistema instala actualizaciones de seguridad y notifica al usuario sobre esta acción?	En todo momento son creadas nuevas amenazas de seguridad, las actualizaciones y su notificación debe ser constantes. Para realizar esta acción, el usuario debe tener ciertos privilegios.	[78, 63]

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Fuente(s)**
¿El sistema confirma al usuario la transmisión de datos antes que estos sean transmitidos?	Para evitar enviar datos sensibles por error, el sistema confirma al usuario si procede a realizar dicha acción.	[63]
¿El sistema notifica a los usuarios sobre los privilegios de acceso que posee?	Los usuarios no pueden poseer privilegios (e.g. modificar archivos de sistema) que afecten la seguridad del sistema.	[78, 91]
¿El sistema concede acceso de acuerdo a una autorización válida?	Si la validación de la información por parte del usuario es correcta, el sistema concede acceso.	[78]
¿El usuario puede actualizar o eliminar información personal incorrecta?	La información personal puede cambiar durante el tiempo o cometer errores cuando son ingresados.	[78, 63, 135]
¿Se presenta al usuario mensajes de notificación concernientes a la seguridad y privacidad antes de acceder al sistema?	El sistema presenta al usuario mensajes sobre políticas de seguridad y privacidad.	[78, 135]
¿El sistema garantiza que la información de acceso público no tenga información privada?	El sistema debe abstenerse de presentar información privada cuando sea público.	[78]
¿La información de privacidad del sistema garantiza al usuario el derecho a optar por compartir información no crítica con terceros?	Las políticas de privacidad del sistema deben permitir al usuario el deseo o no de compartir información que no sea sensitiva.	[135]
¿El sistema emplea herramientas que proveen notificación al usuario sobre discrepancias durante la verificación de identidad?	A partir de mensajes o sonidos puede ser notificado al usuario sobre estas discrepancias.	[78, 127]
Si el sistema facilita el intercambio de datos con otros usuarios, ¿ el sistema permite diferentes políticas de acceso y asociarse a diferentes tipos de datos?	Cuando existe intercambio de datos entre usuarios, el sistema posee políticas de seguridad (e.g. autenticación) para acceder e intercambiar información.	[135]
¿El sistema notifica al usuario sobre vulnerabilidades asociados a incidentes de seguridad detectados?	Cuando se presenta un incidente de seguridad, el sistema presenta las posibles consecuencias de esto.	[78]
En el proceso de configuración de la cuenta, ¿existe la opción de configuración de privacidad y aplicable a todo el sistema?	En el proceso de configuración de la cuenta del usuario, las opciones de configuración de privacidad deben estar disponibles para que el sistema sea mas fácil de usar y evitar que la información sea de acceso público.	[135]

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Fuente(s)**
¿El sistema notifica al usuario sobre realización de copias de seguridad relacionados con la información personal?	Antes de realizar una copia de seguridad, el sistema debe notificar al usuario para realizar esta acción.	[78]
¿El sistema describe cada opción de privacidad en detalle?	Cada opción de privacidad debe describir detalladamente que tipo de información debe ser presentada a terceras personas o no debería presentarse nada.	[135]
¿Existe una política de copia de seguridad que especifica cómo debe realizarse esta acción?	Las copias de seguridad están basadas en planes de acción para afrontar riesgos de seguridad.	[78]
¿El sistema emplea mecanismos criptográficos para evitar la divulgación no autorizada durante el proceso de transmisión de información?	Es necesario implementar protocolos seguros para la transmisión de datos.	[78, 63]
¿El sistema provee confirmación para los usuarios sobre las declaraciones que indican que ellos entienden las condiciones de acceso?	Los mensajes de confirmación permite establecer condiciones de acceso al usuario.	[78]
¿El sistema hace cumplir el nivel de complejidad de la contraseña, con los requisitos mínimos exigidos?	El usuario puede determinar la complejidad de la contraseña y los requisitos a través de barras que cambian de color en función de la complejidad de la contraseña.	[78, 127]
¿El sistema cifra datos solicitados en el proceso de autenticación?	La información solicitada al usuario para poderse certificar debe ser encriptada para aumentar el nivel de seguridad.	[127]
¿La interfaz tiene derechos de autor (copyright)?	El sistema debe cumplir las leyes de privacidad de la información y derechos de autor.	[63]
Si se utiliza tarjetas inteligentes, ¿los datos del propietario están almacenadas en ella?	Para verificar que el propietario es quien dice ser, todo sus datos deben estar almacenados en la tarjeta.	[127]
¿El sistema proporciona consejos u orientaciones de configuraciones de privacidad cuando se usa por primera vez?	El sistema debe orientar a los usuarios de las configuraciones de privacidad cuando el sistema se usa por primera vez (e.g. orientación de las configuraciones de privacidad cuando se crea una cuenta).	[135]

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Fuente(s)**
¿La tarjeta inteligente o token del titular posee mecanismos de política privacidad?	Técnicas criptográficas pueden ser aplicadas a smart cards o tokens (e.g. la seguridad de la información de la credencial es cifrada usando PKI).	[127]
¿El sistema posee políticas de privacidad para comercio o contenido del usuario?	Las políticas de seguridad pueden estar enfocadas a comercio electrónico o datos personales (en estos sitios es fundamental las políticas de privacidad).	[135]
Si es necesario realizar autenticación por multi-factor, ¿el uso de PIN esta implementada?	Para combinaciones de métodos de autenticación, el proceso de autenticación por PIN (i.e., 4 dígitos) es fácil de usar y recordar.	[127]
¿El sistema soporta y hace uso por defecto del protocolo HTTPS?	Destinado a la transferencia segura de datos de hipertexto y utilizado principalmente para e-banking, e-commerce o cualquier tipo de servicio que requiera el envío de datos personales y/o certificados digitales.	[135]

3.8.3. Accesibilidad

Tabla 3.9: Sub-heurísticas para accesibilidad.

Sub-heurística	**Descripción**	**Fuente(s)**
¿El sistema permite usar passwords gráficos para usuarios con dificultades de lectura?	Las imágenes podrían ayudar a las personas a autenticarse cuando tienen problemas de lectura, e.g., dislexia.	[136]
En autenticación por biometría, ¿el sistema esta compuesto por dispositivos estandard?	La inclusion de dispositivos estandard facilita su configuración y uso por parte de los usuario.	[127]
En autenticacion por posesión, ¿el servidor esta equipado con software y hardware adecuado?	La instalacion de software adecuado en hardware eficiente, facilta su uso por parte de los usuarios en el proceso de autenticacion.	[20]
¿El sistema evita el uso de claves aleatorias para la etapa de registro o autenticacion?	El uso de claves aleatorias (e.g. One-Time Password) son difíciles de utilizar por los usuarios, debido a que no es posible memorizarlas todas.	[20]
En un proceso de autenticacion, ¿no es necesario esfuerzo adicional?	El proceso de autenticacion debería ser intuitivo y sin esfuerzo (e.g. cognitivo o físico) extra.	[20]
En un sistema por autenticacion por biometria, ¿el sistema permite ser configurado para personas con limitaciones físicas?	Para problemas psicomotrices que implica una falta de organización del movimiento (e.g. dispraxia), el sistema debería ser configurado fácilmente para estos casos.	[20]
¿El sistema provee a los usuarios otras alternativas para autenticarse?	Esto podría mejorar la disponibilidad y conveniencia del sistema.	[127]
¿El método de autenticación se adapta a usuarios nuevos y experimentados?	El método de autenticación debería tener opciones de configuración para ser usados por usuarios nuevos y experimentados.	[20]

3.8.4. Operabilidad

Tabla 3.10: Sub-heurísticas para operabilidad.

Sub-heurística	**Descripción**	**Fuente(s)**
¿El sistema permite seleccionar algún método de autenticación en especial o combinaciones de ellas?	El usuario tiene la posibilidad de escoger el sistema de autenticación o combinaciones de ellas (autenticación multifactor) de acuerdo a sus necesidades.	[127]
¿Pueden los usuarios personalizar la interfaz en el proceso de autenticación de acuerdo a sus necesidades, sin poner en riesgo la seguridad relacionada con información sensitiva?	A partir de las necesidades del usuario, el cambio de la interfaz no presentará información sensitiva a terceros.	[127]
Para operaciones de alto riesgo de ataque, ¿el sistema permite usar autenticación biométrica?	El ataque informático usando seguridad biométrica, es más difícil comparado con otros métodos de autenticación.	[127]
Si los usuarios olvidan el PIN, ¿el sistema permite restablecerlo a través de una interfaz?	La interfaz del sistema donde el usuario tiene la cuenta, permite cambiar o recordar el PIN en caso de olvido.	[127]
¿El método de autenticación empleado sigue normas estandarizadas?	Varios métodos de autenticación usan algoritmos propios o procesos patentados (e.g. RSA) que son estándares a nivel internacional.	[127]
Si el proceso de registro es requerido, ¿este es corto, sencillo y solo exige información esencial?	Es útil mantener el proceso de registro lo más corto posible y en el caso de la información requerida, explicar brevemente por qué se requiere.	[127][128]
En los campos donde se necesita información para autenticarse, ¿el tamaño de la letra es apropiado para el usuario?	Utilizar un tamaño de fuente adecuado para asegurar la facilidad de lectura.	[127]
¿El sistema informa al usuario que el proceso de autenticación ha sido satisfactorio?	Crear un mecanismo de retroalimentación para que el usuario sepa cuándo el proceso de autenticación ha sido satisfactoria.	[127]
En un proceso de autenticación, ¿este tiene palabras adecuadas para desarrollar una acción en particular?	Usar palabras o frases adecuadas que describan la acción a realizar (e.g. usar *ingresar* (sing in) en lugar de *cuenta* (account))	[127]

3.8.5. Fiabilidad

Tabla 3.11: Sub-heurísticas para fiabilidad.

Sub-heurística	Descripción	Fuente(s)
¿El proceso de autenticación es simple y protege contra usuarios no autorizados?	Para acceder a información privada, el método de autenticación disponible debe ser adecuado y seguro.	[63, 127]
¿La interfaz ayuda al usuario a tener una experiencia segura y satisfactoria con el sistema?	La experiencia con las características de seguridad tiene que ser agradable y satisfactoria, de lo contrario pueden descuidar la seguridad de su sistema.	[74, 128]
¿El sistema presenta certificados de confianza TRUSTe?	Asegura al usuario que pueden confiar en el sistema, respetando su privacidad a partir de certificados estandards.	[20]
En el caso en que el usuario deba proporcionar la información, ¿el sistema determina que medidas son utilizadas para proteger esta información?	El sistema proporciona tranquilidad al usuario a partir de criterios de seguridad para proteger la información sensible (e.g. personal).	[78, 63]
¿Está claramente establecido el propósito de utilizar la información personal del usuario?	El sistema informa al usuario sobre la finalidad en el uso de su información personal.	[78, 128]
¿El sistema notifica al usuario si está interactuando con fuentes no confiables?	Verificar las fuentes y datos de forma segura, permite interactuar de forma responsable y evita el riesgo de tomar decisiones erradas.	[78]
¿El sistema emplea mecanismos para ayudar en la presentación de informes de incidentes de seguridad?	El sistema tiene procesos automatizados en la presentación de informes de seguridad.	[78]
¿El sistema notifica al usuario sobre el procedimiento a seguir en el caso de suplantación o pérdida de información personal?	El sistema posee un plan de acción cuando ha habido suplantación o perdida de información.	[78]
¿El propietario del sistema provee integración a múltiples bases de datos?	La integración de datos mejora la seguridad mediante confirmación de información.	[127]
¿El sistema ofrece servicios de seguridad personalizado que permite tener en cuenta las necesidades y preferencias de los usuarios?	El sistema debería permitir algún tipo de seguridad personalizado (e.g. crear un autenticador de tokens de seguridad personalizado e integrarlo con un administrador de tokens de seguridad personalizado).	[20]

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Fuente(s)**
Si el proceso de inicio de sesión falla, ¿el sistema evita indicarle al usuario qué parte del proceso es incorrecto?	La realimentación de información sensitiva en un proceso de autenticación, podría llevar a ataques informáticos.	[78]
¿El sistema prohíbe la reutilización de contraseñas?	Organizaciones que son susceptibles a ataques informáticos (e-banking), solicitan al usuario cambiar frecuentemente las contraseñas y evitan que sean las mismas.	[78]
¿Se evita cualquier PIN definido por el sistema?	El PIN definido por el sistema puede no tener relación con el usuario, lo que lleva a complicar su memorización fácilmente.	[127]
Para autenticación desafio-respuesta (Challenge–response authentication), ¿las preguntas desafio son pertinentes para los usuarios?	Las preguntas deben ser caracterizadas para la mayor cantidad de los usuarios.	[20]
Si el número de preguntas desafio que contesta el usuario es n, ¿el sistema presenta un número de preguntas t es mayor que n que podrían ser contestadas?	Generalmente los usuarios contestan un máximo tres preguntas desafio para autenticarse, por lo tanto el sistema debe proporcionar un numero de preguntas mayor a tres como opcionales para ser contestadas.	[20]

3.8.6. Desempeño

Tabla 3.12: Sub-heurísticas para desempeño.

Sub-heurística	**Descripción**	**Fuente(s)**
¿El proceso de computo en el método de autenticación es imperceptible por el usuario?	Las instrucciones a realizar el método de autenticación empleado, debe realizarlo en el menor tiempo posible.	[127] [128]
En un sistema de autenticación por biométrica, ¿los algoritmos usados presentan un buen desempeño en tiempo de ejecución?	Debido a la gran cantidad de datos para autenticación biométrica, los algoritmos usados deben presentar alto desempeño.	[127]

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Fuente(s)**
Para reducir el tiempo de cifrado en el proceso de autenticación, ¿el sistema adopta una tarjeta inteligente de alto rendimiento?	El microprocesador de la tarjeta esta diseñado para tareas especificas, esto permite mejorar el rendimiento del proceso.	[127]
¿El proceso de autenticación biométrica posee memoria extra para evitar retrasos de ejecución de las instrucciones?	Como consecuencia de la cantidad de datos en este tipo de proceso, es necesario memoria extra.	[127]
Para un mayor nivel de seguridad, ¿el sistema emplea tecnología múltiple (contacto e inalábrico) junto a métodos biométricos para aplicaciones de acceso?	Se emplean tarjetas que incluyan chip de contacto e identificación por radiofrecuencia (e.g. RFID) junto con métodos biométricos.	[127]
¿Las políticas de contraseñas son estrictas y fáciles de usar?	Las políticas para generar contraseñas son seguras y la carga de trabajo cognitivo de los usuarios es mínimo.	[127]
En un escenario de reautenticación, ¿el sistema integra las medidas de seguridad pertinente?	En los cierres de sesión automáticos, el sistema informa que la sesión se ha cerrado y es necesario autenticarse de nuevo para acceder al sistema.	[127]
¿La información sensitiva asociada a la identificación del usuario es mínima?	Básicamente, la identificación del usuario puede ser realizado a partir de un nombre de usuario apropiado (user name) o un correo electrónico (e-mail).	[127]
¿El sistema evita el uso de "cookie informático" para métodos de autenticación?	Almacenar credenciales del usuario puede afectar la seguridad para quien accede al sistema.	[127, 135]
¿El método de autenticación posee interoperabilidad entre servicios?	El método de autenticación debe proporcionar que dos o más sistemas o componentes puedan intercambiar información de los usuarios (e.g. uso en e-commerce).	[127]
¿El sistema proporciona etiquetas de texto que proporcionan consejos para generar contraseñas?	Junto al campo de contraseña, aparece un recordatorio en forma de enlace (e.g. ¿Qué es una contraseña valida?), sobre políticas de contraseña.	[127]

Capítulo 4

Revisión Heurística del Proceso de Desarrollo

En este capítulo se discutirán las revisiones realizadas por los expertos, quienes utilizaron una herramienta de validación para revisar los principios de seguridad usable y autenticación obtenidos en el Capítulo 3. Además, se establecieron algunos criterios de revisión. Para realizar esta revisión, una serie de actividades se tuvieron en cuenta; planeación, ejecución y análisis de resultados. Esto con el fin de tener un orden establecido para tal revisión. En la Figura 4.1 se presenta el esquema general del contenido que se presentará en este capítulo.

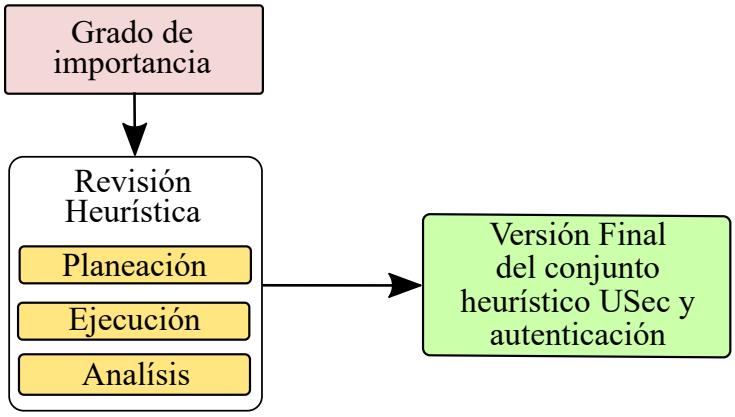


Figura 4.1: Estructura del Capítulo 4 (creación propia).

4.1. Grado de Importancia

Masip [63] afirma que el presupuesto y el tiempo para realizar una evaluación heurística para una aplicación determinada son factores importantes que deben ser considerados estrictamente en las empresas. Por lo tanto, el ajuste presupuestario es una regla ineludible que los directores de proyectos deben aplicar. Además, nuevos requisitos cuando el producto ya está desarrollado, retrasos en las tareas del proyecto o las limitaciones tecnológicas

causan el aumento del tiempo necesario para terminar el producto y, en consecuencia, el aumento del presupuesto inicial.

Teniendo en cuenta estos factores y con el fin de que la evaluación heurística no tenga costos muy elevados y el tiempo de la evaluación no se incremente a medida de que se haga tal revisión (cuando sea necesaria), se propone un grado de importancia para los principios de seguridad usable.

Existen trabajos científicos donde se llevan a cabo este tipo de grado o niveles de importancia. Masip [63] clasifica las heuristicas de experiencia de usuario en tres niveles de importancia: esenciales (U), necesarias (UU) y recomendables (UUU). Leavitt & Shneiderman [123] clasifican principios a través de la *importancia relativa* y la *fuerza de la Evidencia* para el éxito de un sitio web usando una escala de tipo Likert (1-5).

Uno de los objetivos de esta clasificación a través del grado de importancia es identificar un conjunto heurístico útil y preciso con el fin de considerar las restricciones de tiempo. Siguiendo el ejemplo de la clasificación heurística presentado por Masip [63] y de los niveles de conformidad para la accesibilidad[1], en esta propuesta son presentadas tres grados de importancia **S**, **SS** y **SSS** definidas para las sub-heurísticas de USec.

Las sub-heurísticas pertenecientes al grado **S** son vitales para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada. Las sub-heurísticas del grado **SS** son importantes para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada y finalmente son recomendables las sub-heurísticas de grado **SSS** para asegurar que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada. En la Tabla 4.1 se resume lo anteriormente expuesto.

Tabla 4.1: Grado de importancia

Nivel	Descripción
S	Las sub-heurísticas de grado **S** son **vitales** para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.
SS	Las sub-heurísticas de grado **SS** son **importantes** para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.
SSS	Es **recomendable** considerar las sub-heurísticas de grado **SSS** para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.

Para terminar es importante tener en cuenta que debido a que en este trabajo de inves-

[1]Disponible en: http://www.w3.org/TR/WAI-WEBCONTENT/. Consultado en Septiembre de 2015

tigación se está teniendo en cuenta los aspectos de usabilidad y seguridad, se escogió la letra **S** para hacer referencia a la seguridad, no quiere decir que es el único atributo a tener en cuenta, sino, para diferenciarlo de otros trabajos tal como el propuesto por [63] donde escoge la letra **U** para el grado de importancia haciendo referencia a la experiencia de usuario (UX).

4.2. Revisión Heurística

Para realizar esta revisión se tuvo en cuenta una serie de actividades propuestas por Solano [51] para realizar una revisión y análisis de forma ordenada. A continuación se presenta las actividades para tal revisión. Estas actividades se basan en las etapas presentadas en en la Sección 3.3.2 donde se presenta la revisión heurística por parte de los expertos.

Los participantes del proceso de revisión son los siguientes:

Representante de la organización: para esta evaluación César Alberto Collazos de la Universidad del Cauca (Colombia) y Toni Granollers de la Universidad de Lleida (España) asume el rol de representante con el fin de establecer contactos con los expertos que podrían realizar la revisión.

Coordinador: Paulo Cesar Realpe de la Universidad del Cauca (Colombia), es la persona que realizará y enviará el material adecuado a los expertos. Además, es la persona responsable del respectivo análisis de resultados.

4.2.1. Etapa de Planeación

A continuación es presentado las actividades que conforman la etapa de planeación.

4.2.1.1. Actividad 1: Identificar los posibles expertos para participar en la revisión.

Entregable: Lista de posibles expertos a participar en la revisión de USec y autenticación.

A partir de recomendaciones de investigadores, los representantes de la organización identificaron un conjunto de posibles expertos para que participaran en la revisión heurística. Estos expertos son socios de la Asociación Interacción Persona-Ordenador (AIPO)[2]. Luego de enviarles una invitación mediante correo electrónico (ver Anexo B), fueron considerados aquellas personas que tuvieran disponibilidad, experiencia en realizar evaluaciones heurísticas y tener conocimiento en seguridad, usabilidad y ambas.

[2]Disponible en: www.aipo.es

4.2.1.2. Actividad 2: Seleccionar los expertos que van a participar en la revisión.

Entregable: Lista de evaluadores a participar en la revisión.

Después de un tiempo prudente, 8 expertos de la AIPO respondieron a la invitación y 2 expertos y profesores en temas de seguridad de la Universidad del Cauca también respondieron a la invitación.

4.2.1.3. Actividad 3: Identificar el conjunto de heurísticas para la revisión.

Entregable: Lista de heurísticas a utilizar para la revisión.

Después de realizar todo el proceso descrito en el Capítulo 3 se obtuvieron un total de 152 sub-heurísticas. Todas estas son parte de la revisión que será entregada a los expertos.

4.2.1.4. Actividad 4: Desarrollar la herramienta para la revisión.

Entregable: Lista de heurísticas a utilizar en la evaluación.

La herramienta para la revisión fue diseñada en MS Excel el cual esta compuesta por 8 hojas (o secciones). Entre estas se incluyen: perfil del experto, sub-heurísticas para usabilidad, seguridad, accesibilidad, operabilidad, fiabilidad, desempeño y una hoja final para comentarios generales. En la Figura 4.2 se presenta un ejemplo de la herramienta desarrollada en MS Excel para la revisión.

	A	B	C	D	E	F
1	**1. USABILIDAD**					
2	**1.1 Visibilidad del Estado del Sistema**					
3	**Sub-Heurística**	**Descripción**	**Categorización**	**Grado**	**Comentarios**	
4	¿Es posible saber si el sistema es seguro?	Se debe visualizar herramientas que permitan identificar si una aplicación posee seguridad.				
5	¿El usuario puede identificar el nivel de seguridad del sistema y tomar las acciones pertinentes, si es necesario?	El nivel de seguridad del sistema puede ser identificado a partir de indicadores visuales (e.g. mediante colores).				
6	¿El usuario comprende el significado del nivel de seguridad que se presenta en la interfaz?	A partir de la caracteristica del indicador, el usuario puede comprender el nivel de seguridad de la aplicación.				
7	¿Se ha utilizado el color específicamente para llamar la atención e indicar los cambios relacionados con la seguridad?	El tipo de color presentado puede indicar cambio del nivel de seguridad o riesgo del sistema.				
8	Si hay retrasos observables en el tiempo de respuesta del sistema a una acción relacionada con la seguridad, ¿está el usuario informado de los avances del sistema?	Usualmente, un indicador de progreso podria visualizar el estado del sistema.				
9	Después de que el usuario complete una acción de seguridad, ¿la realimentación indica que el siguiente grupo de acciones puede ser iniciada?	A partir de mensajes que visualicen el inicio para el desarrollo de acciones posteriores (e.g. el sistema presenta un mensaje de "inicio de sesión").				
10	¿Hay alguna forma de realimentación para cada acción relacionada con la seguridad?	Diferentes sistemas y niveles de seguridad deben ser visualizado de acuerdo al riesgo.				

Figura 4.2: Herramienta de MS Excel para la revisión heurística.

4.2.1.5. Actividad 5: Proveer a los expertos información general a través de un documento guía

Entregable: Documento guía donde se detalla la información para la revisión.

En esta actividad, el coordinador proporcionó a los expertos un documento guía donde se presenta una descripción de los atributos a revisar, el grado de importancia sub-heurístico y la categorización que permite determinar si cada sub-heurística representa o hace parte del atributo o heurística en el caso de la usabilidad. En el caso de la categorización, se uso la escala de Likert de 1 a 5 donde (1) es "Muy en desacuerdo" y (5) es "Muy de acuerdo". Este documento guía puede verse en el Anexo C.

4.2.1.6. Actividad 6: Solucionar preguntas de los expertos

Entregable: Esta actividad no tiene un entregable asociado.

En esta actividad el coordinador de la revisión solucionó preguntas de los expertos relacionadas a la información proporcionada en la Actividad 5. Durante la realización de esta actividad fue utilizado el correo electrónico para el intercambio de información.

4.2.2. Etapa de Ejecución

A continuación son presentadas las actividades que hacen parte de la etapa de ejecución.

4.2.2.1. Actividad 7: Información de Perfil

Entregable: Se presenta la información del perfil para cada experto.

Como se mencionó en la Actividad 2, 10 expertos en total respondieron a la invitación. En la Tabla 4.2 es presentado el perfil de cada experto. Como puede observarse, los expertos tienen experiencia en usabilidad, seguridad o ambos. La mayoría de ellos tienen estudios doctorales o en curso. Por razones de confidencialidad, la identificación de los expertos no es revelada.

Tabla 4.2: Expertos participantes de la revisión heurística.

Experto	Profesión	Estudios	Área de interés
Experto 1	Profesor	PhD	Seguridad y Usabiliad
Experto 2	Profesor	PhD	Usabilidad, UX
Experto 3	Profesor	PhD(c)	Usabilidad, UX
Experto 4	Profesor	PhD	Usabilidad, UX
Experto 5	Profesor	PhD(c)	Seguridad y Usabilidad
Experto 6	Profesor	Maestría	Seguridad
Experto 7	Profesor	PhD	E-Learning, HCI
Experto 8	Profesor	Maestría	Seguridad
Experto 9	Ingeniero	Universitario	Usabilidad, UX
Experto 10	Profesor	PhD	Usabilidad, UX

4.2.2.2. Actividad 8: Revisión individual del conjunto

Entregable: Plantilla diligenciada por cada experto con los datos de catergorización y nivel de importancia.

En esta actividad el experto revisa una a una las sub-heuristícas según su criterio y conocimiento. Ademas, el coordinador de la revisión le indica al experto que solo debe tener en cuenta el nivel de categorización y de importancia para cada sub-heurística especificado en el documento guía. Además, el coordinador indica que existe un espacio en la parte derecha de cada sub-heurística donde el experto puede realizar un comentario si lo desea. Al finalizar la revisión de todas y cada una de las sub-heurísticas, el experto puede realizar un comentario general de la revisión.

4.2.2.3. Actividad 9: Calificación individual de las sub-heuristicas y comentarios

Entregable: Calificación sub-heurístico con base en su categorización e importancia.

En esta actividad cada experto asigna un valor numérico entero entre 1 y 5 para la catergorización y un nivel de importancia (S, SS o SSS) para cada sub-heurística. Para realizar todo este proceso el experto incluye estos datos en el archivo MS Excel que fue entregado durante la actividad 4.

Uno de los propósitos de la calificación de categorización consiste en determinar si la subheuristica en cuestión puede ser eliminada o mantenida del conjunto final heurístico. Para determinar si se mantiene una sub-heurística se hace uso de una fórmula de ponderación el cual se dará con más detalle en la etapa de análisis de resultados. Para mantener una sub-heurística, el promedio de las respuestas de los expertos debe inferir que es una muy importante para el conjunto.

4.2.3. Etapa de Análisis de resultados

A continuación es presentado el proceso y resultados obtenidos en cada una de las actividades que conforman la etapa de análisis de resultados.

4.2.3.1. Actividad 10: Promediar la categorización heurística por parte de los expertos.

Entregable: Promedios de las categorizaciones asignadas por los evaluadores expertos.

El propósito de esta actividad es promediar la categorización proporcionada por los expertos. La categorización determina si la sub-heurística se mantiene en el atributo actual o es trasladado a otro. En la Tabla 4.3 es presentado la categorización propuesta (tipo Likert) y tenida en cuenta para los expertos.

Tabla 4.3: Categorización

Nivel	Descripción
1	Muy en desacuerdo
2	En desacuerdo
3	Neutral
4	De acuerdo
5	Muy de acuerdo

Debido a que los expertos tienen diferentes áreas de conocimiento e investigación, y por recomendación en un matemático experto en estadística, se decidió dar diferentes pesos a cada experto de acuerdo a su área.

Para lograr lo anterior, primero se estableció tres lineas de investigación, usabilidad, seguridad y seguridad usable (donde se encuentran investigadores que dominan los dos atributos). Para la parte de usabilidad también se encuentran los expertos en HCI y UX. A los expertos que dominan los dos atributos; usabilidad y seguridad, se les dio un peso mas alto, de 15 %, y para los expertos con áreas separadas tienen un peso mas bajo, de 7.5 % para cada uno. Como podemos observar, los expertos que dominan las áreas de seguridad y usabilidad, poseen un peso casi el doble de los otros expertos con una sola área de conocimiento. Lo anterior se realizó con el fin de ser lo más coherentemente posible. En la Tabla 4.4 se resume este concepto.

Tabla 4.4: Peso por área de conocimiento.

Area de conocimiento	Peso
Usabilidad	8.75 %
Seguridad	8.75 %
Usabilidad y Seguridad	15 %

Con el fin de demostrar que la suma total es la unidad o el 100 %. Se establece la siguiente relación: debido a que existen 10 expertos de los cuales 2 abarcan seguridad y usabilidad, y el resto es decir 8 expertos tienen conocimiento en usabilidad o seguridad entonces:

$$2 * (0{,}15) + 8 * (0{,}085) = 1 \tag{4.1}$$

Para obtener un promedio adecuado se hizo necesario aplicar la media ponderada. Esta es una medida de tendencia central, que es apropiada cuando en un conjunto de datos cada uno de ellos tiene una importancia relativa (o peso) respecto de los demás datos. Se obtiene multiplicando cada uno de los datos por su ponderación (peso) para luego sumarlos, obteniendo así una suma ponderada; después se divide esta entre la suma de los pesos (que en este caso la suma es 1, ver Ecuación 4.1), dando como resultado la media ponderada.

$$\overline{x} = \sum_{n=1}^{10} x_i * P(x_i) \tag{4.2}$$

Donde x_i representa la sub-heurística y $P(x_i)$ corresponde al peso del experto que evalúa la sub-heurística en particular.

Debido a la cantidad de sub-heurísticas (152 en total), presentar los resultados de la categorización para cada sub-heurística abarcaría mucho espacio en el documento. Por lo tanto y con base en los pesos, se presenta en la Tabla 4.5 los resultados ponderados y la cantidad de sub-heurísticas que pertenecen a la categorización en cuestión para cada heurística.

Tabla 4.5: Categorización para Usabilidad

Heurística	**1**	**2**	**3**	**4**	**5**
Visibilidad del estado del sistema	-	1	-	7	3
Estética y mínimo diseño	-	-	-	3	1
Control y libertad del usuario	-	-	1	2	4
Utilización del lenguaje del usuario	-	1	-	2	3
Minimizar carga de memoria	-	1	2	6	2
Reconocer, diagnosticar y recuperarse de errores	-	-	-	3	2
Flexibilidad y eficiencia de uso	-	-	2	5	1
Prevención de errores	-	-	-	1	2
Consistencia y estándares	-	-	1	5	-
Ayuda y documentación	-	-	-	4	2
Transmitir características	-	-	-	6	1
TOTAL	0	3	6	44	21

A partir de la Tabla 4.5 los expertos calificaron a 21 sub-heurísticas como "Muy de acuerdo", 44 sub-heurísticas como "De acuerdo", 6 como "Neutral" y 3 sub-heurísticas como "En desacuerdo" para el atributo de usabilidad.

Según los resultados de la Tabla 4.5, existe una mayor distribución para la categorización de *Totalmente de Acuerdo* y *De acuerdo* para las sub-heurísticas de usabilidad. Sin embargo, esto no significa estas sub-heurísticas de usabilidad se mantenga dentro del conjunto propuesto ya que también se tienen en cuenta los comentarios de los expertos.

Igualmente, en la Tabla 4.5 se presenta los resultados de la categorización para los demás atributos: seguridad, accesibilidad, operabilidad, fiabilidad y desempeño. En este caso existe una mayor proporción de aceptación por parte de los expertos en la categorización de las sub-heurísticas de los atributos en cuestión. En la Figura 4.3 es presentado la relación gráfica de categorización para todos los atributos de acuerdo con las Tablas 4.5 y 4.6. Según Figura 4.3, existe una alta tendencia de aceptación por parte de los expertos de

Tabla 4.6: Categorización para Atributos

Atributo	**1**	**2**	**3**	**4**	**5**
Seguridad	-	-	1	11	17
Accesibilidad	-	-	-	6	3
Operabilidad	-	-	-	1	7
Fiabilidad	-	-	1	7	4
Desempeño	-	-	-	7	3
TOTAL	0	0	2	32	34

ubicar las sub-heurísticas donde inicialmente se propusieron.

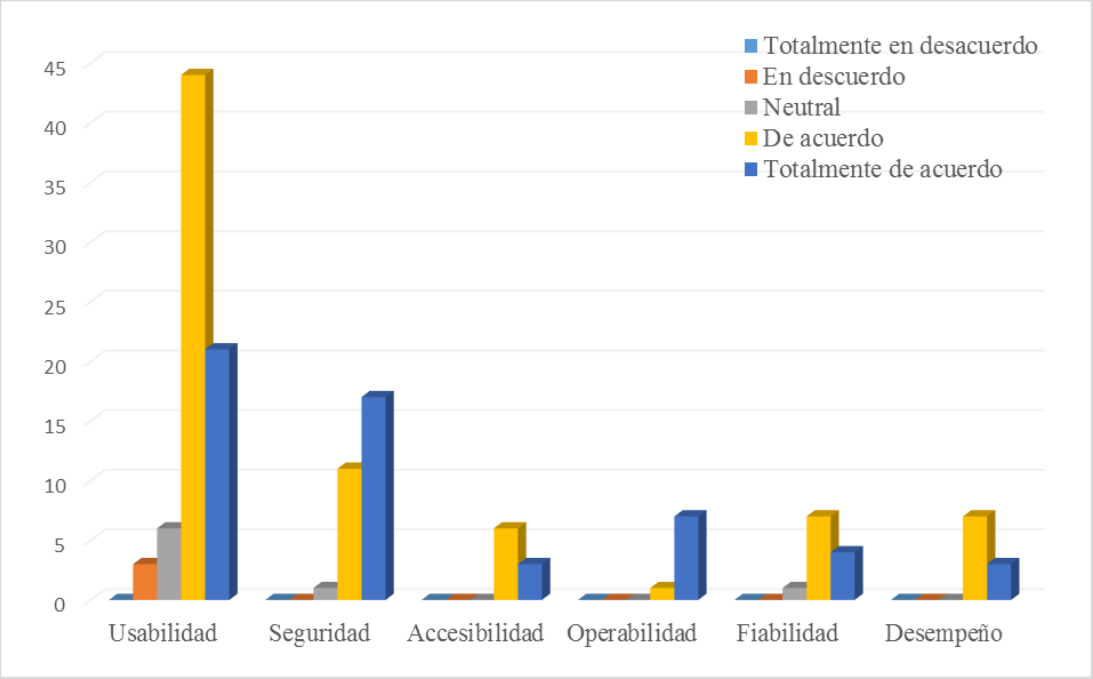


Figura 4.3: Categorización para todos los atributos.

4.2.3.2. Actividad 11: Promediar la nivel de importancia heurística por parte de los expertos.

Entregable: Promedios de los niveles de importancia asignadas por los evaluadores expertos.

El propósito de esta actividad es promediar el nivel de importancia proporcionada por los expertos para cada sub-heurística teniendo en cuenta la Tabla 4.1. Igual que en la actividad anterior, debido a que los expertos tienen diferentes áreas de conocimiento e investigación, y por recomendación de matemáticos expertos en estadística, se decidió también tener

diferentes pesos de acuerdo a estas áreas.

Para lograr lo anterior, primero se estableció igualmente tres lineas de investigación: usabilidad, seguridad y seguridad usable (donde se encuentran investigadores que dominan la usabilidad y seguridad). Para la parte de usabilidad también se encuentran los expertos en HCI y UX. A los expertos que tienen conocimiento en usabilidad y seguridad, se les dio un peso de 15 % y para los expertos con áreas separadas tienen un peso de 8.75 % cada uno. Nuevamente en la Tabla 4.4 se resume este concepto.

En el formato MS Excel que se entregó a los expertos, en la casilla de grado de importancia aparecen 4 opciones: S, SS, SSS o Ninguno. Para la opción de ninguno, el experto considera que la sub-heurística no tiene ningún nivel de importancia y considera que debe de ser eliminada del conjunto propuesto. Debido a que las opciones son expresadas cualitativamente, es necesario proponer un nivel cuantitativo para este grado de importancia con el fin de hacer uso de la Ecuación 4.2 y obtener su respectivo promedio ponderado. La Tabla 4.7 se presenta la asignación cuantitativa para cada grado de importancia.

Tabla 4.7: Valor cuantitativo para el grado de importancia

Grado	Valor cuantitativo
S	1
SS	2
SSS	3
Ninguno	4

Igualmente, debido a la cantidad de sub-heurísticas (152 en total), presentar los resultados del grado de importancia para cada sub-heurística abarcaría mucho espacio en el documento. Por lo tanto y con base en los pesos, se presenta en la Tabla 4.8 los resultados del promedio ponderado y la cantidad de sub-heurísticas que pertenecen a la importancia en cuestión para la usabilidad.

Los resultados de la Tabla 4.8 indica que la mayoría de las sub-heurísticas propuestas presentan un grado de importancia destacado. Por lo tanto, en una evaluación de seguridad usable donde el atributo de usabilidad esté presente, considerar estas sub-heuristicas S y SS es relevante, y permite el diseño de buenas interfaces. Lo anterior indica la importancia de las heurísticas de Nielsen aplicadas al contexto de la seguriad usable.

Igualmente, en la Tabla 4.9 se presenta los resultados del grado de importancia para los demás atributos: seguridad, accesibilidad, operabilidad, fiabilidad y desempeño. En este caso también existe una mayor proporción de grado de importancia de las sub-heurísticas en los atributos en cuestión.

En la Figura 4.4 es presentado la relación gráfica de grado de importancia para todos los

Tabla 4.8: Grado de importancia para Usabilidad

Heurística	S	SS	SSS
Visibilidad del estado del sistema	5	4	2
Estética y mínimo diseño	1	3	-
Control y libertad del usuario	4	2	1
Utilización del lenguaje del usuario	4	2	-
Minimizar carga de memoria	-	6	5
Reconocer, diagnosticar y recuperarse de errores	2	2	1
Flexibilidad y eficiencia de uso	-	7	1
Prevención de errores	3	-	-
Consistencia y estándares	2	4	-
Ayuda y documentación	2	4	-
Transmitir características	5	2	-
TOTAL	28	42	10

Tabla 4.9: Grado de importancia para Atributos

Atributo	S	SS	SSS
Seguridad	17	11	1
Accesibilidad	2	7	-
Operabilidad	1	3	4
Fiabilidad	5	3	4
Desempeño	5	5	-
TOTAL	30	29	9

atributos de acuerdo con las Tablas 4.8 y 4.9. Como podemos ver en Figura 4.4, el atributo de usabilidad y seguridad tienen un número de sub-heurísticas con grado de importancia mayor sobre los demás atributos. Esto hace a la usabilidad y seguridad muy importantes para aplicaciones donde estos dos atributos estén presentes.

Discusión

A partir de los resultados presentados anteriormente y con base en la categorización y el grado de importancia para cada sub-heurística, podemos afirmar que los resultados de la revisión por parte de los expertos es satisfactoria. Esto indica que la propuesta presentada en la Sección 3.5 donde se incluyen diferentes metodologías para el desarrollo heurístico, es apropiado con el fin de obtener principios de diseño para seguridad usable y autenticación de usuario. Lo anterior representa un gran aporte debido a que se podría usar este mismo proceso para obtener principios para otras áreas incluyendo también su respectivo grado de importancia, por ejemplo la privacidad usable que todavía no ha sido estudiada en profundidad.

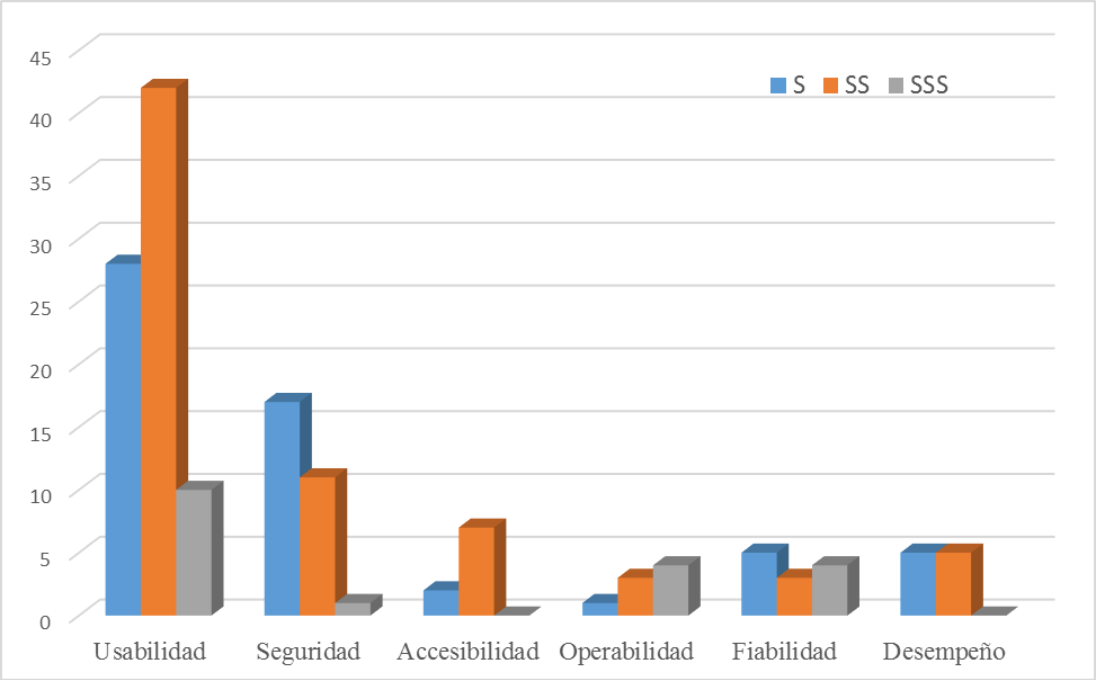


Figura 4.4: Grado de importancia para todos los atributos.

Con base en estos resultados, es posible también afirmar que este proceso de desarrollo puede tambien ser aplicado a algunas aplicaciones especificas con el fin de obtener principios de diseño. Algunas de estas aplicaciones pueden ser para administración pública, comunicación, educación, entornos colaborativos, entretenimiento, servicios interactivos basados en imágenes o correo electronico [141]. Con el propósito de obtener principios de diseño para las aplicaciones anteriormente mencionadas utilizando el proceso de desarrollo heurístico propuesto, una exhaustiva investigación debe llevarse a cabo.

4.2.3.3. Actividad 12: Análisis cualitativo de la revisión

En esta sección se analiza algunos comentarios realizados parte de los expertos a las sub-heurísticas. A partir de estos comentarios y los resultados anteriores (categorización y grado de importancia), se identifican las mejoras y posibles ubicaciones alternas (si es el caso) para las sub-heurísticas propuestas.

Con base en estos comentarios, los expertos dieron su opinión sobre la claridad del conjunto de elementos y también sugieren información adicional que debería haber sido considerada. El objetivo de esta actividad es obtener un consenso entre los expertos para asegurar que la sub-heurística sea lo mas precisa posible. Sin embargo, como los expertos vienen de diferentes áreas del conocimiento científico (usabilidad, seguridad y seguridad usable) este consenso puede ser todo un reto porque a veces, los expertos de diferentes campos del saber humano pueden ofrecer opiniones contradictorias.

Para solventar el problema anterior, igual que en los casos anteriores se da prioridad a los comentarios de los expertos que involucren el campo de la seguridad usable (usabilidad y seguridad). Aunque no es el mejor de los escenarios para solventar esta dificultad, sin embargo, son ellos los que han trabajado ampliamente en el área de la seguridad usable y conocen más a fondo este campo de investigación.

Una de las características que los expertos tienen en cuenta es la claridad de la redacción tanto de la sub-heurística como su descripción. Esta claridad para cada sub-heurística debe de ser clara y fácil de entender, o si se requiere hacer cambios en esta con el fin de que sea lo más comprensible posible para los evaluadores a la hora de analizar una aplicación real.

Por restricción de extensión del documento no se presentan todos los comentarios proporcionados por los expertos para cada sub-heurística en esta sección, sino hemos considerado incluir los comentarios donde los expertos justifican eliminar las sub-heurísticas del conjunto parcial propuesto por alguna u otra razón. La Tabla 4.10 presenta los comentarios de los expertos para las sub-heurísticas eliminadas.

Tabla 4.10: Comentarios de los expertos de las sub-heurísticas eliminadas.

Sub-heurística	**Comentarios**
1. Usabilidad	
Control y libertad del usuario – ¿Los usuarios pueden cancelar las operaciones de seguridad en curso?	*Es lo mismo que la anterior, revertir incluye la cancelación – Que la acción sea cancelable o no, dependerá de la acción en sí y de su compromiso con la integridad del sistema.*
Reconocer, diagnosticar y recuperarse de errores – ¿Los mensajes de error relacionados con la seguridad indican la acción que el usuario debe tomar para corregir el error?	*Esta, no es lo mismo que la primera de este bloque? – No se le debe dar al usuario información técnica del error.*
Prevención de errores – ¿El sistema permite a los usuarios confirmar acciones de seguridad que pueda tener consecuencias severas?	*Esta es semejante a la última de este bloque.*

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Comentarios de expertos**
Prevención de errores – ¿Las funciones importantes que pueden causar resultados serios de seguridad, ¿están ubicados en lugares difíciles de alcanzar?	*Una función puede ser importante o no y causar problemas serios o no, no deben ser accesibles por nadie. – La dificultad en hallar una función por sí solo no compromete la seguridad. Sí que la compromete que el usuario desconozca la amenaza. Hay que facilitar la formación del modelo mental del sistema de seguridad en el usuario.*
Consistencia y estándares – ¿Los títulos de las opciones de seguridad están centrados o justificados a la izquierda?	*Y esto por qué?, no le veo utilidad a este sub-heurístico*
2. Seguridad	
¿El sistema notifica al usuario sobre actualizaciones de seguridad y permite decidir que elementos serán instalados?	*Lo importante es sentirse seguro, independientemente de si se instalan más o menos actualizaciones. – Prefiero sistemas que avisen de que van a instalar y no que instalen y luego avisen.*
¿El sistema emplea mecanismos criptográficos para evitar la divulgación no autorizada durante el proceso de transmisión de información?	*No está repetida?, creo que esta es la 6 de este bloque.*
¿La interfaz tiene derechos de autor (copyright)?	*Debe cumplir las leyes de privacidad, pero no implica que deba tener derechos de autor. Se están mezclando conceptos de privacidad y propiedad intelectual – No le veo importancia a este item.*
Si es necesario realizar autenticación por multi-factor, ¿el uso de PIN es implementada, dándole libertad al usuario para decidir el numero de dígitos?	*El PIN es fácil de usar, recordar y hackear, por eso existen gran cantidad de "buenas prácticas"que aconsejan no usar PIN. – Autenticación multi-factor? Estos sistemas no serán atractivos para los usuarios y dejarán de usarlos aunque sean mas seguros.*
3. Fiabilidad	
¿El sistema notifica al usuario sobre el procedimiento a seguir en el caso de suplantación o pérdida de información personal?	*En mi opinión esta sobra, por estar incluída en la anterior, pues una suplantación o pérdida es un incidente.*

Como podemos ver en la Tabla 4.10, muchas de las sub-heurísticas se eliminan por ser iguales a otras, sin embargo, en otros casos los expertos no le ven utilidad en estas sub-

heurísticas y sugieren eliminarlas.

Debido a que presentar todas los comentarios generaría mucho espacio en el documento, en lugar de ello, en la Tabla 4.11 es presentado los resultados donde se describe la cantidad de modificaciones que se hicieron en las sub-heurísticas y en las descripciones para la usabilidad. Además, se presenta la cantidad de sub-heurísticas eliminadas y el número de sub-heurísticas que cambiaron de lugar, es decir, su ubicación a otras heurísticas o atributos.

Tabla 4.11: Resumen con base en los comentarios de los expertos para Usabilidad.

Heurística	**Cambios Sub-heuristica**	**Cambios Comentarios**	**Sub-heuristicas eliminadas**	**Cambio de lugar**
Visibilidad del estado del sistema	1	6	-	-
Estética y mínimo diseño	-	-	-	2
Control y libertad del usuario	-	2	1	-
Utilización del lenguaje del usuario	-	-	-	-
Minimizar carga de memoria	3	2	-	1
Reconocer, diagnosticar y recuperarse de errores	2	2	1	-
Flexibilidad y eficiencia de uso	-	2	-	-
Prevención de errores	-	-	2	-
Consistencia y estándares	-	1	1	-
Ayuda y documentación	1	1	-	-
Transmitir características	1	2	-	-
TOTAL	**8**	**18**	**5**	**3**

A partir de la Tabla 4.11 surge la siguiente pregunta, ¿Cuál es la variación en porcentaje entre el total de cambios efecutados y el total de sub-heurísticas para el atributo de usabilidad?. Según los datos anteriores, el 11.11 % de las sub-heurísticas fueron modificadas, el 25 % de los comentarios fueron cambiados, el 6.9 % de las sub-heurísticas fueron eliminadas y tal solo el 4 % cambiaron de lugar. Estos resultados son alentadores debido a que pocas sub-heurísticas fueron modificadas, ubicadas o eliminadas, lo anterior ratifica lo que hemos comentado anteriormente cuando se hizo el análisis de categorización y grado de importancia, el proceso de desarrollo heurístico propuesto es válido para obtener principios de diseño con un alto grado de satisfacción.

Adicionalmente, en la Tabla 4.12 es presentado un resumen donde se describe la cantidad de modificaciones que se hicieron en las sub-heurísticas y en las descripciones para los atributos de seguridad, accesibilidad, operabilidad, fiabilidad y desempeño. Además, se presenta la cantidad de sub-heurísticas eliminadas y el número de sub-heurísticas que cambiaron de lugar, es decir, su ubicación a otras heurísticas o atributos.

A partir de la Tabla 4.12 surge la siguiente pregunta, ¿Cuál es la variación en porcentaje entre el total de cambios efecutados y el total de sub-heurísticas para cada atributo?. Según los datos anteriores, El 18.18 % de las sub-heurísticas fueron modificadas, el 32.4 % de los comentarios fueron cambiados, el 6.4 % de las sub-heurísticas fueron eliminadas y tal solo el 6.4 % cambiaron de lugar.

Tabla 4.12: Resumen con base en los comentarios de los expertos para los atributos.

Atributo	Cambios Sub-heuristica	Cambios Comenarios	Sub-heuristicas eliminadas	Cambio de lugar
Seguridad	3	16	4	1
Accesibilidad	1	2	-	1
Operabilidad	2	2	-	1
Fiabilidad	3	4	1	2
Desempeño	5	1	-	-
TOTAL	**14**	**25**	**5**	**5**

Según vemos en la Tabla 4.12, los resultados son ligeramente superiores a los obtenidos para el caso de la usabilidad. Creemos que esto se debe al enfoque de los atributos, este enfoque esta directamente relacionado con seguridad y autenticación de usuario. Es posible que varios expertos no tengan dominio para hacer una revisión exhaustiva llevando con esto confusión y generando comentarios contradictorios.

Para terminar con esta actividad, a continuación se presenta algunos comentarios generales por parte de los expertos junto al área de investigación que dominan.

1. **Experto 1 (USec):**
   a) *Preguntar si se distingue y se comprenden todas las partes un aviso de privacidad en general.*
   b) *Preguntar si se aprecia el impacto del uso de los datos personales por terceros.*
   c) *Para el tema de no repudio, tal vez preguntar directamente si se distingue un elemento que hagan claras las consecuencias de que el usuario que entra al sistema es el responsable de todas las acciones.*
   d) *También sería bueno preguntar sobre realimentación que hace el sistema al usuario relativo a diferentes niveles de seguridad (a nivel de usuario o a nivel de sistema).*

2. **Experto 2 (Usabilidad):** *Después de ver estas dos primeras pestañas (usabilidad y seguridad) tengo la sensación de cierto desconcierto, pues creo que muchas de las preguntas que he visto antes debería estar aquí (seguridad). Si trabajas la seguridad usable y tienes dos atributos (usabilidad y seguridad), ¿por qué mezclas conceptos dentro?. Sigo pensando que cada aspecto en su sitio seria mejor y analizar la USec seria tomar la unión de los dos conjuntos.*

3. **Experto 3 (USec)**: *¿No existe una forma más amena de realizar la revisión? Termina haciéndose un poco pesada, ya que son muchísimos puntos.*

4. **Experto 4 (Seguridad)**: *Siendo la seguridad usable y la autenticación de usuarios los elementos a evaluar por parte del instrumento, hubiese sido mejor que la medida*

fuese en términos de riesgo, teniendo en cuenta las amenazas, vulnerabilidades e impacto.

El Experto 1 con conocimiento en seguridad usable, proporciona ciertos requerimientos adicionales para el conjunto propuesto, sin embargo este comentario no se tuvo en cuenta debido a que la cantidad de principios aumentaría considerablemente, generando con esto algún tipo de malestar por parte de expertos para futuras evaluaciones. Para llevar esto a cabo, es necesario plantear metodologías que permitan obtener las sub-heurísticas más importantes de nuestro conjunto para una aplicación en particular, esto puede ser tema de trabajo futuro.

La sugerencia del Experto 4 sí fue tenido en cuenta para nuestro trabajo de investigación, aunque esto no es parte de los objetivos de la presente tesis, es un elemento adicional muy importante ya que el experto insiste en la necesidad de establecer una medida del nivel de riego para seguridad usable y autenticación.

En la Figura 4.13 es presentado el número de sub-heurísticas para cada atributo revisado.

Tabla 4.13: Número de sub-heurísticas por cada Atributo (Creación propia).

Atributo	**Número de sub-heurísticas**
Usabilidad	74
Seguridad	29
Accesibilidad	9
Desempeño	10
Operabilidad	8
Fiabilidad	12
TOTAL	**142**

Con respecto a la usabilidad, en la Tabla 4.14 se presenta el número de sub-heurísticas para cada heurística.

4.3. Discusión

Este capítulo se centra en revisiones que expertos en usabilidad, seguridad y seguridad usable llevaron a cabo con respecto a los principios presentados en el Capítulo 3, para lo cual se proporcionó una herramienta de revisión (MS Excel). La herramienta consta de varias secciones y comprende una plantilla para revisar las sub-heurísticas propuestas para USec y autenticación. A partir de estas revisiones podemos afirmar que el primer objetivo de esta tesis ha sido realizado satisfactoriamente, pues con base en los resultados y comentarios de los expertos, existe una gran posibilidad de que sean aplicados realmente.

Tabla 4.14: Número de sub-heurísticas para usabilidad (Creación propia).

Heurística	**Número de sub-heurísticas**
Visibilidad del estado del sistema	11
Estética y mínimo diseño	4
Control y libertad de usuario	7
Utilización del lenguaje del usuario	6
Minimizar carga de memoria	11
Reconocer, diagnosticar y recuperarse de los errores	5
Flexibilidad y eficiencia de uso	8
Prevención de errores	3
Consistencia y estándares	6
Ayuda y documentación	6
Transmitir características	7
TOTAL	**74**

El conjunto de principios presentado en este trabajo son una herramienta para desarrolladores y evaluadores basada en atributos y características de la norma ISO/IEC 25010:20011 para revisar los aspectos de una aplicación que pueden afectar la seguridad, la usabilidad, entre otros (accesibilidad, operabilidad, fiabilidad y desempeño) que hacen también parte de métodos de autenticación junto con aspectos de seguridad. Es una lista abierta que podría ampliarse agregando más recomendaciones para crear un conjunto mayor y más exhaustivo de principios de diseño. El conjunto es actualizado y adaptado por modificaciones, actualizaciones y adiciones debido a las revisiones realizadas por los expertos.

Es necesario agregar que el conjunto actual de principios tiene algunas limitaciones. Entre estas limitaciones podemos incluir que una u otra sub-heurística puede ser parte de algún otro atributo, pero la realización de este aspecto se sale de los objetivos de la presente investigación. Otra limitación es el número de expertos en seguridad usable, este número es muy reducido (2 expertos), lo ideal sería que la revisión de este conjunto sea analizado por más personas que dominen este campo, sin embargo, encontrar este tipo de personas es complicado debido a que esta área de investigación es relativamente nuevo.

Con base en lo anterior, es necesario realizar mejoras debido a lo extenso número de principios del conjunto final. Es posible ampliar este conjunto pero es necesario desarrollar metodologías que permitan obtener qué sub-heurísticas realmente se necesitan para una aplicación en particular. Esta metodología podría ser parte de un trabajo futuro.

4.4. La CaixaBank

Uno de los expertos que realizó la revisión pertenece al grupo de usabilidad de la página web de la CaixaBank[3], uno de los bancos más importantes de España.

Después de finalizar la revisión, el experto escribió: "*Estoy especialmente interesado en su tesis por que la confrontación entre seguridad y usabilidad en los procesos de autenticación es habituales en mi entorno de trabajo. Por este motivo, le solicito si, una vez finalizado su estudio, sería posible disponer de los resultados para compartirlos con el grupo responsable de la seguridad informática dentro de mi organización.*

Vemos con esto, la importante contribución que hemos realizado al conocimiento con este conjunto de principios para seguridad usable y autenticación para ser aplicados a situaciones reales. Luego de este comentario por parte del experto, fué posible una reunión en las instalaciones principales del banco (en Barcelona, España) con el experto en usabilidad y el responsable de la seguridad del sitio web de de La CaixaBank. Los dos estuvieron de acuerdo con la relevancia de estos principios para ser aplicados al sitio web con el fin de alcanzar un equilibrio entre seguridad y usablidad que tanta falta hace para los usuarios.

Entre algunas de las recomendaciones más importantes que ellos formularon al finalizar la reunión tenemos las siguientes:

1. "*La evaluación debería ser complementada con una métrica de percepción de seguridad del usuario que ofrece un sitio web de banca electrónica, si la percepción es baja, el usuario no usará la aplicación. Lo anterior puede llevar a pérdida de clientes para el banco*".

2. "*Debería de existir un análisis de seguridad a partir de los principios encontrados, es decir, informar a través de una métrica o un concepto, cuán seguro es la página para realizar transacciones de acuerdo con su interfaz*".

3. "*Analizar la viabilidad de usar diferentes métodos de autenticación teniendo en cuenta el costo, usabilidad, seguridad y confiabilidad ya sea para un sitio web o cajero automático*

4.5. Conjunto Final para USec y Autenticación

Las heurísticas y sub-heurísticas fueron presentadas en en el Capítulo 3 junto con otros atributos de calidad. Basado en la revisión de los expertos, sus comentarios, las modificaciones y mejoras, a continuación es presentado el conjunto final heurístico para USec y autenticación.

[3]Disponible en: https://www.caixabank.es

4.5.1. Usabilidad

Tabla 4.15: Sub-heurísticas para Usabilidad (después de la revisión).

Sub-heurística	**Descripción**	**Grado**
1. Visibilidad del Estado del Sistema		
¿Es posible saber si el sistema es seguro?	Se debe tener herramientas que permita identificar si una aplicacion posee seguridad o que el sistema determine su estado.	S
¿El usuario puede identificar el nivel de seguridad del sistema y tomar las acciones pertinentes, si es necesario?	El nivel de seguridad del sistema puede ser identificado a partir de indicadores visuales (e.g. mediante colores).	S
¿El usuario es capaz de comprender el significado del nivel de seguridad que se presenta en la interfaz?	A partir de la característica del indicador, el usuario es capaz de comprender el nivel de seguridad de la aplicación.	SS
Si hay retrasos observables en el tiempo de respuesta del sistema a una acción relacionada con la seguridad, ¿está el usuario informado de los avances del sistema?	Usualmente, un indicador de progreso podría visualizar el estado del sistema. El indicador debe proporcionar *feedback* que comunique de forma inmediata, clara y unívoca el estado del sistema.	S
Después de que el usuario complete una acción de seguridad, ¿la realimentación indica que el siguiente grupo de acciones puede ser iniciada?	A partir de mensajes que visualicen el inicio para el desarrollo de acciones posteriores (e.g. diseñar un proceso controlado por el sistema que avance paso a paso hasta que se haya completado la seguridad e iniciar, si el proceso de seguridad es satisfactorio, las acciones posteriores).	SS
¿Hay alguna forma de realimentación para cada acción relacionada con la seguridad, cuando sea necesario?	Diferentes sistemas y niveles de seguridad deben ser visualizados de acuerdo al riesgo. Es decir, en caso en que el sistema alcance un estado de no seguridad, debe avisar de forma inmediata al usuario.	S
En las interfaces de alerta, ¿el sistema provee el nombre de las herramientas de seguridad?	Cuando se presenta una interfaz de alerta, el usuario identifica herramientas de seguridad que se están ejecutando (e.g. firewall). Es necesario comprender adecadamente esas herramientas para evitar ataque de terceros.	SS

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿El estado del usuario es visible en el sistema?	A partir de palabras o colores, es posible identificar el estado del usuario (e.g. quién está conectado, que nivel de privilegios tiene, tiempo de espera).	SSS
Al observar el estado de seguridad del sistema, ¿el usuario puede decir las alternativas para las acciones relacionadas con la seguridad, si es necesario?	A partir del nivel de seguridad del sistema, el usuario debe conocer alternativas necesarias con el fin de no poner en riesgo las acciones que se están llevando a cabo.	S
¿El sistema mantiene informado adecuadamente al usuario sobre el estado de conexión del sistema?	La interfaz informa al usuario cuando existen conexiones con entidades que podrían ser no confiables (e.g. se presenta al usuario si el sistema es seguro o no a partir de semáforos).	SS
¿Existen indicadores visuales informando a los usuarios sobre las prácticas de privacidad del sistema?	El sistema puede tener elementos visuales que permitan al usuario conocer políticas de privacidad sobre el uso del sistema	SSS
2. Estética y Mínimo Diseño		
¿La información de seguridad presentada en pantalla es relevante?	Es necesario presentar en pantalla información de seguridad relevante y no aspectos técnicos. Además, información relevante de seguridad visible evita posibles ataques por parte de terceros.	S
¿Los iconos de seguridad son identificables y diferenciables?	Los iconos de seguridad deben ser fácilmente visualizados y distinguibles.	SS
¿Las etiquetas de seguridad son sencillas, fáciles de entender y representativas?	Las etiquetas de seguridad no deben tener términos técnicos abstractos y ser visualizados adecuadamente.	SS
¿La interfaz ayuda al usuario a tener una experiencia segura y satisfactoria con el sistema	La experiencia con las caracteristicas de seguridad tiene que ser agradable y satisfactoria, de lo contrario puede descuidar la seguridad del sistema.	SS
3. Control y Libertad de Usuario		
¿Los usuarios pueden revertir fácilmente sus acciones de seguridad donde sea posible?	El sistema tiene la capacidad de volver al estado anterior fácilmente si el usuario lo desea.	SS
¿Hay una función “desistir o deshacer” para una simple acción o grupo completo de acciones de seguridad?	Una función puede revertir una o varias acciones de seguridad en ejecución.	SSS

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿El sistema esta diseñado de manera que los botones con nombres similares, no desarrollen acciones de seguridad opuesto?	Si los botones tienen etiquetas similares, estos deben cumplir funciones de seguridad adecuado sin ejecutar procedimientos opuestos. Se debe tener cuidado con las etiquetas ya que pueden afectar la usabilidad. Si el sistema tiene botones con nombres similares puede causar un gran problema de entendimiento por parte del usuario.	S
Cuando las indicaciones implican una acción de seguridad necesaria, ¿las palabras del mensaje son coherente con la acción?	Los avisos de seguridad que aparecen en los mensajes desplegados deben coincidir con la acción de seguridad necesaria.	S
¿Las opciones de seguridad en el menú hace evidente si la selección de la opción es posible?	Las opciones del menú son fácilmente seleccionadas. Estas opciones son presentadas dependiendo de la relevancia que cada opción tenga para la seguridad.	SS
¿El usuario es capaz de confirmar cualquier acción que tenga consecuencias drásticas, negativas o destructivas?	En ocasiones, las acciones destructivas no se debe dejar a la elección del usuario. Aunque la mayoría de los usuarios ignoran los mensajes, es necesario que ellos confirmen una acción de seguridad, lo que puede tener consecuencias para su propia seguridad.	S
¿El sistema permite al usuario editar o eliminar información personal incorrecta?	La información personal puede cambiar durante el tiempo o cometer errores cuando son ingresados. Sin embargo, algunos sistemas no permiten esta acción.	S
4. Utilización del Lenguaje del Usuario		
¿Los mensajes de seguridad están nombrados coherentemente en todo sistema?	Los mensajes de seguridad expresados en un lenguaje coherente y adecuado permite al usuario utilizar el sistema con menor riesgo.	S
¿Las sentencias de alerta son simples, cortas y comprensibles?	Toda la información de seguridad que es presentada por el sistema debe ser concisa y sencilla de entender.	S
¿Las preguntas de seguridad son expresadas en un lenguaje claro y sencillo?	Las preguntas de seguridad que permiten mitigar amenazas, son comprensibles por el usuario.	S

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?	Los términos técnicos o avanzados relacionados con el manejo de las políticas de seguridad y privacidad deben ser evitados.	S
¿El sistema evita el uso de palabras diferentes para transmitir la misma idea o concepto?	Usar diferentes palabras para transmitir la misma idea puede confundir a los usuarios, pues esto crea explicaciones incorrectas y generan ambigüedad.	SS
¿Los mensajes de error relacionados con la seguridad son adecuados al lenguaje del usuario?	Los mensajes de error deben tener un lenguaje sencillo que los usuarios puedan entender y tomar decisiones.	SS
5. Minimizar Carga de Memoria		
¿Las tareas de seguridad son fáciles de aprender y recordar?	Es necesario que las operaciones de seguridad realizadas por los usuarios no tengan procedimientos complejos.	SS
¿Existen situaciones predeterminadas de selección de seguridad?	El sistema informa al usuario opciones predeterminadas de selección de seguridad específicas (si existen) durante su interacción. Sin embargo, los usuarios deben ser conscientes de sus valores predeterminados actuales en la interacción con el sistema por primera vez.	SSS
¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	Los elementos de seguridad de los menús en la interfaz son claros para el usuario.	SS
¿La información relacionada con la seguridad es presentada de una manera coherente y estandarizada?	Información coherente y basado en estándares es mas fácil de aprender y recordar. Los usuarios que interactuan con los diferentes sistemas de seguridad requerirían términos estandarizados a través de ellos.	SS
En un proceso de autenticación por conocimiento (e.g. contraseña o PIN), ¿el sistema permite minimizar la carga de memoria para los usuarios?	Cuando se usa contraseña o PIN en un proceso de autenticación, el sistema evita memorizar datos extensos, complicados procedimientos o realizar actividades cognitivas complejas.	SS

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿El sistema permite libertad al usuario para decidir el numero de dígitos del PIN en un proceso de autenticación?	Si el sistema permite libertad al usuario de generar su propio PIN con el numero de dígitos que el quiera, facilita la memorización de claves largas usando algún tipo de nomenclatura. Sin embargo, la mayoría de sistemas actuales permiten claves de 4 dígitos por su facilidad de memorización.	SSS
Si se utiliza el reconocimiento visual para autenticación (e.g. contraseñas gráficas), ¿los usuarios pueden asociar una frase o palabra a una imagen como contraseña?	Una imagen permite al usuario recordar palabras o frases con facilidad. Sin embargo, es necesario asociar una descripcion a cada imagen.	SS
Para PINs de más de 8 caracteres, ¿el sistema hace uso de herramientas nemotécnicas?	La mente humana tiene la posibilidad de recordar fácilmente hasta 8 caracteres, la facilidad de recordar se mejora mediante el uso de herramientas nemotécnias (e.g. Técnica para memorizar un password o PIN asignando una palabra a cada carácter para formar una frase con sentido, más fácil de recordar).	SSS
Si el sistema necesita más de una clave de acceso, ¿el sistema utiliza técnicas fáciles para reducir la carga cognitiva de los usuarios?	El sistema puede usar caracteres alfanuméricos (e.g.contraseñas) y gráficos (e.g. contraseñas gráficas). Es mas fácil recordar una imagen que una palabra.	SSS
¿El sistema evita el uso de claves aleatorias para la etapa de registro o autenticación?	El uso de claves aleatorias (e.g. One-Time Password) son difíciles de utilizar por los usuarios, debido a que no es posible memorizarlas todas.	SS
¿Se evita cualquier PIN definido por el sistema?	El PIN definido por el sistema puede no tener relación con el usuario, lo que lleva a complicar su memorización fácilmente.	SSS
6. Reconocer, Diagnosticar y Recuperarse de los Errores		
¿Los mensajes relacionados con la seguridad son declarados de forma constructiva?	Los mensajes de error relacionados con la seguridad debe obtener aspectos positivos y útiles de acuerdo al error.	SSS
¿Los mensajes de error relacionados con la seguridad informan al usuario de la gravedad del error?	Conocer el nivel de seriedad del error ayuda a tomar acciones adecuadas.	SS

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿El sistema facilita la posibilidad de diagnostico a posibles errores?	Cuando existe una amenaza de seguridad el sistema puede presentar fallas (e.g. bloqueo), por lo tanto es necesario que el sistema informe claramente la forma de solucionar los errores que dejó la amenaza.	SS
¿Los mensajes de error relacionados con la seguridad son significativos y sensibles al problema?	En algunos casos los mensaje de error debe proporcionar la causa del error de seguridad y de una forma que el usuario pueda entenderlo.	S
¿Los mensajes de error relacionados con la seguridad indican al usuario dónde obtener ayuda?	Si el usuario no comprende el mensaje de error, este debe proporcionar ayuda para solucionarlo.	S
7. Flexibilidad y Eficiencia de Uso		
¿Los usuarios pueden cambiar fácilmente entre los niveles de principiante y experto?	El sistema tiene la posibilidad de presentar información y acciones adecuadas para principiantes y expertos.	SS
Si el sistema es compatible con usuarios principiantes y expertos, ¿los niveles de los mensajes de error con respecto a la seguridad están disponibles en detalle?	La información de los mensajes de error de seguridad se adecua a usuarios principiantes y expertos. Sin embargo, es vital que se adecue a usuarios principiantes.	SS
¿Los usuarios pueden elegir entre información de seguridad de texto o gráfico (e.g. ícono), según sea el caso?	El usuario puede visualizar a partir de texto o gráfico, información de seguridad según se adecue a sus preferencias. Sin embargo, si se pretende mostrar información detallada resultaría muy difícil.	SSS
¿El sistema permite configurar fácilmente las propiedades de seguridad?	La facilidad de configuración de seguridad permite al usuario realizar tareas adecuadas de acuerdo a sus necesidades.	SS
Si el sistema es compatible con usuarios principiantes y expertos, ¿los niveles de seguridad están disponibles en detalle?	El nivel de seguridad de una aplicación puede ser cambiada según las habilidades y preferencias del usuario. Sobre todo, es vital que sea compatible con usuarios principiantes.	SS

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿Los usuarios pueden personalizar fácilmente las opciones seguridad y privacidad para satisfacer sus preferencias individuales?	El sistema posee características propias de seguridad y privacidad de acuerdo a una aplicación en particular.	SS
¿El sistema posee atajos a tareas de seguridad frecuente?	El usuario puede usar atajos de teclado o comandos a tareas de seguridad frecuente.	SS
¿Las indicaciones de seguridad son expresadas en sentido afirmativo?	A partir de mensajes que confirmen la acción que desea realizar (e.g. ¿le gustaría revisar sus configuraciones predeterminadas?).	SS
8. Prevención de Errores		
¿La información necesaria para tomar una buena decisión de seguridad, es adecuada y esta disponible antes de que se adopte la medida?	La información y las consecuencias de cualquier decisión relevante para la seguridad, (e.g. revelar información sensible) deben ser claras.	S
¿El sistema advierte a los usuarios si están a punto de cometer un error de seguridad potencialmente grave?	Por desconocimiento, los usuarios pueden realizan tareas sin darse cuenta de las consecuencias que pueden tener (e.g. hacer que sus imágenes sea accesible para todos los usuarios).	S
¿El sistema impide a los usuarios cometer errores de seguridad siempre que sea posible?	El sistema puede adelantarse impidiendo ejecutar acciones del usuario si detecta posibles errores a la seguridad.	S
9. Consistencia y Estándares		
¿Los iconos de seguridad poseen etiqueta?	La etiqueta en los iconos de seguridad permite al usuario conocer su función.	SS
¿Los controles de seguridad son consistentes y están ubicados en lugares específicos?	Con un conjunto consistente de controles de seguridad y ubicación adecuada, existirá más oportunidades para el aprendizaje pasivo y su coste de esfuerzo disminuye.	SS
Para interfaces de preguntas y respuestas sobre seguridad, ¿las entradas válidas para una cuestión están listadas?	Las posibles respuestas con relación a una pregunta de seguridad realizada por el usuario, son presentadas en forma de lista.	SS
¿Los nombres de las opciones de seguridad en los menús, son consistentes con relación a los demás nombres en cuanto a términos técnicos?	Las opciones de seguridad deben tener semejante terminología técnica en cuanto a la seguridad del sistema.	S

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿Las abreviaturas para palabras de seguridad poseen una longitud predeterminada y fácil de identificar?	La longitud de las palabras abreviadas poseen un promedio en su longitud y ser identificada (e.g. SSL - Secure Sockets Layer).	SS
¿Las relaciones entre los controles de seguridad y las acciones de seguridad son claras para el usuario?	Las acciones de seguridad identificadas a partir de controles, deben tener relación para una mejor comprensión	S
10. Ayuda y Documentación		
¿Hay una función de ayuda de seguridad visible?	La función de ayuda debe ser visible e identificable por el usuario (e.g. una etiqueta llamada .ªyuda de seguridad").	S
¿La información proporcionada por la ayuda es relevante?	La información de seguridad debe ser significativo con respecto a las necesidades del usuario.	S
¿Los usuarios pueden cambiar fácilmente entre la ayuda de seguridad y sus tareas?	El usuario puede obtener ayuda mientras realiza tareas y viceversa.	SS
¿Las instrucciones de la ayuda siguen la secuencia de acciones de seguridad del usuario?	Las instrucciones de ayuda para una situación especifica debe seguir unos pasos ordenados para solucionar el inconveniente.	SS
¿El sistema provee actualizaciones oportunas a documentación relacionada con la seguridad?	La documentación de seguridad debe actualizarse periódicamente con el fin de proporcionar nuevas herramientas para los usuarios. Sin embargo, lo más importante es la seguridad del sistema esté o no actualizada.	SS
¿El sistema provee soporte técnico en linea para solucionar problemas de seguridad?	Es importante que exista ayuda técnica en linea a situaciones complejas de seguridad. Sin embargo, se debe tener precaución con ataques de ingeniería social.	SS
11. Transmitir Características		
¿Hay una clara comprensión de las capacidades de seguridad del sistema?	Los usuarios pueden observar en el sistema características y capacidades en seguridad, y actuar en caso de ser necesario.	S

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿El sistema anticipa adecuadamente y pronto la próxima actividad probable relacionada con seguridad?	El sistema tiene la capacidad de proponer la próxima acción de seguridad que permita una solución mas efectiva para los usuarios.	SS
¿El sistema notifica a los usuarios si está interactuando con fuentes no confiables?	La fuente no confiable representa algo que no tiene información sobre su identidad, si esto llega a presentarse, el sistema notifica al usuario que puede existir algún tipo de vulnerabilidad.	S
¿El sistema muestra logos de seguridad?	El logo en función del tipo de interfaz de seguridad transmite confianza (e.g. Symantec).	S
¿El sistema tiene certificados de seguridad otorgado por entidades externas reconocidas?	Es importante conseguir que los usuarios conozcan sus funciones (e.g., VeriSign, ControlScan o SSL).	S
¿Los datos que los usuarios no pueden modificar están desactivados?	Los datos que son propios de la seguridad del sistema sistema no pueden ser editados.	S
¿El sistema proporciona un número limitado de configuraciones de seguridad estandarizados que pueden ser auditados, documentados, y fácilmente aprendido por los usuarios?	Los sistemas informáticos actuales tienen un gran número de políticas de seguridad que son complejos y desconocidos. Es mejor dar una cantidad limitada de políticas estandarizadas que por lo general no necesitan ser personalizadas.	SS

4.5.2. Seguridad y Privacidad

Tabla 4.16: Sub-heurísticas de Seguridad y privacidad (después de la revisión).

Sub-heurística	Descripción	Grado
¿Las áreas protegidas son completamente inaccesibles y seguras?	Es vital que los usuarios sepan que deben utilizar un usuario SIN perfil de administrador para su uso habitual del sistema y utilizar el usuario administrador para tareas específicas como instalar software, configurar la seguridad del sistema. Ademas, las areas deben de ser seguras.	S
¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?	Para información sensitiva, la forma de acceso debe presentar cierta complejidad a nivel de credenciales, para que esta no puedan ser obtenida por mecanismos de fuerza bruta o similares.	S
¿El sistema emplea mecanismos critográficos para la transmisión segura de la información?	Es necesario implementar protocolos seguros para la transmisión de datos.	S
Si el sistema utiliza *cookies* informáticos, ¿la información sobre la privacidad del sistema describe con precisión el uso de estos cookies?	La información de privacidad debe describir si las cookies llevan el control de los usuarios (e.g. almacenamiento de información, contraseñas) o conseguir información sobre los hábitos de navegación del usuario.	S
¿Los caracteres de la clave de acceso están ocultos directamente en el campo y esta acción puede ser habilitada o deshabilitada?	Los caracteres de la clave de acceso (passwords o PIN) aparecen en forma de puntos o asteriscos mientras se digitan. El usuario debe tener el control para habilitar/deshabilitar a voluntad la ocultación de las claves.	SS
¿El proceso de autenticación hace cumplir un límite de intentos de acceso no válidos consecutivos por un usuario?	El sistema se bloquea si el número de intentos posibles consecutivos en un tiempo determinado, no certifican la identidad del usuario.	S
En un método de autenticación por conocimiento (e.g. contraseña o PIN), ¿el sistema permite al usuario modificar su clave de acceso? ?	El sistema facilita el cambio de claves de acceso fácilmente en cualquier momento.	S

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿El sistema confirma al usuario la transmisión de datos antes que estos sean transmitidos?	Para evitar enviar datos sensibles por error, el sistema confirma al usuario si procede a realizar dicha acción.	S
¿El sistema notifica a los usuarios (administradores) sobre los privilegios de acceso que posee?	Los usuarios no pueden poseer privilegios (e.g. modificar archivos de sistema) que afecten la seguridad del sistema. Esta es la función que desempeña el administrador del sistema.	SS
¿El sistema concede acceso de acuerdo a una autorización válida?	Si la validación de la información por parte del usuario es correcta, el sistema concede acceso.	S
¿Se presenta al usuario mensajes de notificación concernientes a la seguridad y privacidad antes de acceder al sistema?	El sistema presenta al usuario mensajes sobre políticas de seguridad y privacidad. Sólo hay que comunicar al usuario los estados relevantes para él y en el momento en que sucedan.	SS
¿El sistema garantiza que la información de acceso público no tenga información privada?	El sistema debe abstenerse de presentar información privada cuando sea público. Dejar que el usuario tenga el control pidiéndole confirmación antes de presentar información privada.	S
¿La información de privacidad del sistema garantiza al usuario el derecho a optar por compartir información no crítica con terceros?	Las políticas de privacidad del sistema deben permitir al usuario el deseo o no de compartir información que no sea sensitiva.	S
¿El sistema emplea herramientas que proveen notificación al usuario sobre discrepancias durante la verificación de identidad?	A partir de mensajes o sonidos puede ser notificado al usuario sobre estas discrepancias.	S
Si el sistema facilita el intercambio de datos con otros usuarios, ¿ el sistema permite diferentes políticas de acceso y asociarse a diferentes tipos de datos?	Cuando existe intercambio de datos entre usuarios, el sistema posee políticas de seguridad (e.g. autenticación) para acceder e intercambiar información.	S
¿El sistema notifica y da posibles soluciones al usuario sobre vulnerabilidades asociados a incidentes de seguridad detectados?	Cuando se presenta un incidente de seguridad, el sistema presenta las posibles consecuencias de esto.	S
¿El sistema notifica al usuario sobre realización de copias de seguridad relacionados con la información personal?	Esta notificación es importante en el diálogo de configuración del sistema de copias de seguridad más que en el momento de realizar una copia.	SS

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
En el proceso de configuración de la cuenta, ¿existe la opción de configuración de privacidad y es aplicable a todo el sistema?	En el proceso de configuración de la cuenta del usuario, las opciones de configuración de privacidad deben estar disponibles para que el sistema sea mas fácil de usar y evitar que la información sea de acceso público.	SS
¿El sistema describe cada opción de privacidad en detalle?	Cada opción de privacidad debe describir detalladamente que tipo de información debe ser presentada a terceras personas o no debería presentarse nada.	SS
¿Existe una política de copia de seguridad que especifica cómo debe realizarse esta acción?	Las copias de seguridad están basadas en planes de acción para afrontar riesgos de seguridad.	SS
¿El sistema provee confirmación para los usuarios sobre las declaraciones que indican que ellos entienden las condiciones de acceso?	Los mensajes de confirmación permiten establecer al usuario que condiciones de acceso al sistema son necesarios. Ademas, es importante que el usuario entienda la condiciones de acceso al configurar el sistema (e.g ¿Acepta que las "cookies"se almacenen en el momento del registro?).	SS
¿El sistema hace cumplir el nivel de complejidad de la contraseña, con los requisitos mínimos exigidos?	El usuario puede determinar la complejidad de la contraseña y los requisitos a través de barras que cambian de color en función de la complejidad de la contraseña. El grado de importancia debe ir ligado al grado de inseguridad de la contraseña. si es muy débil, es vital exigir que cumpla el nivel de complejidad. Si es normal, sólo es recomendable exigirlo.	S
¿El sistema cifra datos solicitados en el proceso de autenticación?	La información solicitada al usuario para poderse certificar debe ser encriptada para aumentar el nivel de seguridad. La encriptación es un proceso totalmente exigible porqué aumenta siempre la seguridad con un impacto nulo o muy bajo para el usuario	S

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
Si se utiliza tarjetas inteligentes, ¿los datos del propietario están almacenadas en ella?	Para verificar que el propietario es quien dice ser, todo sus datos deben estar almacenados en la tarjeta. La tarjeta por sí sola no puede ser la única forma de identificar, hace falta un segundo sistema de identificación.	SS
¿El sistema proporciona consejos u orientaciones de configuraciones de privacidad cuando se usa por primera vez?	El sistema debe orientar a los usuarios de las configuraciones de privacidad cuando el sistema se usa por primera vez (e.g. orientación de las configuraciones de privacidad cuando se crea una cuenta). Si el sistema tiene buena usabilidad esto ya no es necesario.	SS
¿La tarjeta inteligente o token del titular posee mecanismos de política privacidad?	Técnicas criptográficas pueden ser aplicadas a smart cards o tokens (e.g. la seguridad de la información de la credencial es cifrada usando PKI).	S
¿El sistema posee políticas de privacidad para comercio o contenido del usuario?	Las políticas de seguridad pueden estar enfocadas a comercio electrónico o datos personales (en estos sitios es fundamental las políticas de privacidad).	S
¿El sistema soporta y hace uso por defecto del protocolo HTTPS?	Destinado a la transferencia segura de datos de hipertexto y utilizado principalmente para e-banking, e-commerce o cualquier tipo de servicio que requiera seguridad.	S
¿El método de autenticación posee interoperabilidad entre sistemas?	El método de autenticación debe proporcionar que dos o más sistemas o componentes puedan intercambiar información de los usuarios (e.g. uso en e-commerce).	SSS

4.5.3. Accesibilidad

Tabla 4.17: Sub-heurísticas de Accesibilidad (después de la revisión).

Sub-heurística	**Descripción**	**Grado**
¿El sistema permite usar passwords gráficos para usuarios con dificultades de lectura?	Las imágenes podrían ayudar a las personas a autenticarse cuando tienen problemas de lectura (e.g., dislexia).	S
En autenticación por caracteristica, ¿el sistema esta compuesto por dispositivos estandard?	La inclusión de dispositivos estándard facilita su configuración y uso por parte de los usuarios (e.g. Los lectores RFID se utilizan para la autenticación basada en proximidad, la serie de estándares estrictamente relacionada con las RFID y las frecuencias empleadas en dichos sistemas es la serie ISO 18000).	SS
En autenticacion por posesión (token o tarjeta), ¿el sistema está equipado con software y hardware adecuado?	La instalación de software adecuado en hardware eficiente, facilita su uso por parte de los usuarios en el proceso de autenticación.	SS
En un proceso de autenticacion, ¿el sistema evita esfuerzo adicional para personas con algún tipo de limitación fisica o cognitiva	El proceso de autenticación debería ser intuitivo y sin esfuerzo (e.g. cognitivo o físico) extra.	SS
En un sistema por autenticacion por biometría, ¿el sistema permite ser configurado para personas con limitaciones físicas?	Para problemas psicomotrices que implica una falta de organización del movimiento (e.g. dispraxia), el sistema debería ser configurado fácilmente para estos casos.	S
¿El sistema provee a los usuarios otras alternativas para autenticarse?	Esto podría mejorar la disponibilidad y conveniencia del sistema.	SS
¿El método de autenticación se adapta a usuarios nuevos y experimentados?	El método de autenticación debería tener opciones de configuración para ser usados por usuarios nuevos y experimentados, garantizando siempre que tenga la opción para usuarios nuevos.	SS

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿Se ha utilizado el color y algún código específico para llamar su atención e indicar los cambios relacionados con la seguridad?	El tipo de color presentado puede indicar cambio del nivel de seguridad o riesgo del sistema. Ante usuarios con problemas de visión del color, la interfaz de usuario añade algún tipo de código (texto, icono, etc) que comuniquen de forma redundante los cambios relacionados con la seguridad.	SS
En los campos donde se necesita información para autenticarse, ¿el sistema permite cambiar el tamaño de la letra para el usuario?	Utilizar un tamaño de fuente adecuado para asegurar la facilidad de lectura.	SS

4.5.4. Operabilidad

Tabla 4.18: Sub-heurísticas de Operabilidad (después de la revisión).

Sub-heurística	**Descripción**	**Grado**
¿El sistema permite seleccionar algún método de autenticación en especial o combinaciones de ellas?	El usuario tiene la posibilidad de escoger el sistema de autenticación o combinaciones de ellas (e.g. autenticación multifactor) de acuerdo a sus necesidades.	SSS
¿El sistema permite personalizar la interfaz en el proceso de autenticación sin poner en riesgo la seguridad relacionada con información sensitiva?	A partir de las necesidades del usuario, el cambio de la interfaz no presentará información sensitiva a terceros. En especial, la posibilidad de visibilizar el valor de la clave a voluntad del usuario.	SSS
Para operaciones de alto riesgo de ataque, ¿el sistema permite usar autenticación biométrica?	El ataque informático usando seguridad biométrica, es más difícil comparado con otros métodos de autenticación. Sin embargo, por costos en ocasiones no se puede usar seguridad biometrica.	SS
Si los usuarios olvidan el PIN, ¿el sistema permite restablecerlo a través de una interfaz?	La interfaz del sistema donde el usuario tiene la cuenta, permite cambiar o recordar el PIN en caso de olvido.	SS

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿El método de autenticación empleado sigue normas conocidas (sean estandares o no) donde su seguridad sea adecuada?	Varios métodos de autenticación usan procesos propios o patentados que pueden ser o no estándares a nivel internacional.	SSS
Si el proceso de registro es requerido, ¿este es corto, sencillo y solo exige información esencial?	Es útil mantener el proceso de registro lo más corto posible y en el caso de la información requerida, explicar brevemente por qué se requiere.	S
¿El sistema informa al usuario que el proceso de autenticación ha sido satisfactorio?	Crear un mecanismo de retroalimentación para que el usuario sepa cuándo el proceso de autenticación ha sido satisfactoria.	SS
En un proceso de autenticación, ¿este tiene palabras adecuadas para desarrollar una acción en particular?	Usar palabras o frases adecuadas que describan la acción a realizar (e.g. usar ingresar (*sing in*) en lugar de cuenta (*account*))	SSS

4.5.5. Fiabilidad

Tabla 4.19: Sub-heurísticas de Fiabilidad (después de la revisión).

Sub-heurística	**Descripción**	**Grado**
¿El proceso de autenticación es simple y protege contra usuarios no autorizados?	Para acceder a información privada, el método de autenticación disponible debe ser adecuado y seguro.	S
¿El sistema presenta certificados de confianza?	Asegura al usuario que pueden confiar en el sistema, respetando su privacidad a partir de certificados estándar (e.g TRUSTe).	S
En el caso en que el usuario deba proporcionar la información, ¿el sistema determina que medidas son utilizadas para proteger esta información?	El sistema proporciona tranquilidad al usuario a partir de criterios de seguridad para proteger la información sensible (e.g. información personal).	S
¿Está claramente establecido el propósito de utilizar la información personal del usuario?	El sistema informa al usuario sobre la finalidad en el uso de su información personal.	S

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿El sistema notifica al usuario si está interactuando con fuentes no confiables?	Verificar las fuentes y datos de forma segura, permite interactuar de forma responsable y evita el riesgo de tomar decisiones erradas.	S
¿El sistema emplea mecanismos para ayudar en la presentación de informes de incidentes de seguridad si son necesarios?	El sistema tiene procesos automatizados en la presentación de informes de seguridad si el usuario realmente lo requiere. Sin embargo, este informe debe ser presentado en un lenguaje que el usuario entienda.	SSS
¿El sistema provee integración a múltiples bases de datos?	El contenido de la base de datos de control de acceso físico y la base de datos de control de acceso lógico pueden ser integradas por el sistema empleando mecanismos de seguridad.	SSS
¿El sistema ofrece servicios de seguridad personalizado que permite tener en cuenta las necesidades y preferencias de los usuarios?	El sistema debería permitir algún tipo de seguridad personalizado (e.g. crear un autenticador de tokens de seguridad personalizado e integrarlo con un administrador de tokens de seguridad personalizado).	SSS
Si el proceso de inicio de sesión falla, ¿el sistema evita indicarle al usuario qué parte del proceso es incorrecto?	Desde el punto de vista del usuario, espera que el sistema le de cuantas más indicaciones posibles. Sin embargo, la realimentación de información sensitiva en un proceso de autenticación, podría llevar a ataques informáticos.	SS
¿El sistema evita la reutilización de contraseñas?	Organizaciones que son susceptibles a ataques informáticos (e.g. e-banking), solicitan al usuario cambiar las contraseñas y evitan que sean las mismas	SS
Para autenticación desafio-respuesta (*Challenge–response authentication*), ¿las preguntas desafio son pertinentes para los usuarios?	Las preguntas deben ser caracterizadas para la mayor cantidad de los usuarios.	SS
Si el número de preguntas desafio que contesta el usuario es n, ¿el sistema presenta un número de preguntas $t \geq n$ para ser contestadas?	Generalmente los usuarios contestan un máximo tres preguntas desafio para autenticarse, por lo tanto el sistema debe proporcionar un número de preguntas mayor a tres como opcionales para ser contestadas.	SSS

4.5.6. Desempeño

Tabla 4.20: Sub-heurísticas de Desempeño (después de la revisión).

Sub-heurística	**Descripción**	**Grado**
¿El proceso de computo en el método de autenticación es imperceptible por el usuario?	Las instrucciones a realizar el método de autenticación empleado, debe realizarlo en el menor tiempo posible.	S
En un sistema de autenticación por biométrica, ¿los algoritmos usados presentan un buen desempeño en tiempo de ejecución?	Debido a la gran cantidad de datos para autenticación biométrica, los algoritmos usados deben presentar alto desempeño.	S
Para reducir el tiempo de cifrado en el proceso de autenticación, ¿el sistema adopta una tarjeta inteligente de alto rendimiento?	El microprocesador de la tarjeta esta diseñado para tareas especificas, esto permite mejorar el rendimiento del proceso.	SS
¿El proceso de autenticación biométrica posee memoria extra para evitar retrasos de ejecución de las instrucciones?	Como consecuencia de la cantidad de datos en este tipo de proceso, es necesario memoria extra.	SS
Para un mayor nivel de seguridad, ¿el sistema emplea tecnología múltiple (e.g. contacto o inalábrico) junto a métodos biométricos para aplicaciones de acceso?	Se emplean tarjetas que incluyan chip de contacto e identificación por radiofrecuencia (e.g. RFID) junto con métodos biométricos. Sólo apto para sistemas muy complejos donde el nivel de seguridad sea estricto.	SS
¿Las políticas de contraseñas presentan un nivel importante de cumplimiento y son fáciles de usar?	Las políticas para generar contraseñas deben ser seguras y la carga de trabajo cognitivo de los usuarios es mínimo.	S
En un escenario de reautenticación, ¿el sistema integra las medidas de seguridad pertinente según sea el caso?	En los cierres de sesión automáticos, el sistema informa que la sesión se ha cerrado y es necesario autenticarse de nuevo para acceder al sistema. Para el cumplimiento de este requerimiento será importante tener en cuenta la aplicación, el usuario y el contexto de uso.	S

Continua en la próxima página –

– *Continua desde la página anterior*

Sub-heurística	**Descripción**	**Grado**
¿La información sensitiva asociada a la identificación del usuario es mínima según sea el caso?	Básicamente, la identificación del usuario puede ser realizado a partir de un nombre de usuario apropiado (e.g nombre de usuario) o un correo electrónico (e-mail). Para el cumplimiento de este requerimiento será importante tener en cuenta la aplicación, el usuario y el contexto de uso.	SS
¿El sistema evita el uso de "cookie informático" para métodos de autenticación?	Almacenar credenciales del usuario puede afectar la seguridad para quien accede al sistema.	SS
¿El sistema proporciona etiquetas de texto que proporcionan consejos para generar contraseñas?	Junto al campo de contraseña, aparece un recordatorio en forma de enlace (e.g. ¿Qué es una contraseña valida?), sobre políticas de contraseña.	S

Capítulo 5

Aplicación con Expertos y Usuarios

5.1. Introducción

En este capítulo se analizará las evaluaciones realizadas por expertos y usuarios para aplicaciones reales. Para el caso de evaluación con expertos, son tomadas en cuenta los principios USec obtenidos del Capítulo 4 con el fin de realizar una evaluación heurística. Para el caso de usuarios, se definen una serie de tareas relacionadas con aspectos de seguridad para ciertas aplicaciones. En la Figura 5.1 se presenta el esquema general del contenido que se presentará en este capítulo.

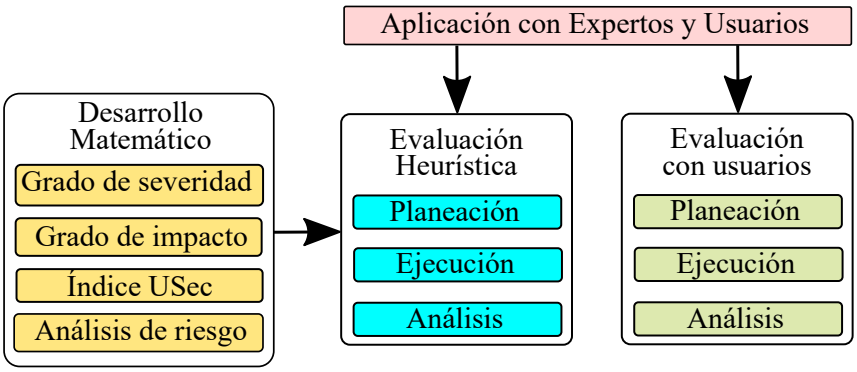


Figura 5.1: Estructura del Capítulo 5 (creación propia).

5.2. Formulación Cuantitativa de Evaluación para Seguridad Usable

Una vez establecido el nivel de importancia para cada sub-heurística (ver Sección 4.1), se propone en esta sección una métrica de evaluación para seguridad usable. Para ello se determina un nivel de severidad de acuerdo al grado de cumplimiento del principio,

para obtener con esto, una métrica de evaluación para USec. Adicional a esto, se propone obtener una matriz de riesgo a partir del nivel de USec y el impacto que pueda tener si los principios no se cumplen satisfactoriamente.

5.2.1. Justificación de la necesidad de una métrica cuantitativa

Muchos trabajos de investigación que se encuentran en la literatura presentan métodos, herramientas y análisis relativos a la evaluación en seguridad usable [115][20][4]. Sin embargo, muchos de estos métodos no han ayudado a los desarrolladores a tener un modelo claro y adecuado para lograr una máxima seguridad usable en sus aplicaciones a partir de una medida cuantificable. Cada investigador o desarrollador en este campo, implementa de acuerdo a su experiencia, sus propios mecanismos de evaluación, por lo que se pueden encontrar métodos muy diversos y que pueden ser diferentes en parte o en todo su aspecto. Por lo tanto, no existe desde nuestro conocimiento, una forma de evaluación cuantitativa que sea aplicada en el campo de la seguridad usable y que ayude a obtener mejores resultados de diseño en USec.

Según lo anterior y teniendo en cuenta la importancia de la usabilidad y seguridad actualmente, se trata de proponer un método de evaluación cuantitativa en seguridad usable y autenticacion que facilite a los desarrolladores, una métrica del nivel de USec para una aplicación dada, y con base en el resultado, puedan realizar las respectivas acciones orientadas a mejorar la aplicación y disminuir el riesgo a ataques de ingeniería social.

Ahora bien, la evaluación del riesgo forma parte de la gestión de seguridad porque cuando existe un riesgo en el sistema, algunas acciones de seguridad deben ser implementadas. Es sorprendente que estandares importantes de calidad como el ISO/IEC 27001:2013 [137] – *para sistemas de gestión de seguridad de la información* y el NIST 800-30 [142] – *para gestión de riesgos de la seguridad de la información*, no se mencione las consecuencias de la mala usabilidad de las características de seguridad en el sistema. Una aproximación del nivel de riesgo en seguridad usable lo aporta Jøsang et al. [5], sin embargo su análisis abarca pocos principios y no da una visión cuantificable y más completa del sistema.

Por lo tanto, existe la necesidad de proporcionar una forma de análisis de riesgo aproximado para seguridad usable a partir de principios y su factor de impacto a partir de expresiones matemáticas.

5.2.2. Grado de Severidad e Impacto

Nielsen [58] otorgó sus propias calificaciones de severidad para su conjunto heurístico de usabilidad. Nielsen utilizó una escala de clasificación de cuatro niveles para medir la gravedad de los problemas de usabilidad. Los expertos evaluarán la interfaz y si encuentran una infracción de usabilidad, la valorarán con un valor de 0 a 4 para medir su extensión. A pesar de que este método ha sido ampliamente adoptado, hay casos en los que son insuficientes para medir el grado de violación de la usabilidad de las características

de seguridad. El mismo razonamiento existe en este estudio con respecto a clasificaciones de severidad para USec, ya que es necesario obtener niveles de severidad adecuadas que pudieran ser efectivas con el fin de medir cuantitativamente el alcance de las violaciones.

Teniendo en cuenta algunos niveles de severidad propuestos por importantes investigadores en el campo de la seguridad usable [96][122][78][134], se analizaron y modificaron con el fin de ser adaptados al campo de la USec y que presente casi el mismo aspecto que el propuesto por Nielsen [58] (escala y descripción) por su facilidad de comprensión. El nivel de severidad en esta propuesta indica el grado de cumplimiento de la sub-heurística. El experto es el responsable de asignar un valor de la sub-heurística en evaluación.

Un aspecto muy importante de la propuesta para el nivel de severidad en USec, es la definición de una opción donde el evaluador no tiene el conocimiento adecuado para realizar la evaluación o la sub-heurística no es aplicable. Este aspecto se basa en la sugerencia proporcionado por Bonastre [128] y necesaria en aquellos casos en los que el evaluador, independientemente del motivo, no pueda evaluar la sub-heurística en cuestión. Lo anterior, también permite no tener en cuenta aquellas preguntas donde el evaluador considere irrelevantes. En la Tabla 5.1 es presentado la propuesta para el nivel de severidad.

Por último, Nielsen [60][61] demuestra que en evaluaciones heurísticas conducidas por profesionales relacionados con las ciencias de la computación, como programadores y estudiantes en informática, los evaluadores no tienen que ser expertos en usabilidad. Sin embargo, y debido a que en el campo de la seguridad usable intervienen aspectos de usabilidad y seguridad, es aconsejable que los evaluadores tengan conocimiento de estos dos aspectos con el fin de que la evaluación sea lo menos subjetiva posible.

Tabla 5.1: Nivel de Severidad para USec.

Nivel	Descripción
1	La aplicación diverge por completo del principio.
2	La aplicación presta cierta atención al principio pero todavía tiene grandes problemas.
3	La aplicación presta cierta atención al principio pero todavía tiene problemas menores.
4	La aplicación sigue el principio en algunas secciones.
5	La aplicación sigue el principio por completo.
Sin valor numérico	No sé/no tengo opinión, o no es aplicable.

La OWASP[1] (por sus siglas en inglés *Open Web Application Security Project*) define el impacto como "*las consecuencias cuando existe un ataque exitoso*". Según el NIST 800-30 [142], el impacto son "*las consecuencias que resultan de la divulgación, modificación,*

[1]Disponible en: https://www.owasp.org

destrucción no autorizada de la información o la pérdida de información". Investigar el impacto potencial por una violación de severidad, proporciona un elemento trascendental para organizaciones e individuos cuando el sistema presenta vulnerabilidades.

Teniendo en cuenta algunos niveles de impacto propuestos por importantes investigadores en el campo de la seguridad usable [111][78], reconocidas empresas a nivel mundial tales como Microsoft[2] y Google[3], e intitutos de estandarización como NIST [142], se analizaron y modificaron con el fin de ser adaptados al campo de la USec y a una formulación cuantitativa de evaluación. El experto o evaluador es el responsable de asignar el valor de impacto para la sub-heurística en evaluación. Para este caso también existe la opción "sin valor numérico", cuando la sub-heurística no se pueda evaluar o no es aplicable. En la Tabla 5.2 es presentado la propuesta para el nivel de impacto, con su nivel cuantitativo, nombre y descripción.

Tabla 5.2: Nivel de Impacto para USec.

Nivel	Nombre	Descripción
1	Bajo	En esta categoría la vulnerabilidad requiere de circunstancias improbables para ser llevadas a cabo, y si estas son ejecutadas con éxito, sus consecuencias son insignificantes o es ampliamente mitigado por las características del componente afectado.
2	Medio	Esta categoría puede comprometer la confidencialidad, integridad y disponibilidad de datos o recursos (físico o humano) pero poco probables para ser efectuado.
3	Alto	Esta categoría pone en peligro la confidencialidad, integridad y disponibilidad de los datos o recursos con una alta probabilidad para ser efectuado.
4	Crítico	El sistema es fácilmente vulnerado y compromete gravemente los datos o recursos sin interacción del usuario.
Sin valor numérico	Ninguno	Para los casos donde el principio no se pueda evaluar o no es aplicable.

5.2.3. Formulación Matemática para la Evaluación

A partir de la justificación presentada anteriormente, se hace necesario obtener una métrica cuantitativa que refleje el nivel de seguridad usable a partir de la evaluación heurística realizada por expertos para una aplicación en particular. Para ello se propone un modelo matemático que tenga en cuenta las variables (severidad e impacto) para la evaluación.

[2]Disponible en: https://technet.microsoft.com/en-us/security/gg309177.aspx. Consultado en Junio de 2016

[3]Disponible en: https://www.chromium.org/developers/severity-guidelines. Consultado en Junio de 2016

Esta propuesta se basa en el modelo propuesto por Suárez [141] donde es estrictamente usada para obtener una métrica cuantitativa de usabilidad.

El modelo matemático propuesto para evaluar el nivel cuantitativo de seguridad usable depende de dos variables: El nivel de importancia de la sub-heurística S_i y el nivel de severidad de la sub-heurística H_i. Es importante recordar que el nivel de importancia representa a (S), (SS) y (SSS) presentadas en la Sección 4.1 y que han sido asignadas a cada sub-heurística a partir de revisiones con expertos.

Peso Sub-heurístico W_i: Representa el valor de ajuste que se le hace a cada sub-heurística dependiendo del nivel de importancia y al número de sub-heurísticas que han sido tenidas en cuenta. Este peso W_i es representado como:

$$W_i = \frac{S_i}{\sum_{i=1}^{n} S_i} \tag{5.1}$$

donde n es el número de sub-heurísticas, cumpliéndose que

$$\sum_{i=1}^{n} W_i = 1$$

Con esto garantizamos que nuestro modelo se encuentre normalizado.

Nivel de seguridad usable $USec$: A partir del peso sub-heurístico anteriormente formulado, se obtiene el nivel de seguridad usable dependiendo de la severidad de las sub-heurística tenidas en cuenta para la aplicación en evaluación. Las sub-heuristicas que no son aplicables no se tienen en cuenta en la evaluación. El valor resultante al obtener este nivel siempre se encuentra entre 0 y 1, el cual se podría llevar a un porcentaje multiplicando el resultado anterior por 100. Este nivel de seguridad usable es representado como:

$$USec = \frac{\sum_{i=1}^{n}(W_i * H_i) - k}{j - k} \tag{5.2}$$

donde j es el número máximo del nivel de severidad de la escala y k es el número mínimo del nivel de severidad de la escala el cual es presentado en la Tabla 5.1.

Para verificar que la Ecuación 5.2 estuviese bien formulada, se realizaron varias verificaciones con ejemplos ficticios con el fin de que:

1. Los resultados de evaluación estuviesen dentro del rango de medición previamente establecido [0, 1].

2. Al incrementar el nivel de severidad de una sub-heurística, se obtuviese un incremento en el nivel de seguridad usable.

3. Debido a que la Ecuación 5.2 tiene operaciones de resta, evitar que el resultado final sea un valor negativo.

4. Sin importar los valores de j y k, sean estos positivos o negativos, el resultado de la evaluación siempre estuviese en el intervalo [0, 1].

Una mejora importante que debemos tener en cuenta en comparación con el modelo presentado por Suárez [141] es que en nuestra propuesta, los valores de la escala del nivel de severidad es independiente de su magnitud y signo. Es decir, la escala de severidad y su signo puede ser seleccionada a criterio del evaluador sin alterar el resultado final y el intervalo seleccionado. Además, presenta menor complejidad matemática ya que presenta menos operaciones aritméticas. Para la presente propuesta la escala de severidad es $k = 1$, $j = 5$ y ambos con signo positivo.

Aunque esta métrica obtenida para la USec es muy útil con el fin de realizar comparaciones (e.g. USec = 0.75), a veces este valor puede dificultar la comparación cuando se quiere complementarlo con una explicación más adecuada. Para abordar esta necesidad, se inició una encuesta a expertos en seguridad y usabilidad para determinar una calificación adjetiva (excelente, bueno moderado, pobre y muy pobre) a cada intervalo que podría estar asociado a un valor numérico de USec, esto con el fin de dar una calificación absoluta a los valores obtenidos del indice de Usec.

En el Anexo E se presenta la encuesta de calificación adjetiva para USec. Esta encuesta fue realizada en Google Drive[4] y enviada a los expertos que aceptaron la invitación para diligenciar el formulario. Hasta la fecha, 10 contestaron las preguntas, de los cuales 2 la completaron de forma errónea. Por lo tanto solo consideramos 8 expertos que desarrollaron la encuesta de forma exitosa. En la Tabla 5.3 es presentado el perfil de los encuestados.

Tabla 5.3: Perfil de los encuestados.

Profesión	Profesor: 80 % Estudiante: 10 % Desarrollador: 0 % Otro: 10 %
Estudios	PhD: 90 % Maestría: 0 % Universitario: 10 %
Área de interés	Usabilidad: 30 % Seguridad: 10 % Seguridad y usabilidad: 40 % Otro: 20 %

A partir de un análisis y tomando en cuenta los promedios de todas las respuestas para cada cada calificación adjetiva, en la Tabla 5.4 se presenta el resultado del intervalo y su respectiva calificación para el nivel de USec teniendo en cuenta la Ecuación 5.2. Como

[4]Disponible en: https://drive.google.com. Realizada en Septiembre de 2016

se observa en los resultados del nivel de USec, es importante tener presente los intervalos cerrados y abiertos, esto con el fin de que el resultado se encuentre en un valor como el presentado en la Tabla 5.4 (e.g. USec = 0.9).

Tabla 5.4: Clasificación adjetiva para el nivel de USec.

Nivel USec	**Clasificación Adjetiva**
(0.9, 1)	Excelente
(0.7, 0.9]	Bueno
(0.4, 0.7]	Moderado
(0.2, 0.4]	Pobre
(0, 0.2]	Muy pobre

Ahora con base en el impacto que puede tener la severidad de la sub-heurística, se propone otra expresión matemática para evaluar cuantitativamente el nivel de impacto, con el fin de obtener el grado de riesgo de la aplicación que se verá en la próxima sección. Este nivel de impacto depende de dos variables: El nivel de importancia de la sub-heurística S_i y el nivel de impacto de la sub-heurística I_i.

Nivel de impacto I_i: A partir del peso anteriormente formulado (ver Ecuación 5.1), se obtiene el nivel de impacto dependiendo del impacto de cada sub-heurísticas tenida en cuenta para la aplicación en evaluación. Las sub-heurísticas que no son aplicables o que el evaluador no tenga conocimiento alguno, no se tendrán en cuenta en la evaluación. El valor resultante al obtener este nivel general de impacto siempre se encuentra entre 0 y 1, el cual se podría llevar a un porcentaje multiplicándolo por 100. Este nivel de impacto es representado como:

$$I = \frac{\sum_{i=1}^{n}(W_i * I_i) - k}{j - k} \tag{5.3}$$

donde j es el número máximo del nivel de impacto de la escala y k es el número mínimo del nivel de impacto de la escala el cual es presentado en la Tabla 5.2.

Para verificar que la Ecuación 5.3 estuviera bien planteada, se realizaron varias verificaciones con ejemplos ficticios con el fin de que:

1. Los resultados del impacto estuviesen dentro del rango de medición previamente establecido [0, 1].

2. Al incrementar el nivel de impacto de una sub-heurística, se obtuviese un incremento en el nivel impacto general.

3. Debido a que la Ecuación 5.3 tiene operaciones de resta, evitar que el resultado final sea un valor negativo.

4. Sin importar los valores de j y k, ya sean positivos o negativos, el resultado del impacto siempre estuviese en el intervalo [0, 1].

Al igual que en el nivel de USec, donde se determina una calificación adjetiva, para el impacto también se obtiene este tipo de calificación con base en la encuesta presentada en el Anexo E y teniendo en cuenta los mismos expertos presentados en la Tabla 5.3. En la Tabla 5.5 se presenta el resultado del intervalo y su respectiva calificación para el nivel de impacto teniendo en cuenta la Ecuación 5.3.

Tabla 5.5: Clasificación adjetiva para el nivel de impacto.

Nivel impacto	**Clasificación Adjetiva**
(0.7, 1)	Crítico
(0.5, 0.7]	Alto
(0.2, 0.5]	Medio
(0, 0.2]	Bajo

5.2.4. Análisis de Riesgo

Si se pueden descubrir vulnerabilidades y sus amenazas junto con el impacto que pueda tener una aplicación en particular, el desarrollador de software (con conocimientos en seguridad) podría obtener un nivel de riesgo a posibles ataques informáticos. Lo ideal sería tener un cálculo del nivel de riesgo para cualquier sistema, pero las vulnerabilidades de un sistema son o pueden ser muy diferentes a otro sistema. A partir de recomendaciones sugeridas por expertos que revisaron los principios presentados en la Sección 4.2.3.3, aquí se presenta una propuesta de análisis de riesgos teniendo en cuenta la severidad y el impacto para aplicaciones donde la seguridad usable sea requisito indispensable.

Como se mencionó en la Sección 2.5.3, la propuesta de análisis de riesgos va a tener en cuenta la vulnerabilidad y el impacto de una aplicación, aunque lo correcto sería tener presente la amenaza, sin embargo, con los resultados obtenidos con esta propuesta podría dar una "luz" a los desarrolladores sobre posibles ataques.

Jøsang et al. [5] afirma que si un sistema presenta pobre seguridad usable entonces esto representa en realidad una grave vulnerabilidad para el sistema en cuestión. Lo anterior significa que si el nivel de seguridad usable presentada en la Ecuación 5.2 es baja, es muy probable que sea vulnerable a ataques. Con base en lo expuesto anteriormente, podemos asociar el concepto de vulnerabilidad al nivel de seguridad usable propuesto en este trabajo y que junto con el impacto se podría tener una aproximación del nivel de riesgo.

Para obtener este nivel riesgo y con base en la Ecuación 2.2, la expresión matemática para la obtención de este riesgo es presentada en la Ecuación 5.4.

$$Riesgo = USec * I \tag{5.4}$$

Teniendo el valor de $USec$, del impacto I y multiplicando estos dos valores, es posible obtener el nivel de riesgo del sistema en evaluación. Con base en la encuesta presentada en el Anexo E y realizada por expertos en usabilidad y seguridad y USec, en la Tabla 5.6 se presenta los resultados de la encuesta para la clasificación adjetiva para la el nivel de vulnerabilidad.

Tabla 5.6: Clasificación adjetiva para vulnerabilidad.

Vulnerabilidad	**Clasificación Adjetiva**
(0.8, 1)	Altamente improbable
(0.7, 0.8]	Improbable
(0.4, 0.7]	Algo probable
(0.2, 0.4]	Muy probable
(0, 0.2]	Casi seguro

Ahora bien, usando la Ecuación 5.4, con base en la clasificación adjetiva del impacto y la vulnerabilidad, podemos encontrar el nivel de riesgo para la aplicación que es objeto de evaluación. El nivel de riesgo es dado por la celda correspondiente a la vulnerabilidad y el impacto como se presenta en la Figura 5.2. Es importante aclarar que los colores (verde, amarillo, rojo y naranja) asociados en la Figura 5.2 están basados en OWASP [77].

Vulnerabilidad	**Impacto**			
	Bajo	Medio	Alto	Crítico
Altamente improbable	Bajo	Bajo	Bajo	Medio
Improbable	Bajo	Bajo	Medio	Medio
Algo probable	Bajo	Medio	Medio	Alto
Muy probable	Medio	Medio	Alto	Alto
Casi seguro	Madio	Alto	Alto	Crítico

Figura 5.2: Matriz de riesgo para USec (Basado en [77]).

5.3. Objeto de estudio: Red social Facebook

5.3.1. Justificación en la selección del sitio web

Con el fin de determinar la opción más favorable para la selección del sitio web, se consideran algunos criterios tenidos en cuenta [51][109].

1. **Información sensible**: Debido a la fuerte proliferación de la información por la red Internet, hay una gran cantidad de datos sensible. Para proteger estos datos, algunos controles de seguridad y privacidad deben ser configurados correctamente.

2. **Disponibilidad**: el sistema interactivo debe estar disponible de forma gratuita. De igual forma, el sistema debe ser de fácil acceso.

3. **Tareas representativas**: el sistema debe contar con una cantidad apropiada de funcionalidades (características de seguridad y privacidad) y un buen nivel de navegabilidad, con lo cual será posible realizar tareas representativas.

Con base en lo anterior, se seleccionó la aplicación de Facebook[5] porque es de acceso gratuito, tiene características de seguridad y privacidad y debido a su popularidad ente las redes sociales actuales, las características de seguridad y privacidad de esta aplicación se vuelve cada vez más compleja y difícil de usar para los usuarios. La evaluación heurística propuesta en esta sección y debido a la importancia de la seguridad usable actualmente, los resultados de esta evaluación pueden contribuir a mejorar interfaces de usuario con el fin de evitar manipulación o divulgación no autorizada de la información.

5.3.2. La red social Facebook

Facebook es la red social más grande del mundo, que contiene más de 1508 millones de usuarios activos según la fuente Alexa.com[6]. Los usuarios de Facebook pueden crear nuevas redes dentro de Facebook y agregar nuevos amigos a través de una previa invitación. Los usuarios de Facebook también pueden enviar mensajes privados a cualquier otro miembro de Facebook, y pueden escribir mensajes públicos de sus amigos. Cualquier usuario de Facebook también puede actualizar su perfil personal para notificar a sus amigos acerca de él o ella [143].

Facebook proporciona una interfaz que permite a los usuarios configurar quién puede acceder a la información de los usuarios. La configuración de seguridad y privacidad predeterminada de Facebook, expone por completo la mayoría de la información sensible del perfil de usuario [143]. Hasta ahora, esta configuración predeterminada se ha mantenido generando con esto, mayor abuso por parte de terceros en manipular o divulgación de la información.

Lo anterior permiten a cualquier usuario de Facebook e incluso a cualquier persona que use Internet, independientemente de si son usuarios registrados o no, en obtener información sobre algún usuario, intereses, fotos o cualquier información disponible. Esto está íntimamente relacionado con los requisitos de seguridad y privacidad necesarios debido al carácter personal de los datos compartidos. Con el fin de evitar el abuso de información personal, los usuarios del servicio están obligados a cambiar la configuración de seguridad

[5]Disponible en: www.facebook.com. Consultado en Septiembre de 2016.
[6]Disponible en: http://www.alexa.com/siteinfo/facebook.com. Consultado en Septiembre de 2016.

y privacidad por su cuenta.

Investigaciones [144][145][146] han demostrado que los usuarios promedio los cuales usan esta aplicación, no cambian sus configuraciones de seguridad y privacidad. La razón principal de este hecho, es la baja usabilidad de la interfaz de configuración de seguridad y privacidad. Por lo tanto, consideramos importante realizar una evaluación heurística con el fin de determinar el grado de seguridad usable para esta aplicación.

5.4. Evaluación con Expertos: Caso Facebook

En esta sección se presenta la aplicabilidad de la propuesta teniendo en cuenta los principios obtenidos en el Capítulo 4 y la formulación cuantitativa de evaluación, ver Sección 5.2, a través de una evaluación heurística desarrollada por expertos.

Se presenta a continuación, la información relacionada con el desarrollo de las diferentes actividades que forman parte de las etapas de planeación, ejecución y análisis de resultados a través de una evaluación heurística par la aplicación de Facebook. La información relacionada con respecto a las actividades desarrolladas ha sido tomado de Solano [51].

5.4.1. Participantes de la evaluación

Los participantes del proceso de evaluación son los siguientes:

Representante de la organización: para esta evaluación César A. Collazos de la Universidad del Cauca (Colombia), asume el rol de representante a causa de que establecer contacto con los expertos para la realización de la evaluación.

Coordinador: Paulo César Realpe de la Universidad del Cauca (Colombia), quien tiene la responsabilidad de coordinar las etapas de la evaluación.

5.4.2. Etapa de Planeación

A continuación son presentadas las actividades que hacen parte de la etapa de planeación.

5.4.2.1. Actividad 1: Definir la aplicación sobre el cual se desea obtener información.

Entregable: Aplicación sobre el cual se desea obtener información.

En este caso la aplicación bajo estudio es la red social Facebook (versión web) el cual es una red social que agrupa el mayor número de personas en el mundo con más de 1508 millones de usuarios activos según la fuente Alexa.com.

5.4.2.2. Actividad 2: Identificar los posibles expertos a participar en la evaluación.

Entregable: Lista de posibles evaluadores a participar en la evaluación de usabilidad.

El evaluador supervisor identificó y contactó un conjunto de posibles evaluadores para que participen en la evaluación heurística. Luego de establecer contacto con ellos mediante correo electrónico, fueron considerados aquellos expertos que tuvieran disponibilidad, experiencia en realizar evaluaciones heurísticas y tuvieran conocimiento en usabilidad, seguridad o ambas.

5.4.2.3. Actividad 3: Seleccionar los expertos que van a participar en la evaluación.

Entregable: Lista de evaluadores a participar en la evaluación heurística.

La información relacionada a los expertos que van a participar en la evaluación heurística es presentada en la Tabla 5.7. La evaluación heurística fue realizada por expertos con el siguiente perfil: experiencia en evaluación heurística, nivel de estudios e investigadores de distintos temas relacionados con usabilidad y seguridad. Por razones de confidencialidad, la identificación de los evaluadores no es revelada.

Tabla 5.7: Expertos participantes de la evaluación heurística.

Experto	Experiencia	Estudios	Área de investigación
Experto 1	15 años	PhD	HCI
Experto 2	2 años	Magíster	Seguridad
Experto 3	20 años	PhD	HCI
Experto 4	8 años	Magíster	HCI

5.4.2.4. Actividad 4: Identificar el conjunto de sub-heurísticas a utilizar.

Entregable: Lista de sub-heurísticas a utilizar en la evaluación.

Las sub-heurísticas a utilizar es el conjunto propuesto final presentado en la Sección 4.5. El documento guía de la evaluación contiene las sub-heurísticas a considerar durante la evaluación, dicho documento es presentado en la actividad 5.

5.4.2.5. Actividad 5: Elaborar el documento guía para la evaluación.

Entregable: Documento guía para la evaluación, el cual será entregado a los expertos.

El evaluador supervisor elaboró el documento guía que tendrán en cuenta los evaluadores durante la evaluación heurística. Dicho documento incluye información sobre el sitio

web a evaluar, procedimiento de evaluación y las sub-heurísticas a evaluar. Debido a la cantidad de sub-heurísticas, la evaluación se realizó en dos fases. La primera fase abarca las sub-herísticas de grado **S** y en una segunda fase las sub-herísticas de grado **SS** y **SSS** respectivamente. Por lo anterior, se realizaron dos documentos guías. En los Anexos F y G, son presentados los documentos guía. Por extensión en el documento, no se presenta las sub-heurísticas en la guía.

5.4.2.6. Actividad 6: Proveer a los expertos la herramienta y el documento guía de la evaluación.

Entregable: Esta actividad no tiene un entregable asociado.

En esta actividad, el coordinador proporcionó a los evaluadores expertos la presentación de la aplicación a evaluar, un archivo en MS Excel donde se encuentra las sub-heurísticas a evaluar y el documento guía de la evaluación por medio de correo electrónico.

5.4.2.7. Actividad 7: Solucionar preguntas de los expertos.

Entregable: Esta actividad no tiene un entregable asociado.

En esta actividad el coordinador solucionó preguntas de los evaluadores expertos relacionadas a la información proporcionada en la actividad 6. Durante la realización de esta actividad fue utilizado el correo electrónico para el intercambio de mensajes.

5.4.3. Etapa de Ejecución

A continuación es presentado las actividades que conforman la etapa de ejecución.

5.4.3.1. Actividad 8: Evaluación individual de la aplicación.

Entregable: Archivo MS Excel diligenciado por cada experto.

En esta actividad cada experto realiza la inspección de la aplicación de Facebook. Es importante tener en cuenta que para desarrollar esta actividad, los expertos deben tener una cuenta personal en Facebook. Los resultados de la inspección, deben ser llenados de acuerdo al un archivo en MS Excel realizado previamente por el coordinador. En la Figura 5.3 es presentado un ejemplo de la planilla en MS Excel para la evaluación con grado de importancia S.

5.4.3.2. Actividad 9: Calificación individual de las sub-heurísticas

Entregable: Calificación individual de las sub-heurísticas.

En esta actividad cada evaluador asignó calificaciones de severidad e impacto a cada sub-heurística y llenadas en el archivo MS Excel. Además, un espacio para comentarios es

USABILIDAD

1. VISIBILIAD DEL ESTADO DEL SISTEMA

No.	Sub-heurística	Descripción	Importancia	Severidad	Impacto	Comentarios
1	¿Es posible saber si el sistema es seguro?	Se debe tener herramientas que permita identificar si una aplicación posee seguridad o que el sistema determine su	S			
2	¿El usuario puede identificar el nivel de seguridad del sistema y tomar las acciones pertinentes, si es necesario?	El nivel de seguridad del sistema puede ser identificado a partir de indicadores visuales (e.g. mediante colores).	S			
3	Si hay retrasos observables en el tiempo de respuesta del sistema a una acción relacionada con la seguridad, ¿está el usuario informado de los avances del sistema?	Usualmente, un indicador de progreso podría visualizar el estado del sistema. El indicador debe proporcionar feedback que comunique de forma inmediata, clara y unívoca el estado del sistema.	S			
4	¿Hay alguna forma de realimentación para cada acción relacionada con la seguridad, cuando sea necesario?	Diferentes sistemas y niveles de seguridad deben ser visualizado de acuerdo al riesgo. Es decir, en caso en que el sistema alcance un estado de no seguridad, debe avisar de forma inmediata al usuario.	S			
5	Al observar el estado de seguridad del sistema, ¿el usuario puede decidir las alternativas para las acciones relacionadas con la seguridad, si es necesario?	A partir del nivel de seguridad del sistema, el usuario debe conocer alternativas necesarias con el fin de no poner en riesgo las acciones que se están llevando a cabo.	S			

Figura 5.3: Planilla de las sub-heurísticas USec para evaluar.

disponible para que los expertos presenten sus puntos de vista de acuerdo con la inspección. En la última hoja de la planilla, un cuadro en blanco esta disponible para realizar comentarios generales.

5.4.4. Etapa de Análisis de Resultados.

A continuación es presentado cada una de las actividades que conforman la etapa de análisis de resultados.

5.4.4.1. Actividad 10: Análisis cuantitativo.

Entregable: Promedios de las calificaciones asignadas por los evaluadores expertos.

El coordinador usó las Ecuaciones 5.2 y 5.3 para calcular el indice de seguridad usable y su impacto para la aplicación de Facebook teniendo en cuenta los datos de los expertos. Adicionalmente, fue calculada la desviación estándar de los resultados correspondientes a las calificaciones de los evaluadores.

La Tabla 5.8 presenta el nivel USec y el impacto obtenido por cada evaluador, el promedio total y la desviación estándar para el nivel USec y el impacto.

Luego de obtener los valores numéricos para el nivel de USec y el impacto realizado por los expertos, se hace la respectiva comparación con la calificación adjetiva para cada uno de los datos anteriormente encontrados. Con base en las Tablas 5.4 para el nivel USec y 5.4 para el nivel de impacto, en la Tabla 5.9 es presentado la calificación adjetiva para cada experto y el promedio total.

En la Figura 5.4 es presentado los resultados del índice de USec y el impacto. Podemos ver que el error estándar no es muy alto, lo que nos indica que la precisión de los datos es bueno y el resultado final podría ajustarse a la realidad. Sin embargo, es necesario tener

Tabla 5.8: Resultados para el índice USec y el impacto.

Experto	USec	Impacto
Experto 1	0.85	0.27
Experto 2	0.38	0.60
Experto 3	0.66	0.69
Experto 4	0.60	0.57
Promedio	**0.62**	**0.53**
Desviación	**0.19**	**0.18**

Tabla 5.9: Clasificación adjetiva para el índice USec y el impacto.

Experto	USec	Impacto
Experto 1	Bueno	Medio
Experto 2	Pobre	Alto
Experto 3	Moderado	Alto
Experto 4	Moderado	Alto
Promedio	**Moderado**	**Alto**

una mayor muestra (10 o mas expertos) para confirmar este resultado debido a la cantidad de muestras presentes en en esta evaluación ($n = 4$), con el fin de evitar sesgos estadísticos.

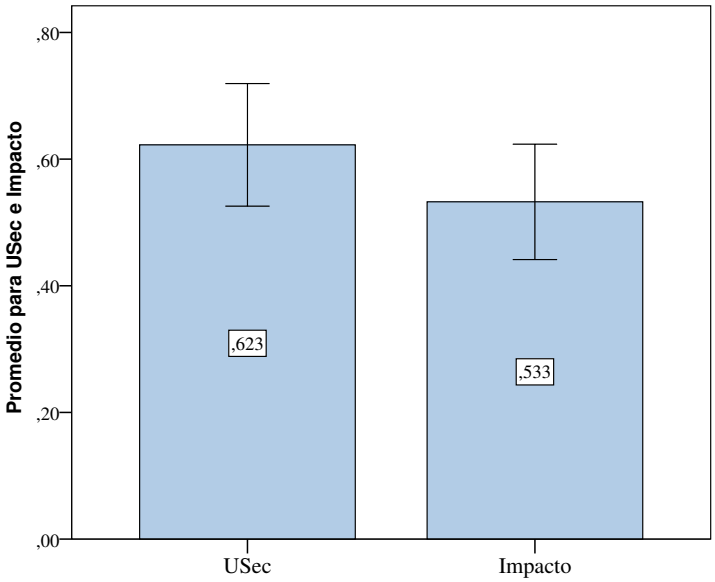


Figura 5.4: Promedios para USec y el impacto.

Una vez obtenido los resultados cuantitativo del índice USec y el impacto, podemos encontrar el riesgo de la aplicación con base en estos dos parámetros. Teniendo en cuenta el nivel USec y con base en las Tablas 5.5 y 5.6, en la Tabla 5.10 se presenta la calificación

adjetiva para la vulnerabilidad, el impacto y el resultado final para la evaluación cuantitativa y adjetiva de Facebook.

Tabla 5.10: Clasificación adjetiva para la vulnerabilidad y el impacto.

Experto	Vulnerabilidad	Impacto
Experto 1	Altamente improbable	Medio
Experto 2	Muy probable	Alto
Experto 3	Algo probable	Alto
Experto 4	Algo probable	Alto
Promedio	**Algo probable**	**Alto**

Debido a que la vulnerabilidad que presenta la aplicación y según los resultados de los expertos es "Algo probable", podemos usar este parámetro junto con la calificación adjetiva del impacto para encontrar el riesgo que puede tener la aplicación de Facebook tomando como base la Figura 5.2. En la Figura 5.5 es presentado el resultado del riesgo para esta aplicación. Según los datos obtenidos, el nivel de riesgo es "Medio".

Vulnerabilidad	Impacto			
	Bajo	Medio	Alto	Crítico
Altamente improbable	Bajo	Bajo	Bajo	Medio
Improbable	Bajo	Bajo	Medio	Medio
Algo probable	Bajo	Medio	Medio	Alto
Muy probable	Medio	Medio	Alto	Alto
Casi seguro	Madio	Alto	Alto	Crítico

Figura 5.5: Matriz de riesgo para Facebook.

Es de notar que en la Figura 5.5 el resultado del nivel de riesgo esta muy cerca de la casilla de "Alto", muchos de los usuarios que realizaron la evaluación el cual se presentara en la próxima sección, estuvieron de acuerdo con este resultado. Para ellos Facebook es una plataforma nada segura con cierto grado de vulnerabilidad para robo de identidad o ataques por medio de ingeniería social.

Ahora bien, como en esta propuesta no se tuvo en cuenta las condiciones de amenaza tal y como lo recomienda la OWASP, consideramos que si se tuviera en cuenta esta variable el resultado del nivel de riesgo habría llegado a "Alto" o inclusive a un nivel "Critico". En los medios de comunicación se presenta casos en los que existen robo de identidad, *hackeo* o manipulación de la información para esta plataforma, dando con esto un verdadero riesgo para los usuarios que usan esta aplicación. Desde nuestro conocimiento creemos que este

nivel de vulnerabilidad, impacto y riesgo esta de acorde con los parámetros establecidos en este trabajo.

5.4.4.2. Actividad 11: Análisis cualitativo.

En esta sección se presenta las opiniones sobre las sub-heurísticas propuesta para USec y autenticación. Es necesario aclarar que el objetivo de este apartado es tratar de mejorar estos principios de acuerdo a los comentarios de los expertos. Por lo tanto, no se incluirá los problemas particulares de seguridad usable que presenta la aplicación Facebook, ya que se sale del alcance de la presente investigación.

A continuación se presenta los comentarios por parte de los expertos sobre las sub-heuristicas propuestas.

- **Experto 1**:

  Flexibilidad y eficiencia de uso – Si el sistema es compatible con usuarios principiantes y expertos, ¿los niveles de los mensajes de error con respecto a la seguridad están disponibles en detalle?. – comentario del experto: *¿Esta pregunta, no debería estar en el apartado anterior?*

  Comentario general: *El primer comentario es que el listado de heurísticas es demasiado extenso. Sé perfectamente que para hacerlo bien es necesario ser muy preciso y conciso, pero si por alguna cosa han triunfado las heurísticas de Nielsen es porqué supo sintetizar en un número muy reducido lo más importante. Además, una vez acabas se tiene la sensación de que muchas cosas se han preguntado varias veces (seguro que son con matices diferentes, pero tras mas de 3 horas evaluando uno ya no sabe donde están estos matices).*

  Creo que debería tener como un proceso rápido con las cosas realmente importantes, quizás tomando solo las "S"(aun así, si sale demasiado largo quizás deberías acortar cuanto más mejor). En la parte de seguridad y desempeño creo que esta parte debería ser solo invaluable por un especialista en seguridad, se hace difícil para uno de HCI. La accesibilidad, no la he hecho debido a que tiene sus propios métodos para evaluarlo.

- **Experto 2**:

  Consistencia y estandares – Para interfaces de preguntas y respuestas sobre seguridad, ¿las entradas válidas para una cuestión están listadas?. – comentario del experto: *Si las respuestas son de más de 2 opciones sí. Si sólo cuenta con 2 opciones tiene check.*

  Seguridad – ¿Los caracteres de la clave de acceso están ocultos directamente en el campo y esta acción puede ser habilitada o deshabilitada? comentario del experto:

Si están ocultos los caracteres, pero la segunda parte de la pregunta no solo depende del sistema sino del navegador.

Comentario general: *En general Facebook presenta su interfaz gráfica sin tener en cuenta a personas con dificultades en habilidades motoras, de identificación de color, etc. Es necesario realizar esta inclusión de las personas con estas limitaciones.*

- **Experto 3**:

Comentario general: *Considerar un mayor número de sub-heurísticas en Desempeño, Fiabilidad y Operabilidad.*

- **Experto 4**:

Flexibilidad y eficiencia de uso – ¿Las indicaciones de seguridad son expresadas en sentido afirmativo? – comentario del experto: *Considero que esta pregunta es ambigua y más por el ejemplo que se cita en la descripción. Se dice se está indagando algo en sentido afirmativo y el ejemplo se plantea como pregunta.*

Seguridad – ¿Los caracteres de la clave de acceso están ocultos directamente en el campo y esta acción puede ser habilitada o deshabilitada? – comentario del experto: *Se preguntan dos aspectos que son muy distintos, deberían existir dos preguntas (una relacionada al ocultamiento de la contraseña y la otra a que si es deshabilitable o no).*

Comentario general: *Las escalas de Likert utilizadas en las métricas de evaluación, deberían tener correspondencia entre ellas, particularmente entre "Nivel de severidad" y "Nivel de impacto". Las dos características principales de una escala de Likert son: (1) expresa el grado de acuerdo con respecto a una declaración, y (2) utiliza un número impar de opciones de respuesta, lo que permite una respuesta neutral. Por lo general, la respuesta neutral está representada en el número 3. En ese sentido tomando las escalas que se han definido en el instrumento, no se podría tomar como respuesta neutral lo que han definido como "Ninguno".*

Como podemos ver, según los comentarios de los expertos, muy pocos comentarios mencionan sobre mejorar el conjunto de principios propuesto. Todos los comentarios de los expertos se encuentran en los atributos de usabilidad y seguridad. Consideramos que lo anterior se debe al poco conocimiento sobre autenticación que es parte de los demás atributos. Lo anterior confirma que el desarrollo heurístico propuesto en el Capítulo 3 es adecuado debido a que muy pocos expertos realizan comentarios de posibles mejoras.

Sin embargo, existe una incongruencia en estos comentarios. Mientras un experto asegura que el conjunto es muy extenso y puede dificultar la evaluación para una aplicación en particular, otro experto afirma que es necesario aumentar el conjunto sub-heurístico para

los atributos de desempeño, fiabilidad y operabilidad.

Según lo anterior podemos afirmar que es necesario realizar una nueva revisión del conjunto heurístico propuesto teniendo en cuenta los comentarios de los expertos, sin embargo, esta nueva revisión debería ser realizada únicamente por expertos en seguridad usable en su totalidad con el fin de evitar un posible conflicto en sus opiniones, y además establecer si es necesario acotar o incluir más sub-heurísticas para seguridad usable que puedan ser importantes.

5.4.5. Discusión

Como parte del proceso de validación de la métrica propuesta, se trata de determinar si los resultados obtenidos tras la aplicación de esta métrica, está en concordancia con investigaciones realizadas a Facebook con base en aspectos de usabilidad, seguridad y privacidad. Para ello, se presenta algunas investigaciones rescatadas de la literatura y compararlo con nuestros resultados.

Jamal & Cole [147] proponen un conjunto de 11 heurísticas teniendo en cuenta la usabilidad, seguridad y privacidad, y aplicadas a Facebook. La mayoría fueron violadas y con mayor grado con respecto a la privacidad. Los autores determinan que los usuarios no tienen control cuando realizan cualquier acción que requiera compartir información personal. Lo anterior representa un grado de riesgo en la manipulación de la información por parte de terceros.

Hoffman [148] afirma que debido al crecimiento exponencial de usuarios en la plataforma de Facebook, los desarrolladores realizan cambios en la interfaz y la configuración de las opciones de seguridad. Con todos estos cambios es difícil para un usuario realizar un seguimiento de todos los ajustes que ocurren en en su cuenta y asi evitar ataques a su perfil. Este estudio concluye que existe un riesgo latente en Facebook con respecto a la seguridad y privacidad para los usuarios, a menos que ellos tengan presente estas configuraciones a fondo y no asumir que Facebook tiene sus mejores intereses para el usuario.

Albesher & Alhussain [149] evalúan parámetros de privacidad de Facebook y determinan los riesgos asociados con las aplicaciones de terceros. Esta investigación destaca la revisión regular de la configuración de privacidad y se debe proporcionar una lista de ajustes para controlar la interacción entre los usuarios y las aplicaciones. Sobre la base de los resultados, sugirieren que Facebook tome una acción para mejorar la privacidad de los usuarios y los usuarios deben ser conscientes del riesgo que implica el uso de este sitio web de una red social.

Con base en las investigaciones anteriormente presentadas con respecto a la usabilidad y seguridad de la aplicación de Facebook, se demuestra que existe una relación directa entre esta investigación y la proporcionada por la literatura tal y como lo muestra los resultados. Todas las investigaciones con respecto al riesgo de la aplicación de Facebok presentadas

en esta sección, concuerdan en que existe un riesgo latente debido a la cantidad de características de seguridad y privacidad que posee esta aplicación y que los usuarios no pueden realizar con facilidad.

Esto nos permite concluir que el valor asignado por la métrica de seguridad usable y autenticación podría estar en concordancia con la estimación de la literatura, por tanto, esta propuesta representa un buen indicador para los desarrolladores de software. Sin embargo, incluir el parámetro de amenaza al modelo matemático propuesto es esencial con el fin de que el resultado final sea mas acorde a la realidad.

Con respecto a la evaluación heurística que realizaron los expertos, es necesario escoger los principios más acordes para esta aplicación de Facebook. Lo anterior con el fin de que dicha evaluación no se convierta en una carga adicional para los expertos y que la realización de esta evaluación sea lo mas objetiva posible.

Como se mencionó anteriormente, el conjunto heurístico para la evaluación de la aplicación de Facebook es muy grande. Para solventar este problema, se planteó la solución de enviar dos conjuntos por separados a los expertos. Primero, se envió el conjunto con las heuristicas S y después de un tiempo, se envió el conjunto con las heurísticas SS y SSS. Lo anterior con el fin de evitar la sobrecarga de trabajo para los expertos. Sin embargo, lo anterior no es la mejor solución ya que se siguen enviando el mismo número extenso de heurísticas. Creemos que la mejor opción, es proponer una metodología para USec con el fin de seleccionar las heurísticas más apropiadas de acuerdo a la aplicación a estudiar. Esta metodología puede ser basada de acuerdo al propuesto por Masip [63].

5.5. Evaluación con Usuarios: Caso Facebook

El estudio aquí presentado tiene por objetivo complementar el proceso de aplicación con usuarios, mediante la integración de actividades con las cuales se pueda obtener información sobre la usabilidad de las características de seguridad y privacidad de un sistema interactivo, en este caso es Facebook[7].

5.5.1. Justificación en la selección del sitio web

El sitio web Facebook.com se seleccionó para contrastar los resultados obtenidos de la evaluación heurística desarrollado por expertos y presentado en la sección anterior donde se presenta los resultados del nivel de seguridad usable, el impacto y el análisis de riesgo.

La Oficina de Bibliotecas y Redes de Información del Reino Unido UKOLN[8] (por sus siglas en inglés *The United Kingdom Office for Library and Information Networking.*) el cual fue un centro de especialización en gestión de la información digital, manifestó en su

[7]Disponible en: www.facebook.com
[8]Disponible en: http://www.ukoln.ac.uk/. Consultado en Enero del 2017.

momento que es necesario tener una propuesta de evaluación de riesgo para la aplicación de Facebook con el fin de analizar peligros potenciales para los usuarios y tener planes de apoyo para tales posibilidades. Con base en lo anterior es también necesario validar el análisis de riesgo presentado en esta propuesta para la plataforma de Facebook.

5.5.2. Justificación de selección del método de evaluación.

El camino más común para hacer una evaluación de usabilidad, y para nuestro caso evaluación de seguridad usable, es combinar métodos de inspección (evaluación heurística) con métodos de prueba (tareas o cuestionarios), dependiendo del escenario que se presente [51]. Los métodos de prueba tenidos en cuenta en esta sección son la ejecución de tareas y cuestionarios para los usuarios. Estos métodos de prueba fueron seleccionados debido a las ventajas que tienen cuando se realiza una evaluación de usabilidad, es decir, su bajo costo, la cantidad de tiempo para ser llevado a cabo y los recursos disponibles.

Además de lo anterior, algunos trabajos de investigación [149][148][143] recomiendan realizar tareas para los usuarios con el fin de determinar la ejecución exitosa o no de las características de seguridad y privacidad para Facebook. Con este análisis de las tareas podríamos confirmar que las cuestiones de seguridad de las aplicaciones, no representan un objetivo principal para los usuarios.

Lo anterior no significa que no se puedan tener en cuenta otros métodos de evaluación, simplemente debido al enfoque de esta investigación y con el fin de tener un orden en los métodos de evaluación seleccionados en este capítulo, se decide tener en cuenta y analizar la ejecución de tareas y cuestionarios para los usuarios.

Se presenta a continuación información relacionada con el desarrollo de las diferentes actividades que forman parte de las etapas de planeación, ejecución y análisis de resultados a partir de un analisis de tareas y las actividades propuestas para cada una de las fases. La información relacionada con las actividades desarrolladas ha sido tomado de Solano [51].

5.5.3. Etapa de Planeación

A continuación son presentadas las actividades que hacen parte de la etapa de planeación.

5.5.3.1. Actividad 1: Definir la aplicación sobre el cual se desea obtener información

Entregable: Aplicación sobre el cual se desea obtener información.

En este caso la aplicación bajo estudio es Facebook el cual es una red social que agrupa el mayor número de personas en el mundo con más de 1508 millones de usuarios activos

según la fuente Alexa.com.

5.5.3.2. Actividad 2: Definir demografía de los participantes

Entregable: Especificación de los perfiles de usuario a los cuales están dirigidas las tareas a evaluar.

La demografía de los 10 participantes del estudio se presenta en la Tabla 5.11. A los participantes se les dio un formulario de consentimiento para realizar el experimento, Ver Anexo H. Nuestra población incluyó 6 (60 %) hombres y 4 mujeres (40 %). Las edades variaron de 27 a 58 años, con una edad media de 37 y una desviación estándar de 9.09. Todos son usuarios regulares de Internet y con estudios universitarios completados o en curso. Cada uno de ellos fue convocado individualmente. Además, se realizó una encuesta preliminar para cada usuario sobre la seguridad y privacidad de facebook e Internet, ver Anexo I.

Tabla 5.11: Demografía de los participantes.

Genero	Masculino: 6 Femenino: 4
Escolaridad	Universitario: 2 Especialización: 2 Maestría: 5 Doctorado: 1
Uso de Internet	Mas de una vez al día: 7 Permanece conectado: 3
Uso de Facebook	Varias veces al día: 5 Una vez al día: 5
Otras redes sociales	Whatsapp: 10 Twitter: 5 Linkdl: 4
Cambio de configuración seguridad y privacidad	Si: 7 No: 3
Preocupación por seguridad de Facebook	Si: 9 No: 1

5.5.3.3. Actividad 3: Definir el escenario en el que se van a realizar las tareas

Entregable: Especificación del escenario en el que se van a realizar las tareas. El evaluador supervisor definió el siguiente escenario para que sea considerado por los usuarios al momento de realizar las tareas:

Usted está interesado en usar la red internet para conocer personas y compartir sus experiencias vividas. Alguien conocido le proporciona información sobre posibles redes sociales

que se encuentran en la red de forma gratuita y le sugiere crear una cuenta en Facebook con el seudónimo de "Felicito Buendía". A usted le gustaría saber si esta red social se acomoda a sus necesidades, que proteja su información personal y sea fácil de usar.

5.5.3.4. Actividad 4: Definir tareas a realizar

Entregable: Definir las tareas que se van a realizar tareas.

Se propuso una serie de tareas para la aplicación. En total, cada usuario debe realizar 7. Estas tareas se obtuvieron teniendo en cuenta la usabilidad de las características de seguridad y privacidad para Facebook por experiencia propia y los propuestos por Paul et al. [143]. La Tabla 5.12 muestra las tareas que cada usuario tiene que realizar para la aplicación.

Tabla 5.12: Tareas a realizar en el sitio web Facebook.com

Tareas
Tarea 1. Cambiar la contraseña actual.
Tarea 2. Determinar qué atributos de su perfil son visibles para las demás personas.
Tarea 3. Averiguar, para quién o quienes el atributo "cumpleaños" es visible.
Tarea 4. Cambie la configuración de privacidad del álbum de fotos "Mi álbum" para que sea visible solo para su amiga "Maritza Rodríguez".
Tarea 5. Activa las alertas cuando se inicie sesión desde un navegador desconocido.
Tarea 6. Cambiar del estado "Amigo" al estado "Con acceso restringido" a su contacto "Irene Delgado".
Tarea 7. Bloquee los mensajes para su amiga "Bety Ramos".

5.5.3.5. Actividad 5: Elaborar el documento guía que será entregado a los usuarios durante la realización del experimento.

Entregable: Documento guía para los usuarios que participan en el experimento.

Este documento guía incluye información sobre el escenario bajo consideración, las tareas a realizar y los cuestionarios pre-test y post-test. En el Anexo I es presentado este documento guía.

5.5.3.6. Actividad 6: Definir métricas

Entregable: Se definen las métricas para la realización del experimento.

Las métricas que se tendran en cuenta y con base en trabajos relacionados [65][64][143], las métricas para este estudio son:

1. **Éxito de la tarea**: la eficacia con que los usuarios pueden completar un conjunto de tareas determinado.

2. **Tiempo de la tarea**: cuánto tiempo se requiere para completar una tarea

3. **Satisfacción de la tarea**: Después de que los usuarios intenten una tarea, responden una pregunta sobre cuán difícil fue la tarea.

5.5.3.7. Actividad 7: Decidir el medio a utilizar para el registro del experimento.

Entregable: Especificación del medio a utilizar para el registro de las tareas.

El coordinador decidió que para el registro de las tareas se utilizará la herramienta software Morae[9] con el fin de registrar los tiempos de las tareas de una forma más precisa.

5.5.3.8. Actividad 8: Elegir el lugar más adecuado para realizar el experimento.

Entregable: Especificación del lugar más adecuado para hacer las pruebas.

El lugar para realizar las pruebas se buscó que fuera silencioso y sin mayores distracciones para los usuarios participantes. Se escogió una de las salas de cómputo del Departamento de Sistemas de la Universidad del Cauca, en este caso la sala de doctorado, por encontrarse en buenas condiciones que permitieran el desarrollo adecuado del experimento.

5.5.3.9. Actividad 9: Realizar una prueba piloto del experimento.

Entregable: Especificación del tiempo empleado por cada usuario para realizar el experimento.

La prueba piloto del experimento fue realizado por un estudiante de pregrado de la Universidad del Cauca. Se determinó que para realizar el conjunto de tareas propuesto toma aproximadamente 11 minutos. Es importante tener presente que el usuario que participó en la prueba piloto, no hace parte de los 10 usuarios que se establecieron en la Actividad 2.

5.5.4. Etapa de Ejecución

A continuación es presentado cada una de las actividades que conforman la etapa de ejecución.

5.5.4.1. Actividad 10: El coordinador del experimento presenta la prueba

Entregable: Esta actividad no tiene un entregable asociado.

[9]Disponible en: http://www.techsmith.com/morae.html

Para el desarrollo del experimento se citó a cada usuario a la sala de doctorado. Después, el coordinador realizaba la presentación del experimento, comentando al usuario que debe realizar las tareas indicadas en el documento guía y diligenciar los cuestionarios, ver Anexo I. Adicionalmente, antes de iniciar el experimento el usuario firma el respectivo acuerdo de confidencialidad, ver Anexo H, donde el usuario aprueba su consentimiento para ser monitoreado.

5.5.4.2. Actividad 11: Realización de tareas y cuestionarios.

Entregable: Registro de tiempo del experimento. Cuestionarios diligenciados.

Una vez el usuario era informado sobre el experimento, comienza a realizar las tareas indicadas en el documento guía y completar los cuestionarios una vez haya terminador de ejecutar todas y cada una de las tareas presentadas. El registro del tiempo se lleva a cabo usando el programa Morae.

5.5.4.3. Actividad 12: Realizar preguntas adicionales a los usuarios.

Entregable: Comentarios adicionales por parte de los usuarios.

Al finalizar la prueba, el coordinador de la prueba realiza preguntas adicionales al usuario con el fin de complementar la información recolectada.

5.5.5. Etapa de Análisis de resultados

A continuación es presentado cada una de las actividades que conforman la etapa análisis de resultados.

5.5.5.1. Actividad 13: Análisis cuantitativo

A partir de las tareas presentadas en la Tabla 5.12, el coordinador del experimento calculó los porcentajes de las tareas exitosas asociadas, el tiempo promedio que los usuarios tardaron en realizar cada una de las tareas y el tiempo total de cada usuario en completar todas las tareas. En la Figura 5.6 es presentado la distribución de éxito de las tareas asociadas.

Como podemos observar en la Figura 5.6, la mayoría de las tareas presentan un pequeño grado de éxito. Con lo anterior podemos confirmar y asegurar que para los usuarios, los temas de seguridad y privacidad en las aplicaciones como es el caso de las redes sociales o podría también ocurrir para cualquier otra aplicación, pasan a un segundo plano u objetivo. Lo anterior puede ser algo muy serio, por que si no tenemos en cuenta estas consideraciones el riesgo a que nos enfrentamos por robo de identidad representa una seria amenaza para nuestra integridad.

Algo que si es preocupante en estos resultados es que lo usuarios que realizaron la prueba no saben lo que otras personas ven sobre su perfil (Tarea 2), 9 usuarios no pudieron

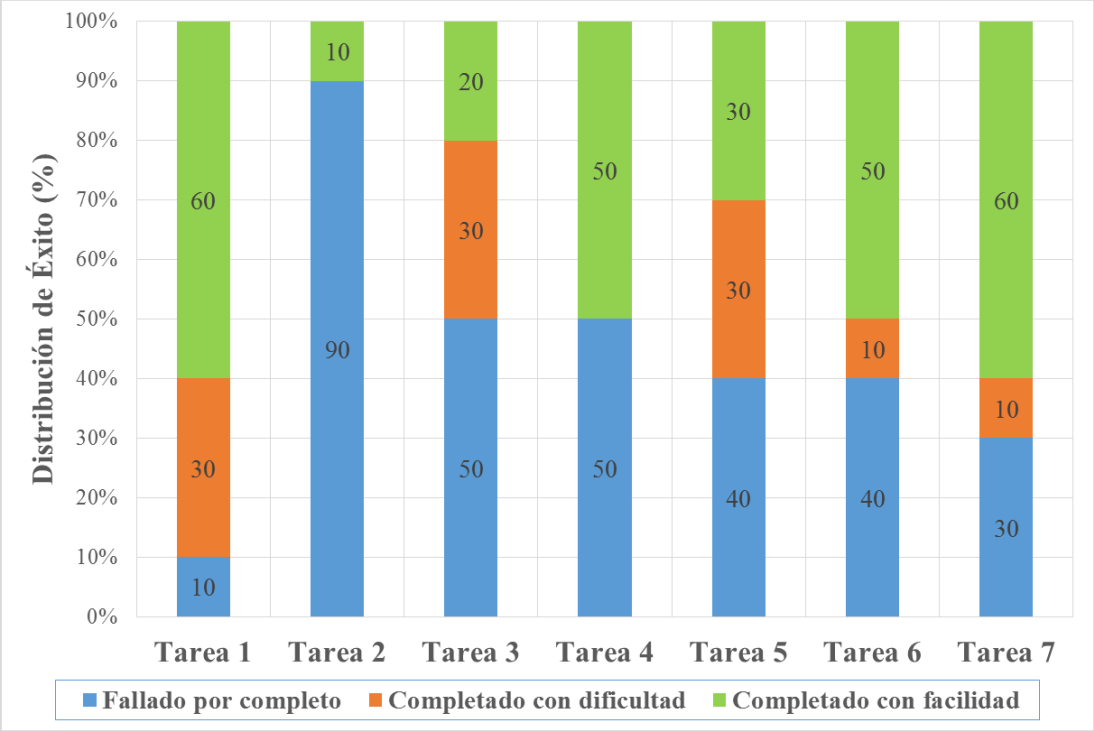


Figura 5.6: Distribución de éxito.

completar la tarea donde se les solicito averiguar qué atributos de su perfil son visibles para las demás personas. Publicar información sin tener presente este aspecto puede tener serias consecuencias, por ejemplo, algunas personas se pueden aprovechar para comerte algún ilícito (e.g. llamadas extorsivas) con base en el perfil de las personas. Al finalizar la prueba, la mayoría de los usuarios se sintieron un poco preocupados por no saber que es lo que otros ven sobre su perfil y decidieron poner mas atención a este tema.

Con base a las otras tareas, la tarea de cambio de contraseña fue la que más taza de éxito tuvo con respecto a las demás tareas. Este cambio de contraseña parece que si es frecuente realizar por la mayoría de los usuarios que usan esta red social. Además, las configuraciones de privacidad y bloqueo que los usuarios pueden realizar a sus contactos tienen aproximadamente un 50 % de taza de éxito. Lo anterior también demuestra que estas tareas son realizadas por algunos usuarios.

En la Figura 5.7 es presentado el tiempo promedio de los usuarios parar realizar cada una de las tareas según la Tabla 5.12. En la Figura 5.8 se presenta el tiempo total que emplea cada usuario en completar todas las tareas.

En la Figura 5.7 podemos ver que el promedio para realizar las tareas es de aproximadamente 2 minutos por tarea. La tarea 2 es la que presenta un gran tiempo para realizarla. Como se comentó en párrafos anteriores, este tiempo tan largo (en comparación con los demás usuarios) es debido a que a los usuarios se les dificultó encontrar el lugar para cono-

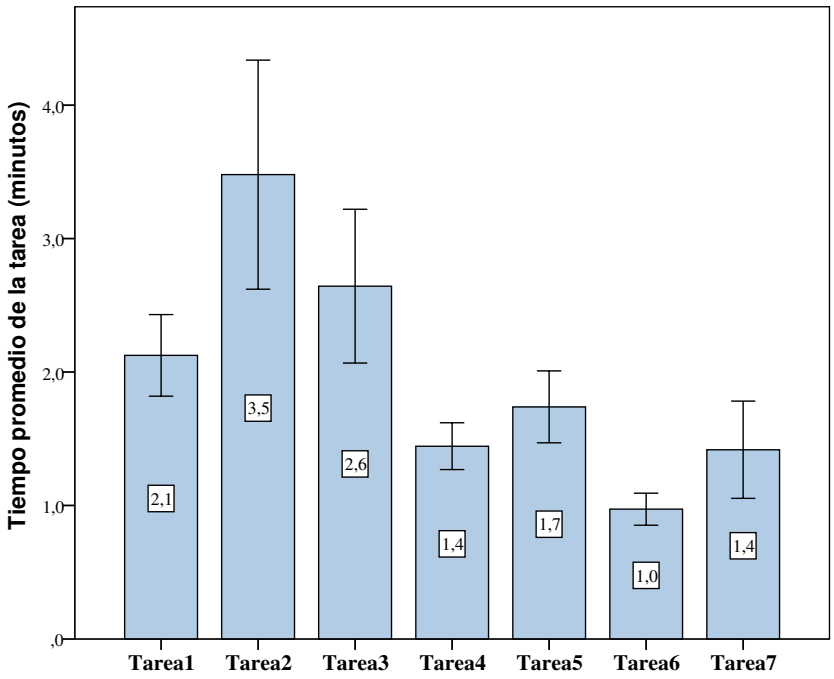


Figura 5.7: Tiempo para realizar las tareas.

cer que es lo que otras personas ven del perfil del usuario. Cuando los usuarios empezaron a realizar esta tarea, algunos de ellos experimentaban cierto grado de ansiedad por no conocer algo que parecía tan obvio. Igual para la tarea 3, se demoraron en completar esta actividad ya que es parte de la tarea 2.

Estos tiempos, que podrían ser un poco altos, ratifican aun más que realizar tareas donde se presente aspectos de seguridad y privacidad, representan cierto grado de complejidad para los usuarios presentando en algunos casos abandono a la hora de realizar dicha tarea. Lo anterior podría tener serias consecuencias si se omite estas características de configuración (e.g. mayor riesgo de robo de identidad).

En la Figura 5.8 se puede observar que 2 usuarios que realizaron la prueba se tardaron mas del promedio a la prueba piloto y a los demás usuarios, 11 minutos aproximadamente. La razón de esta demora surge en que se enfocaron en realizar con éxito la tarea 2, sin embargo, no tuvieron éxito en completarla y desistieron en su realización.

Una vez finalizado las tareas por parte del usuario, se preguntó sobre el nivel de dificultad para realizar cada una de las tareas. Se configuró el software Morae para que cuando haya finalizado todas las tareas seleccionaran el grado de dificultad. El usuario puede escoger el grado de dificultad a partir de una lista de 5 opciones (escala tipo Likert):

1. Muy difícil
2. Difícil

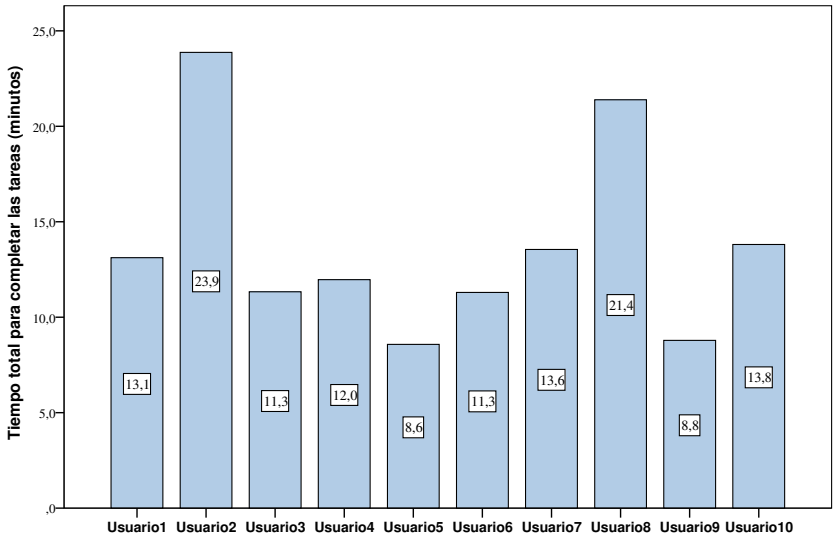


Figura 5.8: Tiempo total para realizar las tareas por cada usuario.

3. Neutral
4. Fácil
5. Muy Fácil

En la Tabla 5.13 es presentado los resultados del nivel de dificultad para realizar las tareas. Como podemos observar la mayoría de los usuarios presentan un cierto grado de indiferencia sobre la dificultad para realizar las tareas. Sin embargo, esta indiferencia podría conllevar a que los usuarios consideren cierto grado de dificultad realizar tareas de seguridad y privacidad para la aplicación de Facebook tal y como se presentó en la Figura 5.6.

Tabla 5.13: Nivel de dificultad de las tareas.

Tarea	Nota Menor	Promedio	Desviación estándar	Nota Mayor
Tarea 1	1	4.1	1.19	5
Tarea 2	1	2.2	1.13	4
Tarea 3	1	3.0	1.82	5
Tarea 4	1	3.1	1.91	5
Tarea 5	1	2.8	1.39	5
Tarea 6	1	3.1	1.52	5
Tarea 7	1	3.4	1.57	5

Después de completar las tareas y diligenciar el nivel de dificultad para cada tarea, el coordinador de la prueba entregó al cada usuario un cuestionario para que respondieran una serie de 13 preguntas sobre la aplicación, donde también se pregunta la percepción de

seguridad y privacidad que ella le ofrece la aplicación (ver Anexo I). Además, se realiza 2 preguntas abiertas de acuerdo con el grado de satisfacción de la aplicación con base en la usabilidad, seguridad y privacidad de la aplicación.

Para cada una de las 13 preguntas de selección múltiple con única respuesta sera utilizado la escala de tipo Likert (1-5). El significado de las opciones para las respuestas han sido creados para que la nota mínima (1) corresponda a una evaluación que reprueba o califica de mala manera lo que se está preguntando, mientras que la nota máxima (5) corresponde a una aprobación o que la pregunta está siendo calificada positivamente. Las preguntas de este tipo intentan obtener información acerca de la impresión de los usuarios acerca del sistema en evaluación [51].

Para las 2 preguntas abiertas, el coordinador de la prueba le pide a los usuarios que diligencien sobre el qué fue lo que más le gustó y disgustó de la aplicación. Este nivel de satisfacción corresponde a evaluar los atributos de usabilidad, seguridad y privacidad que posee la aplicación de Facebook.

A partir del diligenciamiento de los cuestionarios post-test, el coordinador calculó el promedio de las respuestas de los usuarios utilizando la herramienta MS Excel. La Tabla 5.14 presenta los promedios y la desviación estandard de las respuestas de los usuarios.

Se puede observar en la Tabla 5.14 que las calificaciones más bajas están en que los participantes no pudieron completar con satisfacción las tareas y que desconfían en el nivel de seguridad y privacidad que la aplicación ofrece. Esto puede confirmar los resultados del nivel de riesgo encontrado cuantitativamente. Puede verse que la satisfacción de los usuarios con respecto a temas de seguridad de la aplicación no es la adecuada, los usuarios solo quieren usar la aplicación de Facebook para lo que fue creado y no preocuparse en temas de seguridad porque según ellos, “confian” en que la aplicación debe ocuparse de esos detalles.

Con respecto a las calificaciones más altas se encuentra que los usuarios volverían a utilizar la aplicación, aun conociendo los riesgos de seguridad y privacidad que esta posee, y que las opciones que la aplicación ofrece son fáciles de usar. Lo anterior podría tener una explicación, los usuarios han usado tantas veces Facebook que prácticamente conocen todas estas opciones (e.g. enviar mensajes, añadir contactos, publicar información, etc.), excepto las que tienen que ver con opciones de seguridad y privacidad.

5.5.5.2. Actividad 14: Análisis cualitativo

Con base en las respuestas a lo que más les gustó a los usuarios y algunos comentarios de ellos, es de notar que algunos de ellos quedaron sorprendidos por la cantidad de opciones de seguridad y privacidad que ofrece la aplicación, algunos usuarios no sabían que estas opciones existían pues no se habían dado a la tarea de revisar a profundidad la aplicación, aunque sea de uso frecuente.

Tabla 5.14: Promedio de respuestas de los cuestionarios.

Pregunta	Nota Menor	Promedio	Desviación estándar	Nota Mayor
¿Pudo completar las tareas?	1	2.7	1.05	4
¿La aplicación fue fácil de usar?	1	3.1	1.28	5
¿Soy capaz de aprender a utilizar las opciones ofrecidas por la aplicación?	1	4.1	1.19	5
¿Considera que la información requerida en la prueba ha sido fácil de encontrar?	1	2.9	1.37	5
¿Considera que la información disponible en la aplicación es completa (suficiente)?	2	3.1	1.1	5
¿Confía en la integridad, confiabilidad y disponibilidad de la información que ha suministrado?	1	2.7	1.33	5
Usted califica el grado de satisfacción en el uso de la aplicación como:	1	2.8	1.31	5
¿El diseño de la aplicación fue consistente?	2	3.1	1.10	5
La disposición de la información en la aplicación es:	2	2.6	0.96	5
¿La aplicación le inspira confianza con respecto a la privacidad que le podría brindar a su información personal?	1	2.5	1.08	4
¿Volvería a utilizar la aplicación?	1	3.7	1.06	5
¿En comparación con otras redes sociales, la experiencia con esta aplicación le ha parecido?	2	3.2	0.63	4
¿Cómo evalúa la experiencia como colaborador en esta prueba?	2	3.9	1.1	4

A continuación se presenta algunas de las respuestas de los usuarios a la pregunta, ¿qué fue lo que más le gustó de la aplicación con base a su usabilidad, seguridad y privacidad?

"*...que van inventando mas opciones de seguridad y privacidad*".
"*...ofrece diversas opciones de configuración, lo cual brinda un rango mas amplio de preferencias con respecto a la seguridad y privacidad. Con respecto a la usabiliad, la aplicación cuenta con parámetros aceptables relacionados a este atributo*".
"*...aunque es fácil de usar y configurar la seguridad, desconfío a que funcione el 100 %*".
"*...la posibilidad de crear diferentes perfiles par mi información*".
"*...brinda la posibilidad de manejar la privaciadad aunque es necesario buscar las opciones de manera cuidadosa*".
"*...ofrece mucha flexibilidad para el usuario porque configura y personaliza lo que considere apropiado*".

"*...la aplicación ofrece configurar las opciones de perfil para que otras personas vean lo que quiero*".
"*...soy capaz de usar el facebook*".
"*...opciones para personalizar la manera en que quiero que se publique mi información*".

Sin embargo, no todo fue bueno en la parte de usabilidad para la aplicación, gran parte de los problemas que se encontró fue en la parte de configuraciones de seguridad y privacidad que ofrece la aplicación. Cuando se realizaban las tareas, los usuarios mostraban signos de intranquilidad, debido a que pensaban que la aplicación era intuitiva como lo comentaron varios usuarios. Un usuario comento, "*quedé impresionado por lo que tiene Facebook con respecto a su seguridad, no pensé que esto existía pues lo único que hacia era publicar y ver información de otras personas sin darme cuenta lo serio que puede ser esto si se descuida estos temas de seguridad*".

A continuación se presenta algunas de las respuestas de los usuarios a la pregunta, ¿qué fue lo que más le disgustó de la aplicación con base a su usabilidad, seguridad y privacidad?

"*...la forma de configurar la privacidad, es difícil, no es clara y deben de hacerse al crear la cuenta y no después.*".
"*...algunas de las opciones relacionadas a las actividades de la prueba no son tan intuitivos como se esperaba*".
"*...no saber con seguridad que ven los contactos*".
"*...las opciones de cambio de configuración parecen estar muy escondidos para el usuario.*".
"*...la configuración de seguridad y privacidad es confusa y con poca información para realizarlo.*".
"*...no es intuitiva, fue imposible realizar una de las tareas.*".
"*...algunas configuraciones de privacidad y seguridad es confuso*".
"*...no sé realizar correctamente las opciones de configuración de seguridad*".
"*...tiene información poco clara, lo mas fácil es la configuración de seguridad (contraseña)*".
"*...la búsqueda para personalizar y configurar la cuenta resulta confuso*".

A partir de estos comentarios negativos por parte de la aplicación, podemos resaltar que casi todas de ellas son enfocadas a los aspectos de seguridad y privacidad tal como era nuestro objetivo, aunque también se había preguntado sobre aspectos de usabilidad. Lo anterior demuestra la importancia de aplicar los principios de seguridad usable obtenidos en esta tesis con el fin de mejorar estas características se seguridad y sea más intuitiva para los usuarios.

5.5.5.3. Actividad 15: Realizar recomendaciones para dar solución a los problemas de seguridad usable.

Entregable: Recomendaciones.

No se realiza esta actividad porque no está en el alcance de la presente investigación.

5.5.5.4. Actividad 16: Elaborar el informe final de la evaluación.

Entregable: Informe final

No se realiza esta actividad porque no está en el alcance de la presente investigación.

5.5.6. Discusión

Analizando las tareas desarrolladas por los usuarios y la interfaz existente, se identifican varias deficiencias con respecto a las opciones de configuración de seguridad y privacidad, que suponemos es el resultado de un exceso de información mal distribuida y poco clara, lo que lleva a la conclusión de que los usuarios experimentan problemas al ajustar correctamente estas configuraciones.

De acuerdo a nuestro estudio, se podría decir que la seguridad y privacidad debe verse como una característica general de los sistemas interactivos y que una interfaz pobre en este aspecto, podría filtra información personal llevando con esto afectar la reputación del sistema interactivo y de sus usuarios. Aunque Facebook tiene este inconveniente, poca importancia se le dá y los usuarios lo siguen usando sin darse cuenta de las grandes falencias que esta aplicación posee.

Los diseñadores de estas redes sociales deben ser conscientes de la sensibilidad de la información que los usuarios diariamente publican en estas aplicaciones. Específicamente, necesitan tener una mejor visión del contexto social y su interacción. También necesitan adherirse al contexto técnico de la información en la red (e.g. ¿cómo los usuarios comparten información y quién tiene el control?). Los resultados de este estudio sugiere que los usuarios prefieren mantener el control sobre el tipo y la naturaleza de la información compartida pero obviando algunas características que le ayudarían a aumentar ese control.

Por último, los medios de comunicación (televisión, prensa, radio, etc.) han jugado un papel importante no sólo para concienciar a los usuarios sobre los riesgos asociados con su información en las aplicaciones de redes sociales, sino también para obligar a los desarrolladores a mejorar las características de seguridad y privacidad para que estas características sean mas fáciles de usar en este tipo de aplicaciones.

5.6. Evaluación con Expertos: Caso E-Banking

En esta sección se presenta el desarrollo y los resultados de una evaluación heurística aplicada a sistemas de e-banking realizada por Gómez & Daza [150], y dirigido por el autor de esta tesis doctoral, usando algunos los principios encontrados en el Capítulo 4 y planteando un modelo matemático para obtener una correlación entre usabilidad y seguridad con el fin de obtener un nivel de *trade-off* de estos atributos para una aplicación en cuestión.

Debido a que el documento de la evaluación es muy extenso, solo se explicará en esta sección los aspectos más relevantes de este trabajo, donde se concluye que los principios obtenidos en este trabajo, tienen un alto grado de aplicabilidad con base en algunos requerimientos fundamentales de e-banking encontrados en la literatura. Las consideraciones presentadas a continuación son tomadas de Gómez & Daza [150].

5.6.1. Justificación para la Evaluación

El sector bancario ha sido de las industrias que más ha aprovechado la red Internet como canal de distribución de sus productos o servicios. Sin embargo, a pesar de los beneficios que brinda el e-banking, los usuarios no lo han utilizado como se esperaba, en algunos casos se argumenta la falta de entusiasmo o más importante, la clasificación como una zona de alto riesgo con un potencial de pérdidas económicas considerables. Ésta característica convierte a la seguridad en una preocupación primordial, además, debido a la existencia de una gran variedad de usuarios y a la ausencia de entrenamiento, la usabilidad es igual de preocupante.

Teniendo en cuenta la necesidad de que los sistemas e-banking deben ser seguros y usables, es importante conocer qué principios permiten contribuir con la evaluación de estos sistemas. Estos principios deben favorecer en la integración de los aspectos que implican la seguridad y usabilidad.

De acuerdo con lo anterior, el problema de este estudio se centra en el planteamiento de un conjunto de principios partiendo de una revisión sistemática pertinente para los sistemas e-banking, y proponiendo un modelo matemático con el fin de realizar una evaluación cuantitativa y obtener un *trade-off* entre usabilidad y seguridad.

5.6.2. Desarrollo

Es indispensable centrarse en los aspectos importantes del entorno en el que se desarrolla este trabajo. Los sistemas e-banking presentan características y requerimientos básicos para el buen manejo de sus portales. Para obtener estos requerimientos se hace una extensa revisión de la literatura, se analizan y se comparan con las sub-heurísticas presentadas en el Capitulo 4.

Entre las características mas importantes podemos mencionar:

1. *Clientes o usuarios*: La primera característica que debe ser tenido en cuenta es quiénes van a usar la aplicación, es decir los clientes.

2. *Tareas*: Identificar las tareas mas representativas cuando hacen uso de los servicios en linea que ofrece el banco (e.g. autenticación, realizar transferencias o pagos, ver saldo o movimientos, etc.).

3. *Seguridad y confianza*: Presentar una aplicación que permita a los clientes sentir una percepción de seguridad y confianza para realizar las tareas anteriores. Esto incrementa la calidad de la aplicación y evita que los clientes deban trasladarse a las instalaciones físicamente.

4. *Aspectos técnicos*: Se debe tener aspectos técnicos como cifrado de datos, configuración de la red, disponibilidad y servicios contra perdida de datos.

Una vez realizada la especificación de las características de un sistema e-Banking, junto con la revisión de la literatura, se logra recolectar alrededor de 59 requerimientos, tanto funcionales como no funcionales para estos sistemas, y tras una minuciosa revisión se logran identificar y filtrar los requerimientos más relevantes e indispensables. Como ejemplo de los requerimientos encontrados, podemos citar algunos de ellos:

1. El sistema debe establecer una sesión segura entre la máquina del cliente y el servidor del banco, con cifrado de datos.

2. El sistema debe bloquear a los usuarios que superen el máximo número de intentos con la clave incorrecta.

3. La sección de ayuda relevante debe proporcionar explicaciones de las medidas empleadas para garantizar la seguridad.

4. Las medidas de seguridad implementadas por el sistema no deben ser excesivas ni molestas (contraseñas demasiado largas, varios códigos de acceso, preguntas de seguridad demasiado complejas, etc.).

5. Proporcionar autenticación usable (OTP, Tokens, Biométrica, Multi-factor).

6. Las interfaces de usuario deben presentar y destacar la información relevante en el contexto y en el momento correcto.

Por medio de la lista de requerimientos, es posible analizar los diversos artefactos con los que debe contar un sistema e-banking, es claro que existen muchos más, pero este estudio ha considerado aquellos requerimientos que permiten al usuario y entidad bancaria percibir en gran medida la seguridad y la usabilidad del sistema. En este orden, surge la necesidad de verificar el grado de cumplimiento de cada uno de ellos para un estudio de caso en particular, por lo tanto, es necesario recurrir a un conjunto de sub-heurísticas que

permitan la evaluación de los aspectos de seguridad y usabilidad.

Una vez recopilados los requerimientos y el conjunto de sub-heurísticas, ver Sección 4.5, se procede a establecer una relación justificada entre ambos a partir del contexto de uso y otras definiciones rescatadas de la literatura, con el fin de determinar las sub-heurísticas que corresponden a cada requerimiento. También se considera la escala de importancia presentada en la Sección 4.1 para cada sub-heurística, la cual será tenida en cuenta en el modelo matemático propuesto.

Antes de llevar a cabo la evaluación fue necesario preparar los aspectos que se deben considerar en el proceso de evaluación heurística. El primero de ellos, determinar una importancia adjetiva y numérica con la que se califique el cumplimiento de las sub-heurísticas, luego determinar el porcentaje de influencia de los atributos (seguridad y usabilidad) para cada requerimiento. Finalmente, se puede construir el formulario de evaluación que los expertos deberán diligenciar según la aplicación seleccionada.

Luego de establecer todo lo anterior, se presentan los elementos del modelo matemático para evaluar los componentes de usabilidad y seguridad para un sistema de e-Banking, el cual surge a través del método de observación empírica con el cual se logra establecer los diversos atributos (usabilidad y seguridad) que intervienen para lograr el cálculo del valor de seguridad usable.

Se tiene como punto de partida el conjunto de sub-heurísticas, requerimientos y una escala de clasificación obtenidos de la literatura, seguidamente se hace uso de la representación vectorial con lo cual, utilizando los conceptos de producto punto y distancia euclidiana se logran establecer las fórmulas y mecanismos que integren los aspectos de seguridad y usabilidad, generando como resultado una pauta formal que permite evaluar estos aspectos de forma conjunta en el ámbito de e-banking.

El modelo matemático propuesto esta representado en la Ecuación 5.5

$$Usec = \left(\sum_{i=1}^{n} U + \sum_{i=1}^{n} S \right) * (1 - D_e) \tag{5.5}$$

Donde,

$\sum U$ son los valores calificados por el experto en las sub-heurísticas correspondientes al atributo usabilidad.
$\sum S$ son los valores calificados por el auditor en las sub-heurísticas correspondientes al atributo seguridad.
D_e es la distancia euclidiana normalizada teniendo en cuenta el mayor valor de calificación.

La expresión matemática queda sujeta al método de observación empírica, base fundamental para la construcción del modelo matemático. Es importante destacar que esta

expresión puede ser adaptada según los parámetros (escalas de evaluación) que se consideren en futuros trabajos. Para reflejar el resultado de la *USec* (cuyo resultado esta entre 0 y 200), es necesario trabajar en la construcción de una escala cualitativa y cuantitativa, donde se refleja el intervalo donde se encuentra resultado de la Ecuación 5.5 y su respectiva calificación cualitativa. En la Tabla 5.15 es presentada esta escala.

Tabla 5.15: Escala USec (Tomado de [150])

Rango	Calificación cualitativa
[0 – 40)	**Catástrofe**: El potencial de impacto es SEVERO, por lo tanto, es imperativo solucionar los problemas que se presentan de manera inmediata.
[40 – 80)	**Violación Mayor**: El potencial de impacto es ALTO, por lo tanto, es importante solucionar los problemas dándole una prioridad alta.
[80 – 120)	**Violación Moderada**: El potencial de impacto es MODERADO, por lo tanto, los problemas que se presenten pueden ser solucionados dándoles una prioridad media.
[120 – 160)	**Violación Menor**: El potencial de impacto es BAJO, por lo tanto, los problemas que se presenten pueden ser solucionados dándoles una prioridad baja.
[160 – 200]	**Violación Insignificante**: El potencial de impacto es MUY BAJO, los inconvenientes que se presenten pueden ser solucionados dándoles una prioridad muy baja.

5.6.3. Resultados

Desde el inicio de este estudio, se ha proyectado que los artefactos que se desarrollen deben ser contrastados con la realidad. Con el propósito de generar un impacto positivo en el campo de la investigación referente a los atributos de seguridad y usabilidad, por esta razón, los contenidos que han sido desarrollados (ver sección anterior), son validados mediante una aplicación real que contempla una plataforma e-Banking de una entidad financiera.

Inicialmente, se consideró trabajar con plataformas de entidades bancarias colombianas, pues en estas se podrían identificar los requerimientos de un sistema e-Banking. La idea fue rápidamente descartada, debido a la dificultad que se presentaba al encontrar expertos y usuarios que pertenecieran a la misma entidad bancaria.

Para solucionar el inconveniente anterior, la Universidad del Cauca cuenta con una entidad financiera llamada Fondo de Profesores de la Universidad del Cauca – FONDUC[10]. Se estableció un puente de comunicación a través del Grupo de Investigación y Desarrollo en Ingeniería de Software – IDIS y la gerencia de la entidad FONDUC. Luego, la gerencia, decidió citar a los implicados del estudio a una reunión presencial, la cual resultó con el

[10]Disponible en: www.fonduc.com.co. Consultado en Septiembre de 2016.

acuerdo de las partes para llevar a cabo el proceso referente al estudio de caso.

A través de este mutuo acuerdo, fue posible despejar la preocupación de encontrar expertos y usuarios que pertenecieran a la misma entidad, ya que todos los actores implicados en este estudio estarían vinculados a la entidad.

Una vez solucionado lo anterior, se evalúa la aplicación a través método de evaluación heurística que ha sido determinado a través de la literatura y que permite evidenciar las ventajas de este método, destacando su rápida aplicabilidad y bajos costos operacionales. La evaluación heurística contó con una duración de dos (2) a tres (3) horas, ya que los expertos necesitaban analizar detenidamente cada uno de los 23 requerimientos expuestos y paralelamente identificarlos en la plataforma del FONDUC, además, debían calificar los atributos de seguridad y usabilidad según las sub-heurísticas asociadas a cada requerimiento.

Cuando se llevan a cabo una evaluación heurística de un sitio web, un número de tres a cinco expertos es suficiente, pero este número puede ser incrementado si la usabilidad es un criterio prioritario a evaluar. Para este estudio se busca evaluar seguridad y usabilidad en conjunto por lo cual se opta por solicitar la colaboración de sólo tres de ellos (2 expertos en usabilidad y 1 en seguridad informática).

Una vez realizada la evaluación por parte de los expertos, quienes bajo su criterio evaluaron la plataforma del FONDUC con las sub-heurísticas presentadas en esta investigación, se calcula el grado de USec obtenido por cada experto. Los resultados de este valor USec son presentados en la Tabla 5.16.

Tabla 5.16: Resultado final, USec general (Tomado de [150])

Experto	**Nivel USec**	**Cualitativo**
Experto 1	90.56	Violación Moderada
Experto 2	92.34	Violación Moderada
Experto 3	81.58	Violación Moderada
Promedio	**88.16**	**Violación Moderada**

Con base a los resultados presentados en la Tabla 5.16 se puede notar una similitud entre cada evaluación heurística realizado por los expertos, por lo tanto, se podría considerar que el sistema a nivel de seguridad y usabilidad debe ser tratado con una prioridad moderada, para evitar complicaciones que puedan alterar el funcionamiento del sistema, además de influir negativamente en la percepción que el usuario tenga de este.

Además de lo anterior, el resultado obtenido en nivel de USec es muy próximo a una violación mayor según la Tabla 5.15. Esta aproximación lo confirma un experto en seguridad que realizó la evaluación heurística, afirma que la aplicación del FONDUC tiene muchos problemas de seguridad, ademas, la facilidad de uso es pobre debido a que este sitio web fue desarrollado por personas que no tienen experiencia en desarrollar sistemas usables.

5.6.4. Discusión

Con base en los resultados presentados en este estudio, se puede decir que existe una cercanía considerable entre los tres expertos, por lo tanto, es posible afirmar que los expertos en gran medida calificaron de manera similar los requerimientos en cuanto a seguridad y usabilidad, con lo cual podría determinarse que los principios propuestos, el método de evaluación y el modelo matemático para el cálculo de USec podría ser ampliamente aceptado ya que arroja resultados coherentes que cumplen con las condiciones expuestas del modelo matemático.

El modelo matemático ha arrojado resultados con gran similitud durante su validación por parte de los expertos, es prioritario tener en cuenta que los resultados generales presentan un error aproximadamente del 9 %. Teniendo en cuenta los factores de subjetividad que se manejan en el campo de la USec, se puede concluir que con una error aproximado al 9 % con respecto a las calificaciones generales de USec, que el modelo matemático propuesto y las sub-heurísticas utilizadas parecen ser aceptable.

5.7. Evaluación con Usuarios: Voto Electrónico basado en *Eye Tracking*

En los últimos años, se ha puesto en marcha un conjunto de requisitos de usabilidad para los sistemas de votación electrónica. Sin embargo, no existe todavía una percepción coherente del contenido y alcance exactos de estos requisitos. Varias aplicaciones de votación electrónica se han creado con este mismo propósito, pero no han sido totalmente eficaces debido a su fácil de usar. Con el fin de determinar cuáles son los aspectos críticos de la usabilidad para este tipo de aplicaciones, en esta sección se realiza un estudio basado en el comportamiento de los usuarios mientras se utilizan dos aplicaciones de sistemas de votación electrónica.

5.7.1. Tecnología de *Eye tracking*

Debido a los recientes avances tecnológicos en hardware y software, el uso de *eye tracking* o seguimiento ocular para el análisis de aplicaciones en línea ha aumentado rápidamente. El seguimiento de los ojos se está convirtiendo en una herramienta popular para entender

el comportamiento de los usuarios en muchas aplicaciones, desde cómo los usuarios responden a los anuncios publicitarios, cómo interactúan los usuarios con los dispositivos móviles, cómo interactúan con la pantallas tactiles y menús [151] y, cómo estudiar el comportamiento de los usuarios usando múltiples fuentes de datos de información [152]. Debido a los avances tecnológicos, ahora podemos responder más eficazmente a las preguntas sobre cómo un usuario escanea y realiza una votación en línea.

La técnica de seguimiento ocular es el proceso que permite identificar, en una interfaz, dónde alguien está mirando en cada momento [56]. Los ojos de la gente tienen varios tipos de movimientos que pueden ser estudiados usando métricas tales como puntos de fijación, duración de la trayectoria de exploración, dirección de la trayectoria de exploración, tiempo de fijación, duración de fijación, tasa de fijación total y número de fijaciones, entre otros [153, 56, 154].

En este estudio se utilizan las métricas más habituales de acuerdo con [56, 155, 153, 154] para analizar la interacción de los usuarios con las áreas de interés definidas en los estudios de usabilidad: número de fijaciones en cada área de interés, duración de la fijación, duración de la mirada en cada área, fijación media de duración y tasa de fijación. Estos indicadores fueron elegidos porque son las métricas más informativas en términos de señales visuales y facilitan la interpretación objetiva de la exploración visual del usuario [153].

El objetivo de este estudio es analizar el comportamiento de los usuarios cuando utilizan el voto electrónico para identificar problemas de usabilidad mediante la técnica de *eye tracking*, mientras que el trabajos preliminares solo se centran únicamente en encontrar los problemas de usabilidad utilizando otras técnicas de evaluación [156, 157]. Además, se explora una aplicación desarrollada por Godia [158] de votación electrónica donde su seguridad se analiza, pero la usabilidad no ha sido evaluada. De acuerdo con lo anterior, la percepción sobre la seguridad del sistema podría aumentar si la información incluida en las aplicaciones de voto electrónico es clara y comprensible para el usuario.

Para desarrollar este estudio se presenta diferentes etapas y actividades teniendo en cuenta las propuestas por Solano [51].

5.7.2. Participantes de la evaluación

Los participantes del proceso de evaluación son los siguientes:

Representante de la organización: para esta evaluación Toni Granollers de la Universidad de Lleida (España), asume el rol de representante a causa de que establecer contacto con los usuarios para la realización de la evaluación.

Coordinador: Paulo César Realpe de la Universidad del Cauca (Colombia), quien tiene la responsabilidad de coordinar las etapas de la evaluación.

5.7.3. Etapa de Planeación

A continuación es presentado las actividades que conforman la etapa de planeación.

5.7.3.1. Actividad 1: Definir la aplicación sobre el cual se desea obtener información.

Entregable: Lista de aplicaciones sobre las cuales se desea obtener información.

En este caso las aplicaciones bajo estudio son: Helios Open Source[11] y la desarrollada por el grupo de Criptografía y Gráfos de la Universidad de Lleida (UdL)[12].

5.7.3.2. Actividad 2: Definir demografía de los participantes

Entregable: Especificación de los perfiles de usuario a los cuales están dirigidas las aplicaciones a evaluar.

La demografía de los 18 participantes del estudio se presenta en la Tabla 5.17, 9 de ellos para la aplicación de Helios y los otros 9 para la aplicación de UdL. A los participantes se les entregó un formulario de consentimiento para realizar el experimento, ver Anexo J. Nuestra población incluyó 11 (61,1 %) hombres y 7 mujeres (38,9 %). Las edades variaron de 18 a 58, con una edad media de 40 años y una desviación estándar de 12.8. Todos son usuarios regulares de Internet y con estudios universitarios completados o en curso. Cada uno de ellos fue convocado individualmente. Además, se realizó un cuestionario pre-test preliminar para cada usuario sobre el sistema de votación y seguridad en Internet, ver Anexo J.

5.7.3.3. Actividad 3: Definir el escenario en el que se van a realizar las tareas

Entregable: Especificación del escenario en el que se van a realizar las tareas.

El coordinador definió el siguiente escenario para que sea considerado por los usuarios al momento de realizar las tareas:

Usted como ciudadadano mayor de edad tiene derecho ha expresar algún apoyo o preferencia por alguna persona, para el cual deposita su confianza con el fin de que realice un trabajo en particular para beneficio público o privado. Existen tres candidatos A, B y C que proponen alternativas con el único fin de favorecer el bienestar común. Usted como persona piensa cuál de los tres candidatos tiene la mejor propuesta y decide apoyarlo con su voto. Le gustaría saber si el sistema de votación que está usando cumple con sus expectativas de facilidad de uso y los requisitos de seguridad y confidencialidad para emitir su voto.

[11] Disponible en: https://heliosvoting.org/
[12] Disponible en: http://www.cig.udl.cat/evoting

Tabla 5.17: Perfil de los participantes (Total n=18)

	UdL	**Helios**
Usuarios		
N	9	9
Género		
Masculino	66.6 %	55.5 %
Femenino	33.3 %	44.5 %
Edad		
18-25	11.1 %	33.3 %
26-35	11.1 %	11.1 %
36-45	11.1 %	11.1 %
46-55	55.5 %	44.4 %
56+	11.1 %	11.1 %
Educación		
Universitario	22.2 %	66.6 %
Maestría	22.2 %	0 %
PhD	55.5 %	33.3 %
Uso del voto en Internet		
Yes	55.5 %	55.5 %
No	44.5 %	44.5 %
Preferencias de voto		
Online	66.6 %	88.8 %
Voto de papel	33.3 %	11.2 %

5.7.3.4. Actividad 4: Definir tareas a realizar

Entregable: Definir las tareas que se van a realizar tareas.

Se propuso una serie de tareas para cada aplicación debido a las diferencias en su diseño y la implementación. En total, cada usuario debe realizar 4 tareas para cada aplicación con el fin de proporcionar su voto con éxito. Estas tareas se escogieron teniendo en cuenta el procedimiento de verificación y casting propuesto por Karayumak et al. [159], el contexto de uso y esencia de las aplicaciones, es decir, las tareas más relevantes en un sistema de votación electrónica real. La Tabla 5.18 muestra las tareas que cada usuario tiene que realizar para cada aplicación.

5.7.3.5. Actividad 5: Elaborar el documento guía que será entregado a los usuarios durante la realización del experimento.

Entregable: Documento guía para los usuarios que participan en el experimento.

Este documento guía incluye información sobre el escenario bajo consideración, las tareas a realizar y los cuestionarios pre-test y post-test. En el Anexo J es presentado este documento

Tabla 5.18: Tareas a realizar para cada aplicación.

Aplicación	Tareas
E-Voting UdL	T1. Verificar que el nombre esté en el censo. T2. Realizar el voto escogiendo al candidato favorito. T3. Confirmar que el voto haya sido registrado satisfactoriamente. T4. Volver a votar usando su PIN y certificado digital.
E-Voting Helios	T1. Ingresar su nombre de usuario y contraseña. T2. Realizar el voto escogiendo al candidato favorito. T3. Confirmar que el voto haya sido registrado satisfactoriamente. T4.Volver a votar usando su nombre de usuario y contraseña.

guía.

5.7.3.6. Actividad 6: Definir métricas

Entregable: Se definen las métricas mas importantes para la realización del experimento.

La variable independiente es el área de interés (AoI) también conocida como "zona de mirada" en algunas aplicaciones de software. Los investigadores definen áreas de interés sobre ciertas partes de una pantalla o interfaz en evaluación, y analizan sólo los movimientos oculares que se encuentran dentro de esas áreas [153, 155]. En este caso, para la aplicación desarrollada por la Universidad de Lleida las áreas de interés son: proceso de censo, votación, confirmación y votar nuevamente. Para el sistema Helios, las áreas de interés son: proceso de autenticación, votación, confirmación y votar nuevamente.

Las variables dependientes son las fijaciones en cada AoI teniendo en cuenta las métricas más utilizadas para la investigación de seguimiento ocular [56, 155, 153, 154]:

1. *Número de fijaciones en cada área*: el número de veces que los usuarios fijaron su mirada en cada una de las áreas mencionadas.

2. *Duración de las fijaciones en cada área*: tiempo (en segundos), en el cual los usuarios permanecieron con su mirada fija en cada AoI.

3. *Duración de la mirada en cada área*: duración acumulada (en segundos) y ubicación espacial promedio de una serie de fijaciones consecutivas dentro de un área de interés.

4. *Tasa de fijación y duración media de la fijación*: Esta métrica está estrechamente relacionada con la duración de la fijación (en fijaciones/s). Dado que el tiempo entre fijaciones es relativamente pequeño comparado con el tiempo que se gasta, la tasa de fijaciones debe ser aproximadamente la inversa de la duración media de la fijación (en s/fijación).

5.7.3.7. Actividad 7: Decidir el medio a utilizar para el registro del experimento.

Entregable: Especificación del medio a utilizar para el registro de los experimentos.

Para llevar a cabo este estudio se han utilizado el dispositivo Tobii T120, y el software Tobii Studio[13], versión 3.2, herramientas adquiridas por el grupo de investigación GRIHO de la Universidad de Lleida. El software Tobii Studio fue utilizado para mostrar los estímulos visuales y las áreas de interés que podrían analizarse por separado.

5.7.3.8. Actividad 8: Elegir el lugar más adecuado para realizar el experimento.

Entregable: Especificación del lugar más adecuado para hacer el experimento.

El equipo necesario para la obtención de datos experimentales se encuentra en el laboratorio de usabilidad del grupo de investigación GRIHO de la Universidad de Lleida. Este lugar es idóneo ya que a parte de tener los recursos hardware disponibles, cuenta con una sala cómoda para que los usuarios realicen las pruebas tranquilamente.

5.7.3.9. Actividad 9: Realizar una prueba piloto del experimento.

Entregable: Especificación del tiempo empleado por cada usuario para realizar el experimento.

La prueba piloto del experimento fue realizada por un un profesor titular de la Universidad de Lleida quien tiene experiencia en el uso de tecnologías de la información. Se determinó que para la aplicación Helios el tiempo para realizar todas las tareas es de aproximadamente 6 minutos y para la aplicación desarrollada por la Univesidad de Leida es de 5 minutos.

5.7.4. Etapa de Ejecución

A continuación es presentado las actividades que conforman la etapa de ejecución.

5.7.4.1. Actividad 10: Preparación del software.

Entregable: Registro de datos por parte del hardware/software.

El contenido se visualizó en un monitor TFT de 17 pulgadas con una resolución de 1024x768 en un computador personal con Windows 7 Professional e Internet Explorer 9. Se realizó un procedimiento de calibración al principio de cada sesión, antes de la recopilación de datos. Requiere que el participante mire una serie de puntos conocidos en una pantalla de computadora. La razón por la que cada participante tiene que ser calibrado

[13]Disponible en: www.tobii.com

es porque hay diferencias individuales en la forma en que los ojos se ven y se comportan [56].

El software estaba previamente configurado para que los usuarios pudieran ejecutar las tareas. Cuando el participante necesitaba realizar una determinada tarea, el sistema los dirigía automáticamente a la página correspondiente. Para cada aplicación era necesario llevar a cabo diferentes configuraciones en el software Tobii Studio porque los sistemas de votación utilizan diferentes plataformas. Los participantes recibieron instrucciones de sentarse frente al monitor Tobii. Para que el estudio sea satisfactorio, se pide a los participantes que eviten los movimientos corporales durante la prueba.

5.7.4.2. Actividad 11: Desarrollo de sesión.

Entregable: Cuestionarios diligenciados y desarrollo de tareas.

Después de reconocer a cada participante e introducirlos en el experimento, se les pidió que respondieran a una encuesta preliminar que incluía datos demográficos, uso de Internet, participación en votación electrónica y preferencias de voto, ver Tabla 5.17. Luego se calibró el monitor Tobii para asegurar El seguimiento correcto de los ojos para cada usuario. Si hay un error en la calibración, el participante es debe ser colocado en una posición adecuada y re calibrado nuevamente. Sin embargo, la calibración fue correcta para los 18 participantes. El proceso de calibración tomó aproximadamente 1 minuto. Luego se realizaron las 4 tareas consecutivamente para cada aplicación, ver Tabla 5.18.

Cada participante realizó la tarea según sus propios criterios y el objetivo inicial. Cuando el usuario terminó las tareas se le pidió que respondiera a una serie de preguntas sobre el uso de la aplicación, con el fin de recopilar datos cualitativos.

El lugar donde se realizaron las pruebas fue lo más cómodo posible para los usuarios, para evitar el nerviosismo y obtener los resultados más reales posibles. Antes de que el usuario comenzara a realizar las tareas, era necesario comprobar cuidadosamente que el software estaba correctamente configurado para evitar molestias o estrés en los participantes.

5.7.5. Etapa de Análisis de Resultados

En esta etapa se presentan los resultados de las métricas de seguimiento ocular utilizadas para analizar el comportamiento de los usuarios a partir de sus estímulos visuales. Se realizó un análisis estadístico básico de los datos para cada área de interés (AoI) y un análisis cualitativo para cada aplicación.

Cada AoI define el área de la interfaz donde se realizará el análisis cualitativo y cuantitativo. Se identificaron cuatro (4) AoI para la implementación del sistema de votación electrónica de UdL: censo, autenticación, votación y confirmación del voto. Se identificaron tres (3) AoI para la aplicación usando Helios: autenticación, votación y confirmación de

voto. La Figura 5.9 presenta un ejemplo del área de interés (en azul claro) para el censo, por ejemplo, T1. Verifique que su nombre esté en el censo – UdL.

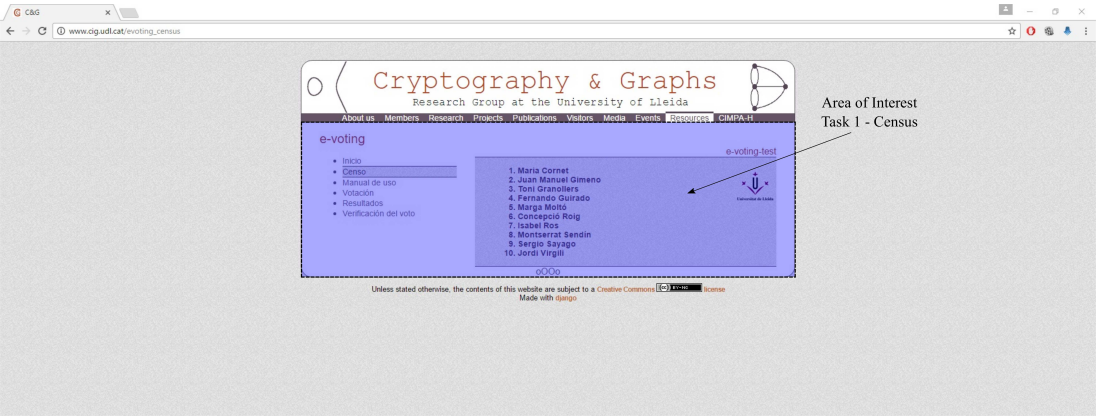


Figura 5.9: Ejemplo de AoI para el censo.

5.7.5.1. Actividad 12: Análisis cuantitativo

El análisis cuantitativo consiste en calcular las estadísticas utilizando las medidas de seguimiento ocular seleccionadas y los datos preparados de acuerdo con algunas instrucciones sobre la extracción y la preparación de los datos [56].

Teniendo en cuenta las áreas de interés, a continuación se presentan los resultados estadísticos para cada aplicación. Las Tablas 5.19 y 5.20 muestran el número de fijaciones, la duración de la fijación y la duración de la mirada en cada área de interés para las aplicaciones de UdL y Helios respectivamente. Se puede ver que el proceso de votación para la implementación de la UdL es más rápido (165.53 segundos), esto se debe al hecho de que Helios tiene inicialmente una extensa introducción que explica el proceso de cómo votar con éxito.

De acuerdo con los resultados anteriores (ver Tablas 5.19 y 5.20), el número de fijaciones, el tiempo que los usuarios permanecieron con su mirada fija y la duración acumulada de las fijaciones dentro del AoI disminuyeron considerablemente para la tarea "votar nuevamente". Con respecto al número de fijaciones, se redujeron en un 79.5 % y 53.9 % para Helios y UdL respectivamente, 56.5 % para UdL y 55.6 % para Helios en términos de duración de la fijación, y 55.38 % para UdL y 51.01 % para Helios de acuerdo con la duración de la mirada. Esto significa que los usuarios recordaron los pasos fácilmente.
Otro factor que puede ser representativo es el idioma, Helios está totalmente escrito en inglés mientras que la aplicación de UdL está escrito en español. Algunos usuarios han expresado antes de comenzar la prueba con Helios que su inglés no era bueno, esta fue una de las razones que podrían haber influenciado en la duración del tiempo para realizar cada tarea. Finalmente, un último factor que podría afectar el tiempo para desarrollar el proceso de votación es que UdL no permita votar nuevamente con la misma identidad,

Tabla 5.19: Promedio en las áreas de interés para UdL

Tarea	**Fijación por área**	**Duración de la fijación por area**	**Duración de la fijación**
Censo	54.33	13.72	17.94
Voto	274.11	60.54	93.02
Confirmación	38.44	7.79	13.07
Votar nuevamente	107.22	25.18	41.50
Promedio	**112.97**	**26.13**	**41.38**
Razón de fijación	4.32 fijaciones/segundo		
Duración promedio para cada fijación	0.23 segundos/fijación		

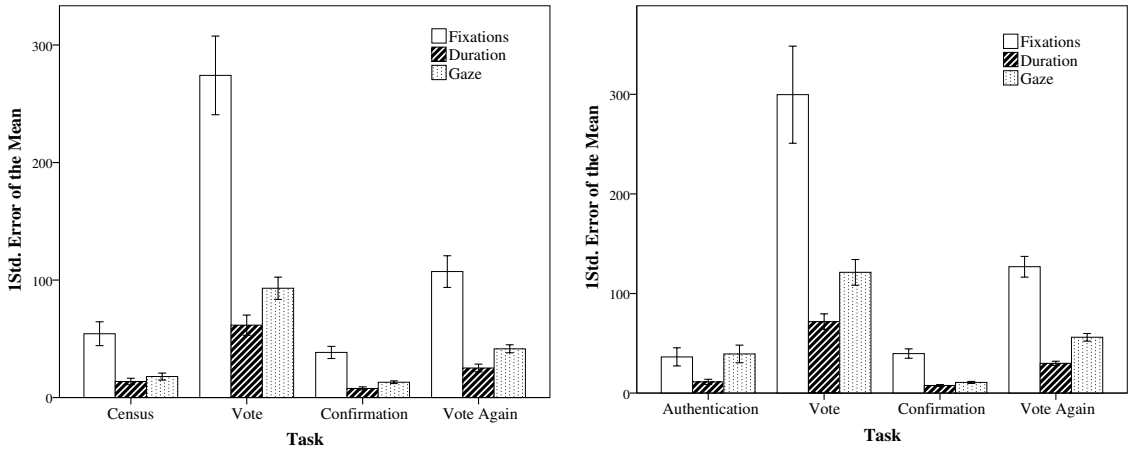
Tabla 5.20: Promedio en las áreas de interés para Helios

Tarea	**Fijación por área**	**Duración de la fijación por área**	**Duración de la mirada**
Autenticación	36.33	11.22	39.26
Voto	299.67	71.76	121.23
Confirmación	39.67	7.67	10.68
Votar nuevamente	126.89	29.84	56.05
Promedio	**132.58**	**31.48**	**59.30**
Razón de fijación	4.21 fijaciones/segundo		
Duración promedio para cada fijación	0.24 segundos/fijación		

esta es una parte importante de su seguridad. Sin embargo, Helios permite llevar a cabo el proceso de votación muchas veces, esto puede ser una desventaja porque no hay control sobre la toma de decisiones.

Debido a los inconvenientes de la aplicación de Helios presentada anteriormente, los usuarios eran mucho más propensos a cometer errores cuando usan esta aplicación que los usuarios que realizan el proceso de votación usando UdL, esto se muestra en la Figura 5.10.

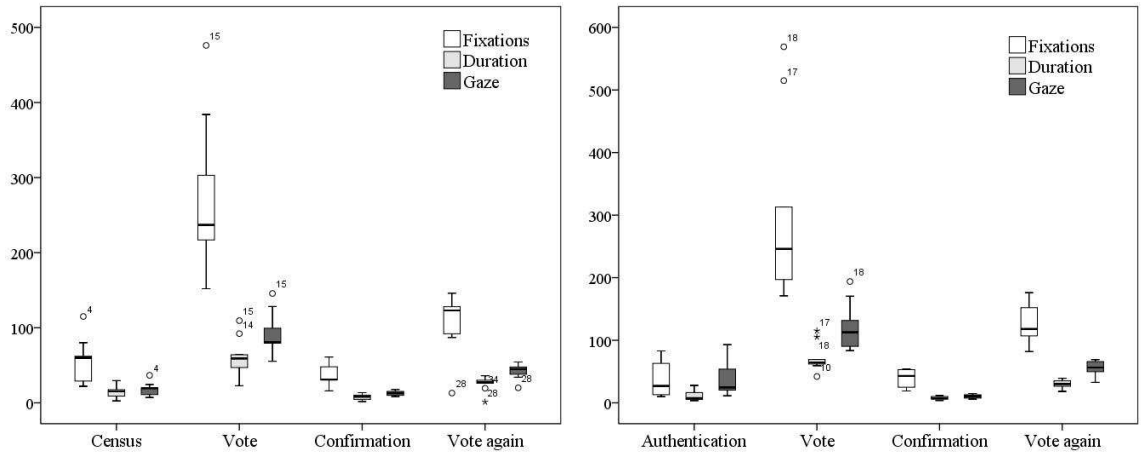
A partir de los datos anteriores, consideramos llevar a cabo otro tipo de análisis estadístico: diagrama de cajas y bigotes. Este diagrama es una pantalla visual que describe varias características importantes, como la dispersión y la simetría de datos. La Figura 5.11 presenta los diagramas para el número de fijaciones, la duración de la fijación y la duración de la mirada en cada área de interés para las aplicaciones de UdL y Helios, respectivamente. Podemos observar que hay valores atípicos que están numéricamente distantes del resto de los datos, esto nos indica que hay una gran dispersión y asimetría de los datos porque era complicado para algunos usuarios realizar algunos tareas, lo que resulta en una



(a) UdL (b) Helios

Figura 5.10: Las barras de error representan el error estándard de la media.

mayor duración y número de fijaciones. Además de lo anterior, esta dispersión se debe a los problemas de usabilidad que tienen las aplicaciones.



(a) UdL (b) Helios

Figura 5.11: Diagrama de cajas y bigotes para las tareas.

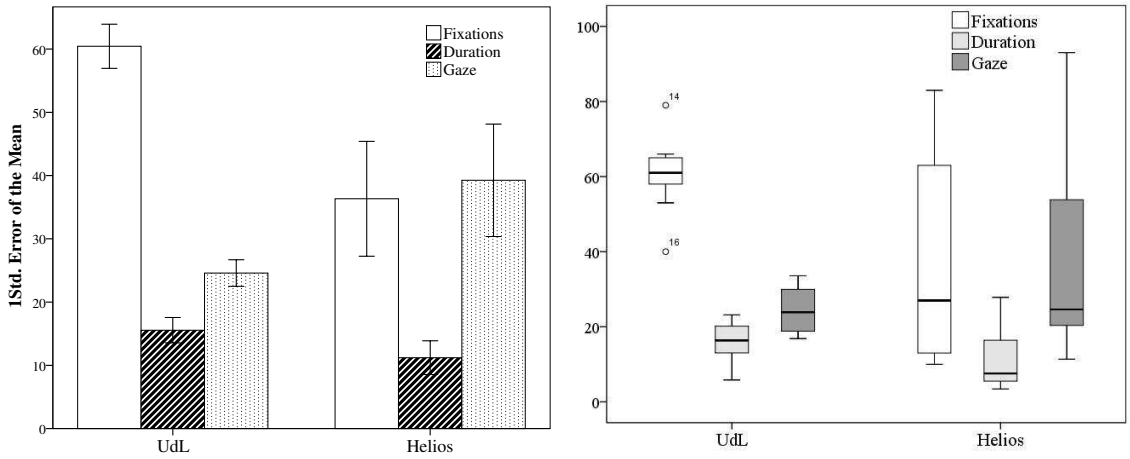
Uno de los objetivos de nuestro estudio fue analizar el comportamiento de los usuarios al utilizar los métodos de autenticación. Para la aplicación de UdL, el proceso de autenticación era múltiple, utilizando un certificado digital y un número PIN de cuatro dígitos, a su vez, la autenticación Helios se llevó a cabo mediante un nombre de usuario y una contraseña. La Tabla 5.21 presenta los datos del proceso de autenticación para UdL y Helios respectivamente. Debido al proceso de autenticación para UdL fue múltiple, la duración y el número de fijaciones fue mayor que en Helios.

Tabla 5.21: Promedio del número de fijaciones y duración en AoI para la autenticación

Aplicación	**Fijación por área**	**Duración de la fijación**	**Duración de la mirada**
UdL	56.00	14.98	23.48
Helios	36.33	11.22	39.26
Promedio	**46.17**	**13.10**	**31.37**
Razón de fijación	3.52 fijaciones/segundo		
Duración promedio por cada fijación	0.28 segundos/fijación		

La Figura 5.12 muestra que el método de autenticación del nombre de usuario y la contraseña tienen una duración y un número de fijaciones más bajos. Sin embargo, para el proceso de autenticación con Helios, el sistema genera una contraseña aleatoria de diez caracteres especiales que es difícil de memorizar, por lo que los usuarios deben introducir caracter por caracter causando retrasos y confusión. Debido a lo anterior, los usuarios eran mucho más propensos a cometer errores al realizar el proceso de autenticación.

En la Figura 5.12 se muestra también el diagrama de caja y bigotes para el proceso de autenticación. Las observaciones realizadas al proceso de autenticación de UdL fueron más simétricas y hubo poca dispersión de datos, esto se debió al hecho de que el usuario debe autenticarse utilizando un certificado digital (un archivo previamente enviado) y un número PIN de cuatro dígitos. Este proceso de autenticación fue fácil para los usuarios al completar la tarea.



(a) Barras de error del promedio (b) Diagrama de cajas y bigotes

Figura 5.12: Barras de error del promedio y diagrama de cajas para autenticación.

A partir de los resultados anteriores, es necesario hacer una comparación entre los dos sistemas de votación electrónica para determinar si la diferencia de los dos sistemas para cada tarea es significativa, para ello se utiliza una prueba *t-test*. La condición que se puso a la prueba *t-test* fue que las dos poblaciones son iguales. De lo anterior, formulamos la siguiente hipótesis:

1. *Hipótesis alternativa* H_1: Existe una diferencia significativa entre la media de X para la UdL y la media X para la aplicación de Helios.

2. *Hipótesis nula* H_0: No existe una diferencia significativa entre la media de la X de la UdL y la media X de la aplicación de Helios.

Donde X representa los datos cuantitativos (número de fijaciones o duración de fijación) para cada tarea. Las tareas que se analizaron fueron votación y autenticación. Los datos cuantitativos fueron elegidos porque son las variables más representativas en nuestro estudio que fueron comentadas anteriormente. La Tabla 5.22 presenta los resultados para la prueba t.

Tabla 5.22: Análisis de promedios usando *t-test*

Tarea	**Fijaciones**	**Duración**
Votar	$F(0{,}97) = 0{,}43$ $p = 0{,}67$	$F(0{,}97) = 0{,}43$ $p = 0{,}67$
Autenticación	$F(11{,}09) = 2{,}48$ $p = 0{,}03$	$F(0{,}71) = 1{,}30$ $p = 0{,}21$

*Nivel de significancia $\alpha = 0{,}05$

Con base en los resultados anteriores, podemos afirmar que no hay una diferencia significativa para la tarea de votar por los dos sistemas de votación electrónica ($p > 0{,}05$). Además, existe una diferencia significativa en el número de fijaciones para la tarea de autenticación ($p < 0{,}05$). Sin embargo, para confirmar esta afirmación, es necesario llevar a cabo nuevas pruebas con un mayor número de usuarios al que se utilizó en este trabajo.

Para realizar este análisis cuantitativo, y para determinar que el sistema de votación tiene una mejor usabilidad, medimos la usabilidad del sistema basado en una métrica de uso estándar. La escala de usabilidad del sistema (SUS) en [160, 161] es una medida estándar de usabilidad ampliamente utilizada con fines académicos y comerciales. La métrica SUS corresponde a una puntuación numérica de 0 (menos utilizable) a 100 (la más útil e ideal), lo que proporciona una estimación aproximada de la facilidad general de uso de un sistema. Muchos factores influyen en las calificaciones de usabilidad de los participantes.

Obviamente, el diseño de interfaz de usuario específico que usan los participantes del estudio juega un papel muy significativo en esas calificaciones [162]. La escala de usabilidad del sistema no es diagnóstica y no dirá qué problemas específicos enfrentan la aplicación, sino que dará una luz roja o verde para saber qué necesita ser mejorado. Después de realizar todas las tareas para cada aplicación, los participantes completaron el cuestionario SUS

que se agregó al software Tobii Studio para acelerar el proceso. La Tabla 5.23 muestra los resultados del SUS para las dos aplicaciones de voto electrónico.

Tabla 5.23: System Usability Scale (SUS)

Aplicación	Promedio	Desviación estándar	Mediana
UdL	58.6	24.1	65.0
Helios	74.1	9.9	77.5

De acuerdo con los resultados de la Tabla 5.23 y basados en la interpretación propuesta por Bangor et al. [162], podemos afirmar que la aplicación Helios tiene una calificación C y su colocación dentro del rango aceptable (70-100), sin embargo la aplicación de UdL tiene una calificación F poniéndola en el rango marginal inferior.

La Figura 5.13 muestra la tendencia SUS para los 9 participantes para cada una de las aplicaciones. A partir de los resultados anteriores, es posible afirmar que es necesario hacer un mayor esfuerzo para mejorar la interfaz de aplicación de UdLs, también es importante proponer nuevas interfaces para que Helios aumente su aceptabilidad por parte de los usuarios.

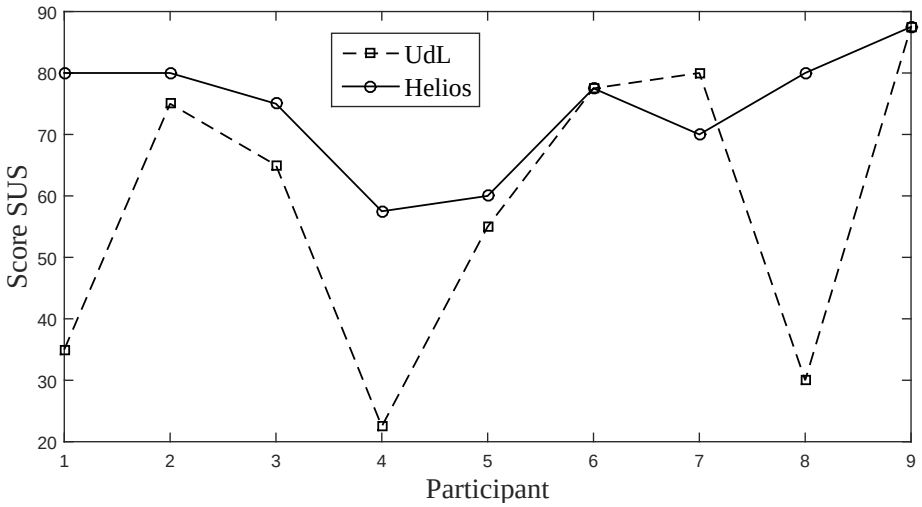


Figura 5.13: Tendencia SUS para cada participante.

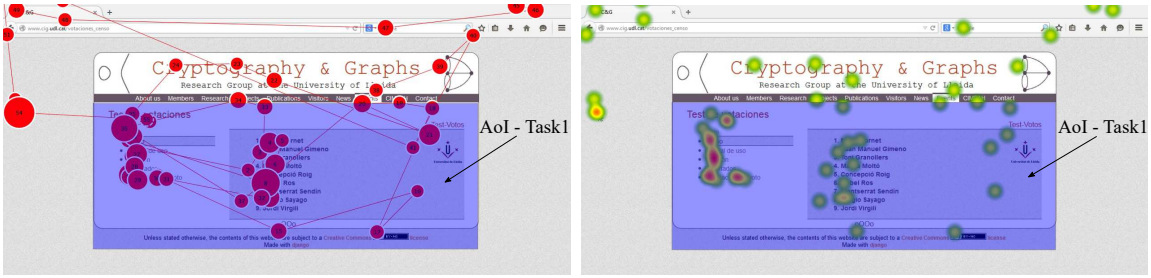
5.7.5.2. Actividad 13: Análisis cualitativo

El análisis cualitativo se centra en cómo alguien miró algo, y se lleva a cabo inspeccionando visualizaciones de datos. El objetivo de la inspección es explicar los problemas de usabilidad descubiertos sobre la base de datos de comportamiento y descubrir problemas

adicionales que pueden no ser fácilmente encontrados de alguna manera [56].

Otra forma de analizar los resultados anteriores es a partir del mapa de calor generado por el seguimiento ocular, donde se pueden observar cuáles fueron los puntos donde los usuarios enfocaron su atención; y el mapa de mirada o el diagrama de mirada demuestran el orden en que los usuarios miran la pantalla y las áreas donde fijan la atención por un tiempo más largo.

La Figura 5.14 presenta el mapa de mirada y de calor para la aplicación de UdL. El comportamiento de los usuarios en el censo está bien definido. La mayoría de los usuarios no tuvieron problemas al buscar su nombre, permitiendo que esta tarea se llevara a cabo en poco tiempo, como se mostró en la Tabla 5.19.



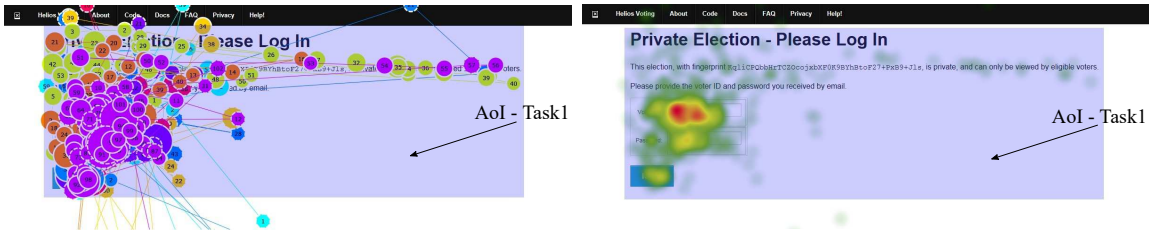
(a) Mapa de mirada (b) Mapa de calor

Figura 5.14: Mapa de mirada y calor para el censo UdL.

Durante el proceso de autenticación para la aplicación UdL o Helios, el sistema genera una firma digital único para cada usuario. La Figura 5.15 ilustra el proceso de autenticación para Helios donde muestra la firma digital generada para el usuario. Debido a que esta firma representa una serie larga de números y letras que es compleja de entender, los usuarios pueden pensar que esta función de votación electrónica no es relevante y se enfocaron sólo en realizar satisfactoriamente la tarea. Este mismo caso ocurrió para la aplicación UdL donde la firma es tres veces más larga que Helios, todos los usuarios preguntaron sobre el significado de ese número y si es necesario mostrarlo en la pantalla.

Para la tarea de votación, se diseñó un conjunto de 3 candidatos (candidato A, B o C) para cada aplicación. La Figura 5.16 muestra el mapa de la mirada de los procesos de votación de Helios y UdL, se puede observar que Helios presenta una cantidad considerable de información, aumentando el tiempo dedicado al área de interés.

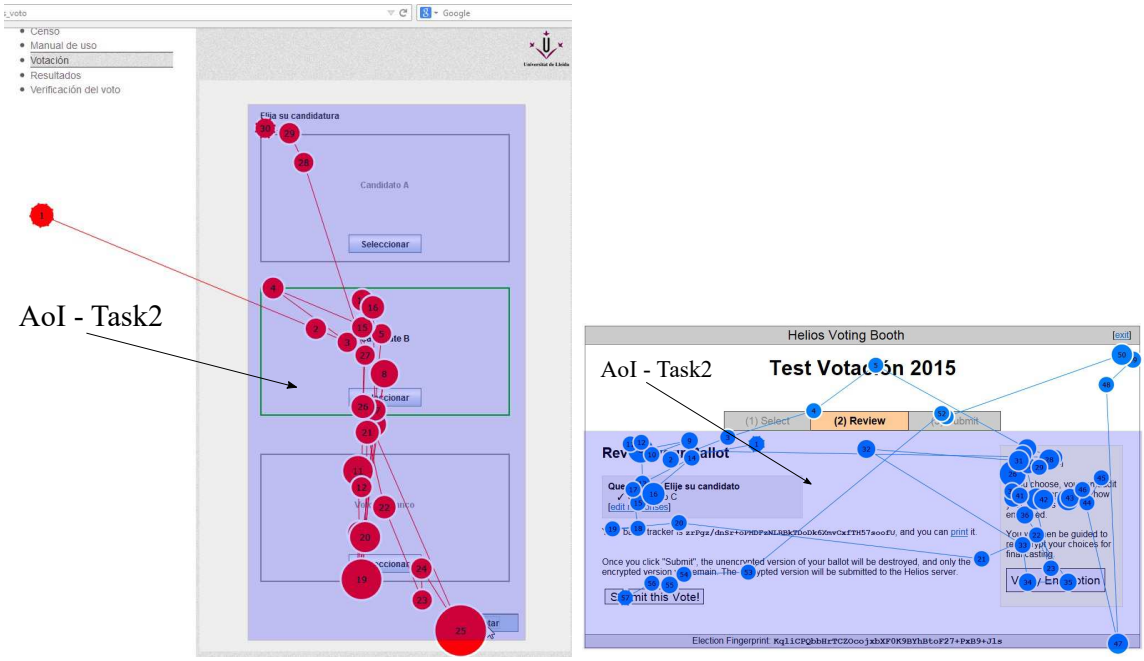
Se puede observar también que los usuarios no prestaron atención a su firma digital, lo que representa una importante característica de seguridad para enviar mensajes cifrados. En el mapa de la mirada para el proceso de votación de la UdL, a diferencia de Helios, hay menos cantidad de información y los usuarios sólo se centraron en la elección rápida de su candidato, véase Figura 5.16. De lo anterior puede deducirse que (usando las Tablas



(a) Mapa de mirada (b) Mapa de calor

Figura 5.15: Mapa de mirada y calor para autenticación usando Helios.

5.19 y 5.20) la duración de la fijación para emitir un voto en Helios es aproximadamente 15,6 % superior a UdL.

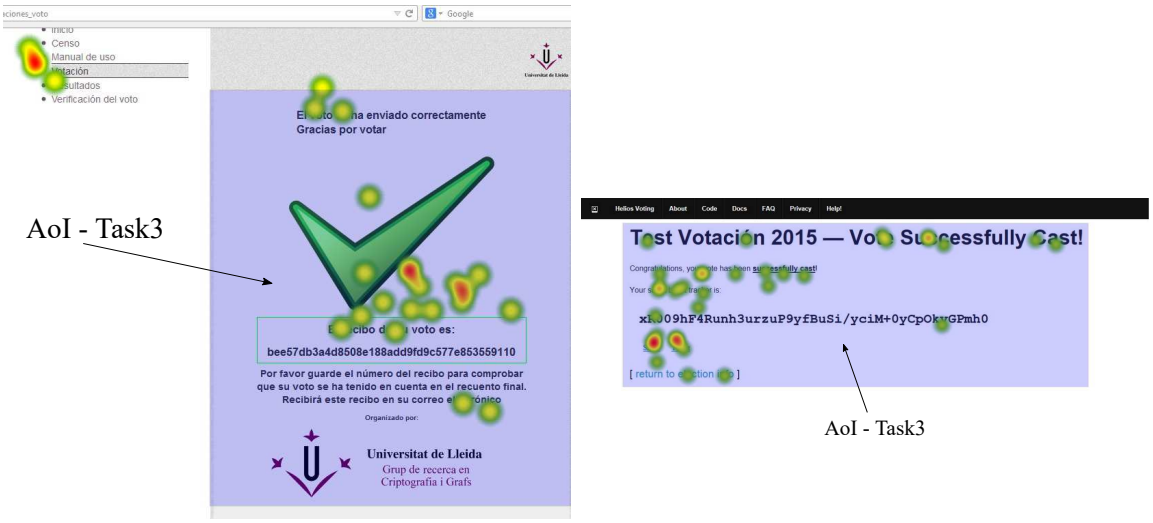


(a) UdL (b) Helios

Figura 5.16: Mapa de mirada para votación usando UdL y Helios.

Cuando se completa el proceso de votación, el sistema imprime un "recibo" en forma de un número hexadecimal para UdL y una combinación de varios caracteres para Helios, lo que indica que el voto encriptado se ha enviado con éxito. La Figura 5.17 presenta el mapa de calor que confirma el voto para las aplicaciones UdL y Helios, respectivamente. Igual que en los casos anteriores, los usuarios no prestaron atención a este "recibo", y creemos que la falta de información sobre su propósito hace que los usuarios no perciban su importancia. Al final de la prueba, cada usuario afirmó que esta cadena de caracteres no debe mostrarse ya que no indica nada. Si se muestra esta cadena, los usuarios expresan

que debe tener algún tipo de información que explique su importancia y significado.



(a) UdL (b) Helios

Figura 5.17: Mapa de calor para confirmar voto usando UdL y Helios.

5.7.5.3. Actividad 14: Realizar recomendaciones para dar solución a los problemas de usabilidad y seguridad identificados.

Entregable: Recomendaciones.

Las recomendaciones de diseño finales para solucionar los problemas de usabilidad y seguridad, no se presentan debido a que esto sobrepasa el alcance de la investigación.

5.7.5.4. Actividad 15: Elaborar el informe final de la evaluación.

Entregable: Informe final

No se realiza esta actividad porque no está en el alcance de la presente investigación.

5.7.6. Discusión

Este estudio se ha realizado utilizando la técnica de seguimiento ocular (*eye tracking*) a través de la cual se pudieron identificar dos áreas problemáticas que reflejan su facilidad de uso. Con esta técnica se realiza un seguimiento visual de los ojos de los usuarios para analizar cualitativamente (mapas de mirada y de calor) y cuantitativamente (estadística) las diferentes tareas que debe realizar el usuario. Los resultados muestran que las aplicaciones tienen problemas en presentar información que no es relevante, así como una ausencia en el sistema de pasos específicos para completar el proceso de votación con éxito y evitar errores de los usuarios. De acuerdo con lo anterior, la percepción sobre la seguridad del

sistema podría aumentar si la información incluida es más clara y comprensible para el usuario.

En cuanto al proceso de experimentación, la disponibilidad y los recursos fueron aspectos clave en nuestro estudio. Además, los experimentos se realizaron en entornos controlados (laboratorio de usabilidad), para asegurar que la planificación, ejecución y resultados no se vieran afectados.

Estos resultados ponen de relieve la importancia de utilizar la tecnología, en este caso el seguimiento visual, para encontrar los problemas de usabilidad que pueden tener sistemas de votación electrónica. A diferencia de los trabajos relacionados en los que no se utiliza algún tipo de tecnología para estudios de usabilidad, consideramos que la anterior es una contribución importante porque hemos encontrado problemas en las interfaces que no podrían ser encontradas usando otros métodos de evaluación donde las componentes usabilidad y seguridad están incluidas. Este estudio demuestra que estos sistemas deben ser desarrollados de una manera adecuada para un uso óptimo. Sin embargo, estos sistemas no son la solución para la votación futura debido a sus vulnerabilidades y amenazas.

Por otro lado, es necesario que los investigadores en las áreas de seguridad de la información e Interacción Humano-Computador (HCI) trabajen juntos para proponer o desarrollar en el voto electrónico, métodos de autenticación que eviten la sobrecarga cognitiva de los usuarios pero al mismo tiempo sean seguro.

Nuestro estudio, sin embargo, no sugiere qué sistema de votación es el mejor y aconsejable. Cada sistema tiene ventajas y desventajas. Del cuestionario del SUS se podría decir que la aplicación Helios tiene mejor usabilidad que la UdL, pero a través de la técnica de seguimiento ocular, los usuarios muestran confusión al realizar sus tareas. Por otro lado, aunque la aplicación de UdL tiene importantes métodos de seguridad (autenticación múltiple) y no muestra mucha información que perturbe al usuario, no presenta de manera adecuada los elementos importantes que guían al usuario para hacer una votación exitosa.

Los usuarios que usaron la aplicación UdL manifestaron que realizar el proceso de votación era complejo debido al hecho de que el sistema no guiaba a los usuarios apropiadamente pero que tenían que “adivinar” los pasos siguientes para emitir con éxito su voto. Ademas, es importante resaltar que su nivel de seguridad es bueno porque tiene dos métodos de autenticación.

Por su parte, en la aplicación Helios, los usuarios afirmaron que era fácil de usar porque el propio sistema guía al usuario para completar satisfactoriamente el proceso de votación. Pero, como la aplicación estaba escrita en inglés, los usuarios solicitaron que la aplicación tuviera la opción de elegir el idioma apropiado. En términos de seguridad, los usuarios aseguraron de que el nombre de usuario y el mecanismo de contraseña no es totalmente seguro, incluso si la contraseña es aleatoria, porque hay herramientas de TI que le permiten “adivinar” ese tipo de contraseñas.

Finalmente, podemos añadir un aspecto importante en la seguridad de las aplicaciones de votación electrónica que se ha estudiado. A partir de los mapas generados por el seguimiento ocular, los usuarios no verificaron si la aplicación tenía los requisitos mínimos de seguridad, es decir, verificar si tienen certificados SSL y HTTPS. Si los usuarios no verifican este certificado en aplicaciones que utilizan Internet, la vulnerabilidad de ser suplantado por terceros puede aumentar. Por lo tanto, el primer paso que deben tomar los usuarios es comprobar si estas aplicaciones están utilizando este tipo de certificado, identificándolos con iconos o colores, por ejemplo, Internet Explorer muestra un candado en la parte inferior izquierda y Google Chrome muestra una barra verde en la parte superior.

De lo anterior, la aplicación de Helios tiene estos tipos de certificados (SSL y HTTPS) que permiten evitar ataques informáticos de los hackers. Sin embargo, la aplicación UdL no tiene estos certificados haciéndolo vulnerable a ataques. Los desarrolladores deben tener esto en cuenta para futuras mejoras en las aplicaciones.

Capítulo 6

Proceso de Diseño de Seguridad Usable y Autenticación basado en DCU

6.1. Introducción

Este capítulo, describe un proceso para el diseño de sistemas seguros y usables mediante un enfoque centrado en el usuario (DCU). A partir de esto, el equipo de desarrollo podría disponer de un proceso mediante el cual es posible implementar soluciones de seguridad y usabilidad para los usuarios. Para el desarrollo de este proceso se toma como base la metodología MPIu+a propuesta por Granollers [41] para implementar aplicaciones interactivas altamente usables y accesibles. En la Figura 6.1 se presenta el esquema general del contenido que se presentará en este capítulo.

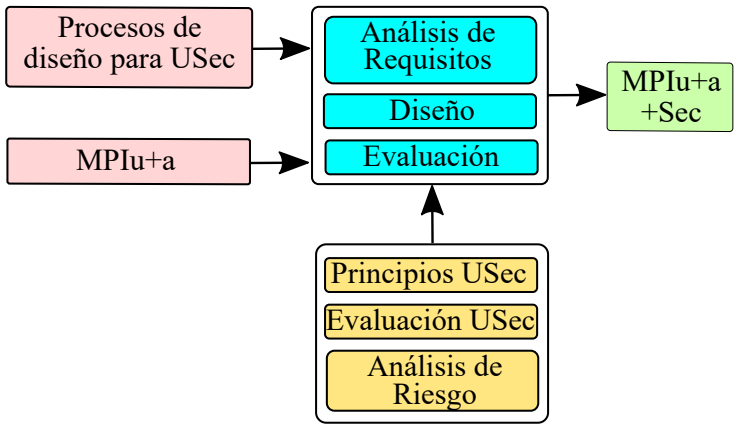


Figura 6.1: Estructura del Capítulo 6 (creación propia).

6.2. Justificación de un proceso de diseño para Seguridad Usable

En el Capítulo 1 a través de la problemática planteada se observa la necesidad indiscutible de proporcionar un proceso de diseño para sistemas donde la seguridad y usabilidad estén presentes, y permita un equilibrio adecuado entre ellos. También se presentaron algunos trabajos propuestos por importantes investigadores donde proponen procesos de diseño que permiten desarrollar aplicaciones bajo los conceptos de seguridad y usabilidad (ver Sección 2.7.2). Sin embargo, ninguno de los modelos presentados ofrece una visión un poco más completa sobre cómo diseñar y evaluar convincentemente las aplicaciones desarrolladas con respecto a la seguridad usable para los usuarios quienes son el objetivo principal.

Además de lo anterior, la falta de principios de diseño comúnmente acordados como se han indicado en la Sección 4.5, plantea un obstáculo en el camino hacia la obtención de un proceso de diseño más completo para el desarrollo y evaluación de sistemas seguros y usables. Los procesos disponibles en la literatura son incompletos o se centran en cierta fase en el proceso de desarrollo, esto hace que sea más difícil para los diseñadores adoptar diferentes modelos disponibles en la literatura y que en algunos casos pueden ser independientes (seguridad y usabilidad por separado).

Desde nuestro punto de vista, la necesidad de proponer un proceso de diseño para usabilidad y seguridad se puede resumir en los siguientes aspectos:

- Algunos desarrolladores creen que **la seguridad es una tarea secundaria** debido a que consideran que los usuarios no están enfocados en asegurar sus sistemas, sino que lo único que quieren es usar sus aplicaciones para lograr sus objetivos.

- Los procesos propuestos **no tienen un verdadero diseño centrado en el usuario** debido a que omiten alguno de los aspectos importantes del DCU tales como tener en cuenta al usuario, sus necesidades y requerimientos.

- **Los procesos para el diseño de sistemas seguros y usables son muy técnicos y su aplicación puede resultar confusa** (difícil de entender o uso de una terminología muy compleja). El campo de la seguridad usable es intrínsecamente interdisciplinario, mezclando técnicas y conceptos del HCI con los de la seguridad y la privacidad. A menudo, es más fácil para los diseñadores trabajar en un área u otra, en lugar de tratar de mezclar los dos.

- Existe una verdadera necesidad de **establecer una forma de evaluación más objetiva** para que los expertos puedan evaluar la usabilidad y la seguridad de forma conjunta a través de datos cuantitativos. Proporcionando con esto, una potente herramienta para los desarrolladores en el diseño de sus aplicaciones.

6.3. La Seguridad y la Ingeniería del Software

Actualmente, los sistemas de software se han convertido en una parte importante de nuestras vidas. Dependemos en gran medida de sistemas de software en varias áreas de nuestras actividades diarias, tales como servicios financieros, comercio electrónico, mensajería instantánea, redes sociales, entre otros [163].

Debido a que el sistema software esta involucrado indiscutiblemente en diversos aspectos de la sociedad, la seguridad se convierte en una cuestión importante y un requisito para el sistema de software. Las características de seguridad tales como la confidencialidad, la disponibilidad, autenticidad, privacidad y la integridad deben tenerse en cuenta para considerar el software como seguro [164].

Tradicionalmente, la seguridad se ha considerado sólo en las últimas etapas del desarrollo del software, mediante la incorporación de las preocupaciones de seguridad. Como consecuencia, aumenta el riesgo de introducir vulnerabilidades de seguridad en el sistema. Investigaciones ha demostrado que tales enfoques para abordar las preocupaciones relacionadas con la seguridad no son suficientes y dan lugar a un número significativo de cambios además de las consecuencias causadas por una violación de la seguridad [165]. Para abordar estas preocupaciones, los desafíos de seguridad deben ser abordados desde el inicio del desarrollo del software es decir, desde el análisis de requisitos [166].

Con el fin de comprender la relación entre seguridad y la ingeniería de software, en la Tabla 6.1 se presenta una serie de actividades de prácticas de seguridad enmarcado a la ingeniería de software. Este relación se basa en los propuestos por [167][103][99][100].

Muchos trabajos relacionados con las actividades de seguridad dentro del desarrollo del software difieren en sus prácticas de seguridad. Esto quiere decir que no existe un modelo único y absoluto que diga las actividades que deben tener, esto se debe a que cada organización se acomoda a sus propios criterios para el desarrollo del software con sus propias características de seguridad. Sin embargo, todos ellos se basan en las fases del desarrollo del software para diseñar e implementar sistemas seguros [167].

En este trabajo, no se dará explicación a cada una de las actividades de la Tabla 6.2 debido al alcance de la investigación. Sin embargo, podemos observar que algunas actividades de las fases de requerimientos (objetivos de seguridad, establecer requisitos de seguridad, y análisis de amenazas y riesgos), diseño (revisiones externas) y evaluación (análisis dinámico) hacen parte de nuestra propuesta que se tendrán en cuenta en la Sección 6.6 y que hacen parte del proceso de diseño de sistemas seguros y usables mediante un enfoque centrado en el usuario.

Tabla 6.1: La seguridad dentro del desarrollo del software.

Fase	Actividad de seguridad
Planeación	Capacitación en seguridad básica
Requerimientos	Objetivos de seguridad. Establecer requisitos de seguridad. Análisis de amenazas y riesgos. Establecer puerta de calidad.
Diseño	Análisis de ataques. Modelo de amenaza. Planes de prueba. Revisión externa. Selección de herramientas de seguridad.
Codificación	Usar herramientas probadas. Análisis estático. Revisión del código.
Evaluación	Revisión de ataques. Análisis dinámico. Prueba de amenazas y fallos.
Lanzamiento	Revisión final de seguridad. Plan de respuesta a la seguridad. Documentación.
Reacción	Actualización de seguridad Realimentación de seguridad.

6.4. Análisis comparativo entre los proceso de diseño para USec

Con el objetivo de situar de una manera más especifica el presente trabajo de investigación, dentro del estado del arte y relacionado con el objetivo específico planteado en el Capítulo 1: "*proponer un proceso de diseño para seguridad usable y autenticación mediante un enfoque centrado en el usuario, a partir de los principios de seguridad usable y su evaluación*", en esta sección se presenta una comparación entre una selección de los estudios más significativos descritos en la Sección 2.7.2 sobre el diseño de aplicaciones seguras y usables.

Con el fin de que el lector tenga presente los trabajos relacionados, se presenta a continuación los estudios de una forma más ordenada junto con un breve resumen.

1. Ursula Holmström [107]: presenta un enfoque centrado en el usuario para el diseño de software de seguridad. Aplica el diseño centrado en el usuario al desarrollo de un concepto de gestor de seguridad para un dispositivo de comunicación.

2. Markotten [23]: propone el nuevo concepto de la ingeniería de seguridad centrada en

el usuario para disminuir la brecha que existe entre seguridad y usabilidad. Con este método se ha desarrollado e implementado una herramienta de manejo de identidad.

3. Flechais et al. [79]: describe AEGIS, una metodología para el desarrollo de sistemas seguros y utilizables. AEGIS define un proceso de desarrollo y un meta-modelo de la definición y el razonamiento sobre los elementos del sistema.

4. Khalid et al. [106]: identifica los requisitos de usabilidad y seguridad para analizar la relación entre los requisitos de seguridad y usabilidad para proponer un modelo de trade-off que pueda ser utilizado en la fase de requisitos.

5. Parven et al. [32]: presenta un diagrama de flujo para el proceso de especificación de requisitos seguros y usables, que describe los principales pasos para identificar requisitos funcionales y no funcionales que identifican requisitos de seguridad y usabilidad.

6. Kainda et al. [34]: proponen un modelo de amenaza de seguridad y usabilidad detallando los diferentes factores que son pertinentes a la seguridad y usabilidad, junto con un proceso para evaluarlos.

7. Faily et al. [35]: describen un estudio utilizando técnicas de seguridad y usabilidad en un proyecto de investigación y desarrollo para desarrollar un entorno de software seguro y multiplataforma para aplicaciones web.

8. Hausawi & Allen [71]: proponen principios para seleccionar las herramientas de diseño adecuadas con el fin de apoyar la integración de usabilidad y requisitos de seguridad en la fase de diseño de software y resolver conflictos entre ellas.

Para que este análisis sea lo más objetivo posible, se establecieron los siguientes criterios comparativos:

1. **Criterio 1**: El proceso propuesto usa principios o guías de diseño para seguridad usable.

2. **Criterio 2**: Uno de sus principales objetivos es lograr un equilibrio entre seguridad y usabilidad para el diseño de interfaces.

3. **Criterio 3**: Se presenta propuestas de evaluación de seguridad usable tanto por expertos como para usuarios y el cumplimiento de los requerimientos relacionados para el mejoramiento de las interfaces.

4. **Criterio 4**: Los resultados de las propuestas están presentados cualitativa y cuantitativamente para un mejor entendimiento o posterior mejoras.

5. **Criterio 5**: Considera el diseño centrado en el usuario en el proceso de desarrollo y diseño para interfaces seguras y usables.

6. **Criterio 6**: El modelo propuesto ha sido validado a partir de casos reales.

Tabla 6.2: Comparación con los trabajos de investigación relacionados.

Criterio	[107]	[23]	[79]	[106]	[32]	[34]	[35]	[71]
Criterio 1	-	✓	-	-	✓	✓	✓	✓
Criterio 2	-	✓	✓	✓	✓	-	✓	✓
Criterio 3	-	-	✓	✓	-	✓	✓	✓
Criterio 4	-	-	✓	✓	-	-	-	-
Criterio 5	✓	✓	-	-	-	-	-	-
Criterio 6	✓	✓	✓	✓	-	-	✓	✓

Como se puede observar en la Tabla 6.2, nuestra propuesta para el proceso de diseño podría cubrir los cinco primeros criterios comparativos establecidos para este análisis, debido a que todos ellos se encuentra de una u otra forma incluidos en el desarrollo de esta tesis. El último criterio no se aborda debido a que se encuentra por fuera del alcance de la presente investigación. Sin embargo, la validación de esta propuesta puede ser realizada como trabajo futuro debido a que los principios y la evaluación ya han sido validadados en capítulos anteriores.

Consideramos que, además de los criterios anteriores, es necesario incluir carencias de los procesos de diseño de seguridad usable como las siguientes: mientras unas están enfocadas al análisis de requisitos [23] [32][34][35][71], otros son procesos muy técnicos, complicados de implementar y no tienen en cuenta a los usuarios para sus diseños [79], otras propuestas no tienen una etapa de diseño como tal [32][34], otras carecen de un componente de usabilidad más amplio [79], la etapa de evaluacion es muy pobre [23] y muy pocas se relaciona con el diseño centrado en el usuario [107][23].

La falta de principios adecuados como se ha indicado anteriormente constituye un obstáculo en el camino hacia la elaboración de un proceso para el desarrollo y evaluación de aplicaciones usables y seguras. La idea con lo anterior no es "*reinventar la rueda*"(proponer un proceso USec desde cero), sino que a partir de modelos ya existentes, unir las piezas más importantes y comunes para que exista un proceso donde la seguridad y usabilidad trabajen en conjunto.

Es posible determinar que a partir de las propuestas de los trabajos previos (ver Tabla 6.2), se puede complementar dichos estudios y adaptarlo a un modelo más completo y validado del diseño centrado en el usuario – el MPIu+a [41]. Los trabajos previos de la Tabla 6.2) junto con el MPIu+a constituyen esas piezas que anteriormente mencionamos debido a que estas propuestas tienen muchas características en común. Además, los resultados obtenidos en esta investigación con respecto a los principios propuestos y la evaluación, permite también ser adaptado al modelo MPIu+a.

6.5. ¿Por qué MPIu+a?

La base científica de la metodología MPIu+a se centra en establecer un puente entre la ingeniería del software (compuesto por análisis de requisitos, diseño, implementación y lanzamiento) y la interacción humano-computador con el fin de constituir una relación adecuada entre ambas [41]. Además, como se detalló en la Sección 6.3, existe también una fuerte relación entre la seguridad y la ingeniería del software debido a un mayor uso de enfoques basados en la seguridad para apoyar las actividades de desarrollo del software, tales como requisitos, diseño e implementación [104]. Por otro lado, debido a que el modelo MPIu+a presenta una base sólida sobre la usabilidad, lo anterior representa una de las razones principales por lo cual se escogió esta metodología como propuesta para incluir los resultados de esta investigación con el fin de incluir la parte de seguridad en el modelo, y con ello poder diseñar aplicaciones seguras y usables.

Como su autor lo menciona [41], el modelo incorpora, además, aspectos relacionados con la necesidad de ofrecer un acceso globalizado para todas las personas, indistintamente de sus cualidades o de sus capacidades físico-cognitivas. Además, sea capaz de adecuarse a los diferentes modelos mentales de los integrantes de los equipos de desarrollo multidisciplinares.

Entre las principales características del modelo con base en las necesidades de nuestra investigación podemos rescatar las siguientes [41]:

1. *Organización conceptual*: A partir del conocimiento científico existente, organiza cada concepto en el lugar adecuado.

2. *El usuario*: El usuario está en el centro del desarrollo y en las fases que son parte del modelo.

3. *Sencillo*: El modelo es conciso, con pocos nodos y ramificaciones y sin caminos condicionales que dificultan su comprensión.

4. *Equipos multidisciplinares*: Existe la necesidad y a la vez la valiosa aportación que supone trabajar con equipos multidisciplinares (sociólogos, psicólogos, diseñadores gráficos, programadores, entre otros). Sin embargo, esta característica puede ser un arma de doble filo para nuestra propuesta ya que aunque área de la seguridad utilizable es intrínsecamente multidisciplinario, mezclar conocimiento del area del HCI con el conocimiento de seguridad y privacidad es todavia un reto para los investigadores [109]. Lo anterior no quiere decir que sea imposible esta mezcla, sino que es necesario mayor investigación para llevar a cabo esta unión.

5. *Flexibilidad*: El modelo no tiene ni un sentido lineal ni restrictivo, sino que fomenta la libre aplicación del mismo.

6. *Validación*: El modelo ha sido validado a través de experimentación real.

Con base en las características anteriores, su base científica y al principal objetivo de este trabajo, **el diseño centrado en el usuario**, consideramos que este modelo es una alternativa acorde a los intereses propuestos en esta investigación.

6.6. Proceso de diseño para USec y Autenticación

A medida que el uso del Internet aumenta, la seguridad se hace cada vez más importante. Para garantizar un nivel de seguridad alto, los enfoques actuales se centran en pruebas de ataques, algoritmos seguros o pruebas de código [104]. La razón principal de la falla de los sistemas de seguridad existentes está en su mal uso . Esto lleva a la conclusión de que los sistemas de seguridad no son apropiados para la mayoría de los usuarios. Además, si la herramienta de seguridad es compleja y difícil de entender, la mayoría de los usuarios no están dispuestos a aplicar esa herramienta [23].

Actualmente existen varios métodos para incorporar los temas seguridad en el diseño del software [104], sin embargo, hay un aspecto importante del diseño de sistemas seguros que ha sido descuidado: la incorporación de la usabilidad en los aspectos de seguridad (USec) [79]. Sin embargo, el enfoque de la USec no es solo diseñar buenas interfaces [83][9], sino emplear procesos de diseño para desarrollar sistemas seguros y usables.

La necesidad anterior introduce un problema serio en el proceso de desarrollo para USec, y se ha hecho poco esfuerzo para llevar esto a cabo. En la Sección 2.6.3 se presentaron algunos principios de diseño para seguridad usable, pero ninguno de ellos proporciona asistencia o guía práctica para los desarrolladores. En el mejor de los casos, se les da un medio de analizar un sistema, no para diseñarlos [79].

Durante las últimas dos décadas, varios investigadores han introducido diferentes modelos para facilitar el desarrollo de sistemas de seguridad usable [35][23][32]. A pesar de ello, la investigación en este ámbito aún requiere dedicar más esfuerzos a fin de llegar a un buen equilibrio entre los requisitos de seguridad y usabilidad [106]. Por lo tanto, un modelo preliminar que integre los aspectos de seguridad y usabilidad es necesario con el fin de garantizar un mayor equilibrio entre estos dos atributos.

Con el propósito de ubicarnos en el estado del arte con respecto a los procesos de diseño para seguridad usable (ver Sección 6.4) y las etapas del modelo MPIu+a, en la Tabla 6.3 es presentado una comparación de los modelos USec más relevantes y cada una de las etapas del MPIu+a.

Como podemos ver en la Tabla 6.3, la mayoría de los modelos para el desarrollo de sistemas seguros y usables se centran en el análisis de requisitos, el diseño y su evaluación que son parte de las etapas del MPIu+a. Además de lo anterior y con base en el trabajo de esta investigación, se intentará ampliará el modelo MPIu+a teniendo en cuenta los aspectos más importantes del análisis de requisitos, el diseño y la evaluación con respecto

Tabla 6.3: Comparación MPIu+a y trabajos relacionados USec.

Fase	[107]	[23]	[79]	[106]	[32]	[34]	[35]	[71]
Análisis de Requisitos	✓	✓	✓	✓	✓	✓	✓	✓
Diseño	-	✓	-	-	-	-	-	✓
Implementación	-	✓	-	-	-	-	-	-
Lanzamiento	-	-	-	-	-	-	-	-
Prototipado	-	-	-	-	-	-	-	-
Evaluación	-	✓	-	-	✓	-	-	✓

a la seguridad usable y que puedan contribuir a su equilibrio.

Las fases de implementación, lanzamiento y prototipado no se tuvieron en cuenta en la propuesta debido a que con base en los resultados de esta tesis y de trabajos previos, no existe una fundamentación sólida de cómo desarrollar estas fases para el área de la seguridad usable. Sin embargo, consideramos que debido a que el modelo MPIu+a se basa en la ingeniería de software y esta a su vez en la ingeniería de la seguridad, las fases de implementación, lanzamiento y prototipado podría llevarse a cabo para diseñar sistemas seguros y usables. Para asegurar lo anterior, es necesario una investigación adicional con el fin de comprobar lo anteriormente mencionado.

Con base en los resultados de los capítulos anteriores, se presenta una aproximación gráfica de los elementos que se añaden a la metodología MPIu+a con el fin de que esta metodología tenga la componente de seguridad, ver Figura 6.2. Consideramos que realizar una notación gráfica completa para seguridad usable y autenticación es una tarea compleja, esto es debido a que se deben estudiar más a fondo algunos de los elementos que no se han tenido en cuenta en este proceso (implementación, lanzamiento y prototipado) que puedan ser aplicados al área de la seguridad usable, además, es necesario tener un consenso entre las personas involucradas (HCI, USec y seguridad) para realizar tal notación.

En la Figura 6.2 se puede observar algunas de los elementos que se han añadido a la metodología MPIu+a. En la etapa de análisis de requisitos se ha agregado los principios de USec y autenticación, la inclusión de expertos en seguridad en el equipo multidisciplinar y el análisis de riesgo como base para un sistema seguro. En la etapa de diseño se incluye los principios de USec y autenticación que son necesarios para el diseño de interfaces usables y seguras, usando una aproximación empírica. Por último, en la etapa de evaluación se incluye la métrica para obtener el nivel USec e impacto, la matriz de riesgo usando las métricas anteriores, y un conjunto de actividades (ver Sección 5.5) para realizar test de usuario para aspectos de seguridad y privacidad.

Con el fin de realizar un resumen de las actividades que se añaden al modelo MPIu+a con los aportes de este trabajo de investigación, en la Tabla 6.4 se presenta cada fase de modelo (análisis de requisitos, diseño y evaluación) junto con sus principales actividades

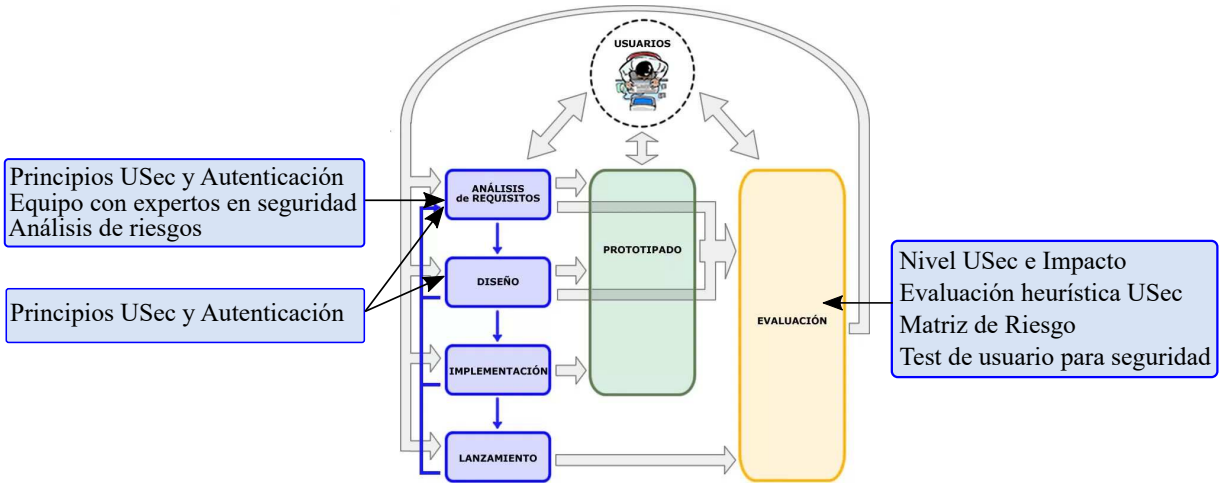


Figura 6.2: Aproximación gráfica del MPIu+a con los resultados del trabajo (MPIu+a+s) (Basado en [41]).

propias en el campo de la USec. Es importante aclarar que para que la Tabla 6.4 esté completa, es necesario mayor estudio ya que estas actividades se basan en los resultados de la presente investigación. En las siguientes secciones se analizará cada una de estas fases con cada una de sus actividades.

6.6.1. Análisis de Requisitos

La usabilidad es un factor crítico que afecta el éxito o el fracaso de los sistemas desarrollados. Además, el factor de seguridad no es menos importante, cuyo propósito es proteger a los usuarios de posibles ataques informáticos [168]. Debido a que la usabilidad y la seguridad son requisitos no funcionales [168], los requisitos de seguridad como los de usabilidad no deben agregarse al sistema en etapas posteriores sino, manejarlos en etapas tempranas de desarrollo.

Sin embargo, el equipo de desarrollo por lo general se ocupa de estos requisitos (usabilidad y seguridad) de una manera separada, donde siempre centran sus esfuerzos para desarrollar sistemas con propiedades de alta seguridad sin tener en cuenta cómo estas propiedades son fáciles de usar para los usuarios finales. Este comportamiento conducirá a desarrollar sistemas seguros que no satisfagan los objetivos de los usuarios finales [106].

La seguridad y la usabilidad son dos atributos importantes de calidad del software que deben incorporarse al software durante la fase de requisitos [32]. Sin embargo, la implementación de ambos es problemática porque los objetivos de seguridad y usabilidad pueden ser conflictivos [9].

Por tal motivo, la comunicación con los usuarios es un aspecto prioritario para las empresas que desarrollan sistemas software; aun así confían más en la experiencia acumulada

Tabla 6.4: Actividades USec para las fases del modelo MPIu+a. (Basado en [41])

Fase	Características	Actividades
Análisis de Requisitos	- Clasificación de Usuarios - Implicados - Objetivos - Análisis de riesgo	- Para la clasificación de los usuarios se realizan cuestionarios de acuerdo a sus perfiles, con base en una encuesta y al contexto. - Se identifican los implicados a partir de posibles aproximaciones metodológicas (e.g. *Center for HCI Design y Computer Science Department*). Luego de su identificación se realiza reuniones donde se decide entre otras cosas, el propósito de desarrollo del sistema interactivo donde la seguridad es pieza fundamental, quienes son los usuarios potenciales, cuáles son los principales objetivos de la seguridad usable, etc. - En los objetivos se tienen en cuenta aspectos de usabilidad y seguridad concretos para cada aplicación. Para llevar a cabo esto se tienen en cuenta las las heurísticas de Nielsen para USec y las recomendaciones presentadas en en Anexo D. - En el caso del análisis de riesgo, las actividades que se podrían tener en cuenta es el comportamiento de los usuarios usando el método de *eye tracking* presentado en la Sección 5.7. En ella es presentado las etapas organizadas para tal fin.
Diseño	- Aproximación empírica	En este caso, es posible adoptar algunas actividades de la Sección 5.6. Se inicia una recogida de información de la literatura con base en requerimientos USec de acuerdo al contexto, y luego se adapta a los principios de diseño de acuerdo al Anexo D.
Evaluación	- Indice USec e Impacto - Evaluación heurísica USec - Método de test USec - Matriz de Riesgo	Las actividades para la evaluación USec han sido presentadas en las Secciones 5.4 y 5.5. Estas actividades se dividen en planeación, desarrollo y análisis de resultados.

que no en la aplicación de métodos pensados para capturar la experiencia de los usuarios y sus verdaderas necesidades [41].

6.6.1.1. Clasificar a los usuarios

Una forma de clasificar a los usuarios es a través del perfil de usuario, siendo los cuestionarios y las entrevistas los más utilizados y con más que probada utilidad para esta finalidad [41].

El objetivo principal de las entrevistas con los usuarios es hacerse una idea de lo que los usuarios piensan de la seguridad de la información. Más específicamente, estar interesados en los riesgos que los usuarios perciben y en lo que ellos sienten que necesitan proteger, así como cuánto quieren estar involucrados en tomar estas decisiones de seguridad. Otro objetivo es conocer en quién confia el usuario y sobre qué base y también qué tipo de conceptos y términos usan cuando se habla de seguridad [107].

Las entrevistas o la observación de los grupos de usuarios objetivo es indispensables como se comentó anteriormente. Sin embargo, preguntar a los usuarios sobre sus objetivos de seguridad deseados puede causar un problema. Ciertamente, ellos quieren ser protegidos lo más efectivamente posible. Pero la pregunta realmente interesante es qué esfuerzo están dispuestos a soportar, es decir sus tareas con el fin de garantizar su nivel personal de seguridad sin que esto conlleve a una frustración [23].

Una vez obtenido estos datos, es posible identificar algunas características de los usuarios y las tareas que podrían realizar el cual será incluido en el sistema, permitiendo que el conflicto entre seguridad y usabilidad sea evitado.

6.6.1.2. Implicados (*stakeholders)*

Los implicados representan a las diferentes partes interesadas en el sistema y están activamente involucradas en el proceso de obtener los requisitos de usabilidad y seguridad, con el fin de decidir los objetivos de la usabilidad y las posibles medidas de seguridad. Esto se debe a que los interesados del sistema tienen el conocimiento de dominio más pertinente. Por lo tanto, cualquier decisión tomada por estas partes interesadas debe tener en cuenta sus diferentes necesidades – específicamente la necesidad de la seguridad usable [79].

El primer paso es, por lo tanto, identificar y asegurar el compromiso de las partes interesadas que participarán en ese diseño del sistema seguro y usable. Hay cuatro tipos principales de roles que pueden diferenciarse (aunque en el modelo MPIu+a encontramos otros):

1. **Tomar las decisiones**: consisten en la gestión del proyecto, los propietarios (clientes que comisionan el sistema) y cualquier otra persona que tenga un papel decisorio en el desarrollo del sistema seguro.
2. **Desarrolladores**: representa el aspecto técnico del equipo de diseño, responsable de la captura y análisis de los requisitos del sistema hasta el diseño y la implementación. Estos incluyen programadores, diseñadores, expertos en seguridad, diseñadores de interfaces usables, etc.

3. **Usuarios**: Son las personas con las que debe diseñarse el sistema y, como tales, son una fuente importante de requisitos del sistema.

4. **Facilitadores**: Son las personas que documentan las reuniones y sirven como mediadores en general.

Es fundamental garantizar la participación de estos implicados ya que las personas que toman las decisiones están mejor preparados para hacer frente a la aplicación los requisitos de seguridad, los desarrolladores son necesarios para la implementación de técnicas de seguridad, los usuarios representan la fuente vital para los requisitos de usabilidad del sistema y los facilitadores que garantizan el buen funcionamiento del proceso de diseño [79].

Un aspecto adicional importante durante esta fase es determinar a un solo individuo que tendrá el rol de lider para la implementacion de las características seguridad del proyecto. La responsabilidad asociada con este rol es documentar la toma de decisiones, citando los argumentos y razones de la decisión, y dar una palabra final en cualquier desacuerdo que pueda ocurrir durante el proceso [79].

6.6.1.3. Objetivos

Uno de las tareas más importantes de cualquier proceso es recopilar los requisitos y luego identificar los requisitos funcionales y no funcionales. Se utiliza básicamente para obtener los objetivos de calidad del proceso. En este proceso se identificarán básicamente los objetivos con respecto a la seguridad y su usabilidad [32].

Algunos de los objetivos con el fin de obtener un equilibrio adecuado entre los atributos de usabiliad y seguridad son presentados por Realpe et al. [169] y Khalid et al. [106]. En ellos, los autores presentan un conjunto de requerimientos para USec y una relación adecuada de las propiedades de seguridad (confidencialidad, autenticidad, no repudio, registro e integridad) junto con algunos principios de usabilidad (facilidad de aprendizaje, estética, protección contra errores, efectividad, eficiencia, productividad, satisfacción y operabilidad). El principal objetivo de los autores es aclarar los requisitos de usabilidad que se requieren se logran a través de cada requisito de seguridad con el fin de identificar tales requerimientos de una manera más adecuada.

A modo de ejemplo, vamos a listar algunos de estos objetivos teniendo en cuenta en esta investigación y los presentados por Realpe et al. [169] y Khalid et al. [106]:

- El usuario será capaz de comprender el significado del nivel de seguridad que se presenta en la interfaz.

- La información de seguridad presentada en pantalla será relevante.

- Los usuarios deben aprender y recordar fácilmente los pasos de autenticación.

- Es necesario que existan indicadores visuales informando a los usuarios sobre las prácticas de privacidad del sistema.
- Los usuarios serán capaces de autenticarse de manera efectiva y segura con el menor número de recursos.

6.6.1.4. Análisis de riesgo

El análisis de riesgos y amenazas tienen que estar necesariamente presente porque constituye la base del desarrollo para un sistema seguro. El usuario como tal constituye la primera amenaza para el sistema. El usuario puede ser un atacante si intenta perjudicar la integridad y privacidad de terceros [23].

El comportamiento de los usuarios debe considerarse como parte de los riesgos. Por ejemplo, si el usuario comete errores, esto constituye una seria amenaza de seguridad. El análisis visto en la Sección 5.7 es un claro ejemplo sobre la amenaza a la seguridad cuando los usuarios comenten errores en el sistema de votación electrónica. El análisis de riesgo se lleva a cabo teniendo en cuenta si la interfaz presenta pobre seguridad usable (e.g. no teniendo cifrado de mensajes usando el protocolo HTTPS) y las posibles consecuencias que podría esto tener.

El análisis de riesgos intenta determinar qué vulnerabilidades afronta el sistema para incorporar al diseño, las medidas necesarias de seguridad apropiadas a las amenazas latentes y ser lo más eficientemente posible frente a estas vulnerabilidades. El conocimiento de las amenazas y vulnerabilidades existentes y pasadas es esencial, así como la presencia de conocimientos especializado en seguridad para interpretar y adaptar esta información a la situación real [79].

Debido a que en esta investigación no se tienen en cuenta las amenazas, se explicará brevemente los elementos que podrían llevar a cabo un análisis de riesgos muy aproximado a la realidad [142].

1. **Identificar impacto**: El nivel de impacto de una amenaza es la magnitud del daño que se puede esperar que resulte de las consecuencias de la divulgación, modificación o la pérdida no autorizada de la información.
2. **Identificar Vulnerabilidades**: Las vulnerabilidades son áreas del sistema que son susceptibles de explotación. Aquí es donde se vuelven importantes los avisos de seguridad (e.g. iconos), el buen conocimiento de las tecnologías que se están utilizando y la información sobre los ataques pasados.
3. **Identificar los riesgos**: El riesgo es la probabilidad de que un ataque sea llevado con éxito una o una secuencia de vulnerabilidades para comprometer un sistema. Esta información es generalmente mejor adquirida de expertos en seguridad que tienen el conocimiento y la experiencia necesarios para evaluar estos riesgos.

6.6.2. Diseño

Se llega a la fase de diseño tras realizar actividades relacionadas con el análisis de requisitos que proporcionan información necesaria para que el equipo de desarrollo sea capaz de modelar el sistema para, posteriormente, proceder a su codificación [41].

Básicamente existen dos maneras de abordar el diseño de los sistemas interactivos [41]:

1. *Aproximación empírica*: El diseño se basa en la propia experiencia del diseñador o bien en la de otros diseñadores que se recoge mediante compendios de recomendaciones (principios de diseño, reglas de oro, estándares, etc.), más o menos relevantes para la construcción de un interfaz con éxito. Estos resultados generalmente están avalados por unos estudios de evaluación realizados por el usuario (evaluación de usabilidad).

2. *Aproximación metodológica*: Basada en unos fundamentos teóricos y en la aplicación de una serie de pasos para la realización del diseño.

Debido al enfoque de la presente investigación, el diseño de sistemas seguros y usables esta basado en principios o guías de diseño de las aportaciones teóricas más relevantes, por lo tanto, la manera para diseñar sistemas donde la seguridad y usabilidad estén presentes es a partir de la aproximación empírica. Aunque no es la mejor forma de realizar este tipo de diseños, sin embargo, consideramos que es un punto de partida para futuras investigaciones donde se plantee el diseño de sistemas usando aproximaciones metodológicas para seguridad usable.

Con base en la aproximacion empírica, en la fase de diseño se deben obtener sugerencias para la interfaz de usuario sin depender de mecanismos de seguridad abstractos y complicados [71]. Nielsen [58] sugiere seguir ciertos principios para diseñar una interfaz de usuario usable. Sin embargo, estos principios no tiene en cuenta aspectos de seguridad y por lo tanto no son suficientes para el diseño de sistemas interactivos seguros y usables [23].

A partir de los resultados obtenidos en el Capítulo 4, se presenta en el Anexo D las recomendaciones para el diseño aplicaciones seguros y usables. Recomendaciones que hacen parte de la aproximación empírica con el fin de diseñar sistemas interactivos, en este caso, aplicaciones donde la componente de usabilidad y seguridad se encuentran presentes.

6.6.3. Evaluación

Evaluar consiste en probar algo. Tanto para saber si funciona correctamente como no, si cumple con las expectativas o no, o simplemente para conocer cómo funciona una determinada herramienta o producto. En esta fase es donde se aplican las técnicas necesarias para recibir la realimentación por parte de los usuarios y/o evaluadores expertos que se verá reflejado en el diseño de los sistemas interactivos seguros y usables. [41].

6.6.3.1. Evaluación Heurística

La evaluación heurística es un método de inspección cuya principal característica es que hay unos expertos, conocidos como evaluadores, que examinan (inspeccionan) aspectos de la interfaz del sistema relacionados con la usabilidad y la seguridad que la misma ofrece a sus usuarios.

Este es quizás el "corazón" de esta investigación (justificado en la Sección 2.4.1), el cual se basa en principios de seguridad usable y autenticación de usuario. Haciendo referencia a estos principios, los expertos en usabilidad y seguridad analizan la interfaz de usuario. Es necesario mencionar que aplicar la evaluación heurística sola no es suficiente porque se centra en el diseño de la interfaz de usuario sin tener en cuenta las funcionalidades y procesos subyacentes. Con un base en metodos de test, los problemas subyacentes causados por el modelado de procesos inadecuados pueden ser reconocidos [23].

Aportes de esta investigación al método heurístico

Después de realizar la validación de los principios propuestos para seguridad usable y autenticación, introducimos algunos aportes con respecto a este método.

1. Se toman las heurísticas de Nielsen para ser adaptadas a aspectos de seguridad y usabilidad.
2. Se tienen en cuenta algunos atributos de calidad (accesibilidad, operablidad, fiabilidad y desempeño) para ser incluidos en la evaluación heurística para USec y autenticacion.
3. Cada atributo dispone de una serie de sub-heurísticas y descripciones que ayudan notablemente a los expertos con el fin de mejorar los resultados de la prueba.
4. El evaluador a partir de su conocimiento valora cada sub-heurístico con base:
   - **Severidad**: este nivel de severidad es un indicador del nivel de cumplimiento de cada sub-heurística teniendo en cuenta la usabilidad y seguridad.
   - **Impacto**: el impacto evalúa la consecuencia de un sistema cuando la sub-heurística evaluada presenta algún grado de debilidad.

6.6.3.2. Método de Test

En los métodos de evaluación por test, usuarios representativos trabajan en tareas concretas utilizando el sistema, y el coordinador de la evaluación, utiliza los resultados para ver cómo la interfaz de usuario da soporte a los usuarios con sus tareas [41].

Whitten & Tygar [9] afirman que los aspectos de seguridad y privacidad rara vez son el objetivo principal del usuario. Debido a lo anterior, las tareas de seguridad pueden ser omitidas en la interfaz generando con ello riesgos debido a los errores que puedan cometer.

Un análisis de tareas puede ser usada para comprender las tareas básicas e infrecuentes que los usuarios necesitan o desean completar para lograr sus objetivos. Con base en un análisis en la realización de tareas, los usuarios proporcionarán información que ayudará a establecer las mejoras que podría tener el sistema para obtener una mayor seguridad usable.

De acuerdo con Markotten [23], la evaluación heurística no es suficiente para encontrar problemas de seguridad usable, para ello, se combina la evaluación heurística con la observación del usuario. A cada usuario se le presentan tareas para que sean capaces de realizar en el sistema. Estos usuarios son observados durante la ejecución de cada tarea para ver cómo utilizaban la interfaz durante su realización, cuánto tiempo tardan y la éxito o fracaso de la misma.

La evaluación heurística y el desarrollo de tareas presentan datos cualitativos y cuantitativos a la vez que distingue las dificultades de los usuarios cuando la seguridad esta inmerso en la tarea. Los datos recopilados son analizados para proporcionar aspectos importantes relacionados con la usabilidad de la seguridad del sistema.

Un aspecto importante en la realización del método por test, es seleccionar las tareas más representativas que los usuarios deben realizar para aplicaciones donde la usabilidad y seguridad están presentes. En esta investigación se seleccionan las tareas teniendo en cuenta la literatura donde consideran las tareas más habituales del sistema con el fin de obtener resultados sobre las dificultades que pueden tener los usuarios donde aspectos de seguridad estén presentes. En este método, métricas de tiempo y porcentaje de éxito en las tareas son obtenidas.

También es importante aclarar que realizar el metodo de test a partir de análisis de tareas y observaciones es respaldada por algunas investigaciones [120][26][119]. Estas investigaciones afirman que en el campo de la seguridad usable, la evaluación por el método de test para la usabilidad es perfectamente válido para evaluar sistemas donde la seguridad es parte fundamental. En esta investigación, no se propone un método de test específico para seguridad usable debido a que no forma parte del alcance de la presente investigación, sin embargo, esto puede ser parte de una propuesta de investigación para proponer métodos de evaluación particular para el área de la seguridad usable, debido a que no se presenta en la literatura actual este tipo de métodos aplicados exclusivamente para seguridad usable.

6.6.3.3. Matriz de riesgo

Una matriz de riesgo representa un resultado de la cantidad de daño (con respecto a la confidencialidad, integridad y disponibilidad de la información), que se puede esperar que ocurra durante un período de tiempo dado debido a un evento de específico por ejemplo, una vulnerabilidad o amenaza.

Los datos severidad e impacto proporcionado por los expertos pueden usarse para de-

terminar una matriz de riesgo de la aplicación. Con base en esta métrica, el equipo de desarrollo puede saber si el sistema diseñado es lo suficientemente bueno con respecto a posibles ataques debido a la pobre seguridad usable que pueda tener.

6.7. Discusión

Las herramientas de seguridad de hoy en día son complejas e incluirlas eficientemente en interfaces de usuario representan todo un reto. Se necesitan nuevas ideas y conceptos para resolver este problema. De alguna manera, la usabilidad y la seguridad están orientadas en oposición. Con el fin de tratar de que estos dos objetivos no se alejen entre sí y teniendo como pilar principal las necesidades de los usuarios, se propone una serie de elementos que permitirían a los desarrolladores y a la comunidad científica, tener un primer proceso de diseño para seguridad usable mediante un enfoque centrado en el usuarios.

Ciertamente, el proceso propuesto aún no se ha completado o ha sido elaborado en detalle. Pero en esta etapa, es posible dar una impresión del gran impacto que podría tener sobre algunas mejoras para las aplicaciones con respecto a la usabilidad de las herramientas de seguridad. Además, si la propuesta demuestra su validez, permitiría a los usuarios concentrarse en los aspectos de seguridad y con esto aumentar su satisfacción, evitando con esto posibles riesgos de seguridad con respecto a su información privada.

Como se observa en todo es capítulo, integrar las actividades de la Interacción Humano–Computador con las actividades de desarrollo en el dominio de seguridad es un reto muy prometedor. Para validar esta propuesta es necesario empezar con una aplicación o proyecto pequeño o mediano como un caso de prueba o medio de aprendizaje. Es importante como lo dice el autor de la metodología MPIu+a, incluir en él, un equipo multidisciplinario de expertos en seguridad informática o de seguridad usable con el fin de que la experiencia del equipo sea más grande y optima. Para tal fin, es necesario mantener discusiones del equipo adecuadas en ambos campos (HCI y seguridad), aunque puedan existir diferencias con la finalidad de que pueda construirse productos cada vez mejores para las organizaciones y el bien de los usuarios.

Como una de las principales aportaciones en este capítulo, podemos decir que se introduce por primera vez y muy escuetamente, la seguridad en la metodología MPIu+a como requisito de calidad en el ciclo de vida del desarrollo del software, aspecto que se ha visto casi siempre como parte separada del diseño centrado en el usuario.

Capítulo 7

Conclusiones y Trabajo Futuro

7.1. Conclusiones

Tradicionalmente, los factores humanos y los problemas de usabilidad han desempeñado un papel limitado en la investigación de seguridad y en el desarrollo de sistemas seguros. Los expertos en seguridad han ignorado en gran medida los problemas de usabilidad, ya que a menudo no reconocen la importancia de los factores humanos porque carecen de la experiencia necesaria para abordarlos. Pero hay un creciente reconocimiento de que los problemas de seguridad actuales pueden resolverse si se abordan problemas de usabilidad y factores humanos.

La seguridad y la Interacción Humano-Computador son cada vez más importantes para los usuarios para todo tipo de aplicaciones. Para desarrollar un software seguro y usable, los expertos en seguridad y HCI deben trabajar juntos en la etapa más temprana posible del diseño y participar en un debate para determinar la solución más óptima. Mantener el proceso particularmente simple para el usuario y sea claro y transparente en su comunicación. Sólo se encontrará el equilibrio óptimo al tenerlo probado minuciosamente por los usuarios.

A medida que la autenticación de usuario se vuelve más necesaria, las tecnologías para lograrlo serán más convenientes a través del uso de requisitos y herramientas de diseño. Dado que la comunicación de la intención es vital para la seguridad, la interfaz de usuario también es un componente clave para lograr la seguridad, no el único aspecto al diseñar los métodos de autenticación para el usuario. Con base en lo anterior, en este trabajo se ha investigado los principios en el área de la suguridad usable para métodos de autenticación de usuario el cual se espera guiar el desarrollo de sistemas de autenticación verdaderamente seguros y usables.

La importancia que tiene la seguridad usable en los sistemas informáticos actuales ha sido mencionado varias veces a lo largo de este trabajo de investigación. Sin embargo, y aunque la investigación en esta área del conocimiento ha ido incrementándose, hace falta mas trabajo en este campo y esto debido a, como se mencionó en el Capitulo 2, es una tarea difícil llevar a la seguridad y usabilidad de forma lineal. Realizar trabajos de investigación

en el campo de la seguridad usable es un desafío grande, esto se debe principalmente a que el investigador debe tener una clara comprensión de las áreas de seguridad informática y la usabiliad, que como se dijo anteriormente, estos dos atributos entran en conflicto principalmente como consecuencia de las metodologías y objetivos que tienen.

Tratando de obtener soluciones para tener un *trade-off* entre estos dos atributos (usabilidad y seguridad) se propone un conjunto de principios para aquellas aplicaciones (e-commerce, e-banking, redes sociales y autenticación) donde el usuario deba usar las características de seguridad y que sean fáciles de entender y usar. Un conjunto de principios para seguridad usable, incluyendo la autenticación de usuario, permite a los desarrolladores tener herramientas solidas que pueden ayudarles a mejorar sus diseños. Por lo tanto, obtener en este trabajo un conjunto de principios de diseño más completo junto con un grado de importancia, constituye una contribución fundamental para los desarrolladores de software. El hecho de obtener este conjunto usando un proceso de desarrollo heuristico a través de distintas metodologías donde se demostró su validez y eficacia, no solo constituye una gran aportación para la seguridad usable sino también para el campo del HCI que podría hacer uso de dicho proceso.

Con base los principios obtenidos en este trabajo, se propuso una integración entre el estándar ISO 9241-210 con el proceso de desarrollo heurístico donde se presenta ciertas actividades para evaluar la seguridad usable y métodos de autenticación de forma cualitativa y cuantitativa, teniendo en cuenta algunos atributos y características de la norma ISO/IEC 25010:2011. Muchos usuarios no son capaces de percibir los problemas de seguridad correctamente, generando con esto un grado un riesgo en los aspectos de seguridad debido a posibles malentendidos y evitar tácticas para proteger el sistema. Aunque existen diferentes métodos para evaluar la usabilidad de los sistemas de seguridad, estos métodos no están lo suficientemente maduros debido a la falta de principios adecuados.

Con el fin de obtener resultados lo mas objetivamente posible, en este trabajo de investigación se lleva a cabo una serie de actividades de forma ordenada. Estas actividades se agrupan en un proceso el cual está constituido por una etapa de planeación, ejecución y análisis de resultados. Solano [51] presenta estas actividades para la evaluación de la usabilidad de sistemas interactivos. Con base en los resultados obtenidos, encontramos que estas etapas son perfectamente aplicables al área de la seguridad usable, confirmando algunos de los postulados presentados en la literatura como el que las personas son en realidad el eslabón mas débil en cuanto a seguridad se refiere.

Los resultados obtenidos por parte de los usuarios con base en la realización de distintas tareas para la red social Facebook y de voto electrónico, demuestra lo mencionado con respecto a la literatura, los aspectos de seguridad y privacidad no representa un objetivo importante para los usuarios. Es más preocupante para la red social Facebook ya que en ocasiones, la información es publica y cualquier persona con acceso a Internet puede acceder a ella. El porcentaje de éxito para realizar tareas de configuración de seguridad y privacidad es bajo, esto representa un riesgo latente con respecto a la información privada

que los usuarios puedan tener.

De acuerdo al modelo de desarrollo heurístico, se plantea que los usuarios a partir del desarrollo de ciertas tareas para una aplicación en particular (Facebook y e-Voting), también contribuyan con el mejoramiento del conjunto heurístico propuesto para USec y autenticación. Sin embargo la realidad fue otra, se propone que los usuarios comenten sobre mejoras en la usabilidad de las características de seguridad de la interfaz, pero debido a que los usuarios no poseen el conocimiento básico con respecto a la seguridad, la mayoría de ellos no responden de una forma objetiva a lo solicitado. Con base en lo anterior, no fue posible realizar una mejora objetiva del conjunto heurístico propuesto. Sería interesante como trabajo adicional, realizar las mismas tareas presentadas en este trabajo de investigación por usuarios con algún conocimiento en usabilidad y seguridad con el fin de que se haga una mejora al conjunto heurístico propuesto.

A lo largo de nuestra investigación, nos hemos centrado en integrar dos atributos de calidad de software conflictivos que son importantes para la mayoría de los productos de software, la seguridad y usabilidad. El objetivo de este trabajo de investigación es proponer un proceso de desarrollo heurístico y un conjunto de principios que ayude a mejorar la relación entre los dos atributos para que puedan interactuar en concordancia. Para llegar a este objetivo, esta investigación planteó tres situaciones a tratar. En primer lugar, la naturaleza de la relación entre seguridad y usabilidad no está suficientemente clara. En segundo lugar, hay una falta de trabajo de investigación sobre la integración de seguridad y usabilidad en el diseño de sistemas interactivos. Y finalmente, la mayoría de las soluciones propuestas presentan debilidades o están incompletas. Para solucionar los anterior, se hace necesario averiguar qué aspectos entre ellos son comunes entre ellos, es decir, las actividades de la seguridad y la usabilidad, e iniciar el trabajo de diseño desde los primeros pasos del proceso de desarrollo.

Una de las principales aportaciones de este trabajo de investigación representa la evaluación cuantitativa para seguridad usable. Este componente proporciona una expresión matemática de evaluación con base en los principios propuestos y su grado de importancia. Esta forma de evaluación podría ayudar que ayuda a obtener el equilibrio deseado entre seguridad y usabilidad durante el desarrollo de la aplicación. Esta forma de evaluación cuantitativa es el primero que usa principios de diseño y grado de importancia de acuerdo a la literatura. El proceso de evaluación se basa en técnicas bien conocidas del campo de la usabilidad y seguridad, principios con nivel de severidad e importancia.

Se propone un proceso, MPIu+a + USec, para un posible diseño e implementación de sistemas para seguridad usable. Como se presentó en el Capítulo 2, varias de las etapas de la ingeniería de seguridad y procesos propuestos para USec, no son del todo diferentes, muchos aspectos entre ellos son comunes. Gracias a estas similitudes, es posible proponer un proceso el cual pude ser sencillo para futuras aplicaciones en el campo de la USec. Además, este proceso puede ser útil para que expertos en seguridad se integren al equipo multidisciplinario con el fin de que la brecha entre seguridad y usabilidad se acorte aun más.

El proceso presentado en el Capítulo 6 podría constituir una primera aproximación a una metodología para ayudar a obtener el *trade-off* entre seguridad y usabilidad durante las etapas del desarrollo del software. Este proceso se basa en metodologías bien conocidas y adaptadas desde el campo de la ingeniería de software y la ingeniería de la seguridad. Aunque este proceso solo esta basado en el análisis de requisitos, diseño y evaluación para USec, esto podría proporcionar una guía sistemática para vincular los requisitos de usabilidad, seguridad y seguridad usable a herramientas de diseño apropiadas (es decir, principios de diseño, prácticas y técnicas). Aunque las fases de implementación, lanzamiento y prototipado no se aplica en este trabajo de investigación, la metodología MPIu+a muestra suficiente estabilidad y capacidad el cual podría satisfacer las necesidades de estas fases para USec que no se ha discutido.

Con base en los resultados de la presente investigación, en la Tabla 7.1 se presenta una relación entre los objetivos presentados en el Capítulo 1 y los resultados de nuestro trabajo.

Tabla 7.1: Relación entre los objetivos y resultados de la investigación.

Objetivos	**Resultados**
Identificar posibles principios de seguridad usable que permita un balance adecuado entre seguridad y usabilidad particularmente para autenticación de usuario.	1. Atributos y sub-heurísticas para USec y autenticación. 2. Adaptación de las heurísticas de Nielsen con los principios de USec. 3. Grado de importancia y su respectivo comentario para cada sub-heurística. 4. Integración de algunos atributos y características del estándar 25010:2011 con los principios de seguridad usable y autenticación. 5. Reunión con expertos en usabilidad y seguridad de La CaixaBank (España). 6. Revisión y realimentación por parte de expertos para mejorar el conjunto propuesto.
Proponer un método de evaluación para los principios de seguridad usable y que pueda contribuir en el diseño de servicios de autenticación.	1. Modelo matemático para obtener un nivel USec e impacto con base en los principios obtenidos. 2. Grado de severidad e impacto adaptados a los principios de USec. 3. Una matriz de riesgo teniendo en cuenta la vulnerabilidad (nivel USec) y el impacto.
Validar los principios y el método de evaluación en aplicaciones reales.	1. Evaluación heurística a la red social Facebook con base en los principios propuestos. 2. Matriz de riesgo a la red social Facebook con base en la evaluación heurística. 3. Validación de los principios para un sistema de e-banking (FONDUC). 4. Comportamiento de los usuarios en el uso de votación electrónica usando la técnica de *eye tracking*.
Presentar un proceso de diseño para seguridad usable y autenticación mediante un enfoque centrado en el usuario, a partir de los principios de seguridad usable y su evaluación.	1. Relación entre la ingeniería de la seguridad y el desarrollo del software. 2. Adaptación de los principios de seguridad usable y su evaluación al modelo MPIu+a. 3. Aportes al método de evaluación heurística tomando como base los principios y su evaluación.

7.2. Limitaciones

Las principales limitaciones de este trabajo de investigación son las siguientes:

- En el proceso de revisión del conjunto heurístico participaron 10 expertos, 2 de USec, 2 de seguridad informática y 6 de HCI. Aunque este número de expertos es adecuado ya que la literatura establece se que por lo general deben ser entre 3 a 5 expertos, garantizaría mejores resultados y calidad en el conjunto heurístico propuesto si el número de expertos en USec fuera mayor. Sin embargo, identificar a estos expertos y que realicen una revisión es un desafío, debido a la cantidad limitada de especialistas en esta área.

- La evaluación heurística realizada a la aplicación real fue realizada por 4 expertos de diferentes áreas, 3 de HCI y 1 de seguridad informática. Preferiblemente, los expertos en la evaluación deberían haber sido personas que tuvieran conocimiento en las dos áreas como fue posible en la revisión heurística. Sin embargo, por motivos de tiempo y disponibilidad, no fue posible realizar la evaluación a la aplicación.

- La cantidad de principios presentados en el Capítulo 4 y evaluados en el Capítulo 5, minimiza la objetividad de los evaluadores. Un evaluador afirmó que le tomó alrededor de 3 horas en completar la evaluación, proponiendo después de esto, alguna forma de evaluación mas corta. Esto se discute con más detalle en la próxima sección porque también ofrece un área para posibles investigaciones futuras.

- Los resultados del análisis de riego para la aplicación de Facebook no existe de forma cuantitativa. Por lo tanto, el análisis de este resultado se tomo con base en estudios realizados y publicados en la literatura para esta aplicación teniendo en cuenta la seguridad y usabilidad. El análisis de estas publicaciones puede ser muy subjetivo debido a que en ellos existen muchas variables externas que pueden afectar el resultado y no confirmar por completo, el riesgo real de Facebook con los resultados presentados en esta investigación.

- Los principios y su nivel de importancia propuestos en este trabajo de investigación en general no ofrecen soluciones definitivas al problema de seguridad usable. Sin embargo, este trabajo proporciona posibles soluciones de nivel severidad, impacto y riesgo con el fin de recomendar soluciones prácticas a problemas aplicaciones donde la usabilidad y seguridad sean pieza fundamental en las interfaces de usuario.

7.3. Trabajo Futuro

Como trabajo futuro de acuerdo con esta investigación podemos citas las siguientes:

- Aplicar los principios a aplicaciones de autenticación de usuario, por conocimiento, posesión o biométrico. Esto proporciona un nuevo contexto en el que evaluar USec. Con base en los resultados que podría arrojar la evaluación a estas aplicaciones, se

podría defender aun más que los principios propuestos en este trabajo se ajustan con la realidad. Es decir, aplicar estos principios en otro contexto permitirá verificar su eficacia.

- Con base en el proceso de desarrollo heurístico, se podría proponer principios para el área de la privacidad usable que aun esta en etapa inicial de investigación. Por lo tanto, la revisión de la literatura que hace parte del proceso de desarrollo heurístico se centrará en el diseño de aplicaciones donde la privacidad de los usuarios sea elemento clave. Una futura aplicación de estos principios de privacidad usable la podríamos tener en las redes sociales, donde la privacidad de los usuarios es muy cuestionada.

- Mejorar el instrumento de evaluación heurística para los expertos. La mayoría de los expertos comentaron que debido a la cantidad de principios presentados en el instrumento de evaluación, fue muy complicado realizar la evaluación de la aplicación en cuestión de una manera mas objetiva y amena. Los expertos sugieren proporcionar un proceso o metodología para obtener los principios adecuados de acuerdo a una aplicación en particular. Aumentar el interés del experto para realizar cualquier evaluación, contribuirá a un resultado optimo en la evaluación.

- Implementación de diseño de interfaz de usuario para seguridad usable aplicando la metodología del MPIu+a incluyendo aspectos de seguridad. Las implementaciones reales para USec son todavía muy limitadas. Empleando los principios y métodos de evaluación propuestos en este trabajo junto con el MPIu+a, pueden aplicarse para dar soluciones de diseño a las interfaces de usuario.

7.4. Publicaciones

A partir de los resultados de este trabajo de investigación, fueron realizadas algunas publicaciones, no obstante queda pendiente generar más publicaciones donde sean presentados los resultados finales logrados. Las publicaciones realizadas hasta el momento son las siguientes:

7.4.1. Publicaciones en Revistas

- Paulo Realpe-Muñoz, C. Collazos, J. Hurtado, T. Granollers, J. Velasco, "An integration of usable security and user authentication into the ISO 9241-210 and ISO/IEC 25010:2011", *Lecture Notes in Computer Science, Human Aspects of Information Security, Privacy, and Trust*, Vol. 9750, pp. 65-76, 2016.

- Paulo Realpe-Muñoz, César A. Collazos, Julio Hurtado, Toni Granollers, Jaime Muñoz-Arteaga, Jaime Velasco-Medina, "Eye Tracking-based Behavioral Study of Users Using E-Voting Systems", *Computer Standards and Interfaces*, 2017 (En evaluación).

7.4.2. Publicaciones en Eventos

- P. Realpe-Muñoz, C. Collazos, J. Hurtado, J. Muñoz, "Laboratorio virtual colaborativo: aprendizaje en la nube", *IX Conferencia Latinoamericana de Objetos y Tecnologías de Aprendizaje LACLO*, Manizales, Colombia, 2014.

- P. Realpe-Muñoz, C. Collazos, J. Hurtado, T. Granollers,"Towards an integration of usability and security for user authentication", *XVI International Conference on Human Computer Interaction (Interacción 2015)*, Vilanova i la Geltrú, España, 2015.

- A. Orozco, A. Gómez, P. Realpe-Muñoz, Cesar A. Collazos, "Revisión Sistemática para el Planteamiento de una Evaluación Heurística Aplicada a Sistemas E-Banking". *11 Congreso Colombiano de computación (11CCC)*, Popayán, Colombia, 2016.

- P. Realpe-Muñoz, Cesar A. Collazos, J. Hurtado, T. Granollers, "A Set of Heuristics for Usable Security and User Authentication", *XVII International Conference on Human Computer Interaction (Interacción 2016)*, Salamanca, España, 2016.

- P. Realpe-Muñoz, Cesar A. Collazos, T. Granollers, Jaime Muñoz-Arteaga, Eduardo Fernández, "Design Process for Usable Security and Authentication using an User-Centered Approach", *XVIII International Conference on Human Computer Interaction (Interacción 2017)*, Cancún, México, 2017 (en evaluación).

7.5. Trabajos de Grado Dirigidos

Título Trabajo de grado: Evaluación Heurística de Seguridad Usable Aplicada en Sistemas E-Banking.
Estudiantes: Andrés Felipe Gomez y Andrés Felipe Orozco.
Director: PhD(c) Paulo César Realpe Muñoz.
Codirector: PhD. César A. Collazos O.
Año de ejecución: 2016
Requisito: Requisito para optar al título de Ingeniero de Sistemas de la Universidad del Cauca.
Estado: Aprobado.

Anexo A

Análisis comparativo de los métodos de Autenticación

Tabla A.1: Análisis comparativo resumido de los métodos de autenticación (Creación propia).

Método	Clasificación	Ventaja/Desventaja	Usabilidad	Seguridad
Constraseña y PINs	Autenticación por conocimiento	Fácil implementación. Pueden ser olvidados.	Bajo	Bajo
Contraseñas gráficas	Autenticación por conocimiento	Puede ser recordado fácilmente. Poca aplicación.	Medio	Alto
Frases de contraseña	Autenticación por conocimiento	Fácil de implementar y usar. La seguridad se basa totalmente en la fuerza de la contraseña.	Medio	Medio
OTP	Autenticación por posesión	No son vulnerables a ataques de repetición. Incompatibilidad del software para ciertos sistemas operativos.	Bajo	Alto
Autenticación sin contraseña	Autenticación por posesión	Las contraseñas no necesitan ser recordadas. El acceso a las claves puede resultar difícil en algunos dispositivos.	Alto	Alto

Continua en la próxima página –

– *Continua desde la página anterior*

Método	**Clasificación**	**Ventaja/desventaja**	**Usabilidad**	**Seguridad**
Autenticación de acceso resumido	Autenticación por posesión	Las contraseñas no son usadas de forma directa. Algunos servidores requieren que las contraseñas se almacenen utilizando cifrado reversible.	Alto	Alto
Tarjeta electrónica	Autenticación por posesión	Las contraseñas no son usadas de forma directa. Algunos servidores requieren que las contraseñas se almacenen utilizando cifrado reversible.	Alto	Alto
Tarjeta sin contacto	Autenticación por posesión	Sin contacto físico. Fácil de perder.	Alto	Medio
Token USB	Autenticación por posesión	Más seguro que la contraseña. Requiere un dispositivo adicional de lectura de tarjetas.	Alto	Alto
Voz humana	Autenticación por comportamiento	Puede llevarlo donde quiera. Requiere un dispositivo adicional para la captura de voz.	Alto	Bajo
Firma humana	Autenticación por comportamiento	Permite ahorrar tiempo. Requiere una tableta electrónica.	Alto	Medio
Pulsación de tecla	Autenticación por comportamiento	Verificar rápidamente la identidad del usuario. Requiere un dispositivo electrónico adicional.	Medio	Alto

Continua en la próxima página –

– *Continua desde la página anterior*

Método	**Clasificación**	**Ventaja/desventaja**	**Usabilidad**	**Seguridad**
Huella dactilar	Autenticación por característica	Fácilmente muestreado. Requiere un dispositivo electrónico adicional.	Alto	Alto
Reconocimiento óptico	Autenticación por característica	Altamente aceptable. Requiere mas cooperación por parte de los usuarios.	Alto	Alto
Geometría de mano	Autenticación por característica	Fácilmente muestreado. Requiere un dispositivo electrónico adicional.	Alto	Alto
Basado en localización	Autenticación por posición	Fácilmente localización para autenticar. Requiere un dispositivo GPS.	Medio	Alto

Anexo B

Invitación para Socios de AIPO

INVITACIÓN

Asunto: [SOCIOS-AIPO-L] Colaboración para un estudio de doctorado.
Para: Lista Socios AIPO SOCIOS-AIPO-L@uam.es

Apreciadas/os compañeras/os de AIPO,

El motivo de este correo es para comentaros que el estudiante Paulo Cesar Realpe se encuentra actualmente realizando su doctorado en la Universidad del Cauca (Colombia) y su pasantía en la Universidad de Lleida (España). Parte de su tema de tesis doctoral es *estudiar principios y evaluación para seguridad y usabilidad (seguridad usable) incluyendo la autenticación de usuario.*

En su estudio, tiene como primer objetivo obtener un conjunto de principios que sirvan para diseñar y para evaluar interfaces de este tipo de sistemas. Tras una profunda revisión de la literatura ha sintetizado un conjunto de principios que, a su vez, ha organizado a partir de algunas facetas y atributos del estándar ISO/IEC 25010:2011.

Antes de continuar, necesitaría la ayuda de expertos en HCI para que le ayuden en una revisión de dicho conjunto, por lo que te agradecería que aceptaras la invitación para realizar esta revisión. Tus aportes serán muy valiosos para su estudio y mejorar así estos principios.

Si aceptas realizar dicha evaluación, por favor, contacta con Paulo mediante su correo-e: prealpe@hotmail.com, quien te enviará el documento con los principios y la revisión a realizar. De antemano, muchas gracias y saludos cordiales.

Toni Granollers
Miembro de AIPO

Anexo C

Documento guía para la revisión

REVISIÓN HEURÍSTICA

Organización Heurística

Las sub-heurísticas presentadas en este documento estan agrupadas teniendo en cuenta algunas facetas y atributos de la ISO/IEC 25010:2011. Estas sub-heurísticas se basan en seguridad usable y autenticación de usuario. A continuación se presenta los atributos a evaluar y su respectiva descripción.

- **Usabilidad**: La usabilidad esta basado en las 10 reglas heurísticas de Nielsen y el principio transmitir características de Johnston et al. El principio de transmitir características informa al usuario de las características de seguridad disponibles, a diferencia del criterio de visibilidad del estado del sistema el cual le permite al usuario "ver" si estas características están activas y están siendo usadas (para mayor información consultar el paper *Security and human computer interface* de Johnston et al.).
- **Seguridad**: El sistema tiene en cuenta 5 características importantes en cuanto a este atributo: integridad, autenticidad, confidencialidad, registro y disponibilidad. Los aspectos anteriores están basados en la ISO/IEC 25010:2011. En este atributo, también se tiene en cuenta los aspectos de privacidad.
- **Accesibilidad**: La accesibilidad asegura que sin importar la parte cognitiva, la movilidad y las habilidades sensoriales, puede utilizar un mecanismo de autenticación. Esto incluye discapacidades como el oído, la vista, la movilidad, el aprendizaje y el color, que son pertinentes en un contexto de autenticación.
- **Operabilidad**: Hace referencia a la cantidad de esfuerzo necesario para operar o controlar un método de autenticacion.
- **Fiabilidad**: La fiabilidad indica la capacidad de realizar funciones específicas que permitan llevar a cabo una autenticación satisfactoria. En este aspecto también es importante tener en cuenta algunos aspectos de seguridad (integridad y confidencialidad), mantenimiento y soporte técnico.

- **Desempeño**: Para autenticación de usuario se tienen en cuenta dos aspectos: la mínima acción el cual indica la capacidad de la aplicación para ayudar a los usuarios a alcanzar sus tareas en el menor número de pasos y el comportamiento en el tiempo el cual representa el tiempo requerido por la aplicación para cargar, es decir, que tan rápido responde el sistema de acuerdo a las instrucciones del usuario.

EVALUACIÓN

Grado de Importancia: Cada sub-heurística puede tener una de las posibles 4 opciones para medir el grado de importancia. Ud. como experto deberá marcar una de ellas tal y como se presenta en la Figura C.1.

Tabla C.1: Grado de importancia

Nivel	Descripción
S	Las sub-heurísticas de grado **S** son **vitales** para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.
SS	Las sub-heurísticas de grado **SS** son **importantes** para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.
SSS	Es **recomendable** considerar las sub-heurísticas de grado **SSS** para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.

Categorización: Permite determinar si la sub-heurística a revisar representa o hace parte de la heurística o atributo general, ver Tabla C.2.

Tabla C.2: Categorización

Nivel	Descripción
1	Muy en desacuerdo
2	En desacuerdo
3	Neutral
4	De acuerdo
5	Muy de acuerdo

Anexo D

Recomendaciones para Seguridad Usable y Autenticación

D.1. Usabilidad

Requerimiento
1. Visibilidad del Estado del Sistema
Debería ser posible saber si el sistema es seguro.
El usuario debería identificar el nivel de seguridad del sistema y tomar las acciones pertinentes, si es necesario.
El usuario debería ser capaz de comprender el significado del nivel de seguridad que se presenta en la interfaz.
Si hay retrasos observables en el tiempo de respuesta del sistema a una acción relacionada con la seguridad, el usuario debería estar informado de los avances del sistema?
Después de que el usuario complete una acción de seguridad, la realimentación debería indicar que el siguiente grupo de acciones puede ser iniciada.
Debería existir alguna forma de realimentación para cada acción relacionada con la seguridad, cuando sea necesario.
En las interfaces de alerta, el sistema debería proveer el nombre de las herramientas de seguridad.
El estado del usuario debería ser visible en el sistema.
Al observar el estado de seguridad del sistema, el usuario podría decir las alternativas para las acciones relacionadas con la seguridad, si es necesario.
El sistema debería mantener informado adecuadamente al usuario sobre el estado de conexión del sistema.
Deberían existir indicadores visuales informando a los usuarios sobre las prácticas de privacidad del sistema.
2. Estética y Mínimo Diseño
La información de seguridad presentada en pantalla debería ser relevante.

Continua en la próxima página –

– *Continua desde la página anterior*

Requerimiento
Los iconos de seguridad debería ser identificables y diferenciables.
Las etiquetas de seguridad debería ser sencillas, fáciles de entender y representativas.
La interfaz debería ayudar al usuario a tener una experiencia segura y satisfactoria con el sistema.
3. Control y Libertad de Usuario
Los usuarios deberían poder revertir fácilmente sus acciones de seguridad donde sea posible.
Debería existir una función "desistir o deshacer" para una simple acción o grupo completo de acciones de seguridad.
'El sistema debería estar diseñado de manera que los botones con nombres similares, no desarrollen acciones de seguridad opuesto.
Cuando las indicaciones implican una acción de seguridad necesaria, las palabras del mensaje deberían ser coherentes con la acción.
Las opciones de seguridad en el menú debería hacer evidente si la selección de la opción es posible.
El usuario debería ser capaz de confirmar cualquier acción que tenga consecuencias drásticas, negativas o destructivas.
El sistema debería permitir al usuario editar o eliminar información personal incorrecta.
4. Utilización del Lenguaje del Usuario
Los mensajes de seguridad deberían estar nombrados coherentemente en todo sistema.
Las sentencias de alerta deberían ser simples, cortas y comprensibles.
Las preguntas de seguridad debería ser expresadas en un lenguaje claro y sencillo.
Se debería evitar el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad.
El sistema debería evitar el uso de palabras diferentes para transmitir la misma idea o concepto.
Los mensajes de error relacionados con la seguridad deberían ser adecuados al lenguaje del usuario.
5. Minimizar Carga de Memoria
Las tareas de seguridad deberían ser fáciles de aprender y recordar.
Deberían existir situaciones predeterminadas de selección de seguridad.
Los menús en la interfaz de usuario debería hacer evidente cuáles elementos de seguridad pueden ser seleccionados.
La información relacionada con la seguridad debería ser presentada de una manera coherente y estandarizada.
En un proceso de autenticación por conocimiento (e.g. contraseña o PIN), el sistema debería permitir minimizar la carga de memoria para los usuarios.
El sistema debería permitir libertad al usuario para decidir el número de dígitos del PIN en un proceso de autenticación.

Continua en la próxima página –

– *Continua desde la página anterior*

Requerimiento
Si se utiliza el reconocimiento visual para autenticación (e.g. contraseñas gráficas), los usuarios debería poder asociar una frase o palabra a una imagen como contraseña.
Para PINs de más de 8 caracteres, el sistema debería hacer uso de herramientas nemotécnicas.
Si el sistema necesita más de una clave de acceso, el sistema debería utilizar técnicas fáciles para reducir la carga cognitiva de los usuarios.
El sistema debería evitar el uso de claves aleatorias para la etapa de registro o autenticación.
Se debería evitar cualquier PIN definido por el sistema.
6. Reconocer, Diagnosticar y Recuperarse de los Errores
Los mensajes relacionados con la seguridad deberían ser declarados de forma constructiva.
Los mensajes de error relacionados con la seguridad debería informar al usuario de la gravedad del error.
El sistema debería facilitar la posibilidad de diagnostico a posibles errores.
Los mensajes de error relacionados con la seguridad deberían ser significativos y sensibles al problema.
Los mensajes de error relacionados con la seguridad debería indicar al usuario dónde obtener ayuda.
7. Flexibilidad y Eficiencia de Uso
Los usuarios deberían poder cambiar fácilmente entre los niveles de principiante y experto.
Si el sistema es compatible con usuarios principiantes y expertos, los niveles de los mensajes de error con respecto a la seguridad deberían estar disponibles en detalle.
Los usuarios deberían poder elegir entre información de seguridad de texto o gráfico (e.g. ícono), según sea el caso.
El sistema debería permitir configurar fácilmente las propiedades de seguridad.
Si el sistema es compatible con usuarios principiantes y expertos, los niveles de seguridad deberían estar disponibles en detalle.
Los usuarios debería poder personalizar fácilmente las opciones seguridad y privacidad para satisfacer sus preferencias individuales.
El sistema debería poseer atajos a tareas de seguridad frecuente.
Las indicaciones de seguridad deberían ser expresadas en sentido afirmativo.
8. Prevención de Errores
La información necesaria para tomar una buena decisión de seguridad, debería ser adecuada y estar disponible antes de que se adopte la medida.
El sistema debería advertir a los usuarios si están a punto de cometer un error de seguridad potencialmente grave.
El sistema debería impedir a los usuarios cometer errores de seguridad siempre que sea posible.
9. Consistencia y Estándares
Los iconos de seguridad deberían tener etiqueta.

Continua en la próxima página –

– *Continua desde la página anterior*

Requerimiento
Los controles de seguridad deberían ser consistentes y están ubicados en lugares específicos.
Para interfaces de preguntas y respuestas sobre seguridad, las entradas válidas para una cuestión deberían estar listadas.
Los nombres de las opciones de seguridad en los menús, deberían ser consistentes con relación a los demás nombres en cuanto a términos técnicos.
Las abreviaturas para palabras de seguridad deberían tener una longitud predeterminada y fácil de identificar.
Las relaciones entre los controles de seguridad y las acciones de seguridad deberían ser claras para el usuario.
10. Ayuda y Documentación
Hay una función de ayuda de seguridad visible.
La información proporcionada por la ayuda debería ser relevante.
Los usuarios deberían poder cambiar fácilmente entre la ayuda de seguridad y sus tareas.
Las instrucciones de la ayuda deberían seguir una secuencia de acciones de seguridad para el usuario.
El sistema debería proveer actualizaciones oportunas a documentación relacionada con la seguridad.
El sistema debería proveer soporte técnico en linea para solucionar problemas de seguridad.
11. Transmitir Características
Debería existir una clara comprensión de las capacidades de seguridad del sistema.
El sistema debería anticipar adecuadamente y pronto la próxima actividad probable relacionada con seguridad.
El sistema debería notificar a los usuarios si está interactuando con fuentes no confiables.
El sistema debería mostrar logos de seguridad.
El sistema debería tener certificados de seguridad otorgado por entidades externas reconocidas.
Los datos que los usuarios no pueden modificar, deberían estar desactivados.
El sistema debería proporcionar un número limitado de configuraciones de seguridad estandarizados que pueden ser auditados, documentados, y fácilmente aprendido por los usuarios.

Tabla D.1: Requerimientos para Usabilidad.

D.2. Seguridad y Privacidad

Requerimiento
Las áreas protegidas deberían ser completamente inaccesibles y seguras.
El sistema debería permitir acceder a las áreas protegidas o confidenciales con algún método de autenticación.
El sistema debería emplear mecanismos critográficos para la transmisión segura de la información.
Si el sistema utiliza *cookies* informáticos, la información sobre la privacidad del sistema debería describir con precisión el uso de estos cookies.
Los caracteres de la clave de acceso deberían estar ocultos directamente en el campo y esta acción puede ser habilitada o deshabilitada.
El proceso de autenticación debería hacer cumplir un límite de intentos de acceso no válidos consecutivos por un usuario.
En un método de autenticación por conocimiento (e.g. contraseña o PIN), el sistema debería permitir al usuario modificar su clave de acceso.
El sistema debería confirmar al usuario la transmisión de datos antes que estos sean transmitidos.
El sistema debería notificar a los usuarios (administradores) sobre los privilegios de acceso que poseen.
El sistema debería conceder acceso de acuerdo a una autorización válida.
El sistema debería presentar al usuario mensajes de notificación concernientes a la seguridad y privacidad antes de acceder al sistema.
El sistema debería garantizar que la información de acceso público no tenga información privada.
La información de privacidad del sistema debería garantizar al usuario el derecho a optar por compartir información no crítica con terceros.
El sistema debería emplear herramientas que proveen notificación al usuario sobre discrepancias durante la verificación de identidad.
Si el sistema facilita el intercambio de datos con otros usuarios, el sistema debería permitir diferentes políticas de acceso y asociarse a diferentes tipos de datos.
El sistema debería notificar y da posibles soluciones al usuario sobre vulnerabilidades asociados a incidentes de seguridad detectados.
El sistema debería notificar al usuario sobre realización de copias de seguridad relacionados con la información personal.
En el proceso de configuración de la cuenta, debería existir la opción de configuración de privacidad y es aplicable a todo el sistema.
El sistema debería describir cada opción de privacidad en detalle.
Debería existir una política de copia de seguridad que especifica cómo debe realizarse esta acción.
El sistema debería proveer confirmación para los usuarios sobre las declaraciones que indican que ellos entienden las condiciones de acceso.
El sistema debería hacer cumplir el nivel de complejidad de la contraseña, con los requisitos mínimos exigidos.

Continua en la próxima página –

– *Continua desde la página anterior*

Requerimiento
El sistema debería cifra datos solicitados en el proceso de autenticación.
Si se utiliza tarjetas inteligentes, los datos del propietario deberían estar almacenadas en ella.
El sistema debería proporcionar consejos u orientaciones de configuraciones de privacidad cuando se usa por primera vez.
La tarjeta inteligente o token del titular debería poseer mecanismos de política privacidad.
El sistema debería poseer políticas de privacidad para comercio o contenido del usuario.
El sistema debería soportar y hace uso por defecto del protocolo HTTPS.
El método de autenticación debería poseer interoperabilidad entre sistemas.

Tabla D.2: Requerimientos para seguridad y privacidad.

D.3. Accesibilidad

Requerimiento
El sistema debería permitir usar passwords gráficos para usuarios con dificultades de lectura.
En autenticación por característica, el sistema debería estar esta compuesto por dispositivos estandard.
En autenticacion por posesión (token o tarjeta), el sistema debería estar equipado con software y hardware adecuado.
En un proceso de autenticacion, el sistema debería evitar esfuerzo adicional para personas con algún tipo de limitación física o cognitiva.
En un sistema por autenticación por biometría, el sistema debería permitir ser configurado para personas con limitaciones físicas.
El sistema debería proveer a los usuarios otras alternativas para autenticarse.
El método de autenticación debería ser adapta a usuarios nuevos y experimentados.
Se debería utilizar el color y algún código específico para llamar su atención e indicar los cambios relacionados con la seguridad.
En los campos donde se necesita información para autenticarse, el sistema debería permitir cambiar el tamaño de la letra para el usuario.

Tabla D.3: Requerimientos para Accesibilidad.

D.4. Operabilidad

Requerimiento
El sistema debería permitir seleccionar algún método de autenticación en especial o combinaciones de ellas.
El sistema debería permitir personalizar la interfaz en el proceso de autenticación sin poner en riesgo la seguridad relacionada con información sensitiva.
Para operaciones de alto riesgo de ataque, el sistema debería permitir usar autenticación biométrica.
Si los usuarios olvidan el PIN, el sistema debería permitir restablecerlo a través de una interfaz.
El método de autenticación empleado debería siguir normas conocidas (sean estandares o no) donde su seguridad sea adecuada.
Si el proceso de registro es requerido, este debería ser corto, sencillo y solo exigir información esencial.
El sistema debería informar al usuario que el proceso de autenticación ha sido satisfactorio.
En un proceso de autenticación, este debería tiene palabras adecuadas para desarrollar una acción en particular.

Tabla D.4: Requerimientos para Operabilidad.

D.5. Fiabilidad

Requerimiento
El proceso de autenticación debería ser simple y proteger contra usuarios no autorizados.
El sistema debería presentar certificados de confianza.
En el caso en que el usuario deba proporcionar la información, el sistema debería determinar que medidas son utilizadas para proteger esta información.
Debería estar claramente establecido el propósito de utilizar la información personal del usuario.
El sistema debería notificar al usuario si está interactuando con fuentes no confiables.
El sistema debería emplear mecanismos para ayudar en la presentación de informes de incidentes de seguridad si son necesarios.
El sistema debería proveer integración a múltiples bases de datos.
El sistema debería ofrecer servicios de seguridad personalizado que permitan tener en cuenta las necesidades y preferencias de los usuarios.
Si el proceso de inicio de sesión falla, el sistema debería evitar indicarle al usuario qué parte del proceso es incorrecto.

Continua en la próxima página –

– Continua desde la página anterior

Requerimiento
El sistema debería evitar la reutilización de contraseñas.
Para autenticación desafío-respuesta (*Challenge–response authentication*), las preguntas desafío debería ser pertinentes para los usuarios.
Si el número de preguntas desafío que contesta el usuario es n, el sistema debería presentar un número de preguntas $t \geq n$ para ser contestadas.

Tabla D.5: Requerimientos para Fiabilidad

D.6. Desempeño

Requerimiento
El proceso de computo en el método de autenticación debería ser imperceptible por el usuario.
En un sistema de autenticación por biométrica, los algoritmos usados debería presentar un buen desempeño en tiempo de ejecución.
Para reducir el tiempo de cifrado en el proceso de autenticación, el sistema debería adoptar una tarjeta inteligente de alto rendimiento.
El proceso de autenticación biométrica debería poseer memoria extra para evitar retrasos de ejecución de las instrucciones.
Para un mayor nivel de seguridad, el sistema debería emplear tecnología múltiple (e.g. contacto o inalábrico) junto a métodos biométricos para aplicaciones de acceso.
Las políticas de contraseñas debería presentar un nivel importante de cumplimiento y son fáciles de usar.
En un escenario de reautenticación, el sistema debería integrar las medidas de seguridad pertinente según sea el caso.
La información sensitiva asociada a la identificación del usuario debería ser mínima según sea el caso.
El sistema debería evitar el uso de “cookie informático” para métodos de autenticación.
¿El sistema debería proporcionar etiquetas de texto que muestren consejos para generar contraseñas.

Tabla D.6: Recomendaciones para desempeño.

Anexo E

Encuesta de Clasificación Adjetiva

CLASIFICACIÓN ADJETIVA Y NUMÉRICA

En esta encuesta se pretende obtener una clasificación adjetiva y numérica de algunos atributos de la ISO/IEC 25010:2011 para sistemas donde sea necesario la usabilidad, seguridad, accesibilidad, desempeño, fiabilidad y operabilidad en el contexto de seguridad usable y autenticación de usuario. Además, se pretende también encontrar una clasificación para el impacto y amenaza cuando un principio o heurística de los atributos anteriores presenta algún grado de debilidad.

Los atributos presentados en este documento están agrupadas teniendo en cuenta algunos del estándar ISO/IEC 25010:2011. Cada atributo posee un conjunto de sub-heurísticas para ser evaluados. Los atributos aquí presentados abarcan algunas aplicaciones de seguridad usable y autenticación de usuario.

1. **Usabilidad**: la usabilidad está basado en las 10 reglas heurísticas de Nielsen y el principio de transmitir características de Johnston et al. (para mayor información puede consultar el articulo - *Security and human computer interface*).

2. **Seguridad**: el sistema tiene en cuenta 5 características importantes en cuanto a este atributo: integridad, autenticidad, disponibilidad, confidencialidad, responsabilidad y no repudio. En este también se tiene en cuenta los aspectos de privacidad.

3. **Accesibilidad**: la accesibilidad asegura que sin importar la parte cognitiva, la movilidad y las habilidades sensoriales, puede utilizar un mecanismo de autenticación. Esto incluye discapacidades como el oído, la vista, la movilidad, el aprendizaje y el color, que son pertinentes en un contexto de autenticación.

4. **Desempeño**: para autenticación de usuario se tienen en cuenta dos aspectos: a) Mínima acción: Capacidad de la aplicación para ayudar a los usuarios a alcanzar sus tareas en el menor número de pasos. b) Comportamiento en el tiempo: Representa el tiempo requerido por la aplicación para cargar, es decir, que tan rápido responde el sistema de acuerdo a las instrucciones del usuario.

5. **Fiabilidad**: La fiabilidad indica la capacidad de realizar funciones específicas que permitan llevar a cabo una autenticación satisfactoria. En este aspecto también es importante tener en cuenta algunos aspectos de seguridad (integridad y confidencialidad), mantenimiento y soporte técnico.

6. **Operabilidad**: Hace referencia a la cantidad de esfuerzo necesario para operar o controlar un método de autenticación.

Impacto: Evalúa el impacto de vulnerabilidades de seguridad de un sistema cuando un principio o heurística presenta algún grado de debilidad. Este impacto está dividido en 4 categorías.

1. Bajo: en esta categoría la vulnerabilidad requiere de circunstancias improbables para ser llevadas a cabo, y si estas son ejecutadas con éxito, sus consecuencias son insignificantes o es ampliamente mitigado por las características del componente afectado.

2. Moderado: esta categoría puede comprometer la confidencialidad, integridad y disponibilidad de datos o recursos (físico o humano) pero poco probables para ser efectuado.

3. Alto: esta categoría pone en peligro la confidencialidad, integridad y disponibilidad de los datos o recursos con una alta probabilidad para ser efectuado.

4. Crítico: el sistema es fácilmente vulnerado y compromete gravemente los datos o recursos sin interacción del usuario (e.g. ejecutar código malicioso).

Vulnerabilidad: Estima la probabilidad de un ataque cuando un principio o heurística presenta algún grado de debilidad. Esta amenaza está dividido en 5 categorías.

1. Altamente improbable
2. Improbable
3. Algo probable
4. Muy probable
5. Casi seguro

La encuesta es presentada a continuación:

1. **Perfil**

2. **Escala de atributos:** En una evaluación adecuada el significado de una puntuación numérica es importante en todo proceso de medida. Aunque existen trabajos donde se presenta una escala de clasificación adjetiva y numérica para la usabilidad de un producto (e.g. System Usability Scale presenta un rango dentro de 0 a 100, donde 100 es el mejor absoluto y 0 es lo peor), es necesario también encontrar métricas más intuitiva sin ningún tipo de interpretación especial para un conjunto más amplio de atributos.

A partir del estado del arte se determinó 5 categorías para decidir el grado de calidad o estimación de un sistema a partir de los atributos presentados en la primera sección.

1. Excelente
2. Bueno
3. Moderado
4. Pobre
5. Muy pobre

Cada grado anterior representa un intervalo el cual debe estar dentro del rango entre 0 y 1. Por lo tanto, es importante aclarar que la escala de clasificación anterior debe cubrir todo el intervalo [0, 1] y cumplirse que 'Excelente' es el máximo superior del intervalo y 'Muy pobre' el mínimo inferior.

Por ejemplo, Muy pobre = [0, 0.1), Pobre = [0.1, 0.3), Moderado = [0.3, 0.6), Bueno = [0.6, 0.8) y Excelente = [0.8, 1.0], donde '[' representa intervalo cerrado y '(' representa intervalo abierto (nota: este mismo ejemplo se puede aplicar para las siguientes secciones).

a) ¿Cuál intervalo considera que debería estar el adjetivo 'Excelente' para cada uno de los atributos mencionados en la primera sección?
b) ¿Cuál intervalo considera que debería estar el adjetivo 'Bueno' para cada uno de los atributos mencionados en la primera sección?
c) ¿Cuál intervalo considera que debería estar el adjetivo 'Aceptable' para cada uno de los atributos mencionados en la primera sección?
d) ¿Cuál intervalo considera que debería estar el adjetivo 'Pobre' para cada uno de los atributos mencionados en la primera sección?
e) ¿Cuál intervalo considera que debería estar el adjetivo 'Muy pobre' para cada uno de los atributos mencionados en la primera sección?

3. Escala de impacto: A partir de la primera sección y del estado del arte se determinó 4 categorías para decidir el impacto ante eventuales vulnerabilidades de un sistema en particular.
1. Bajo
2. Medio
3. Alto
4. Critico

Cada categoría anterior representa un intervalo el cual debe estar dentro del rango entre 0 y 1. Por lo tanto, es importante aclarar que la escala de clasificación anterior debe cubrir todo el intervalo [0, 1] y cumplirse que 'Bajo' es el mínimo inferior del intervalo y 'Critico' el máximo superior.

a) ¿Cuál intervalo considera que debería estar el adjetivo 'Bajo'?
b) ¿Cuál intervalo considera que debería estar el adjetivo 'Medio'?
c) ¿Cuál intervalo considera que debería estar el adjetivo 'Alto'?
d) ¿Cuál intervalo considera que debería estar el adjetivo 'Critico'?

4. Escala de vulnerabilidad: A partir de la primera sección y del estado del arte se determinó 5 categorías para decidir la amenaza de un sistema cuando un principio o heurística presenta algún grado de debilidad.

1. Altamente improbable
2. Improbable
3. Algo probable
4. Muy probable
5. Casi seguro

Cada categoría anterior representa un intervalo el cual debe estar dentro del rango entre 0 y 1. Por lo tanto, es importante aclarar que la escala de clasificación anterior debe cubrir todo el intervalo [0, 1] y cumplirse que 'Altamente improbable' es el máximo superior del intervalo y 'Casi seguro' el mínimo inferior.

a) ¿Cuál intervalo considera que debería estar el adjetivo 'Altamente improbable'?
b) ¿Cuál intervalo considera que debería estar el adjetivo 'Improbable'?
c) ¿Cuál intervalo considera que debería estar el adjetivo 'Algo probable?
d) ¿Cuál intervalo considera que debería estar el adjetivo 'Muy probable?
e) ¿Cuál intervalo considera que debería estar el adjetivo 'Casi seguro?

Anexo F

Documento Guía para las sub-heurísticas de grado de importancia S

DOCUMENTO GUIA PARA LA EVALUACION HEURÍSTICA

Estimado evaluador(a), de antemano muchas gracias por su colaboración. La presente evaluación heurística tiene como objetivo **detectar problemas de seguridad usable para una aplicación en particular**. Para que los resultados de esta evaluación sean satisfactorios, se le solicita evaluar la aplicación lo más objetivamente posible. Además, se requiere tener la mayor confidencialidad posible, con el objetivo de resguardar la privacidad del sistema a evaluar.

1. APLICACION A EVALUAR

La aplicación para el cual se va a realizar la evaluación heurística es la red social *Facebook.*

Facebook es la red social que agrupa el mayor número de personas en el mundo con más de 1508 millones de usuarios activos según la fuente Alexa.com. Los miembros de Facebook pueden hacer nuevas redes dentro de Facebook y pueden agregar nuevos amigos en esas redes, realizándole la respectiva invitación. Los miembros de Facebook también pueden enviar mensajes(s) de carácter público o privado y compartir imágenes a cualquier otro miembro de Facebook.

2. ATRIBUTOS A EVALUAR

Durante la evaluación se tendrá en cuenta varios atributos los cuales son fundamentales en nuestro estudio: **usabilidad, seguridad, accesibilidad, desempeño, fiabilidad y operabilidad**. Cada uno de estos atributos está compuesto por un conjunto sub-heurístico el cual permitirá evaluar la aplicación detallada anteriormente. A continuación se presenta las características más importantes para cada uno de estos atributos.

1. **Usabilidad**

Basado en las 10 reglas heurísticas de Nielsen y el principio de transmitir características de Johnston et al[1]. **NOTA: Para la presente evaluación solo se tendrán en cuenta las siguientes heurísticas**.

[1] Disponible en: https://www.researchgate.net/publication/223598908_Security_and_human_computer_interfaces

Visibilidad del estado del sistema	El sistema debe mantener informado al usuario sobre el estado de seguridad del sistema y de las acciones que pueda estar haciendo. Algunos ejemplos de esta categoría podrían estar: visibilidad del nombre de la alerta, establecer colores de seguridad estándar (rojo, amarillo y verde) e iconos como indicadores visuales.
Estética y Mínimo diseño	El sistema debe aplicar apropiadamente representación visual de los elementos de seguridad de manera reconocible y diferenciable. Únicamente información de seguridad relevante debe ser desplegada evitando información irrelevante (e.g. datos técnicos).
Utilización del lenguaje de los usuarios	El sistema debe utilizar un lenguaje consistente y significativo en materia de seguridad para que los usuarios puedan entenderlo fácilmente. Es importante evitar el uso de términos técnicos avanzados que resultan incomprensibles para el usuario.
Control y libertad para los usuarios	El sistema debe permitir a los usuarios deshacer fácilmente cualquiera de sus acciones de seguridad, siempre que sea posible. Lo anterior conlleva a volver a un estado anterior si una acción de seguridad pueda tener consecuencias imprevistas.
Reconocer, Diagnosticar y Recuperarse de Errores.	El sistema debe proporcionar a los usuarios con mensajes de error de seguridad detallada que puedan comprender y actuar. Es importante que el mensaje sea significativo e indicar donde obtener ayuda.
Prevención de errores	El efecto de cualquier acción relevante para la seguridad debe ser comprensible para el usuario. El sistema debe informar a los usuarios con antelación sobre las consecuencias de las acciones de seguridad. A partir de mensajes, los usuarios serán informados sobre cualquier acción que afecte la seguridad del sistema.
Consistencia y estándares	Los controles relacionados con la seguridad en la interfaz de usuario pueden ser estandarizados, el uso de estándares en la interfaz facilita el aprendizaje. Los usuarios deben ser capaces de encontrar los elementos de seguridad que necesiten en un lugar adecuado y en un tiempo razonable.
Ayuda y documentación	Es necesario que el sistema disponga de ayuda y documentación con respecto a la seguridad para los usuarios. El usuario debe ser capaz de encontrar ayuda fácilmente a sus preguntas, centrada en las tareas del usuario y no ser muy extensa.
Transmitir características	La interfaz debe proporcionar al usuario de una manera clara las características de seguridad disponibles (e.g. integridad y confidencialidad disponible en el sitio web). El uso de imágenes puede ser una manera eficaz sobre todo para usuarios sin conocimientos técnicos en seguridad. **NOTA**: Transmitir características informa al usuario de las características de seguridad disponibles, mientras el criterio de visibilidad del estado del sistema permite al usuario "ver" si estas características están activas y se utilizan.

2. **Seguridad**

El sistema tiene en cuenta 5 aspectos importantes en cuanto a este atributo: integridad, autenticidad, confidencialidad, no repudio y privacidad.

Integridad	Grado en que un sistema, producto o componente impide la modificación de los datos, tomando las medidas para asegurar que los datos no pueden ser alterados por personas no autorizadas.
Autenticidad	La identidad de una persona o recurso puede ser demostrado y ser quien dice ser.
Confidencialidad	Grado en que un producto o sistema asegura que los datos sean accesibles a aquellos usuarios autorizados a tener acceso.
No repudio	Acciones o eventos que han sido probadas en un momento determinado, por lo que dichos eventos o acciones no pueden ser repudiados más tarde.

Privacidad	La relación entre la tecnología y las cuestiones legales que lo rodean, o la expectativa pública de la intimidad en la recopilación e intercambio de datos sobre la persona.

3. **Accesibilidad**

Permite que todas las personas, independientemente de la habilidad cognitiva, movilidad y sensorial, puedan utilizar cualquier mecanismo de autenticación. Esto incluye discapacidades como el oído, la vista, la movilidad, el aprendizaje y el color, que son pertinentes en un contexto de autenticación. La accesibilidad también se aplica a los niveles de alfabetización y habilidades técnicas, así como la calidad de los equipos de los usuarios.

4. **Fiabilidad**

La fiabilidad indica la capacidad de realizar funciones específicas que permiten llevar a cabo una autenticación correcta. En este sentido, también es importante tener en cuenta algunos aspectos de la seguridad (e.g. integridad y confidencialidad), mantenimiento y soporte técnico.

5. **Operabilidad**

Se refiere al esfuerzo que se requiere para operar un método de autenticación.

6. **Desempeño**

Para métodos de autenticación, está tomando en cuenta dos aspectos: a) **Acción mínima** que indica la capacidad de la aplicación para ayudar a los usuarios para la realización de sus tareas en unos pocos pasos, y (b) **Tiempo de respuesta** que representa el tiempo necesario para cargar la aplicación, es decir, la rapidez con que el sistema responde de acuerdo con las instrucciones del usuario.

3. MÉTRICA DE EVALUACIÓN

A la hora de evaluar cada sub-heurística se establecen dos tipos de valores de medición.

1. **Nivel de severidad:** Este nivel de severidad es un indicador del nivel de cumplimiento de cada sub-heurística. El evaluador asigna un valor en la escala de Likert (1-5) con el fin de evaluar cuantitativamente el cumplimiento de cada sub-heurística, no la relevancia del mismo. Si usted considera que la sub-heurística no es aplicable o no tiene opinión alguna, seleccione la opción “Ninguno”. En la Tabla I se presenta la cuantificación para el nivel de severidad.

Tabla I: Nivel de severidad

NIVEL DE SEVERIDAD	
Nivel	**Descripción**
1	La aplicación diverge por completo del principio.
2	La aplicación presta cierta atención al principio pero todavía tiene grandes problemas.
3	La aplicación presta cierta atención al principio pero todavía tiene problemas menores.

4	La aplicación sigue el principio en algunas secciones.
5	La aplicación sigue el principio por completo.
Ninguno	No sé/no tengo opinión, o no es aplicable.

2. **Nivel de impacto:** El impacto evalúa la vulnerabilidad de un sistema cuando la sub-heurística evaluada presenta algún grado de debilidad. Si la sub-heurística en evaluación tiene la opción "Ninguno" para el nivel de severidad, la opción "Ninguno" en el nivel de impacto debe ser seleccionada. En la Tabla II se presenta la cuantificación para el nivel de impacto.

Tabla II: Nivel de impacto

NIVEL DE IMPACTO		
Nivel	**Nombre**	**Descripción**
1	**BAJO**	En esta categoría la vulnerabilidad requiere de circunstancias improbables para ser llevadas a cabo, y si estas son ejecutadas con éxito, sus consecuencias son insignificantes o es ampliamente mitigado por las características del componente afectado.
2	**MEDIO**	Esta categoría puede comprometer la confidencialidad, integridad y disponibilidad de datos o recursos (físico o humano) pero poco probables para ser efectuado.
3	**ALTO**	Esta categoría pone en peligro la confidencialidad, integridad y disponibilidad de los datos o recursos con una alta probabilidad para ser efectuado.
4	**CRITICO**	El sistema es fácilmente vulnerado y compromete gravemente los datos o recursos sin interacción del usuario (e.g. ejecutar código malicioso).
Sin valor numérico	**NINGUNO**	Para los casos donde el principio no se pueda evaluar o no es aplicable.

3. **Grado de importancia:** Las sub-heurísticas que se tienen actualmente tienen tres niveles de importancia tal como se presenta en la Tabla III. Esta importancia fue obtenida previamente a partir encuestas a expertos en HCI y seguridad. Debido a que la cantidad de sub-heurísticas es muy grande (142 en total según el *checklist* general que se encuentra al final de este documento), **es necesario que la evaluación de la aplicación se realice por etapas con el fin de que la evaluación se haga más agradable para el experto**. En una primera etapa se evalúa las sub-heurísticas del nivel S, en una segunda etapa se evalúa las sub-heurísticas del nivel SS y finalmente las del nivel SSS.

Nota: En esta evaluación solo se tendrán en cuenta las sub-heurísticas del nivel S.

Tabla III: Grado de importancia

Nivel	**Descripción**
S	Las sub-heurísticas del grado S son **vitales** para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.
SS	Las sub-heurísticas del grado SS son **importantes** para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.
SSS	Es **recomendable** considerar las sub-heurísticas de grado SSS para asegurar que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.

4. DESCRIPCION GENERAL DEL EXCEL

El archivo Excel que se entrega junto con este documento está compuesto por diferentes pestañas:

1. **Información**: en esta pestaña se llenan los datos generales de la evaluación y de la aplicación a evaluar.

2. **Pestaña de la 2-7**: Cada pestaña representa el atributo a evaluar y sus respectivas sub-heurísticas. Usted como evaluador debe valorar cada sub-heurística seleccionando las opciones disponibles a partir de un desplegable en las columnas de "Severidad" e "Impacto". Sí tiene algún comentario, puede añadirlo a cada sub-heurística. Se recomienda poner la referencia si el comentario viene de alguna fuente externa. No debe rellenarse ningún campo más.

3. **Comentarios Generales**: Si tiene comentarios sobre la evaluación en general, puede anexarla en la última pestaña del archivo.

Nota: No debe modificar la columna donde se encuentra la importancia del sub-heurístico.

5. DESCRIPCION DEL PROCESO DE EVALUACIÓN

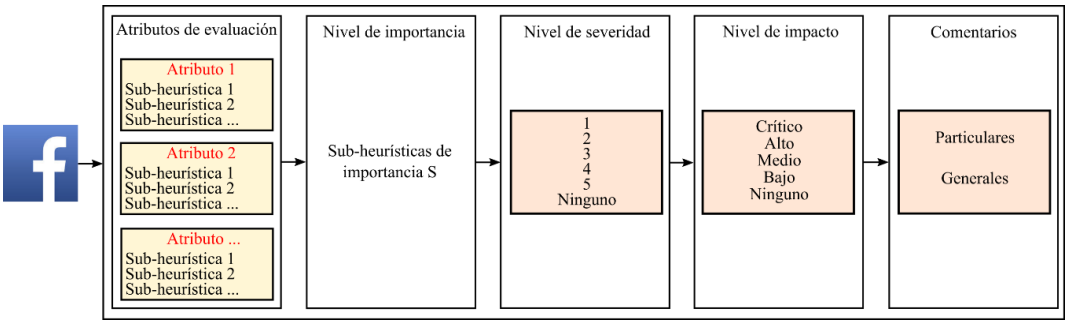
PASO 1. Usted como evaluador trabajará de forma independiente, inspeccionando el sistema y basándose en los principios y sub-heurísticas, que se anexan en este documento, evaluará cada una de ellas a partir la escala de severidad presentada en la Tabla I.

PASO 2. A cada grado de severidad, Usted determinará el grado de impacto (crítico, alto, medio, bajo o ninguno) que tendrá cada sub-heurística, dependiendo de la escala de severidad del cual evaluó y su grado de importancia. El nivel de impacto y el grado de importancia de cada sub-heurística son presentadas en las Tablas II y III respectivamente.

PASO 3. Una vez Ud. como evaluador ha realizado la calificación a cada sub-heurística de acuerdo a su severidad e impacto para las aplicaciones, enviará sus resultados en formato Excel al coordinador de la evaluación. El coordinador realizará todo el análisis de los resultados usando modelos matemáticos con el fin de encontrar la "calidad" de la aplicación en términos de los atributos anteriormente mencionados, y presentar una propuesta sobre el riesgo que puede presentar la aplicación en términos de vulnerabilidad e impacto.

PASO 4. Al finalizar este análisis, el coordinador de la evaluación le enviará los resultados y conclusiones con el fin de obtener realimentación y proponer mejoras en el conjunto sub-heurístico.

En la siguiente figura se resume el proceso de evaluación heurística para esta primera etapa.



¡¡GRACIAS POR SU COLABORACIÓN!!

Anexo G

Documento Guía para las sub-heurísticas de grado de importancia SS y SSS

DOCUMENTO GUIA PARA LA EVALUACION HEURÍSTICA

Estimado evaluador(a), de antemano muchas gracias por su colaboración. La presente evaluación heurística tiene como objetivo **detectar problemas de seguridad usable para una aplicación en particular**. Para que los resultados de esta evaluación sean satisfactorios, se le solicita evaluar la aplicación lo más objetivamente posible. Además, se requiere tener la mayor confidencialidad posible, con el objetivo de resguardar la privacidad del sistema a evaluar.

1. APLICACION A EVALUAR

La aplicación para el cual se va a realizar la evaluación heurística es la red social *Facebook.*

Facebook es la red social que agrupa el mayor número de personas en el mundo con más de 1508 millones de usuarios activos según la fuente Alexa.com. Los miembros de Facebook pueden hacer nuevas redes dentro de Facebook y pueden agregar nuevos amigos en esas redes, realizándole la respectiva invitación. Los miembros de Facebook también pueden enviar mensajes(s) de carácter público o privado y compartir imágenes a cualquier otro miembro de Facebook.

2. ATRIBUTOS A EVALUAR

Durante la evaluación se tendrá en cuenta varios atributos los cuales son fundamentales en nuestro estudio: **usabilidad, seguridad, accesibilidad, desempeño, fiabilidad y operabilidad**. Cada uno de estos atributos está compuesto por un conjunto sub-heurístico el cual permitirá evaluar la aplicación detallada anteriormente. A continuación se presenta las características más importantes para cada uno de estos atributos.

1. **Usabilidad**

Basado en las 10 reglas heurísticas de Nielsen y el principio de transmitir características de Johnston et al[1]. **NOTA: Para la presente evaluación solo se tendrán en cuenta las siguientes heurísticas**.

[1] Disponible en: https://www.researchgate.net/publication/223598908_Security_and_human_computer_interfaces

Visibilidad del estado del sistema	El sistema debe mantener informado al usuario sobre el estado de seguridad del sistema y de las acciones que pueda estar haciendo. Algunos ejemplos de esta categoría podrían estar: visibilidad del nombre de la alerta, establecer colores de seguridad estándar (rojo, amarillo y verde) e iconos como indicadores visuales.
Estética y Mínimo diseño	El sistema debe aplicar apropiadamente representación visual de los elementos de seguridad de manera reconocible y diferenciable. Únicamente información de seguridad relevante debe ser desplegada evitando información irrelevante (e.g. datos técnicos).
Utilización del lenguaje de los usuarios	El sistema debe utilizar un lenguaje consistente y significativo en materia de seguridad para que los usuarios puedan entenderlo fácilmente. Es importante evitar el uso de términos técnicos avanzados que resultan incomprensibles para el usuario.
Control y libertad para los usuarios	El sistema debe permitir a los usuarios deshacer fácilmente cualquiera de sus acciones de seguridad, siempre que sea posible. Lo anterior conlleva a volver a un estado anterior si una acción de seguridad pueda tener consecuencias imprevistas.
Minimizar carga de memoria	El sistema debe asegurar que las acciones de seguridad sean fáciles de aprender y recordar. El uso de metáforas del mundo real ayuda a recordar fácilmente estas acciones a los usuarios.
Reconocer, Diagnosticar y Recuperarse de Errores.	El sistema debe proporcionar a los usuarios con mensajes de error de seguridad detallada que puedan comprender y actuar. Es importante que el mensaje sea significativo e indicar donde obtener ayuda.
Consistencia y estándares	Los controles relacionados con la seguridad en la interfaz de usuario pueden ser estandarizados, el uso de estándares en la interfaz facilita el aprendizaje. Los usuarios deben ser capaces de encontrar los elementos de seguridad que necesiten en un lugar adecuado y en un tiempo razonable.
Flexibilidad y eficiencia de uso	
Ayuda y documentación	Es necesario que el sistema disponga de ayuda y documentación con respecto a la seguridad para los usuarios. El usuario debe ser capaz de encontrar ayuda fácilmente a sus preguntas, centrada en las tareas del usuario y no ser muy extensa.
Transmitir características	La interfaz debe proporcionar al usuario de una manera clara las características de seguridad disponibles (e.g. integridad y confidencialidad disponible en el sitio web). El uso de imágenes puede ser una manera eficaz sobre todo para usuarios sin conocimientos técnicos en seguridad. **NOTA**: Transmitir características informa al usuario de las características de seguridad disponibles, mientras el criterio de visibilidad del estado del sistema permite al usuario "ver" si estas características están activas y se utilizan.

2. **Seguridad**

El sistema tiene en cuenta 5 aspectos importantes en cuanto a este atributo: integridad, autenticidad, confidencialidad, no repudio y privacidad.

Integridad	Grado en que un sistema, producto o componente impide la modificación de los datos, tomando las medidas para asegurar que los datos no pueden ser alterados por personas no autorizadas.
Autenticidad	La identidad de una persona o recurso puede ser demostrado y ser quien dice ser.
Confidencialidad	Grado en que un producto o sistema asegura que los datos sean accesibles a aquellos usuarios autorizados a tener acceso.

No repudio	Acciones o eventos que han sido probadas en un momento determinado, por lo que dichos eventos o acciones no pueden ser repudiados más tarde.
Privacidad	La relación entre la tecnología y las cuestiones legales que lo rodean, o la expectativa pública de la intimidad en la recopilación e intercambio de datos sobre la persona.

3. **Accesibilidad**

Permite que todas las personas, independientemente de la habilidad cognitiva, movilidad y sensorial, puedan utilizar cualquier mecanismo de autenticación. Esto incluye discapacidades como el oído, la vista, la movilidad, el aprendizaje y el color, que son pertinentes en un contexto de autenticación. La accesibilidad también se aplica a los niveles de alfabetización y habilidades técnicas, así como la calidad de los equipos de los usuarios.

4. **Fiabilidad**

La fiabilidad indica la capacidad de realizar funciones específicas que permiten llevar a cabo una autenticación correcta. En este sentido, también es importante tener en cuenta algunos aspectos de la seguridad (e.g. integridad y confidencialidad), mantenimiento y soporte técnico.

5. **Operabilidad**

Se refiere al esfuerzo que se requiere para operar un método de autenticación.

6. **Desempeño**

Para métodos de autenticación, está tomando en cuenta dos aspectos: a) **Acción mínima** que indica la capacidad de la aplicación para ayudar a los usuarios para la realización de sus tareas en unos pocos pasos, y (b) **Tiempo de respuesta** que representa el tiempo necesario para cargar la aplicación, es decir, la rapidez con que el sistema responde de acuerdo con las instrucciones del usuario.

3. MÉTRICA DE EVALUACIÓN

A la hora de evaluar cada sub-heurística se establecen dos tipos de valores de medición.

1. **Nivel de severidad:** Este nivel de severidad es un indicador del nivel de cumplimiento de cada sub-heurística. El evaluador asigna un valor en la escala de Likert (1-5) con el fin de evaluar cuantitativamente el cumplimiento de cada sub-heurística, no la relevancia del mismo. Si usted considera que la sub-heurística no es aplicable o no tiene opinión alguna, seleccione la opción “Ninguno”. En la Tabla I se presenta la cuantificación para el nivel de severidad.

Tabla I: Nivel de severidad

NIVEL DE SEVERIDAD	
Nivel	**Descripción**
1	La aplicación diverge por completo del principio.
2	La aplicación presta cierta atención al principio pero todavía tiene grandes problemas.
3	La aplicación presta cierta atención al principio pero todavía tiene problemas menores.
4	La aplicación sigue el principio en algunas secciones.
5	La aplicación sigue el principio por completo.
Ninguno	No sé/no tengo opinión, o no es aplicable.

2. **Nivel de impacto:** El impacto evalúa la vulnerabilidad de un sistema cuando la sub-heurística evaluada presenta algún grado de debilidad. Si la sub-heurística en evaluación tiene la opción "Ninguno" para el nivel de severidad, la opción "Ninguno" en el nivel de impacto debe ser seleccionada. En la Tabla II se presenta la cuantificación para el nivel de impacto.

Tabla II: Nivel de impacto

NIVEL DE IMPACTO		
Nivel	**Nombre**	**Descripción**
1	**BAJO**	En esta categoría la vulnerabilidad requiere de circunstancias improbables para ser llevadas a cabo, y si estas son ejecutadas con éxito, sus consecuencias son insignificantes o es ampliamente mitigado por las características del componente afectado.
2	**MEDIO**	Esta categoría puede comprometer la confidencialidad, integridad y disponibilidad de datos o recursos (físico o humano) pero poco probables para ser efectuado.
3	**ALTO**	Esta categoría pone en peligro la confidencialidad, integridad y disponibilidad de los datos o recursos con una alta probabilidad para ser efectuado.
4	**CRITICO**	El sistema es fácilmente vulnerado y compromete gravemente los datos o recursos sin interacción del usuario (e.g. ejecutar código malicioso).
Sin valor numérico	**NINGUNO**	Para los casos donde el principio no se pueda evaluar o no es aplicable.

3. **Grado de importancia:** Las sub-heurísticas que se tienen actualmente tienen tres niveles de importancia tal como se presenta en la Tabla III. Esta importancia fue obtenida previamente a partir encuestas a expertos en HCI y seguridad. Debido a que la cantidad de sub-heurísticas es muy grande (142 en total según el *checklist* general que se encuentra al final de este documento), **es necesario que la evaluación de la aplicación se realice por etapas con el fin de que la evaluación se haga más agradable para el experto**. En una primera etapa se evalúa las sub-heurísticas del nivel S, en una segunda etapa (el cual es este caso) se evalúa las sub-heurísticas del nivel SS y las del nivel SSS.

Nota: En esta evaluación solo se tendrán en cuenta las sub-heurísticas del nivel SS y SSS.

Tabla III: Grado de importancia

Nivel	Descripción
S	Las sub-heurísticas del grado S son **vitales** para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.
SS	Las sub-heurísticas del grado SS son **importantes** para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.
SSS	Es **recomendable** considerar las sub-heurísticas de grado SSS para asegurar que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.

4. DESCRIPCION GENERAL DEL EXCEL

El archivo Excel que se entrega junto con este documento está compuesto por diferentes pestañas:

1. **Información**: en esta pestaña se llenan los datos generales de la evaluación y de la aplicación a evaluar.

2. **Pestaña de la 2-7**: Cada pestaña representa el atributo a evaluar y sus respectivas sub-heurísticas. Usted como evaluador debe valorar cada sub-heurística seleccionando las opciones disponibles a partir de un desplegable en las columnas de "Severidad" e "Impacto". Sí tiene algún comentario, puede añadirlo a cada sub-heurística. Se recomienda poner la referencia si el comentario viene de alguna fuente externa. No debe rellenarse ningún campo más.

3. **Comentarios Generales**: Si tiene comentarios sobre la evaluación en general, puede anexarla en la última pestaña del archivo.

Nota: No debe modificar la columna donde se encuentra la importancia del sub-heurístico.

5. DESCRIPCION DEL PROCESO DE EVALUACIÓN

PASO 1. Usted como evaluador trabajará de forma independiente, inspeccionando el sistema y basándose en los principios y sub-heurísticas, que se anexan en este documento, evaluará cada una de ellas a partir la escala de severidad presentada en la Tabla I.

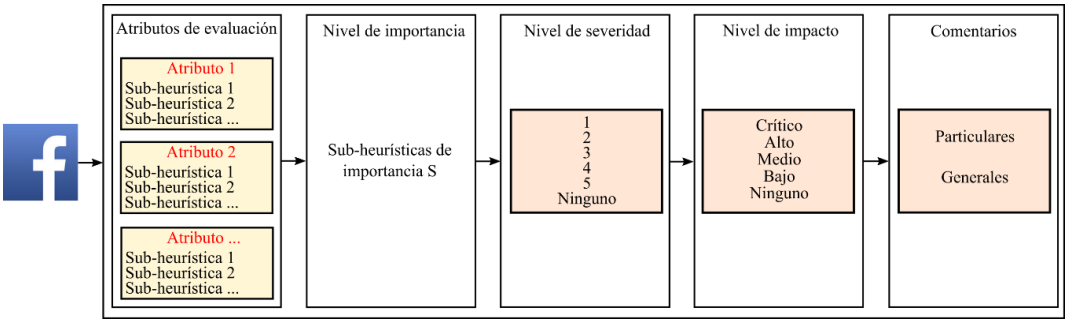
PASO 2. A cada grado de severidad, Usted determinará el grado de impacto (crítico, alto, medio, bajo o ninguno) que tendrá cada sub-heurística, dependiendo de la escala de severidad del cual evaluó y su grado de importancia. El nivel de impacto y el grado de importancia de cada sub-heurística son presentadas en las Tablas II y III respectivamente.

PASO 3. Una vez Ud. como evaluador ha realizado la calificación a cada sub-heurística de acuerdo a su severidad e impacto para las aplicaciones, enviará sus resultados en formato Excel al coordinador de la evaluación. El coordinador realizará todo el análisis de los resultados usando modelos matemáticos con el fin de encontrar la "calidad" de la aplicación

en términos de los atributos anteriormente mencionados, y presentar una propuesta sobre el riesgo que puede presentar la aplicación en términos de vulnerabilidad e impacto.

PASO 4. Al finalizar este análisis, el coordinador de la evaluación le enviará los resultados y conclusiones con el fin de obtener realimentación y proponer mejoras en el conjunto sub-heurístico.

En la siguiente figura se resume el proceso de evaluación heurística para esta primera etapa.



¡¡GRACIAS POR SU COLABORACIÓN!!

Anexo H

Acuerdo de confidencialidad

Acuerdo de Confidencialidad

YO _____ **ACEPTO** participar en una prueba de seguridad usable supervisada por _____, el día ___/___/_____, en las instalaciones de la *Universidad del Cauca*. Entiendo y estoy de acuerdo con las condiciones mencionadas en adelante.

Comprendo que la prueba se hace solo para evaluar un sistema interactivo, NO mis capacidades, habilidades y conocimientos.

Comprendo que los resultados de la prueba se utilizarán solo para propósitos académicos y/o de investigación, sin que mi identidad sea revelada.

Entiendo que puedo comunicar al supervisor de la prueba, en cualquier momento, mi malestar, molestia o inconformidad.

Comprendo que puedo abandonar la prueba y el lugar en cualquier momento.

_____

Firma

Anexo I

Información proporcionada a los usuarios para la aplicación de Facebook

Hoja de Bienvenida al Participante

Buenos días/tardes, mi nombre es ***Paulo Cesar Realpe Muñoz*** estudiante de doctorado en ciencias de la electrónica de la Universidad del Cauca (Colombia) y le acompañaré durante esta prueba[1].

Antes que nada, le agradezco su presencia aquí, y que haya aceptado realizar la prueba de usuarios. **Para realizar el test debemos dejar en claro varios aspectos**:

El primero y el más importante es que debe tener claro que **no le estamos evaluando a usted sino lo que queremos evaluar es las funcionalidades de la aplicación de Facebook**, esto significa que si por alguna razón ve que no puede realizar alguna acción o simplemente se equivoca, no es por culpa suya sino que significa que el producto no está bien diseñado.

Otro aspecto que debe conocer es que como la prueba es analizada posteriormente, debemos obtener algunos datos personales y uso de la aplicación. Por ello si lo desea, deberá **firmar el documento de consentimiento para aprobar dichos datos.**

¿Y en que va a consistir el test? **El test consiste de realizar diversas tareas.** Antes de realizar estas tareas, se le solicitara responder algunas preguntas iniciales sobre el perfil de usuario. **Después de finalizar las tareas, se le solicitara responder algunas preguntas sobre las acciones que ha realizado.**

Si siente la **necesidad de parar la prueba**, por cualquier razón, usted está en su derecho de hacerlo en cualquier momento.

Si tiene **alguna duda se la responderé con gusto**. A continuación lea y firme el **documento de consentimiento de participación** y procederemos a comenzar la prueba.

Muchas gracias por su participación.

[1] La información original de este documento pertenece el Grupo de Interacción Persona Ordenador e Integración de Datos de la Universidad de Lleida (España).

DOCUMENTO GUIA PARA LOS USUARIOS

Estimado(a) usuario(a)

Usted participará en una prueba para evaluar el grado de seguridad usable para la aplicación de *Facebook*. Facebook es una red social que agrupa el mayor número de personas en el mundo con más de 1508 millones de usuarios activos según la fuente Alexa.com. La prueba tiene como objetivo detectar la existencia de problemas en el uso de dicho sitio web, en el marco de un estudio de seguridad usable.

SE ESTA EVALUANDO LA APLICACIÓN, NO EL DESEMPEÑO DE USTED COMO USUARIO, POR LO TANTO, NO SE PREOCUPE SI COMETE ALGUN ERROR.

Toda la información que usted nos proporcionara es absolutamente confidencial y muy relevante para nuestro estudio, por lo cual le agradecemos su participación.

La prueba consta de 3 etapas:

1. En la primera etapa usted deberá completar un cuestionario con preguntas relativas a su perfil, experiencia en el uso de tecnologías de la información y el uso de Facebook.
2. En la segunda etapa se le proporcionará un conjunto de tareas que deberá realizar a través de la aplicación.
3. En la tercera etapa usted deberá completar un cuestionario que tiene como objetivo obtener la percepción general sobre su experiencia en el uso de la aplicación.

SI TIENE ALGUNA DUDA DURANTE EL DESARROLLO DE LA PRUEBA, PREGUNTE AL EVALUADOR COORDINADOR.

CUESTIONARIO PRE-TEST

I. Datos personales

1. Género: Femenino ( ) Masculino ( )

2. Edad: _____

3. Nivel más alto de educación completado o en proceso

Universitario ( ) Completa ( ) En proceso
Especialización ( ) Completa ( ) En proceso
Maestría ( ) Completa ( ) En proceso
Doctorado ( ) Completa ( ) En proceso
Otro ¿Cuál?_____

4. ¿Cuál es su ocupación? _____

II. Información sobre el uso de tecnologías de la información y Facebook

1. ¿Con qué frecuencia utiliza internet?
( ) Nunca ( ) Ocasionalmente ( ) Una vez al día ( ) Más de una vez al día
( ) Permanece contactado todo el día

2. ¿Con qué frecuencia usa Facebook?
( ) Varias veces al día ( ) Una vez al día ( ) Una vez por semana ( ) Una vez por mes

3. ¿Cuánto tiempo estas en Facebook viendo o publicando información en tu perfil cada semana?
( ) Menos de 1 hora ( ) Entre 1 y 2 horas ( ) Entre 2 y 4 horas ( ) 4 horas o más

4. ¿Tiene cuenta en alguna otra red social? En caso afirmativo seleccione:
( ) Twitter ( ) Instagram ( ) Linkedln ( ) Whatsapp ( ) Otro ¿Cuál? _____

5. ¿Ha cambiado en algún momento la configuración de seguridad y privacidad de su cuenta de Facebook?
( ) Si ( ) No

6. ¿Ha sentido preocupación por el mal uso de su información personal que se encuentra en su cuenta de Facebook?
( ) Si ( ) No

LISTA DE TAREAS

Considere el siguiente escenario para realizar las siguientes tareas.

Usted está interesado en usar la red internet para conocer personas y compartir sus experiencias vividas. Alguien conocido le proporciona información sobre posibles redes sociales que se encuentran en la red de forma gratuita y le sugiere crear una cuenta en Facebook con el seudónimo de "Felicito Buendía". A usted le gustaría saber si esta red social se acomoda a sus necesidades, que proteja su información personal y sea fácil de usar.

Tarea 1. Cambiar la contraseña actual

Tarea 2. Determinar qué atributos de su perfil son visibles para las demás personas.

Tarea 3. Averiguar, para quién o quienes el atributo "cumpleaños" es visible.

Tarea 4. Cambie la configuración de privacidad del álbum de fotos "Mi álbum" para que sea visible solo para su amiga "Maritza Rodríguez".

Tarea 5. Activa las alertas cuando se inicie sesión desde un navegador desconocido.

Tarea 6. Cambiar del estado "Amigo" al estado "Con acceso restringido" a su contacto "Irene Delgado".

Tarea 7. Bloquee los mensajes para su amiga "Bety Ramos"

CUESTIONARIO POST-TEST

Encierre con un círculo la respuesta a las siguientes preguntas que considere más apropiada

1. ¿Pudo completar las tareas?

(a) Muy difícilmente (b) Difícilmente (c) Neutral (d) Fácilmente (e) Muy fácilmente

2. ¿La aplicación fue fácil de usar?

(a) Muy en desacuerdo (b) En descuerdo (c) Neutral (d) De acuerdo (e) Totalmente de acuerdo

3. ¿Soy capaz de aprender a utilizar las opciones ofrecidas por la aplicación?

(a) Muy en desacuerdo (b) En descuerdo (c) Neutral (d) De acuerdo (e) Totalmente de acuerdo

4. ¿Considera que la información requerida en la prueba ha sido fácil de encontrar?

(a) Muy difícilmente (b) Difícilmente (c) Neutral (d) Fácilmente (e) Muy fácilmente

5. ¿Considera que la información disponible en la aplicación es completa (suficiente)?

(a) Muy en desacuerdo (b) En descuerdo (c) Neutral (d) De acuerdo (e) Totalmente de acuerdo

6. ¿Confía en la integridad, confiabilidad y disponibilidad de la información que ha suministrado?

(a) Muy en desacuerdo (b) En descuerdo (c) Neutral (d) De acuerdo (e) Totalmente de acuerdo

7. Usted califica el grado de satisfacción en el uso de la aplicación como:

(a) Insatisfactorio (b) Poco satisfactorio (c) Neutral (d) Satisfactorio (e) Muy satisfactorio

8. ¿El diseño de la aplicación fue consistente?

(a) Muy en desacuerdo (b) En descuerdo (c) Neutral (d) De acuerdo (e) Totalmente de acuerdo

9. La disposición de la información en la aplicación es:

(a) Muy difusa (b) Difusa (c) Neutral (d) Clara (e) Muy clara

10. ¿La aplicación le inspira confianza con respecto a la privacidad que le podría brindar a su información personal?

(a) Muy en desacuerdo (b) En descuerdo (c) Neutral (d) De acuerdo (e) Totalmente de acuerdo

11. ¿Volvería a utilizar la aplicación?

(a) Muy en desacuerdo (b) En descuerdo (c) Neutral (d) De acuerdo (e) Totalmente de acuerdo

12. ¿En comparación con otras redes sociales, la experiencia con esta aplicación le ha parecido?

(a) Mucho peor (b) Peor (c) Neutral (d) Mejor (e) Mucho mejor

13. ¿Cómo evalúa la experiencia como colaborador en esta prueba?

(a) Muy desagradable (b) Desagradable (c) Neutral (d) Agradable (e) Muy agradable

¿Qué fue lo que más le gustó de la aplicación con base en su usabilidad, seguridad y privacidad?

_____
_____
_____
_____

¿Qué fue lo que más le disgustó de la aplicación con base en su usabilidad, seguridad y privacidad?

_____
_____
_____
_____

MUCHAS GRACIAS POR SU COLABORACION!!

Anexo J

Documentos para la Prueba de *Eye tracking*

Código Ético para pruebas de usabilidad

1. Consideraciones generales

No tratar a los participantes como "sujetos" y usar palabras más apropiadas como "participantes" o "usuarios". Respetar su derecho y dignidad vigilando su bienestar psicológico y ético durante la prueba. No hacerle partícipe de prácticas discriminatorias o injustas y, en caso que el usuario se sienta afectado de modo negativo, eliminar la prueba del proceso de evaluación.

2. Privacidad y confidencialidad

Preservar la confidencialidad del participante en el contexto de la investigación, siempre que el participante no haya dado permiso expreso para ello. Registrar únicamente grabaciones de audio, video o fotografía cuando el participante de su consentimiento expreso y por escrito al inicio de la prueba. En caso de estudios observacionales, respetar del mismo modo la privacidad y bienestar psicológico del participante, siempre y cuando las pruebas se realicen en entornos donde el participante esperara ser observado.

3. Consentimiento informado previo a la investigación

Se le presentará al participante, para ser leído y firmado, un documento que recoja todos los aspectos que debe conocer sobre la investigación, el cual se denominará Consentimiento Informado. Los investigadores proporcionarán una oportunidad explícita a los participantes para obtener información apropiada sobre la naturaleza, resultados y conclusiones de la investigación. Si dicha información no puede ser dada antes de la prueba, podrá ser proporcionada posteriormente. En caso de tratarse de menores de edad o discapacitados, el consentimiento deberá proporcionarlo la persona responsable.

Debemos asegurarnos que la persona responsable del usuario evaluador del producto conozca con detalle toda la información que el usuario testeador no puede tener.

4. Proporcionar y discutir con los participantes los resultados de la investigación

Al finalizar el test de usabilidad se debe guardar un espacio de tiempo para interaccionar directamente con el usuario y resolver las posibles dudas que se le hayan generado, así como encontrar posibles confusiones o mejoras para el producto testeado. Es en este momento

cuando resulta muy importante realizar el formulario post-test para recoger toda esta información.

5. Abandono o renuncia a participar en la investigación

Se debe informar al usuario que tiene el derecho de abandonar la sesión de testeo en el momento en que él lo desee, sin necesidad de proporcionar ningún tipo de explicación. Aunque el usuario venga condicionado por la recepción final de una remuneración, sigue teniendo dicho derecho.

6. Tratamiento de la decepción

Es esencial comunicar a los participantes que en el caso de no poder cumplir los objetivos planteados en las tareas propuestas en las pruebas de usabilidad, el responsable es la tecnología y/o el producto evaluado. Por lo tanto, las pruebas de usabilidad deben ser siempre percibidas como pruebas de la tecnología y/o del producto evaluado y, en ningún caso, como pruebas de capacidad o formación del participante.

Hoja de Bienvenida al Participante

Buenos días/tardes, mi nombre es ***Paulo Cesar Realpe*** estudiante de doctorado en ciencias de la electrónica de la Universidad del Cauca (Colombia) y le acompañaré durante este test[1].

Antes que nada, le agradezco su presencia aquí, y que haya aceptado realizar la prueba de usuarios. **Para realizar el test debemos dejar en claro varios aspectos**:

El primero y el más importante es que debe tener claro que **no le estamos evaluando a usted sino lo que queremos evaluar es las funcionalidades de la aplicación de voto electrónico desarrollada por el departamento de matemáticas de la universidad de Lleida**, esto significa que si por alguna razón ve que no puede realizar alguna acción o simplemente se equivoca, no es por culpa suya sino que significa que el producto no está bien diseñado.

Otro aspecto que debe conocer es que como la prueba es analizada posteriormente, debemos grabar la sesión que usted realice. Por ello si lo desea, deberá **firmar el documento de consentimiento para aprobar dicha grabación.**

¿Y en que va a consistir el test? **El test consiste de realizar diversas tareas.** Antes de realizar estas tareas, se le solicitara responder algunas preguntas iniciales sobre el perfil de usuario. **Después de finalizar las tareas, se le solicitara responder algunas preguntas sobre las acciones que ha realizado.**

Si siente la **necesidad de parar la prueba**, por cualquier razón, usted está en su derecho de hacerlo en cualquier momento.

Si tiene **alguna duda se la responderé con gusto**. A continuación lea y firme el **documento de consentimiento de participación y grabación,** y procederemos a comenzar el test.

Muchas gracias por su participación.

[1] La información original de este documento pertenece el Grupo de Interacción Persona Ordenador e Integración de Datos de la Universidad de Lleida (España).

Consentimiento de Participación y Grabación

En cumplimiento de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), mediante el presente documento confirmo que[2]:

1. Acepto participar en esta prueba de usuario que lleva a cabo el laboratorio de usabilidad UsabiliLAB.
2. Autorizo la filmación en vídeo de la prueba.
3. Esta grabación podrá ser utilizada con finalidades científicas para el análisis de los datos recogidos en el proyecto o para divulgar los resultados, ya sea por parte del GRIHO o por la empresa cliente en presentaciones o reuniones profesionales.
4. Renuncio a los derechos de la grabación de vídeo y entiendo que la grabación se puede utilizar para los fines descritos sin permiso adicional.
5. En ningún caso se podrá hacer un uso que pueda vulnerar mi imagen o dignidad personal ni hacer un uso comercial.
6. Puedo ejercitar los derechos de acceso, rectificación, cancelación y oposición de mis datos personales, de acuerdo a la normativa vigente, comunicándolo a los datos de contacto de los que dispongo.
7. He tomado esta decisión basándome en la información que se me ha proporcionado por escrito y he tenido la oportunidad de recibir información adicional en caso de haberla solicitado.
8. Entiendo que la participación es voluntaria y que puedo retirar este consentimiento en cualquier momento sin recibir una penalización por ello.

Nombre y apellidos del participante:

_____

DNI: _____ Teléfono: _____ Email: _____

Fecha: _____

_____ _____

Firma participante Firma administrador del test

Para más información o para cualquier tema relacionado con el proyecto se puede usted dirigir a: **Paulo Cesar Realpe** - Universidad del Cauca - prealpe@hotmail.com.

[2] La información original de este documento pertenece el Grupo de Interacción Persona Ordenador e Integración de Datos de la Universidad de Lleida (España).

Cuestionario Preliminar

Agradecemos lea con atención las siguientes preguntas y las responda con la mayor sinceridad posible.

Usuario #: _____

1. Género ( ) Femenino ( ) Masculino

2. Edad: _____

3. Nivel más alto de educación alcanzado o en proceso:

Estudios de grado ( ) Completo ( ) En proceso

Grado de master ( ) Completo ( ) En proceso

Doctorado ( ) Completo ( ) En proceso

Otro ¿cuál?_____

4. ¿Cuál es su ocupación?: _____

5. ¿Con qué frecuencia utiliza internet?

( ) Nunca ( ) Ocasionalmente ( ) Una vez al día

( ) Más de una vez al día ( ) Permanece conectado todo el día

4. Cuando hay un proceso de votación, participas:

( ) Siempre ( ) Casi siempre ( ) Ocasionalmente ( ) Nunca

6. ¿Ha usado la red internet para realizar algún tipo de votación?

( ) Si ( ) No

7. Dar una opción, ¿le gustaría usar el voto electrónico o continuar usando el voto por papel?

( ) Voto electrónico ( ) Papel

¿Por qué? _____

_____

8. ¿Siente que el internet es seguro para almacenar datos personales o realizar tareas que involucre información sensitiva?

( ) Muy seguro ( ) Seguro ( ) Poco seguro ( ) Inseguro

Cuestionario SUS para Usabilidad

Agradecemos lea con atención las siguientes preguntas y las responda con la mayor sinceridad posible.

Usuario #: _____

1. Creo que me gustará utilizar este sistema frecuentemente.

1	2	3	4	5
Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Completamente de acuerdo

2. Encontré este sistema innecesariamente complejo.

1	2	3	4	5
Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Completamente de acuerdo

3. Pienso que el sistema es fácil de usar.

1	2	3	4	5
Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Completamente de acuerdo

4. Creo que necesitaría del apoyo de un experto para utilizar el sistema.

1	2	3	4	5
Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Completamente de acuerdo

5. Encontré que las diversas funciones en este sistema fueron bien integradas.

1	2	3	4	5
Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Completamente de acuerdo

6. Pensé que había demasiada inconsistencia en el sistema.

1	2	3	4	5
Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Completamente de acuerdo

7. Imagino que la mayoría de las personas aprenderían muy rápidamente a utilizar el sistema.

1	2	3	4	5
Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Completamente de acuerdo

8. Encontré el sistema muy incómodo para usarlo.

1	2	3	4	5
Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Completamente de acuerdo

9. Me sentí muy satisfecho en el manejo del sistema.

1	2	3	4	5
Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Completamente de acuerdo

10. Necesito aprender muchas cosas antes de utilizar el sistema.

1	2	3	4	5
Muy en desacuerdo	En desacuerdo	Neutral	De acuerdo	Completamente de acuerdo

12. ¿Qué fue lo que más le gustó en la aplicación?

_____
_____
_____
_____
_____
_____
_____

13. ¿Qué fue lo que más le disgustó en la aplicación?

_____
_____
_____
_____
_____
_____
_____

Bibliografía

[1] F. Sahar, "Tradeoffs between usability and security," *IACSIT International Journal of Engineering and Technology*, 2013.

[2] M. Guo, H. Liaw, L. Hsiao, C. Huang, and C. Yen, "Authentication using graphical password in cloud," in *15th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2012.

[3] C. Braz and J. Robert, "Security and usability: The case of the user authentication methods," in *18th International Conference of the Association Francophone D'Interaction Homme-Machine*. ACM, 2006, pp. 199–203.

[4] C. Braz, A. Seffah, and D. MRaihi, "Designing a trade-off between usability and security: A metrics based-model," in *Human-Computer Interaction INTERACT 2007*, vol. 4663, 2007, pp. 114–126.

[5] A. Jøsang, B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara, "Security usability principles for vulnerability analysis and risk assessment," in *Twenty-Third Annual Computer Security Applications Conference*. IEEE, 2007, pp. 269 – 278.

[6] M. Zurko and R. T. Simon, "User-centered security," in *New Security Paradigms Workshop (NSPW)*, 1996.

[7] M. Zurko, "User-centered security: stepping up to the grand challenge," in *Computer Security Applications Conference*, 2005.

[8] A. Pedersen, "Usability of authentication in applications web. a literature review," University of Copenhagen, Tech. Rep., 2010.

[9] A. Whitten and J. Tygar, "Why johnny can't encrypt: A usability evaluation of pgp 5.0," in *The 9th USENIX Security Symposium*, 1999.

[10] M. Wu, R. Miller, and S. Garfinkel, "Do security toolbars actually prevent phishing attacks?" in *SIGCHI Conference on Human Factors in Computing Systems*, 2006.

[11] S. Chiasson and R. Biddle, "Issues in user authentication," in *Security user studies: methodologies and best practices*, 2007.

[12] S. Garfinkel, "Design principles and patterns for computer systems that are simultaneously secure and usable," Ph.D. dissertation, 2005.

[13] H. al Khateeb, "Security and usability in click-based authentication system," Ph.D. dissertation, University of Bendfordshire, 2011.

[14] S. Peisert, E. Talbot, and T. Kroeger, "Principles of authentication," in *Workshop on New security paradigms*, 2013.

[15] A. H. Lashkari and S. Farmand, "A survey on usability and security features in graphical user authentication algorithms," *International Journal of Computer Science and Network Security*, 2009.

[16] E. B. Fernandez and J. M. Arteaga, "Extending a secure software methodology with usability aspects," in *Third InternationalWorkshop on Software Patterns and Quality*, 2009.

[17] A. Whitten and J. Tygar, "Usability of security: A case study," School of Computer Science EECS Carnegie Mellon University Pittsburgh and University of California SIMS, Tech. Rep., 1998.

[18] G. Mathew and S. Thomas, "A novel multifactor authentication system ensuring usability and security," *International Journal of Security, Privacy and Trust Management*, 2013.

[19] M. S. Murty, D. Veeraiah, and A. S. Rao, "Digital signature and watermark methods for image authentication using cryptography analysis," *An International Journal Signal & Image Processing*, 2011.

[20] K. Renaud, "Quantifying the quality of web authentication mechanisms a usability perspective," *Journal of Web Engineering*, vol. 3, no. 2, pp. 95–123, October 2003.

[21] B. Schneiderman, *Designing the User Interface.* Addison-Wesley Publishing Company, 1998.

[22] K. P. Yee, *Guidelines and Strategies for Secure Interaction Design*, 2005, ch. Thirteen, p. 253.

[23] D. Markotten, "User-centered security engineering," in *NordU2002 - The 4th EurOpen/USENIX Conference*, 2002.

[24] S. Chiasson, P. C. V. Oorschot, and R. Biddle, "A usability study and critique of two password managers," in *Proceedings of 15th USENIX UNIX Security Symposium*, 2006.

[25] J. Kaiser and M. Reichenbach, "Evaluating security tools towards usable security," in *IFIP 17th World Computer Congress*, 2002.

[26] T. Straub and H. Baier, "A framework for evaluating the usability and the utility of pki-enabled applications," in *1st European PKI Workshop Research and Applications*, 2004.

[27] A. Jøsang, M. Patton, and A. Ho, "Authentication for humans," in *9th International Conference on Telecommunication Systems*, 2001.

[28] A. Jøsang and M. Patton, "User interface requirements for authentication of communication," in *Fourth Austrasian user interface conference on User interfaces*, 2003.

[29] S. Flinn and S. Stoyles, "Omnivore: Risk management through bidirectional transparency," in *Workshop on New Security Paradigms*, 2004.

[30] I. Flechais, M. Sasse, and S. Hailes, "Bringing security home: A process for developing secure and usable systems," in *Workshop on New Security Paradigms*, 2003.

[31] A. Gupta, U. Chandrashekhar, S. Sabnis, and F. Bastry, "Building secure products and solutions," vol. 12, pp. 21–38, 2014.

[32] N. Parveen, R. Beg, and H. Khan, "Integrating security and usability at requirement specification process," vol. 10, pp. 236–240, 2014.

[33] L. Collett, "Designing usable security for effective security," Duke University, Tech. Rep., 2003.

[34] R. Kainda, I. Flechais, and A. Roscoe, "Security and usability: Analysis and evaluation," in *2010 International Conference on Availability, Reliability and Security*, 2010.

[35] S. Faily, J. Lyle, I. Fléchais, and A. Simpson, "Usability and security by design: A case study in research and development," in *Network and Distributed System Security (NDSS) Symposium*, 2015.

[36] E. Churchill, A. Bowser, and J. Preece, "Teaching and learning human-computer interaction: Past, present, and future," vol. 20, no. 2, pp. 44–53, 2013.

[37] M. Hassenzahl, *User Experience and Experience Design*, 2nd ed., 2012.

[38] T. Hewett, R. Baecker, S. Card, T. Carey, J. Gasen, M. Mantei, G. Perlman, G. Strong, and W. Verplank, "Acm sigchi corricula for human-computer interaction," Tech. Rep., 2004.

[39] R. Gupta, "Human computer interaction - a modern overview," vol. 3, no. 5, pp. 1736–1740.

[40] K. Saroha, S. Sharma, and G. Bhatia, "Human computer interaction: An intellectual approach," 2011.

[41] T. Granollers, "Mpiu+a. una metodología que integra la ingeniería del software, la interacción persona - ordenador y la accesibilidad en el contexto de equipos de desarrollo multidisciplinares," Ph.D. dissertation, 2004.

[42] L. Leventhal and J. Barnes, *Usability engineering: process, products and examples*, 1st ed. Pearson.

[43] ISO, "Iso 9241:210 ergonomics of human-system interaction – part 210: Human-centred design for interactive systems," International Organization for Standardization, Tech. Rep., 2010.

[44] D. Vidal, J. Ibarra, B. Flores, and G. Lopez, "Adopción del estándar iso 9241-210:2010 en la construcción de sistemas interactivos basados en computadora," in *International Conference on Research and Innovation in Software Engineering*, 2012.

[45] R. M. González, "Metodología para la especificación de la usabilidad en sistemas interactivos en línea seguros," Ph.D. dissertation, 2009.

[46] T. Granollers, J. Lorés, and J. Cañas, *Diseño de sistemas interactivos centrados en el usuario*, E. Media, Ed. Editorial UAO, 2005.

[47] J. Nielsen, *Designing web usability*, D. GmbH, Ed. Pearson, 2004.

[48] J. Caroll, *The Encyclopedia of Human-Computer Interaction*, 2nd ed., M. Dam and R. Friis, Eds. Aarhus - The Interaction Design Foundation, 2014.

[49] N. Bevan, J. Kirakowski, and J. Maissel, "What is usability?" in *Human Aspects in Computing: Design and Use of Interactive Systems with Terminals,*, 1991.

[50] J. Nielsen, *Usability engineering.* San Francisco, CA, USA: Morgan Kaufmann Publishers, 1994.

[51] A. Solano, "Metodología para la evaluación colaborativa de la usabilidad de sistemas software interactivos," Ph.D. dissertation, 2015.

[52] A. Dix, J. Finlay, G. Abowd, and R. Beale, *Human-Computer Interaction*, 3rd ed. Pearson, 2004.

[53] X. Ferré, "Integration of usability techniques into the software development process," in *International Conference on Software Engineering (Bridging the gaps between software engineering and human-computer interaction)*, 2003, pp. 28–35.

[54] D. Mayhew, *The Usability Engineering Lifecycle.* Morgan Kaufmann, 1999.

[55] J. Karat, *User-centered software evaluation methodologies*, M. Helander, T. Landauer, and P. Prabhu, Eds. Elsevier Science, 1997.

[56] A. Bojko, *Eye Tracking the User Experience: A Practical Guide to Research*, 1st ed., M. Justak, Ed. Rosenfeld Media, 2013.

[57] R. Otaiza, "Metodología de evaluación de usabilidad para aplicaciones web transaccionales," Master's thesis, 2008.

[58] J. Nielsen and R. Mack, *Usability Inspection Methods*. John Wiley & Sons, 1994.

[59] A. Dillon, *Encyclopedia of Human Factors and Ergonomic*, 1st ed., W. Karwowski, Ed. CRC Press, 2001.

[60] J. Nielsen and R. Molich, "Heuristic evaluation of user interfaces," in *SIGCHI conference on human factors in computing systems*. ACM, 1990, pp. 249–256.

[61] J. Nielsen, "Finding usability problems through heuristic evaluation," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1992, pp. 373–380.

[62] Usability.gov. (2015) Heuristic evaluations and expert reviews. [Online]. Available: https://www.usability.gov/how-to-and-tools/methods/heuristic-evaluation.html

[63] L. M. Ardévol, "User experience methodology for the design and evaluation of interactive systems," Ph.D. dissertation, University of Lleida, December 2013.

[64] W. Albert and T. Tullis, *Measuring the User Experience*. Elseiver, 2013.

[65] J. Nielsen. (2003) Introduction to usability. Nielsen Norman Group. [Online]. Available: https://www.nngroup.com/articles/usability-101-introduction-to-usability/

[66] ——, "Usability metrics," 2001. [Online]. Available: https://www.nngroup.com/articles/usability-metrics/

[67] ISO, "Iso/iec 25010 software engineering software product quality requirements and evaluation (square) guide to square," International Organization for Standardization, Tech. Rep., 2011.

[68] M. Gasser, *Building a Secure Computer System*. Van Nostrand Reinhold, 1988.

[69] G. McGraw, "The security lifecycle-the 7 touchpoints of secure software-just as you can not test quality into software, you can not bolt security features onto code and expect it to become hack-proof security," vol. 13, no. 9, 2005.

[70] C. Pfleeger and S. Pfleeger., *Security in Computing*. Prentice Hall PTR, 2006.

[71] Y. Hausawi and W. Allen, "Usablity and security trade-off: A design guideline," in *Proceedings of the 2014 ACM Southeast Regional Conference*. ACM, 2014, pp. 21:1–21:6.

[72] D. Sanz, P. Días, and I. Aedo, *Modelado de la Seguridad en Sistemas de Información Web*. Prentice Hall, 2005, ch. 7.

[73] S. D'Hertefelt, "Trust and the perception of security," Interact Architect, Tech. Rep., 2000.

[74] J. Johnston, J. H. P. Eloff, and L. Labuschagne, "Security and human computer interfaces," *Computers & Security*, 2003.

[75] M. Caloyannides, "Privacy vs. information technology," vol. 99, no. 1, pp. 100–103, 2003.

[76] R. Herold, "What is the difference between security and privacy," CSI Alert newsletter, Tech. Rep., 2002.

[77] OWASP, "Risk rating methodology," 2014.

[78] A. Yeratziotis, D. Greunen, and D. Pottas, "A framework for evaluating usable security: The case of online health social networks," in *6th International Symposium on Human Aspects of Information Security & Assurance*, 2012.

[79] I. Flechais, C. Mascolo, and A. Sasse, "Integrating security and usability into the requirements and design process," vol. 1, no. 1, pp. 12–26, 2007.

[80] L. Cranor and S. Garfinkel, "Guest editors' introduction: Secure or usable?" vol. 2, no. 2, pp. 16–18, 2004.

[81] A. Ferreira, C. Rusu, and S. Roncagliolo, "Usability and security patterns," in *Second International Conferences on Advances in Computer-Human Interactions*, 2009.

[82] S. Garfinkel, "Design principles and patterns for computer systems that are simultaneously secure and usable," Ph.D. dissertation, Massachusetts Institute of Technology, 2005.

[83] K. P. Yee, "User interaction design for secure systems," in *4th International Conference on Information and Communications Security*, 2002.

[84] A. Jøsang and M. Patton, "User interface requirements for authentication of communication," in *Fourth Australasian user interface conference on User interfaces*, vol. 18, 2003, pp. 75–80.

[85] S. Furnell, S. Jusoh, and D. Katsabas, "The challenges of understanding and using security: A survey of end-users," vol. 25, pp. 27–35, 2006.

[86] B. Lampson, "Privacy and security: Usable security: how to get it," vol. 52, pp. 25–27, 2009.

[87] P. Gutmann and I. Grigg, "Security usability," vol. 3, pp. 56–58, 2005.

[88] A. DeWitt and J. Kuljis, "Is usable security an oxymoron?" vol. 13, 2006.

[89] J. Saltzer and M. Schroeder, "The protection of information in computer systems," in *Security and Privacy on the Internet*. ACM, 2000.

[90] D. Balfanz, G. Durfee, D. Smetters, and R. Grinter, "In search of usable security: five lessons from the field," 2004.

[91] A. Herzog and N. Shahmehri, "Usable set-up of runtime security policies," in *International Symposium on Human Aspects of Information Security and Assurance*, vol. 15, no. 5. Emerald Group, 2007, pp. 394–407.

[92] I. Flechais and A. Sasse, "Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-science," vol. 67, pp. 281–296, 2009.

[93] T. Roessler and A. Saldhana, "Web security context: User interface guidelines," 2012. [Online]. Available: https://www.w3.org/TR/wsc-ui/

[94] H. Saltzer and M. Schroeder, "The protection of lnformation in computer systems," in *IEEE*, 1975.

[95] S. Chiasson, R. Biddle, and P. C. V. Oorschot, "A second look at the usability of click-based graphical passwords," in *Proceedings of the 3rd symposium on Usable privacy and security*, 2007.

[96] D. Katsabas, S. Furnell, and P. Dowland, "Using human computer interaction principles to promote usable security," in *5th International Network Conference*, 2005.

[97] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed., J. Wiley and Sons, Eds. Wiley, 2008.

[98] N. Davis, "Secure software development life cycle processes: A technology scouting report," Carnegie Mellon University, Tech. Rep., 2005.

[99] A. Alkussayer and W. Allen, "The isdf framework: Integrating security patterns and best practices," in *International Conference on Information Security and Assurance*, 2009.

[100] C. Eckert, *IT Security: Concepts, Procedures and Protocols*. Oldenbourg Wissenschaftsverlag, 2011.

[101] ISO, "Information technology – security techniques – it network security – part 2: Network security architecture," International Organization for Standardization, Tech. Rep., 2006.

[102] ITU, "Security architecture for systems providing end-to-end communications," International Telecommunication Union, Telecommunication Standardization Sector, Tech. Rep., 2003.

[103] M. Howard and S. Lipner, "The security development lifecycle," Microsoft Corporation, Tech. Rep., 2009.

[104] N. Mohammeda, M. Niazia, M. Alshayeba, and S. Mahmooda, "Exploring software security approaches in software development lifecycle: A systematic mapping study," *Computer Standards and Interfaces*, vol. 50, pp. 107–115, 2017.

[105] A. Alkussayer and W. Allen, "A scenario-based framework for the security evaluation of software architecture," in *3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)*, 2010.

[106] K. Al-Sarayreh, L. Hasan, and K. Almakadmeh, "A trade-off model of software requirements for balancing between security and usability issues," *International Review on Computers and Software*, vol. 10, no. 12, 2016.

[107] U. Holmstrom, "User-centered design of security software," 1999.

[108] L. F. Cranor and S. Garfinkel, *Security and Usability: Designing Secure Systems that People Can Use*, 1st ed., L. F. Cranor and S. Garfinkel, Eds. O'Reilly Media, September 2005.

[109] S. Garfinkel and H. Lipford, *Usable Security: History, Themes, and Challenges*, E. Bertino and R. Sandhu, Eds. Morgan & Claypool, 2014.

[110] R. Smith, *Authentication: From Passwords to Public Keys*. Addison-Wesley Longman Publishing Co., Inc., 2001.

[111] C. Braz, "Integrating a usable security protocol for user authentication into the requirements and design process," Ph.D. dissertation, Universite du Quebec a Montreal, 2011.

[112] H. Joachim, J. Mirkovic, I. Milanovic, and O. Bakkely, "Authentication methods," University of Oslo, Tech. Rep., 2010.

[113] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies*, vol. 63, no. 1, pp. 102–127, 2005.

[114] A. Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems," vol. 63, pp. 128–152, 2005.

[115] E. D. Cristofaro, H. Du, J. Freudiger, and G. Norcie, "A comparative usability study of two-factor authentication," *CoRR*, 2013.

[116] K. Renaud, *Evaluating authentication mechanisms*, security and usability: designing secure systems that people can use ed., L. F. Cranor and S. Garfinkel, Eds. O'Reilly, 2005.

[117] D. S. Carstens, P. R. McCauley-Bell, L. C. Malone, and R. F. DeMara, "Evaluation of the human impact of password authentication practices on information security," *Informing Science Journal*, 2004.

[118] M. Mihajlov, B. J. Blazic, and S. Josimovski, "Quantifying usability and security in authentication," in *35th IEEE Annual Computer Software and Applications*, 2011.

[119] L. Xia, Y. Yang, and Y. Wang, *A Method of Evaluating Authentication Mechanisms*. Springer Netherlands, 2009, pp. 179–184.

[120] C. Eliasson, M. Fiedler, and I. Jørstad, "A criteria-based evaluation framework for authentication schemes in ims," in *International Conference on Availability, Reliability and Security*, 2009.

[121] G. Sim, J. Read, and G. Cockton, "Evidence based design of heuristics for computer assisted assessment," in *12th IFIP TC 13 International Conference, Uppsala, Sweden*, vol. 5726. Springer Berlin Heidelberg, 2009, pp. 204–216.

[122] M. Mujinga, M. Eloff, and J. Kroeze, "Towards a heuristic model for usable and secure online banking," in *24th Australasian Conference on Information Systems (ACIS)*. RMIT University, December 2013, pp. 1–13.

[123] M. Leavitt and B. Shneiderman, "Research-based web design and usability guidelines," US Government Printing Office, Whashington D.C., Tech. Rep., 2006.

[124] C. Wilson, *Credible Checklists and Quality Questionnaires: A User-Centered Design Method*, 1st ed., E. Inc., Ed. Morgan Kaufmann, 2013.

[125] C. Ling and G. Salvendy, "Extension of heuristic evaluation method:a review and reappraisal," *International Journal of Ergonomics and Human Factors*, vol. 27, no. 3, pp. 179–197, 2005.

[126] D. Pierotti, "Heuristic evaluation: A system checklist," Xerox Corporation, Usability analysis and design, Tech. Rep., October 1995.

[127] C. Braz, A. Seffah, and P. Poirier, "Designing usable, yet secure user authentication services: A user authentication protocol," in *5th International Conference on Applied Human Factors and Ergonomics*, vol. 20. AHFE, July 2014, pp. 155–165.

[128] L. Bonastre and T. Granollers, "A set of heuristics for user experience evaluation in e-commerce websites," in *The Seventh International Conference on Advances in Computer-Human Interactions*. IARIA, March 2014, pp. 27–34.

[129] C. Paddison and P. Englefield, "Applying heuristics to accessibility inspections," vol. 16, pp. 507–521, 2004.

[130] C. Rusu, S. Roncagliolo, V. Rusu, and C. Collazos, "A methodology to establish usability heuristics," in *4th International Conferences on Advances in Computer-Human Interactions, IARIA*, 2011, pp. 59–62.

[131] Y. Rogers, H. Sharp, and J. Preece, *Interaction Design: Beyond Human-Computer Interaction*, J. W. . Sons, Ed. Rogers Sharp, 2011.

[132] T. Ibrahim, S. Furnell, M. Papadaki, and N. Clarke, "Assessing the usability of end-user security software," in *Conference in Trust, Privacy and Security in Digital Business*. Springer-Verlag Heidelberg, August 2010, pp. 177–189.

[133] J. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Guidelines for usable cybersecurity: Past and present," in *Third International Workshop on Cyberspace Safety and Security (CSS)*. IEEE, 2011, pp. 21–26.

[134] P. Jaferian, K. Hawkey, A. Sotirakopoulos, M. Rojas, and K. Beznosov, "Heuristics for evaluating IT security management tools," in *Symposium on Usable Privacy and Security (SOUPS)*. New York: ACM, 2011, pp. 1633–1638.

[135] B. Miller, K. Buck, and J. Tygar, "Systematic analysis and evaluation of web privacy policies and implementations," in *The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012)*. IEEE, December 2012, pp. 534–540.

[136] L. Fritsch, K. Fuglerud, and I. Solheim, "Towards inclusive identity management," *Identity in the Information Society*, vol. 3, no. 3, pp. 515–538, December 2010.

[137] ISO, "Iso/iec 27001:2006– information technology – security techniques – information security management systems – requirements," ISO/IEC, Tech. Rep., 2013.

[138] M. Skelton, "What is operability?" 2015. [Online]. Available: https://blog.softwareoperability.com/what-is-operability

[139] P. Realpe, C. Collazos, J. Hurtado, and T. Granollers, "Towards an integration of usability and security for user authentication," in *XVI International Conference on Human Computer Interaction (Interacción 2015)*, 2015.

[140] P. Realpe, C. Collazos, J. Hurtado, T. Granollers, and J. Velasco, "An integration of usable security and user authentication into the iso 9241-210 and iso/iec 25010:2011," *Lecture Notes in Computer Science*, 2016.

[141] M. del Carmen Suúrez Torrente, "Sirius: Sistema de evaluación de la usabilidad web orientado al usuario y basado en la determinación de tareas críticas," Ph.D. dissertation, universidad de Oviedo, 2011.

[142] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems – nist special publication 800-30," National Institute of Standards and Technology, Tech. Rep., 2012.

[143] T. Paul, D. Puscher, and T. Strufe, "Improving the usability of privacy settings in facebook," *CoRR*, 2011.

[144] B. Berjani and T. Strufe, "A recommendation system for spots in location-based online social networks," in *EuroSys Workshop on Social Network Systems*, 2011.

[145] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: Automated identity theft attacks on social networks," in *18th International World Wide Web Conference*, 2009, pp. 551–560.

[146] S. Catanese, P. D. Meo, E. Ferrara, G. Fiumara, and A. Provetti, "Crawling facebook for social network analysis purposes," *CoRR*, vol. abs/1105.6307, 2011.

[147] A. Jamal and M. Cole, "A heuristic evaluation of the facebook's advertising tool beacon," in *1st International Conference on Information Science and Engineering (ICISE)*, 2009.

[148] B. Hoffmann, "An exploratory study of a user's facebook security and privacy settings," Master's thesis, Minnesota State University, 2012.

[149] A. Abdulmohsen and A. Thamer, "Privacy and security issues in social networks: An evaluation of facebook," in *International Conference on Information Systems and Design of Communication*, 2013.

[150] A. Gómez and A. Orozco, "Evaluación heurística de seguridad usable aplicada en sistemas e-banking," Universidad del Cauca, Tech. Rep., 2016.

[151] J. Goldberg, M. Stimson, M. Lewenstein, N. Scott, and A. Wichansky, "Eye tracking in web search tasks: Design implications," in *Proceedings of the 2002 Symposium on Eye Tracking Research & Applications*. ACM, 2002, pp. 51–58.

[152] T. Blascheck, M. John, S. Koch, L. Bruder, and T. Ertl, "Triangulating user behavior using eye movement, interaction, and think aloud data," in *Proceedings of the Ninth Biennial ACM Symposium on Eye Tracking Research & Applications*. ACM, 2016, pp. 175–182.

[153] A. Poole and L. Ball, "Eye tracking in human-computer interaction and usability research: Current status and future," in *Prospects, Chapter in C. Ghaoui (Ed.): Encyclopedia of Human-Computer Interaction. Pennsylvania: Idea Group, Inc*, 2005.

[154] J. Nielsen and K. Pernice, *Eyetracking Web Usability*, N. Riders, Ed. New Riders, 2009.

[155] R. Jacob and K. Karn, *The Mind's Eye - Cognitive and Applied Aspects of Eye Movement Research*. Elsevier, 2003, ch. Eye Tracking in Human-Computer Interaction and Usability Research: Ready to Deliver the Promises, pp. 573–605.

[156] D. MacNamara, F. Carmody, T. Scully, K. Oakley, and E. Quane, "Dual vote: A novel user interface for e-voting systems," in *IADIS International Conference Interfaces and Human Computer Interaction*, 2010.

[157] D. MacNamara, P. Gibson, and K. Oakley, "The ideal voting interface: Classifying usability," *Journal of democracy and open government*, vol. 6, no. 2, pp. 182–196, 2014.

[158] S. Godia, "An electronic voting platform with elliptic curve cryptography," University of Lleida, Tech. Rep., 2011.

[159] M. Karayumak, M. Olembo, M. Kauer, and M. Volkamer, "Usability analysis of helios - an open source verifiable remote electronic voting system," in *Conference on Electronic voting technology/workshop on trustworthy elections*, 2011, pp. 5–5.

[160] J. Brooke, "Sus a quick and dirty usability scale," Usability Evaluation in Industry, 1996, cRC Press.

[161] ——, "Sus: A retrospective," *Journal of Usability Studies*, vol. 8, pp. 29–40, 2013.

[162] A. Bangor, P. Kortum, and J. Miller, "Determining what individual sus scores mean: Adding an adjective rating scale," *Journal of Usability Studies*, vol. 4, pp. 114–123, 2009.

[163] P. Salinia and S. Kanmani, "Survey and analysis on security requirements engineering," *Computers and Electrical Engineering*, vol. 38, no. 6, pp. 1785–1797, 2012.

[164] P. Salini and S. Kanmani, "Security requirements engineering process for web applications," *Procedia Engineering*, vol. 38, pp. 2799–2807, 2012.

[165] M. Khan and M. Zulkernine, "On selecting appropriate development processes and requirements engineering methods for secure software," in *Annual IEEE International Computer Software and Applications Conference*, 2009, pp. 353–358.

[166] J. Jurjens, *Secure Systems Development with UML*. Springer, 2005.

[167] Y. Hausawi and L. Mayron, "Towards usable and secure natural language processing systems," in *HCI International 2013 – Posters Extended Abstracts*, 2013, pp. 109 – 113.

[168] A. Abran, K. Al-Sarayreh, and J. Cuadrado, "A standards-based reference framework for system portability requirements," *Computer Standards and Interface*, vol. 35, no. 4, 2013.

[169] P. Realpe, C. A. Collazos, J. Hurtado, and T. Granollers, "A set of heuristics for usable security and user authentication," in *XVII International Conference on Human Computer Interaction (Interacción 2016)*, 2016.