Evaluación Heurística de Seguridad Usable Aplicada en Sistemas e-Banking

Monografía para optar al título de
Ingeniero de Sistemas

Andrés Felipe Gómez Daza
Andrés Felipe Orozco Orozco

Director: Ph.D(c). Paulo Cesar Realpe Muñoz
Codirector: Ph.D. César Alberto Collazos Ordoñez

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Grupo de I + D en Ingeniería de Software – IDIS
Línea de Investigación en Ingeniería del Software
Popayán, Noviembre de 2016

TABLA DE CONTENIDO

INDICE DE TABLAS……I

INDICE DE FIGURAS..……..III

CAPÍTULO 1.....1

1.1 MOTIVACIÓN.....1
1.2 PLANTEAMIENTO DEL PROBLEMA.....1
1.2.1 Descripción del problema.....*1*
1.2.1 Pregunta de investigación.....*3*
1.3 JUSTIFICACIÓN.....4
1.4 OBJETIVOS.....6
1.4.1 Objetivo general.....*6*
1.4.2 Objetivos específicos.....*6*
1.5 METODOLOGÍA.....6
1.5.1 Fase de exploración.....*6*
1.5.2 Fase de formulación – planificación.....*7*
1.5.3 Fase de ejecución.....*7*
1.5.4 Fase de consolidación.....*7*
1.5.5 Fase de divulgación y documentación.....*7*
1.6 APORTES.....7
1.7 ESTRUCTURA DEL DOCUMENTO.....8

CAPÍTULO 2.....10

2.1 ESTADO DEL ARTE Y TRABAJOS RELACIONADOS.....10
2.1.1 Usabilidad y sistemas seguros.....*11*
2.1.2 HCI y seguridad.....*11*
2.1.3 HCISec.....*11*
2.1.4 Modelos de evaluación y principios de Seguridad Usable (Usec).....*12*
2.1.5 HCISec aplicado en sistemas e-Banking.....*12*
2.1.6 Requerimientos e-Banking.....*13*
2.1.7 Principios aplicables para Software Seguro y Usable.....*13*
2.1.7.1 Usabilidad.....13
2.1.7.2 Seguridad.....14
2.1.7.3 Accesibilidad.....14
2.1.7.4 Operabilidad.....15
2.1.7.5 Fiabilidad.....15
2.1.8 Métodos de evaluación para interfaces de usuario.....*16*
2.1.8.1 Evaluación Heurística.....16
2.1.8.2 Caminata Cognitiva.....16
2.1.8.3 Inspecciones de Usabilidad.....16
2.1.8.4 Caminatas plurales.....16

2.1.8.5 Inspección de funciones 16
2.2 TRABAJOS RELACIONADOS 16
2.2.1 Usabilidad y sistemas seguros *17*
2.2.2 HCI y Seguridad *17*
2.2.3 HCISec *18*
2.2.4 Modelos de evaluación y principios de Seguridad Usable (USec) *18*
2.2.5 Requerimientos e-Banking *19*
2.2.6 Métodos de evaluación para interfaces de usuario *19*

CAPÍTULO 3 22

3.1. DEFINICIÓN DE CONCEPTOS 22
3.2. CONTEXTO DE USO E-BANKING 23
3.2.1 Clientes o Involucrados *23*
3.2.2 Tareas *23*
3.2.3 Aspectos de calidad [66] *23*
3.2.3.1 Seguridad y Confianza 23
3.2.3.2 Servicios Básicos de Calidad 24
3.2.3.3 Servicios de Compra Cruzada 24
3.2.3.4 Valor agregado 24
3.2.3.5 Apoyo de Transacción 24
3.2.3.6 Responsabilidad / Sensibilidad 24
3.2.4 Aspectos técnicos *24*
3.2.4.1 Apoyo, recuperación y disponibilidad [65][67] 24
3.2.4.2 Cifrado de datos [65] 25
3.2.4.3 Servicio de prevención de perdida de datos [67] 25
3.2.4.4 Configuración de la infraestructura de red [67] 25
3.2.4.5 Protección del cliente y apoyo [67] 25
3.3. REQUERIMIENTOS E-BANKING 25
3.4. PRINCIPIOS DE USEC PARA SISTEMAS E-BANKING 26
3.5. REQUERIMIENTOS Y SUB-HEURÍSTICAS 28
3.6 SOPORTE DE EXPERTOS Y PARTICIPACIÓN DE USUARIOS 34
3.6.1 Escala Adjetiva y Numérica *34*
3.6.2 Porcentaje de influencia de los atributos Seguridad y Usabilidad *35*
3.6.3 Grado de importancia de las sub-heurísticas *36*

CAPÍTULO 4 39

4.1. RELACIÓN ENTRE LOS ATRIBUTOS SEGURIDAD Y USABILIDAD 40
4.1.1 Tipo de correlación entre los atributos Seguridad y Usabilidad *41*
4.1.2 Taxonomía – Tipo Correlación *41*
4.2. MODELOS DE MEDICIÓN PARA LA USEC 42
4.2.1 Taxonomía – Aproximaciones *42*
4.3. CONCEPTOS ASOCIADOS 43
4.3.1 Variables Independientes *43*
4.3.2 Representación Vectorial *43*
4.3.3 Distancia Euclidiana y Producto Punto *45*
4.4. FORMULA PARA EL CÁLCULO DE LA USEC 47
4.4.2 Mecanismo para el equilibrio de calificaciones *50*
4.4.3 Transformación de calificaciones *52*

4.4.4 Escala para la medición de la USec *52*
4.5. REPRESENTACIÓN MATEMÁTICA 53
4.5.1 Primer caso *54*
4.5.3 Ejemplos Ilustrativo *56*
4.5.3.1 Ejemplo #1 56
4.5.3.2 Ejemplo #2 58
4.5.3.3 Ejemplo #3 61
4.5.3.4 Ejemplo #4 62
CAPÍTULO 5 66
5.1 ESTUDIO DE CASO 66
5.1.1 Entidad Financiera *68*
5.1.2 Propuesta *68*
5.1.3 Acuerdo de confidencialidad *68*
5.1.4 Alcance del estudio de caso *68*
5.2 ANÁLISIS DE RESULTADOS 69
5.2.1 Encuesta de Satisfacción *69*
5.2.1.1 Fase 1 69
5.2.1.2 Fase 2 70
5.2.1.3 Fase 3 70
5.2.2 Análisis de desempeño de la Evaluación Heurística a cargo de Auditores *75*
5.2.3 Resultados referentes a la plataforma virtual – FONDUC *77*
5.3 RECOMENDACIONES PARA APLICACIÓN FUTURA 80
CAPÍTULO 6 82
6.1 CONCLUSIONES 82
6.2 LIMITACIONES 83
6.3 TRABAJO FUTURO 84
REFERENCIAS BIBLIOGRAFICAS 85

ÍNDICE DE TABLAS

TABLA 1. COMPARACIÓN DE TRABAJOS CON RESPECTO A PRINCIPIOS DE SEGURIDAD Y USABILIDAD.....4
TABLA 2. SEGURIDAD EN UN PRODUCTO SOFTWARE.....14
TABLA 3. REQUERIMIENTOS GENERALES DE UN SISTEMA E-BANKING.....26
TABLA 4. CONJUNTO DE SUB-HEURÍSTICAS ASOCIADAS A UNA FACETA O ATRIBUTO.....28
TABLA 5. GRADO DE IMPORTANCIA PARA SUB-HEURÍSTICAS.....29
TABLA 6. REQUERIMIENTO, SUB-HEURÍSTICAS, GRADO DE IMPORTANCIA Y JUSTIFICACIÓN.....34
TABLA 7. ESCALA DE CALIFICACIÓN.....35
TABLA 8. PORCENTAJE DE INFLUENCIA DE LOS ATRIBUTOS SEGURIDAD Y USABILIDAD.....36
TABLA 9. GRADO DE IMPORTANCIA NUMÉRICO DE LAS SUB-HEURÍSTICAS.....36
TABLA 10. EJEMPLO DEL PROCESO DE CÁLCULO DEL GRADO DE IMPORTANCIA DE LAS SUB-HEURÍSTICAS..37
TABLA 11. TRABAJOS QUE CONTEMPLAN LA RELACIÓN ENTRE SEGURIDAD Y USABILIDAD.....41
TABLA 12. TRABAJOS CENTRADOS EN LA USEC.....42
TABLA 13. EJEMPLO - REQUERIMIENTO DE MAYOR INFLUENCIA.....50
TABLA 14. ESCALA USEC.....53
TABLA 15. REPRESENTACIÓN GENERAL DE LAS CARACTERÍSTICAS PRESENTES EN LA VALORACIÓN INICIAL.....54
TABLA 16. REPRESENTACIÓN GENERAL DE LAS CARACTERÍSTICAS AJUSTADAS.....55
TABLA 17. EJEMPLO#1 ILUSTRATIVO – PRIMER CASO.....56
TABLA 18. EJEMPLO #1 – NUEVOS VALORES DE S.....57
TABLA 19. EJEMPLO #1 – MULTIPLICACIÓN IH.....57
TABLA 20. EJEMPLO #1 – CALIFICACIÓN USEC.....58
TABLA 21. EJEMPLO#2 ILUSTRATIVO – PRIMER CASO.....58
TABLA 22. EJEMPLO #2 – NUEVOS VALORES DE S.....59
TABLA 23. EJEMPLO #2 – MULTIPLICACIÓN IH.....59
TABLA 24. EJEMPLO #2 – CALIFICACIÓN USEC.....60
TABLA 25. EJEMPLO#3 ILUSTRATIVO – SEGUNDO CASO.....61
TABLA 26. EJEMPLO #3 – MULTIPLICACIÓN IH.....61
TABLA 27. EJEMPLO #3 – CALIFICACIÓN USEC.....62
TABLA 28. EJEMPLO#4 ILUSTRATIVO – SEGUNDO CASO.....63
TABLA 29. EJEMPLO #4 – MULTIPLICACIÓN IH.....63
TABLA 30. EJEMPLO #4 – CALIFICACIÓN USEC.....64
TABLA 31. RESULTADOS ENCUESTA DE SATISFACCIÓN.....70
TABLA 32. FRECUENCIAS Q1.....71
TABLA 33. FRECUENCIAS Q2.....71
TABLA 34. FRECUENCIAS Q3.....72
TABLA 35. FRECUENCIAS Q4.....72
TABLA 36. FRECUENCIAS Q5.....73
TABLA 37. FRECUENCIAS Q6.....73
TABLA 38. FRECUENCIAS Q7.....73
TABLA 39. FRECUENCIAS Q8.....74
TABLA 40. FRECUENCIAS Q9.....74
TABLA 41. FRECUENCIAS Q10.....74
TABLA 42. RESULTADOS USEC - FONDUC.....76
TABLA 43. COMPARACIÓN CALIFICACIONES AUDITORES.....77

TABLA 44. CALIFICACIÓN GENERAL DEL SISTEMA 78
TABLA 45. SÍNTESIS CALIFICACIÓN GENERAL 78
TABLA 46. RESULTADO FINAL, USEC GENERAL 79

ÍNDICE DE FIGURAS

FIGURA 1. ESQUEMA CONCEPTUAL DEL ESTADO DEL ARTE (CREACIÓN PROPIA) 10
FIGURA 2. ESQUEMA CONCEPTUAL DEL MODELO MATEMÁTICO (CREACIÓN PROPIA) 39
FIGURA 3. TAXONOMÍA DE CORRELACIÓN. (TOMADA DE [83]) 41
FIGURA 4. DISTRIBUCIÓN GRÁFICA – REPRESENTACIÓN VECTORIAL 44
FIGURA 5. DISTRIBUCIÓN GRÁFICA – ATRIBUTOS Y DISTANCIA EUCLIDIANA 46
FIGURA 6. AMBIGÜEDAD PRESENTADA DE ACUERDO A CALIFICACIONES 48
FIGURA 7. ANULACIÓN DE AMBIGÜEDAD 49
FIGURA 8. COMPORTAMIENTO DE LOS VECTORES APLICANDO EL MECANISMO PARA EL EQUILIBRIO DE CALIFICACIONES 51
FIGURA 9. PROCESO PARA LLEVAR A CABO EL ESTUDIO DE CASO 67
FIGURA 10. DISTRIBUCIÓN DE LOS DATOS 71

Capítulo 1

Introducción

Los artefactos generados en este capítulo, pueden ser evidenciados en el Sprint 1 de la metodología (véase **Anexo L**).

1.1 MOTIVACIÓN

Actualmente la usabilidad es uno de los aspectos ampliamente aplicados al momento de desarrollar software de uso cotidiano para los usuarios. Las técnicas para el diseño de sistemas usables ofrece varias ventajas para los usuarios del sistema, ya que les permite el aumento de la productividad, la disminución de los errores, la disminución de los costes en capacitación y la disminución de apoyo a los usuarios, además los mecanismos de evaluación heurística han tenido un gran desarrollo **[1]**. Por otro lado la gran expansión que ha tenido internet hasta la fecha ha llevado a que cada vez más información sea almacenada en bases de datos de la red **[2]**, caso particular, en el ámbito bancario, donde estas aplicaciones incluyen varias funciones, tales como retirar dinero, consultar cuentas, hacer depósitos, transacciones bancarias de venta libre, información de la cuenta del cliente, el seguimiento de mensajes y SWIFT (Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales) **[1]**. Es aquí donde el aspecto de seguridad juega un papel muy importante como una contramedida a los distintos ataques cibernéticos que a diario intentan vulnerar y/o corromper la información privada de los usuarios o diversas instituciones **[2]**. Ahora bien, partiendo de la frase, “entre más seguro se hace algo, menos usable llega a ser” **[3]** se considera la necesidad de identificar objetivos para la seguridad y la usabilidad, de manera colectiva, que ayudarán con el equilibrio de forma proactiva entre estos **[3]**. Este es el punto de inicio para formular una hipótesis teniendo en cuenta estos dos términos en conjunto, que a través de una evaluación heurística apoyada en una herramienta, permita fortalecer los puntos críticos y vulnerables que una aplicación bancaria presente, y además contribuir con el área de investigación Interacción Humano Computador y Seguridad (HCISec).

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 Descripción del problema

Los factores humanos son quizá el mayor obstáculo para hacer efectiva la seguridad computacional. Muchos de los componentes que hacen parte de la seguridad son poco entendibles y en ocasiones frustrantes para un significativo número de usuarios quienes tienen como objetivo manejarlos correctamente, esto se debe, a que la seguridad es un objetivo secundario para los usuarios **[32]**. Pese a que, el diseño de software de seguridad emplea patrones de usabilidad específicos, el problema aún persiste **[4]**.

La opinión generalizada sobre la seguridad y usabilidad es que son dos objetivos incompatibles en el diseño de un sistema. Se sostiene que, "hay muchos casos en los que la seguridad y la usabilidad pueden ser sinérgicamente mejoradas mediante la revisión de cómo una funcionalidad específica es implementada en muchos de los sistemas operativos y aplicaciones actuales". Si bien es cierto que hoy en día un sistema seguro y usable puede ser difícil de construir, es posible su realización si se contase con un modelo de integración entre ambos aspectos, elemento que será parte de la propuesta a trabajar **[5]**.

Si bien existe una estructura de técnicas de diseño de interfaces de usuario específica que involucre la seguridad, ésta ha sido criticada por la comunidad científica **[6] [12]**, debido a que es necesario mayor investigación que permita encontrar metodologías para que tanto la seguridad como la usabilidad puedan coexistir, por lo tanto, no ha llegado a convertirse en un modelo ideal. Preocupante es entonces, que las investigaciones del área Interacción Humano-Computador (HCI) en el cual podría apoyarse este trabajo no se han centrado mucho en la seguridad de las aplicaciones **[4]**, es decir, que las prácticas existentes en HCI asumen como prioridad mejorar la eficacia, la eficiencia o la satisfacción de los usuarios, apartando las posibles amenazas y vulnerabilidades que puedan introducir **[6]**, aunque recientemente se han definido enfoques como HCISec que aborda este aspecto y establece un equilibrio entre la seguridad y la usabilidad **[7]**.

El campo de Interacción Humano Computador y Seguridad (HCISec) reconoce que para que un sistema sea seguro, también debe ser fácil de usar. Incluso el sistema técnicamente más seguro fracasará en la práctica si los usuarios no pueden usarlo correctamente. Para evitar esto, las proposiciones del área HCI deben ser asumidas desde el ciclo inicial del proceso de desarrollo de los mecanismos de seguridad, no en la última etapa cuando el desarrollo es dejado en manos del grupo de mejora de interfaces **[4]**.

La comunidad de HCISec ha presentado avances en el desarrollo de interfaces de usuario final, eficaces para software anti-phishing, gestores de contraseña, y otras áreas de seguridad **[8]**. Los servicios del comercio electrónico (e-Commerce) mezclan las actividades de la vida cotidiana con las transacciones digitales, principalmente involucran dinero por medio de compras como vestuario (e-Retail), viajes (e-Travel), pagos y transacciones en línea (e-Banking); estos se convierten en típicos ejemplos de lo señalado. Aún con las estrictas recomendaciones de seguridad, los usuarios tienden a ignorarlas, sin embargo, la mayoría de usuarios tan sólo las desconocen, lo que les impide dimensionar las devastadoras consecuencias **[9]**.
Tomando el último ejemplo de las categorías e-Commerce ya mencionadas, se procede con la propuesta de investigación para éste trabajo, **[10]** pues el sector bancario es una de las industrias que han acogido con mayor rapidez al internet como canal de distribución de sus 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 las investigaciones realizadas hasta la fecha **[11] [12] [13]**, se ha detectado que los factores que motivan a los usuarios a la adopción de los servicios e-Banking se pueden generalizar en dos conceptos, usabilidad y seguridad. **[11].**

Los problemas de usabilidad y las pruebas llevadas a cabo en el campo de e-Banking, giran en torno a la seguridad **[12]**. Si bien es cierto que los problemas de seguridad de un sistema e-Banking puede dar lugar a pérdidas monetarias sustanciales o daño en la reputación, las deficiencias de usabilidad también pueden dar como resultado mayores costos operacionales en la medida que un cliente requiere atención adicional a través de los centros de llamadas, o en el momento que decide dejar de usar el servicio de e-Banking, volviendo a hacer sus trámites del modo tradicional **[13]**.

El propósito general de la investigación presentada en **[14]** es proponer un modelo heurístico para la seguridad y usabilidad en los sistemas e-Banking. El conjunto propuesto parte de una revisión sistemática de la literatura que contribuirá en el diseño de sistemas e-Banking seguros y usables. Además, es claramente un modelo de principios generales de sistemas e-Banking. El Diccionario de Oxford define una heurística como "permitir a una persona descubrir o aprender algo para sí mismos." **[35]** Las heurísticas son generalmente usadas para representar características o aspectos del mundo real, facilitan la comprensión del problema en cuestión (sistemas e-Banking seguros y usables) **[12]**.

Se argumenta que los métodos de evaluación de usabilidad actuales no tienen en cuenta plenamente los componentes especiales de aplicaciones y software de seguridad. Esta opinión está respaldada por materiales clave en ésta área **[6] [36]**, que critican a la comunidad de investigadores en HCISec por la adopción de los métodos de usabilidad empleados para la evaluación **[12]**.

Los métodos de evaluación que intentan comparar estos sistemas, no se han abordado adecuadamente en la literatura hasta la fecha **[12]**.

1.2.1 Pregunta de investigación

De acuerdo con lo anterior, el problema de investigación se centra en el planteamiento de un conjunto de principios de evaluación partiendo de una revisión sistemática pertinente para los sistemas e-Banking, teniendo en cuenta la interacción de la seguridad y la usabilidad. En el marco de ésta iniciativa surge la pregunta de investigación de este proyecto, *¿Bajo qué principios de Seguridad Usable (USec) y con qué herramienta es posible la evaluación de sistemas e-Banking que integren aspectos de seguridad y usabilidad?*

1.3 JUSTIFICACIÓN

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. En la ***Tabla 1***, se presentan algunos trabajos que integran ambos aspectos, en algunos casos se plantean de forma conjunta. Cabe destacar que esta investigación estará ajustada al contexto de e-Banking, por lo tanto, es necesario resaltar que Mujinga & Kroeze **[14]** proponen un conjunto de heurísticas para estos sistemas, sin embargo, son principios generales que requieren la intervención a través de su desglosamiento y permitir una evaluación de sistemas e-Banking seguros y usables.

A continuación se presentan las investigaciones más relevantes que presentan aproximaciones para la evaluación de sistemas seguros y usables, con el fin de hacer un análisis para la respectiva justificación de éste trabajo.

Trabajo	Descripción	U.	S.	Entorno
"Towards a Heuristic Model for Usable and Secure Online Banking"[14]	Modelo de principios generales para e-Banking seguro y usable. No se ha llevado a la práctica.	Sí	Sí	e-Banking
"Security Usability Challenges for End-Users"[34]	Directrices para evaluar aspectos HCI en software de seguridad.	Sí	Sí	Aplicaciones software
"A Set Of Heuristics for User Experience Evaluation in E-commerce Websites"[37]	Conjunto de heurísticas para evaluar la experiencia de usuario es espacios e-Commerce.	Sí	No	e-Commerce
"Guidelines for Usable Cybersecurity: Past and Present"[21]	Conjunto de directrices recopiladas para el desarrollo de sistemas seguros y usables.	Sí	Sí	Aplicaciones seguras y usables
"A Framework to Evaluate Usable Security in Online Social Networking"[32]	Framework de evaluación de Seguridad Usable (USec).	Sí	Sí	Online Social Networking
"Usable security: User preferences for authentication methods in eBanking and the effects of experience"[22]	Experimento para medir las preferencias de los usuarios por métodos de autenticación en sistemas e-Banking.	Sí	Sí	e-Banking
"Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science"[43]	Modelo de diseño de sistema seguro socio-técnico.	Sí	Sí	e-Science

Tabla 1. Comparación de Trabajos con Respecto a Principios de seguridad y usabilidad

- *U*: Hace referencia a los estudios que abarcan el campo de usabilidad.
- *S*: Hace referencia a los estudios que abarcan el campo de la seguridad.
- *Entorno*: Hace referencia al contexto en el cual son aplicados los estudios.

Algunos de los estudios indicados en la ***Tabla 1***, proponen algunas alternativas de evaluación o análisis de seguridad y usabilidad en algunos entornos. Mujinga & Kroeze **[14]** proponen un modelo heurístico para la seguridad y usabilidad en e-Banking, pero éste sólo se centra en principios generales sin entrar en detalle de los mismos, además, se trata de una propuesta que aún no se ha llevado a la práctica, sin embargo, como trabajo futuro propone realizar la evaluación de este modelo a través del método de evaluación heurística basado en un checklist de escala propuesto por Nielsen **[24]**.

Por otro lado, Furnell **[34]** hace uso de algunos principios del HCI con el fin de apoyar algunas funcionalidades de seguridad en algunas aplicaciones software, con lo cual elabora 10 directrices que ayudan a verificar el grado de cumplimiento de dichas aplicaciones.

Con el fin de que los sistemas e-Commerce tengan un alto grado de competitividad, Bonastre & Granollers **[37]** afirman que estos sistemas deben proporcionar a los clientes una experiencia de usuario satisfactoria, por ello diseñan 64 heurísticas que permitan evaluar el logro de este aspecto.

Nurse et al. **[21]** Recapitulan algunas de las principales novedades en los dominios de seguridad y usabilidad, particularmente basándose en estudios relativos a la orientación y recomendaciones para los sistemas de seguridad altamente usables. Como tal, una de las principales contribuciones de esta investigación es la recopilación de los trabajos existentes y la propuesta de una lista inicial de pautas generales.

Yeratziotis et al. **[32]** Mencionan el riesgo que tiene la información personal de un usuario que hace uso de sistemas de redes sociales debido a la complejidad que involucra la comprensión de las funcionalidades de seguridad y privacidad, es por ello que se hace un estudio partiendo de los conceptos de HCI y seguridad, con el cual ofrecen un framework de evaluación heurística en redes sociales, teniendo en cuenta las características de seguridad y usabilidad.

Weir et al. **[22]** Realizan un estudio con tres métodos de autenticación diferentes que se presentan en un sistema e-Banking, los tres métodos son comparados de manera similar a través de un experimento de repetidas medidas con 141 participantes, todos con conocimiento en e-Banking. Finalmente, el método de mayor aprobación fue el del uso de la contraseña tradicional. Los resultados permiten evidenciar importantes actitudes de los participantes al momento de enfrentarse a diferentes métodos de autenticación: la comodidad, la propiedad personal y la experiencia habitual de los procesos.

Flechais & Sasse. **[43]** Resaltan la necesidad de diseñar sistemas seguros y usables para e-Science. Destacan la existencia de dos problemas fundamentales en el diseño de estos sistemas, el primero, los mecanismos de seguridad deben ser usables para los diferentes usuarios del sistema, y el segundo, la seguridad de todo el sistema satisface la necesidad requerida por todo el conjunto de interesados. El objetivo de esta investigación es poner en evidencia los problemas anteriormente mencionados e identificar cómo pueden presentarse en el diseño de aplicaciones e-Science. El análisis concluye con un modelo que explica las relaciones entre los factores más importantes que rodean la Seguridad Usable (USec).

Teniendo en cuenta los trabajos recopilados, en esta investigación se propone un conjunto de principios los cuales estarán adaptados al contorno de e-Banking y permitirán evaluar dichos sistemas en los aspectos de seguridad y usabilidad, del mismo modo, los sistemas podrán ser diseñados con referencia a las pautas de los principios permitiendo una mejor adaptación de los aspectos en mención. Él conjunto de principios pretende apoyar a cualquier involucrado de los sistemas e-Banking y contribuirá a la comunidad científica al permitir la evaluación de la seguridad y usabilidad en los sistemas e-Banking a través de una herramienta de evaluación cuantitativa para medir el grado de severidad de cada principio la cual será suministrada en esta investigación.

1.4 OBJETIVOS

1.4.1 Objetivo general

- Proponer y evaluar un conjunto de principios de Seguridad Usable (USec) en el contexto de e-Banking que permita contribuir en el diseño del sistema con respecto a su seguridad y usabilidad.

1.4.2 Objetivos específicos

- Proponer y evaluar un conjunto de principios en un contexto especifico que pueda contribuir en la evaluación de sistemas e-Banking seguros y usables.

- Desarrollar una herramienta que permita evaluar el conjunto de principios teniendo en cuenta la seguridad y usabilidad.

- Evaluar los principios y la herramienta a partir del estudio de caso.

1.5 METODOLOGÍA

Para el desarrollo del presente trabajo de grado se seguirá la metodología de estudio de caso **[37]** adaptada a las necesidades de éste proyecto de investigación, Scrum como marco de gestión del trabajo de investigación **[39]** basado en el método original **[40]**. A continuación se describe la metodología como se desarrollara el proyecto:

1.5.1 Fase de exploración

En esta fase se realizará un estudio inicial, en donde se estructurará de manera detallada el proyecto a desarrollar, aportando así, al planteamiento de estrategias y elementos necesarios para lograr los objetivos de este proyecto.

Con el fin de fortalecer la base conceptual, se hará una exploración más elaborada acerca de los antecedentes que hacen parte de los siguientes núcleos temáticos: Seguridad Usable (USec), heurísticas de evaluación, principios de evaluación, e-Banking, HCISec, a través de la consulta de libros, artículos, monografías, consultas a expertos en los temas y demás fuentes de información que nos faciliten las herramientas necesarias para consolidar la investigación y así poder disponer de criterios suficientes para establecer un estudio robusto. Se incluye una planificación general inicial.

En esta fase se hace entrega del Anteproyecto de trabajo de grado y se complementa el estado del arte realizando un estudio profundo de los núcleos temáticos.

1.5.2 Fase de formulación – planificación

En esta fase se crea una lista de requisitos para e-Banking a partir de la fase de exploración. Se validan los requisitos necesarios para el determinar el desarrollo de un primer estudio de caso, proposición de sub-heurísticas y modelo matemático.

1.5.3 Fase de ejecución

A partir de los requisitos anteriores, adecuar el conjunto de principios para e-Banking. Consolidar el estudio de caso a partir de los requisitos preliminares y evaluar los principios. Realizar la evaluación del modelo a través del estudio de caso y la retrospectiva (análisis y reflexión del trabajo de investigación).

1.5.4 Fase de consolidación

Esta fase es concluida con los requisitos cumplidos. En este caso, son análisis de resultados, conclusiones, exposición de puntos sensibles y trabajo futuro.

1.5.5 Fase de divulgación y documentación

En esta fase final se hace entrega de la monografía del trabajo de grado incluyendo ahí los resultados obtenidos de la investigación. Por último se realizará el proceso de sustentación del trabajo de grado ante los respectivos jurados de la facultad de Ingeniería Electrónica y Telecomunicaciones.

1.6 APORTES

A partir del estado del arte, se han realizado estudios que integran la seguridad y la usabilidad, en algunos planteados de forma conjunta. Cabe destacar que esta investigación estará ajustada al contexto de e-Banking, por lo tanto, es necesario resaltar que existe un estudio que propone un conjunto de heurísticas **[14]** en la literatura, sin embargo, son principios generales que requieren la intervención a través de su desglosamiento, para

permitir una minuciosa evaluación de sistemas e-Banking seguros y usables. Actualmente, la carencia de estudios en el ámbito centra esta investigación en la proposición y consolidación del conjunto de principios, el cual beneficiará enormemente a la comunidad de interesados de más herramientas que permita un equilibrio adecuado entre seguridad y la usabilidad en el contexto de e-Banking. Por lo tanto, el aporte que se pretende generar con este proyecto al área de investigación, consiste en proponer un conjunto de principios que permitirá a la comunidad científica evaluar la usabilidad y seguridad de sistemas e-Banking de forma conjunta a partir de sus requerimientos, apoyados en una herramienta de evaluación cuantitativa para medir el grado de equilibrio del principio en conflicto (i.e. grado del problema encontrado en la interfaz de acuerdo con el principio a evaluar).

1.7 ESTRUCTURA DEL DOCUMENTO

La estructura del presente trabajo se describe a continuación:

Capítulo 1: Se exponen las bases del presente trabajo de grado. Se presenta la motivación del tema del trabajo, el planteamiento detallado del problema, la justificación y se definen los objetivos investigativos y todas las contribuciones del trabajo.

Capítulo 2: Se establece el estado del arte y trabajos relacionados, se hace una recolección de los distintos aspectos que intervienen en la propuesta del trabajo y se expone una taxonomía de los distintos modelos e investigaciones en los que se apoya este estudio. En este capítulo se describen los primeros criterios a tener en cuenta para la construcción de la herramienta de evaluación (*modelo matemático*) y sus atributos.

Capítulo 3: Se describen cada uno de los parámetros a tener en cuenta para la construcción del formato de evaluación heurística para sistemas e-Banking. Se definen de manera formal los requerimientos y las sub-heurísticas a considerar en el proceso de evaluación del estudio de caso.

Capítulo 4: En este capítulo se definen conceptos asociados al modelo matemático en construcción para el cálculo de la USec, se establecen las fórmulas matemáticas que intervienen y finalmente se presenta de manera formal su estructura de representación.

Capítulo 5: En este capítulo se describen las pruebas realizadas para la evaluación del trabajo desarrollado. A partir del formulario construido en los capítulos 3 y 4 para la evaluación heurística del sistema e-Banking, se lleva a cabo el estudio de caso, posteriormente se hace el procesamiento de datos obtenidos por los auditores a través del modelo matemático, y se exponen los resultados.

Capítulo 6: Se entregan las conclusiones obtenidas en el desarrollo del presente trabajo; adicionalmente, se presentan limitaciones y trabajos futuros.

Capítulo 2

Proceso Conceptual Y Revisión De La Literatura

Los artefactos generados en este capítulo, pueden ser evidenciados en el Sprint 2 de la metodología (véase **Anexo L**).

2.1 ESTADO DEL ARTE Y TRABAJOS RELACIONADOS

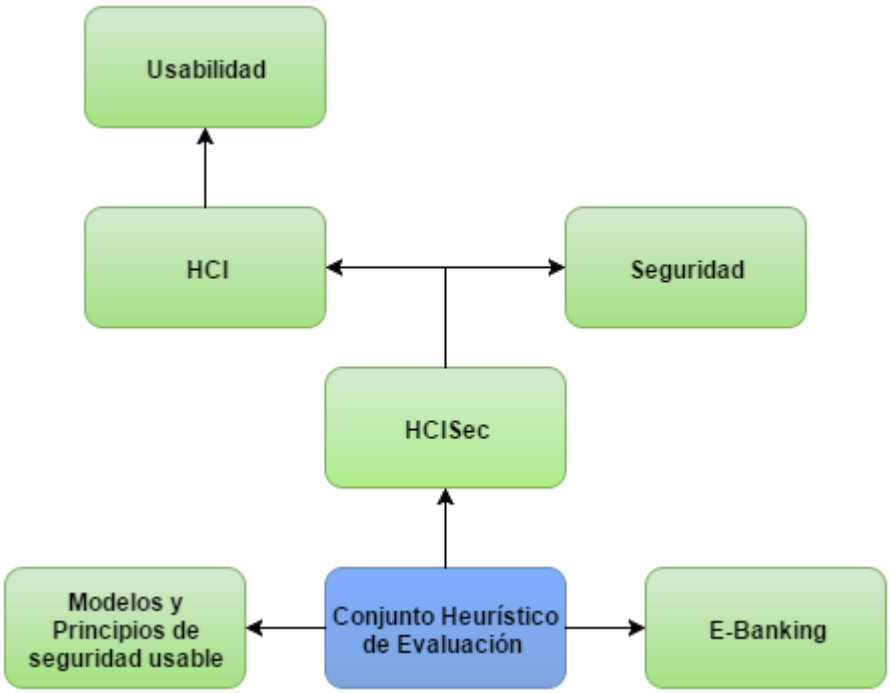

Figura 1. Esquema Conceptual del Estado del Arte (Creación Propia)

En la figura anterior, se reflejan las distintas temáticas en las que se fundamenta el estado del arte, siendo los principales tópicos ***Usabilidad***, ***Seguridad***, ***Modelos y Principios de Seguridad Usable*** y ***sistemas e-Banking***, los cuales en conjunto, permitirán llevar a cabo el desarrollo de los objetivos de esta investigación.

2.1.1 Usabilidad y sistemas seguros

En **[15] y [16]** rescatan el innovador campo de usabilidad aplicada a los mecanismos de seguridad. Contextualizan a **[17]** quienes serían los primeros en realizar señalamientos afirmando que, los mecanismos de seguridad requerían exigencias poco razonables en muchas de las partes interesadas (usuarios, administradores e incluso desarrolladores de sistemas) y resaltando el abrumador incremento de la complejidad característica de considerables sistemas de seguridad en cualquiera de sus posibles niveles (hardware, sistema operativo, red, aplicaciones).
Es importante destacar los lineamientos que permiten la definición de un sistema usable (basado en **[18]**)

- Los usuarios involucrados pueden conocer el rendimiento operativo de un proceso
- El aprendizaje y práctica requeridos para alcanzar un objetivo es el apropiado
- El sistema en uso no genera alguna tensión física o mental para el involucrado; y
- Los usuarios se muestran satisfechos con la experiencia de interacción con el sistema **[15]**, critica fuertemente la no existencia de los principios clave de la usabilidad en el diseño de los mecanismos de seguridad, **[15] [9] [7]** pues se argumenta que la ayuda ofrecida al usuario también puede ser explotada por un atacante potencial, generando pérdidas en ocasiones irremediables.

2.1.2 HCI y seguridad

En los diversos estudios llevados a cabo por distintos autores del área de HCI, se han desarrollado algunos de los criterios que a la fecha son pieza fundamental en el desarrollo de interfaces usables, pero la gran limitante encontrada, es que, en dichos estudios no se consideró el impacto que tiene la seguridad en su diseño **[19]**, sin embargo, en **[7]** se menciona que los distintos conceptos de HCI pueden ser aplicados en las distintas tecnologías de seguridad, mejorando su uso significativamente, en la medida que, actuando como disciplina de investigación, esta área es un campo de estudio bien desarrollado. **[9]** Menciona algunas áreas de interés donde HCI y seguridad se cruzan, se exponen como ejemplo 1) la autenticación de usuarios, 2) diseño de interfaces seguras, 3) capacidad de uso de los productos de seguridad, y 4) Protección de sistemas que usan técnicas de CAPTCHA, por lo tanto en casos específicos los criterios de HCI de Nielsen **[24]** han sido modificados y condensados, de tal forma que puedan ser aplicados en los distintos aspectos que conlleva la seguridad de un sistema **[7]**.

2.1.3 HCISec

Interacción Humano Computador y Seguridad (HCISec) surge como una necesidad identificada por los expertos en el área de HCI, cuyo objetivo consiste en mejorar la usabilidad de sistemas seguros **[6]**. Los expertos en esta área han llegado a afirmar que en la mayoría de los casos los problemas de seguridad han sido ignorados por los investigadores del área de usabilidad, y los problemas de usabilidad han sido ignorados por los especialistas en seguridad **[5]**, entonces es correcto afirmar que una evaluación de la usabilidad de software seguro no debería centrarse solo en la usabilidad excluyendo la seguridad, por esta razón la comunidad de investigadores ha detectado la necesidad de reexaminar el diseño e implementación de sistemas seguros **[6].** La investigación

interdisciplinaria en el campo HCISec reúne a investigadores de los dos campos hacia el desarrollo de la Seguridad Usable (USec) **[9]** por lo cual HCISec se proyecta como un área muy activa **[6]**.

2.1.4 Modelos de evaluación y principios de Seguridad Usable (Usec)

Autores importantes han contribuido en el campo del HCI especialmente a la usabilidad de sistemas interactivos. Las ocho reglas de oro de Shneiderman **[23]** permiten diseñar buenas interfaces. Las heurísticas de Nielsen **[24]** permiten el éxito en la Interacción Humano-Computador. Dix et al. y Preece et al. **[26]** 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 heurísticas en el campo de la USec, entre los más importantes se encuentran: Los diez principios de Yee **[27]** permiten el diseño de sistemas seguros. Los criterios de Johnston et al. **[7]** permite el éxito en la relación entre HCI y seguridad. Los 5 principios de Whitten **[4]** permiten establecer cuando es usable un sistema de seguridad. Los seis principios generales de Garfinkel **[5]** permiten alinear seguridad y usabilidad. Finalmente, los principios de Herzog **[28]** permiten diseñar aplicaciones que establecen políticas de seguridad.
En este trabajo también se tienen en cuenta algunas heurísticas en el campo de la USec propuestas por Chiasson **[8]**, Saltzer **[29]**, Ibrahim et al. **[19]**, Nurse et al. **[21]**, Katsabas et al. **[30]**, Zhou et al. **[31]** y Yeratziotis **[32]**.

2.1.5 HCISec aplicado en sistemas e-Banking

El fuerte desarrollo de los sistemas e-Banking en las últimas décadas ha conllevado a los bancos a la constante búsqueda de su seguridad, incluyendo medidas eficaces contra el fraude financiero, la delincuencia informática y sus ataques maliciosos relacionados **[12]**. Los usuarios de internet en general hacen uso de e-Banking, pero esta es una de las tareas que requieren de mucho cuidado para ser ejecutada; la tendencia de los bancos tradicionales es a alentar a sus usuarios a que hagan uso de este tipo de servicio de manera tranquila, aunque aparentemente ofrecen una garantía del 100%, es la letra pequeña (políticas de seguridad) la que condiciona a los usuarios a cumplir con ciertos requisitos de seguridad **[20]**, por lo tanto podría ser útil separar los atributos de usuario de las políticas de seguridad del sistema **[21]**. Ahora bien, **[22]** plantea que la seguridad no es el objetivo primordial de la interacción de un usuario con un sistema informático, sin embargo, en el diseño de los procedimientos de seguridad, los problemas de usabilidad con frecuencia se pasan por alto en el deseo de ofrecer una solución tecnológicamente segura **[41]**, ignorando el factor humano **[42]**. En **[12]** se manifiesta la necesidad de crear una pauta más formal para que los bancos garanticen la USec de sus sistemas e-Banking. La comprensión y la formalización de la interacción entre la seguridad y usabilidad en este espacio tendrán un impacto significativo en la mejora de los sistemas e-Banking para todos los usuarios.

2.1.6 Requerimientos e-Banking

Los crecientes avances en las telecomunicaciones y tecnologías de la información han permitido que los canales de comunicación aumenten progresivamente y se encuentren disponibles en cualquier periodo de tiempo para algún individuo **[44]**. Las instituciones bancarias han optado por el empleo de dichos canales de comunicación para atraer a sus clientes y están adaptando sus servicios y productos en la web **[44] [45]**. En la creciente demanda de los servicios tecnológicos, es necesario destacar que las aplicaciones bancarias deben contar con estrictas funciones que garanticen al usuario el cumplimiento de las actividades cuando haga uso de la aplicación, por esta razón, es esencial poner en práctica la técnica de definición de requerimientos, que permite capturar las necesidades de los usuarios para luego ser convertidas en servicios del sistema, y cuyo objetivo principal es suplir las necesidades anteriormente mencionadas **[46]**.
En este trabajo se tienen en cuenta algunos requerimientos en el campo de sistemas e-Banking propuestos por Carlo **[44]**, Iyengar et al. **[45]**, AlAbdullah et al. **[46]**, Fajfr **[47]**, Babatunde **[48]**, Abrazhevich et al. **[49]** y "Monetary Authority of Singapore" **[50]**.

2.1.7 Principios aplicables para Software Seguro y Usable

Estos principios son una base para alcanzar niveles adecuados de calidad a nivel de seguridad y usabilidad en aplicaciones web en general **[51]**. A continuación se definen cada uno de estos atributos que serán parte fundamental del núcleo de esta tesis.

2.1.7.1 Usabilidad

La usabilidad en **[52]** se define como la facilidad de uso en cualquier tipo de sistemas que interactúan con un usuario, para el estudio de caso de esta monografía, un sitio web e-Banking. Para Jacob Nielsen "La gente tiene que ser capaz de comprender el funcionamiento del sitio inmediatamente después de escanear la página principal, por unos pocos segundos al menos". Éste término también es considerado como *una medida de calidad* de la experiencia de interacción entre el usuario y el sistema o producto.

La usabilidad universal, es la característica de un sistema, en este caso e-Banking, que pretende ser utilizado por:

1. El tipo específico de usuario (Usuarios de un determinado banco)
2. La tarea para la cual el sistema se ha hecho (Trámites bancarios)
3. El contexto en el que se da la interacción (Tramites bancarios en línea).

En la investigación **[52]** se presenta la ejecución de una evaluación heurística a un sistema e-Banking donde uno de los puntos a evaluar es la usabilidad, y ésta, al no poder ser medida directamente la clasifica en la categoría de requisito no funcional.

Adicionalmente según la **Norma ISO/IEC 25022:2016 [53]** "La usabilidad se refiere a la capacidad de un software de ser comprendido, aprendido, usado y ser atractivo para el usuario, en condiciones específicas de uso".

2.1.7.2 Seguridad

Ferrer et al. **[55]** Exhiben la seguridad como uno de los puntos fundamentales cuando es necesario afrontar tareas en sistemas informáticos, ya que así se puede garantizar que estas tareas se lleven a cabo de la misma forma a como se dan en el mundo físico. Por ejemplo si se guarda dinero en una caja fuerte de un banco, no se piensa que cualquier persona en el mundo pueda llegar a ésta inmediatamente, sólo los usuarios legítimos. La seguridad, la privacidad, la confidencialidad y la autenticidad son características de vital importancia en la construcción y desarrollo de un sistema de banca en línea, y estas medidas de seguridad evitan que usuarios no autorizados inicien sesión en el sitio web y no sólo eso, también es necesario proteger la información del cliente, que se envía desde su computadora hasta el servidor **[48]**.

Carvallo et al. **[51]** Exponen la siguiente *tabla*, explicando con mayor precisión este concepto.

Seguridad	**Capacidad del producto software para proteger información y datos de manera que las personas o sistemas o autorizados puedan leerlos o modificarlos, al tiempo que no se deniega el acceso a las personas o sistemas autorizados.**		
	Seguridad en la aplicación	Capacidad del producto software para proporcionar mecanismos para prevenir el acceso no-autorizado deliberado o accidental a la funcionalidad del producto.	
		Gestionada por la aplicación	Capacidad del producto software para proporcionar mecanismos para prevenir el acceso no autorizado deliberado o accidental a la funcionalidad del producto.
		Gestionada por terceros	Capacidad del producto software según reportes publicados por terceras organizaciones para proporcionar mecanismos para prevenir el acceso no-autorizado deliberado o accidental a la funcionalidad del producto.
	Seguridad en los datos	Capacidad del producto software para proporcionar mecanismos para prevenir el acceso no-autorizado deliberado o accidental a los datos gestionados.	
		Datos almacenados	Capacidad del producto software para proporcionar mecanismos para prevenir el acceso no-autorizado deliberado o accidental a los datos almacenados
		Datos transmitidos	Capacidad del producto software para proporcionar mecanismos para provenir el acceso no-autorizado deliberado o accidental a los datos transmitidos

Tabla 2. Seguridad en un producto software

2.1.7.3 Accesibilidad

Textualmente la Norma **ISO 9241-171:2008 [56]** señala lo siguiente: “Usabilidad de un producto, servicio, ambiente o instalación por personas con la más amplia gama de capacidades” - “El concepto de accesibilidad se refiere a la gama completa de capacidades de usuario y no se limita a los usuarios quienes son reconocidos formalmente por tener una discapacidad(auditiva, física, cognitiva, etc.)” por otro lado “el concepto orientado a la usabilidad de la accesibilidad tiene como objetivo lograr niveles de eficacia, eficiencia y satisfacción tan alto como sea posible teniendo en cuenta el contexto de uso, prestando especial atención a la gama completa de capacidades dentro de la población de usuarios”. Un software que cuenta con la característica de ser accesible implica que está diseñado

para aumentar la capacidad de uso de un producto para aquellos que sufren alguna discapacidad.

Con la anterior definición evidentemente se habla de que la accesibilidad beneficia a las personas con discapacidad, hoy en día ofrece un enorme beneficio a personas deficientes visuales, pero no debe verse solamente como una serie de requisitos aislados para un colectivo en concreto, también debe considerarse como un mecanismo para mejorar la calidad y usabilidad en general de cualquier aplicativo web **[57].**

2.1.7.4 Operabilidad

En **[57]** este término es definido como la capacidad del componente de software para ser operado y controlado por el usuario (programador del sistema). Una medida de operabilidad debería ser capaz de evaluar si los desarrolladores del sistema pueden operar y controlar el componente fácilmente. Las medidas de operabilidad se pueden clasificar según los principios de diálogo descritos en la norma **ISO / IEC 9241-110:2006 [59]**:

- Idoneidad del componente para la tarea;
- Auto-descriptividad del componente;
- Capacidad de control del componente;
- La conformidad del componente con las expectativas del usuario (requisitos);
- Tolerancia de error del componente;
- Idoneidad del componente para la individualización.

2.1.7.5 Fiabilidad

Carvallo et al. **[51]** manifiestan textualmente lo siguiente, “la capacidad del producto software para mantener un nivel especificado de prestaciones cuando se usa bajo unas ciertas condiciones”. Pham **[60]** menciona que la fiabilidad de un sistema determina el nivel de éxito en su comportamiento para las especificaciones para las que haya sido fijado. Si en un determinado instante dicho comportamiento no va acorde al especificado, se dice que hay una avería o en otras palabras, una manifestación externa de problemas internos que el sistema presenta los cuales son llamados errores. Los algoritmos que presentan dichos errores se denominan fallas. Una pequeña avería que se presenta en un componente o sub-sistema puede causar grandes inconvenientes en el sistema que lo contiene y manifestar problemas en cadena en todo este, tal como se evidencia a continuación.

Avería -> **Fallo** -> **Error** -> **Avería** -> **. . .**

2.1.8 Métodos de evaluación para interfaces de usuario

Actualmente para validar una interfaz se hace uso de diversos métodos de inspección con el fin de evaluar que tan usable resulta ser una aplicación de software. En su mayoría se requiere evaluadores expertos quienes apoyados en un método específico tendrán como objetivo encontrar problemas de usabilidad en un diseño **[61].** Este mismo autor hace una recopilación de los métodos de evaluación existentes y los define de manera formal, algunos de ellos son:

2.1.8.1 Evaluación Heurística

Es uno de los métodos más informales. Se requieren especialistas en usabilidad quienes se encargan de juzgar si cada elemento de la interfaz cumple con principios de usabilidad establecidos.

2.1.8.2 Caminata Cognitiva

Requiere de un procedimiento más detallado que implica simular resolución de problemas, el usuario sigue una secuencia de pasos, los cuales deben contrastar con los que se planeó la interfaz. Se debe verificar si el usuario cumple con el objetivo en cada problema.

2.1.8.3 Inspecciones de Usabilidad

Se combinan la evaluación heurística y una forma simplificada de caminata cognitiva a partir de un procedimiento de seis pasos con funciones estrictamente definidas.

2.1.8.4 Caminatas plurales

Son reuniones en las que los usuarios, desarrolladores y personas del factor humano discuten sobre nuevas ideas, se analiza cada elemento del diálogo de las tareas dadas a los usuarios.

2.1.8.5 Inspección de funciones

Enumera la secuencia de funciones que se utilizan para realizar las tareas típicas, verifica si hay secuencias largas, pasos complejos, pasos que no sería normal que los usuarios prueben, y los pasos que requieren un amplio conocimiento / experiencia con el fin de evaluar un conjunto de características propuesto.

2.2 TRABAJOS RELACIONADOS

Los siguientes trabajos exhiben gran influencia en la realización de esta investigación. Se han resaltado aquellos cuyo aporte permitirá la aproximación y desarrollo de los artefactos resultantes.

2.2.1 Usabilidad y sistemas seguros

Hertzum et al. **[11]** El estudio llevado a cabo por estos autores donde se evalúa a seis sistemas e-Banking daneses, arrojó como resultado las serias debilidades en estos sistemas respecto a la usabilidad. Concretamente se evalúa la usabilidad y la seguridad. Para efectuar la evaluación se seleccionó el servicio de transferencia de dinero ya que se considera el más importante para los usuarios comunes y además todo banco debe proporcionar una manera segura y fácil de usar, las tareas que se consideraron fueron Instalación, inicio de sesión, transferencia y cierre de sesión, con el objetivo de que los usuarios respondiesen a una serie de preguntas, que se basan en algunas definiciones hechas por Whitten & Tygar **[4]** sobre USec, con el fin de verificar el éxito en las tareas, errores de alto riesgo y comodidad del usuario en el uso. Como resultado se habla de los conceptos de automatización y entendimiento, siendo el primero un camino para simplificar las interfaces de usuario y reducir el número de pasos que los usuarios deben seguir, pero que a su vez abre brechas importantes en la seguridad lo cual obstaculiza al usuario la compresión de la misma. A diferencia del estudio propuesto donde se evalúan los sistemas a través de 'caminatas cognitivas' y sin mencionar el proceso inherente de éstas, este trabajo pretende evaluar un estudio de caso a través del método de evaluación heurística.

Mannan et al. **[20]** Cualquier mecanismo de seguridad por ejemplo una contraseña necesita como requerimiento principal que la usabilidad sea tenida en cuenta en sistemas seguros, es por eso que en la mayoría de bancos canadienses se cuestiona sobre los actuales requisitos de seguridad. Según este autor los sistemas de e-Banking son los que más problemas de seguridad y usabilidad presentan, debido a que la mayoría de requerimientos para los usuarios son difíciles de seguir, además, los mensajes relacionados con la seguridad tienden a ser confusos. Entre los puntos de discusión para facilitar la comprensión se describen problemas específicos de seguridad y usabilidad en sistemas e-Banking, encuestas de usuario en la satisfacción de requerimientos de e-Banking, revisión de sistemas de seguridad que impliquen tareas altamente sensibles. La mayoría de usuarios no cuentan con las garantías de seguridad que los bancos prometen, por el contrario, se afirma que estas no son más que un eslogan de marketing que induce a los usuarios a usar el servicio. A diferencia del estudio propuesto, este trabajo involucra, en el estudio de caso, a evaluadores expertos en usabilidad y seguridad que tienen como objetivo desarrollar una evaluación heurística.

2.2.2 HCI y Seguridad

Möckel. **[12]** El desarrollo de métodos de evaluación pertinentes para los sistemas de e-Banking considerando la interacción de los criterios de seguridad y usabilidad es el objetivo principal en este trabajo, considerando las limitantes halladas hasta la fecha según las áreas de HCI, Seguridad y HCISec. El enfoque metodológico propuesto para dar solución a una serie de preguntas planteadas, que hacen énfasis en los aspectos ya mencionados, consiste en llevar a cabo dos investigaciones, una cuantitativa y una cualitativa, teniendo en cuenta algunas pautas como modelo de amenaza de soluciones de seguridad o análisis de contenido de estudios de usabilidad en sistemas e-Banking, además de un estudio de caso para probar el Marco Teórico el cual indica la relación e interacción entre la seguridad,

usabilidad y otros factores que involucra esta última en dichos sistemas. Una muestra de sistemas e-Banking tanto de Alemania y Reino Unido, para este autor, es un escenario ideal donde aplicar el marco propuesto. Por ello se espera tener una recopilación de las amenazas comunes contra e-Banking, una descripción de las soluciones de seguridad E-Banking y modelado de amenazas. A diferencia del estudio propuesto, este trabajo pretende definir un método de evaluación específico sin descartar la aplicación de principios de HCISec mencionados.

2.2.3 HCISec

Nurse et al. **[21]** Recopilan los mayores desarrollos en el campo de la seguridad, usabilidad y HCISec. Las investigaciones principalmente se refieren a las orientaciones y recomendaciones para sistemas de seguridad altamente usable. A través de las mismas, logran consolidar una lista básica inicial de pautas generales y recomendaciones específicas en campos como autenticación, control de acceso, cifrado, firewalls y la interacción segura. Hacen referencia a los métodos empleados para la evaluación de la usabilidad en los sistemas comprometidos como 'caminatas cognitivas' y 'evaluación heurística'. A diferencia del estudio propuesto, este trabajo pretende recopilar, filtrar y seleccionar los mayores desarrollos en el campo del e-Banking, para posteriormente ser evaluados en el estudio de caso seleccionado.

2.2.4 Modelos de evaluación y principios de Seguridad Usable (USec)

Mujinga et al. **[14]** Plantean que los sistemas e-Banking han permitido que los bancos obtengan beneficios competitivos, reducir los costos operativos y mejorar su desempeño, Sin embargo se expone que la privacidad y seguridad de las transacciones bancarias en línea y la confidencialidad de la información personal se encuentran entre las mayores preocupaciones tanto de las instituciones bancarias como para los usuarios de estos servicios, por lo cual a través de modelos de evaluación y principios de USec, definen principios heurísticos generales que aún no han sido evaluados. Las heurísticas expuestas por estos autores fueron sometidas a un proceso de selección o modificación con el fin de que fueran aplicables a los sistemas e-Banking. A diferencia del estudio propuesto, este trabajo implica desglosar dichos principios heurísticos generales con el objetivo de consolidar un conjunto de heurísticas específicas que permita evaluar diversos aspectos en sistemas e-Banking.

S.Furnell. **[33]** Destaca los problemas de configuración de interfaces de seguridad en los usuarios finales. Se cuestiona cómo los diseñadores de aplicaciones pueden mejorar el diseño y la evaluación de interfaces de seguridad. Hacen uso de la red 802.11 comúnmente conocida como Wi-Fi proponiéndola como caso de estudio. Primero, diseñan e implementan una interfaz de configuración que guía a los usuarios a través de una configuración de red segura. La idea principal es que los usuarios tienen una difícil experiencia al traducir sus objetivos de seguridad en las características específicas requeridas. Además, resaltan el desarrollo de una metodología con base en modelos mentales para la medición de la

efectividad en su diseño. Como conclusión, resalta que la interfaz implementada en este trabajo, permite a los usuarios crear configuraciones de redes como si lo hiciera un experto en ésta área. Considerando las ventajas que exponen los autores al emplear modelos mentales, este trabajo pretende aprovechar de manera similar esta herramienta para lograr la identificación de puntos de falla potenciales en el estudio de caso que se llevará a cabo. S.Furnell. **[34]** Resalta la necesidad de implementar soluciones de seguridad que sean usables para cualquier tipo de involucrado. Examina los problemas que pueden ser enfrentados en el momento que se intentan usar las características de seguridad en aplicaciones comunes. Muchos de los problemas examinados caen en manos de la terminología técnica, funcionalidad no clara o confusa, falta de visualización del estado y retroalimentación informativa, son causas que obligan a los usuarios a tomar decisiones desinformadas y a la ausencia de integración entre los elementos de la seguridad software. Ésta investigación toma como muestra un conjunto de aplicaciones populares donde se realizan encuestas y pruebas de usuario que se llevaron a cabo con el objetivo de evaluar los posibles problemas de primera mano. El estudio propuesto, se apoya de métodos de usabilidad para la evaluación de sistemas que implican seguridad computacional, sin embargo, utilizan directrices generales para realizar la evaluación. A diferencia del estudio propuesto, este trabajo empleará heurísticas específicas para la evaluación de los sistemas e-Banking, sin descartar la metodología de evaluación propuesta, la cual es realizada a través de una escala numérica.

2.2.5 Requerimientos e-Banking

Carlo. **[44]** Implementa una solución de un sistema e-Banking el cuál es aplicado al “Banco de Guayaquil”. Destaca la importancia de realizar una transacción bancaria desde cualquier parte del mundo, a cualquier lugar, de manera ágil y segura. Inicialmente, se analizan las tendencias y perspectivas que tienen los bancos por brindar soluciones Web, además contiene un estudio de los posibles usuarios del sistema e-Banking en cuestión. Posteriormente, el estudio contempla la descripción de un análisis puntual de requerimientos para sistemas e-Banking. Finalmente, se detalla el diseño y la implementación del sistema. El estudio propuesto, presenta algunos requerimientos fundamentales que permiten el diseño de sistemas e-Banking, este trabajo pretende emplear los requerimientos presentados aplicando un filtro que permitirá identificar los requerimientos que contrasten con el estudio de caso propuesto. Asimismo, algunos requerimientos serán debidamente evaluados por expertos en seguridad y usabilidad.

2.2.6 Métodos de evaluación para interfaces de usuario

Mtimkulu et al. **[62]** Hacen énfasis en la gran adopción generada por los bancos hacía los sistemas e-Banking, sin embargo, inciden en la no existencia de directrices validadas en las funcionalidades de estos sistemas. Presentan un estudio el cual se encuentra enfocado hacía los clientes entre 18 y 35 años clasificados como “Generación-Y”. Haciendo uso de la literatura rescatan directrices generales que son evaluadas por medio de métodos de evaluación de usabilidad. A manera de resumen, es plasmada la experiencia que se obtuvo usando 3 métodos de evaluación de usabilidad, entrevistas, evaluación heurística y validación de funcionalidad a través de prototipos. A diferencia del estudio propuesto, este trabajo implica desglosar las directrices permitiendo mayor índice de detalle en ellas y

conjuntamente, haciendo uso de un método de evaluación, evaluar con expertos en seguridad y usabilidad las directrices propuestas, generando así, un conjunto preliminar de heurísticas que permitan contribuir en el ámbito.

Capítulo 3

Parámetros asociados al estudio de la USec en sistemas e-Banking

Los artefactos generados en este capítulo, pueden ser evidenciados en el Sprint 3 de la metodología (véase **Anexo L**).

Una vez hecha la revisión sistemática y habiendo recopilado los diversos trabajos relacionados hasta la fecha con el fin de abarcar los conceptos más relevantes en la investigación, en este capítulo es indispensable centrarse en los aspectos importantes del entorno en el que se desarrolla este trabajo, los sistemas e-Banking junto con su contexto de uso, recopilación y filtro de requerimientos básicos para estos sistemas y la recopilación y filtro de sub-heurísticas que evaluará cada uno de los requerimientos que se especifiquen.

3.1. DEFINICIÓN DE CONCEPTOS

Maguire. **[63]** Define el contexto de uso como el entorno particular en el que un producto o sistema desarrollado se puede utilizar; establece una población de usuarios con determinadas características que lo usaran. Además estos usuarios tendrán objetivos y deseos para realizar diferentes tareas. Por otro lado, su uso se puede ver afectado dependiendo de un cierto rango de entornos técnicos, físicos, sociales o de organización. En estos términos, Marete et al. **[78]** define e-Banking como: "un portal de internet, a través del cual los clientes pueden usar diferentes servicios bancarios que parten desde el pago de facturas hasta la realización de importantes inversiones". A excepción de la obtención de fondos en efectivo, el servicio de e-Banking ofrece a sus usuarios cualquier tipo de transacción que puede ser ejecutada con tan solo una pulsación **[78]**. Actualmente los sistemas de e-Banking están siendo usados cada vez con mayor frecuencia. La mayoría de los bancos cuentan con el servicio en línea ya que permite atender a más clientes. El acceso en línea claramente reduce las visitas físicas a los bancos y permite el ahorro de tiempo a sus usuarios además de brindarles costos operacionales menores comparados con transacciones tradicionales **[43]**. El desarrollo de un sistema e-Banking parte de una serie de requerimientos, el diccionario de Oxford[1] define esta palabra como algo que se necesita o se desea, en este caso, las necesidades de un usuario para alcanzar un objetivo o realizar una tarea en un sistema e-Banking. En la ingeniería del software los requerimientos se clasifican en dos grandes partes, tales como los requerimientos funcionales que se ocupan de la funcionalidad del sistema y no funcionales que se ocupan de las limitaciones, la calidad, datos, normas, reglamentos, interfaces, el rendimiento, la fiabilidad, y otros

[1] https://en.oxforddictionaries.com/definition/requirement

requisitos de implementación **[2]** en función del grado de cumplimiento de esos requerimientos se puede evaluar un sistema, con el fin de garantizar su usabilidad, seguridad, accesibilidad, fiabilidad, operabilidad, entre otros. La verificación de los requerimientos se hace a través de sub-heurísticas proceso que se desarrollará a lo largo de este capítulo.

3.2. CONTEXTO DE USO E-BANKING

Según la definición anterior se especifica que un sistema e-Banking debe reflejar al menos las siguientes características.

3.2.1 Clientes o Involucrados

El primer criterio que debe ser tenido en cuenta son los clientes del banco, este banco ofrece servicios de banca online y el cliente tiene acceso a internet y sabe cómo utilizar el internet**[64]**.

3.2.2 Tareas

Los clientes del banco que hagan uso de los servicios online podrán realizar las siguientes tareas

- **Autenticarse / Cerrar sesión [65]**: Haciendo uso de un usuario y una contraseña el cliente puede tener acceso a todas las funciones de la oficina virtual a las que está permitido. El nombre de usuario y la contraseña deben ser correctos para evitar los problemas de bloqueo de cuenta por exceso de intentos.
- **Ver / Modificar Cuenta [65]**: Visualizar transferencias, depósitos, estados de cuenta, ver historiales bancarios y actualizar datos.
- **Realizar transferencias[65]**: Al haberse autenticado un usuario tiene la posibilidad de ejecutar movimientos bancarios en la oficina virtual (Pago de cuentas, solicitud de cheques, bonos, etc).
- **Solicitar ayuda / sección de ayuda[66]**: El usuario requiere de acceso a un método de ayuda convencional ante cualquier duda en la oficina virtual.

3.2.3 Aspectos de calidad [66]

3.2.3.1 Seguridad y Confianza

- **Seguridad:** La sensación de seguridad puede ser transmitida garantizando una mayor fiabilidad durante las transacciones de dinero electrónico (por ejemplo, pagos, transferencias y débitos), así como la presentación de información relevante en este aspecto.
- **Integridad:** Es fomentado de forma intensiva a través de un alto nivel de discreción en el manejo de datos.

3.2.3.2 Servicios Básicos de Calidad

- **Elección:** Aumenta la percepción de control del usuario de los procesos y elementos de la oficina virtual.
- **Condiciones de servicios básicos:** Servicios adquiridos de otros proveedores, condiciones de transacciones de pago, condiciones de valores, condiciones de adquisición de fondos.
- **Pagos y transacciones:** Pago de facturas, visualización de estado de cuenta, compra de acciones, y otros productos financieros.

3.2.3.3 Servicios de Compra Cruzada

- Prestamos en línea.
- Todo en productos de financiación.

3.2.3.4 Valor agregado

- Entretenimiento.

3.2.3.5 Apoyo de Transacción

- **Comodidad en el proceso de transacción**
- **Interactividad:** Fácil realización de transacciones, ayuda / tutoriales directos.
- **Retroalimentación:** Como proporcionar información sobre intereses especiales, realidad en la información y datos personales.
- **Apoyo a las decisiones:** Hoja informativa, atención al cliente, herramientas interactivas.
- **Cuidado del cliente:** Garantizar la percepción de amabilidad, velocidad, conexión inmediata, disponibilidad a través de e-mail hacía el cliente.

3.2.3.6 Responsabilidad / Sensibilidad

- **Disponibilidad y Accesibilidad:** Disponibilidad de servicio (24/7), línea directa, rapidez y precisión de respuesta.
- **Personalización:** Campo de noticias, consejos individuales de inversión, servicios adaptados a los usuarios e información sobre intereses personales.
- **Comunidad:** Posibilidad de salas de chat o grupos de noticias.
- **Gestión de quejas:** Contar con un dispositivo independiente para tramitar alguna queja.

3.2.4 Aspectos técnicos

3.2.4.1 Apoyo, recuperación y disponibilidad **[65][67]**

Se debe contar con mecanismos de recuperación de datos, además la entidad bancaria debe tener mecanismos para la continuidad de la organización.

3.2.4.2 Cifrado de datos [65]

Uso de las últimas técnicas de cifrado de datos, donde se traduzcan los datos de manera ininteligible sin un mecanismo de descifrado.

3.2.4.3 Servicio de prevención de perdida de datos [67]

Garantía de que se usa canales cifrados para la transmisión de información (Protocolo electrónico de cifrado, SSL) y medidas para contrarrestar ataques a los dispositivos de almacenamiento.

3.2.4.4 Configuración de la infraestructura de red [67]

Implementación de servidores de seguridad, antivirus, cortafuegos y detección de intrusos.

3.2.4.5 Protección del cliente y apoyo [67]

Los clientes deben ser informados y orientados sobre los riesgos y beneficios al hace uso de los servicios financieros en línea.

3.3. REQUERIMIENTOS e-BANKING

Una vez realizada la especificación del contexto de uso de los sistemas e-Banking, junto con la revisión de la literatura, se logró recolectar alrededor de 59 requerimientos, tanto funcionales como no funcionales para estos sistemas, y tras una minuciosa revisión y apoyándose en el contexto de uso planteado se lograron identificar y filtrar los requerimientos más relevantes e indispensables, generando una lista de 23 requerimientos que se muestran a continuación en la ***Tabla 3***.

ID_REQ	Requerimiento	Referencia
1	El sistema debe establecer una sesión segura entre la máquina del cliente y el servidor del banco, con cifrado de datos.	**[44], [65], [68]**
2	El sistema debe bloquear a los usuarios que superen el máximo número de intentos con la clave incorrecta.	**[44]**
3	Una vez el usuario ingrese al sistema, se le debe presentar una vista con las diferentes opciones que le permitan usar los servicios.	**[44] ,[69], [68], [65]**
4	La sección de ayuda relevante debe proporcionar explicaciones de las medidas empleadas para garantizar la seguridad.	**[70]**
5	El sistema debe presentar la información más relevante en letra grande y/o resaltada. Además, el lenguaje que se presente en él debe ser sencillo y conversacional.	**[70], [71]**
6	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.)	**[70]**
7	El sistema debe informar al usuario sobre medidas de seguridad y proporcionar unas políticas de seguridad.	**[70]**
8	El usuario debe poder iniciar sesión con un usuario y una contraseña que ha creado anteriormente y se ha guardado en la base de datos.	**[65]**
9	Si el usuario se equivoca al ingresar el usuario o la contraseña, el sistema debe mostrar un mensaje de alerta de Usuario y/o contraseña incorrecta	**[65]**
10	El cliente debe haber iniciado sesión para estar habilitado a hacer transacciones o transferencia de fondos	**[65]**

11	El sistema debe ser explícito con los detalles de la información personal que será retenida, por qué y cómo será usada (e.g. El correo será usado para enviar publicidad).	**[70]**
12	El sistema debe permitir a los usuarios controlar las acciones críticas e información crítica	**[70]**
13	El sistema debe tomar medidas para hacer frente a los riesgos, e inmediatamente informar a los usuarios acerca de estas medidas.	**[70]**
14	Proporcionar autenticación usable (OTP, Tokens, Biométrica, Multi-factor)	**[70]**
15	Las interfaces de usuario deben ser presentadas con una lógica clara y ser entendibles.	**[70]**
16	El sistema en el proceso de autenticación debe hacer uso de criptografía fuerte o protocolos y funciones relacionadas, tales como, TripleDES, AES, RC4, IDEA, RSA, ECC, OATH y RFC 2104 HMAC.	**[72]**
17	El sistema debe incluir las respectivas instrucciones para una adecuada interacción del usuario, en el sitio web u otros medios de comunicación.	**[72]**
18	Después que un usuario se haya autenticado y obtenido acceso. El sistema debe asegurarse que el usuario pueda invocar únicamente la funciones que se le permiten (e.g. ver, escribir, ejecutar, modificar, crear y / o borrar datos).	**[72]**
19	El sistema debe implementar técnicas de prevención de errores.	**[72]**
20	Claridad en los enlaces y en las etiquetas de los botones donde se sugiere la acción requerida.	**[71]**
21	Las interfaces de usuario deben presentar y destacar la información relevante en el contexto y en el momento correcto.	**[71]**
22	El sistema debe implementar canales de soporte al cliente mejores y más rápidos (e.g. El chat en línea para resolver los obstáculos bancarios).	**[71]**
23	El sistema debe entregar retroalimentación (e.g. Su dinero será transferido en 24 horas).	**[71]**

Tabla 3. Requerimientos generales de un sistema e-Banking

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 esta investigación 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.

3.4. PRINCIPIOS DE USec PARA SISTEMAS e-BANKING

En el reciente estudio Realpe et al. **[73]** logran recolectar un total de 152 sub-heurísticas que evalúan los aspectos de seguridad y usabilidad conjuntamente en procesos de autenticación en sistemas e-Commerce. Analizando la propuesta se logra observar que muchas de las sub-heurísticas planteadas son aplicables a la evaluación de sistemas e-Banking, ya que estos constituyen una rama de los sistemas e-Commerce, por lo tanto, basándose en el contexto de uso, los requerimientos anteriores, y apoyados en los conceptos y definiciones de la literatura (véase **Capítulo 2** y **Apartado 3.2**), se realizó un filtro que permitió generar una clasificación específica de 46 sub-heurísticas. Las sub-heurísticas se agrupan teniendo en cuenta algunas facetas (usabilidad, seguridad, operabilidad, accesibilidad y fiabilidad) (véase **Capítulo 2**) y atributos de la **ISO/IEC 25010:2011 [74] [77]**, las cuales se basan en USec y autenticación de usuario. Se presentan a continuación en la siguiente *tabla*.

Atributo o Faceta	Sub-Heurística

USABILIDAD	U1- Después de que el usuario complete una acción de seguridad, ¿la realimentación indica que el siguiente grupo de acciones puede ser iniciado?
	U2- ¿La información de seguridad presentada en pantalla es relevante?
	U3- ¿Los íconos de seguridad son identificables y diferenciables?
	U4- ¿Las etiquetas de seguridad son sencillas, fáciles de entender y representativas?
	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?
	U6- ¿El sistema está diseñado de manera que los botones con nombres similares, no desarrollen acciones de seguridad opuesto?
	U7-¿Las sentencias de alerta son simples, cortas y comprensibles?
	U8- ¿Las preguntas de seguridad son expresadas en un lenguaje claro y sencillo?
	U9- ¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?
	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?
	U11- ¿La información relacionada con la seguridad es presentada de una manera coherente y estandarizada?
	U12- En un proceso de autenticación por conocimiento, ¿el sistema permite minimizar la carga de memoria para los usuarios?
	U13- ¿Los mensajes de error relacionados con la seguridad informan al usuario de la gravedad del error?
	U14- ¿El sistema facilita la posibilidad al usuario de solucionar problemas a posibles errores?
	U15- ¿Los mensajes de error relacionados con la seguridad son significativos y sensibles al problema?
	U16- ¿Los mensajes de error relacionados con la seguridad indican la acción que el usuario debe tomar para corregir el error?
	U17- ¿Los mensajes de error relacionados con la seguridad son adecuados al lenguaje del usuario?
	U18- ¿Los mensajes de error relacionados con la seguridad indican al usuario dónde obtener ayuda?
	U19- ¿La información necesaria para tomar una buena decisión de seguridad, es adecuada y está disponible antes de que se adopte la medida?
	U20- ¿Los iconos de seguridad poseen etiqueta?
	U21- ¿Hay una función de ayuda de seguridad visible?
	U22- ¿La información proporcionada por la ayuda es relevante?
	U23- ¿El sistema provee soporte técnico en línea para solucionar problemas de seguridad?
	U24- ¿El sistema notifica a los usuarios si está interactuando con fuentes no confiables e interpone algún tipo de bloqueo que evita males mayores?
	U25- ¿El sistema muestra logos de seguridad?
	U26- ¿El sistema tiene certificados de seguridad otorgados por entidades externas reconocidas?
SEGURIDAD	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?
	S2- Si el sistema utiliza "cookies informáticos", ¿la información sobre la privacidad del sistema describe con precisión el uso de estas cookies?
	S3- ¿El proceso de autenticación hace cumplir un límite de intentos de acceso no válidos consecutivos por un usuario?

	S4- ¿Se presenta al usuario mensajes de notificación concernientes a la seguridad y privacidad antes de acceder al sistema?
	S5- ¿La información de privacidad del sistema garantiza al usuario el derecho a optar por compartir información no crítica con terceros?
	S6-6 ¿El sistema notifica y da posibles soluciones al usuario sobre vulnerabilidades asociados a incidentes de seguridad detectados?
	S7- ¿El sistema describe cada opción de privacidad en detalle?
	S8- ¿El sistema hace cumplir el nivel de complejidad de la contraseña, con los requisitos mínimos exigidos?
	S9- ¿El sistema posee políticas de privacidad para comercio o contenido del usuario?
	S10- Si es necesario realizar autenticación por multi-factor, ¿el uso de PIN es implementada, dándole libertad al usuario para decidir el número de dígitos?
	S11- El sistema soporta y hace uso por defecto del protocolo HTTPS?
OPERABILIDAD	O1- ¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?
ACCESIBILIDAD	A1- ¿El sistema permite usar passwords gráficos para usuarios con dificultades de lectura?
	A2-¿El sistema evita el uso de claves aleatorias para la etapa de registro o autenticación?
	A3- En un proceso de autenticación, ¿el sistema evita esfuerzo adicional?
	A4- ¿El sistema provee a los usuarios otras alternativas para autenticarse?
	A5- ¿El método de autenticación sirve a usuarios nuevos y experimentados?
FIABILIDAD	F1- ¿La interfaz ayuda al usuario a tener una experiencia segura y satisfactoria con el sistema?
	F2- ¿Está claramente establecido el propósito de utilizar la información personal del usuario?
	F3- Si el proceso de inicio de sesión falla, ¿el sistema evita indicarle al usuario qué parte del proceso es incorrecto?

Tabla 4. Conjunto de sub-heurísticas asociadas a una faceta o atributo

3.5. REQUERIMIENTOS Y SUB-HEURÍSTICAS

Una vez recopilados los requerimientos y el conjunto de sub-heurísticas, 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 (véase **Tabla 6**).

Realpe et al. **[74]** También consideran una escala de importancia presentada en la ***Tabla 5*** para cada sub-heurística, la cual será tenida en cuenta en los capítulos posteriores de este documento.

Grado de Importancia Sub-Heurísticas	
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.

Tabla 5. Grado de importancia para sub-heurísticas

REQ_ID	Requerimiento	Importancia	Sub-Heurística asociada	Criterio de Relación
1	El sistema debe establecer una sesión segura entre la máquina del cliente y el servidor del banco, con cifrado de datos.	**S**	S11- El sistema soporta y hace uso por defecto del protocolo HTTPS?	La relación se establece a partir del apartado 3.2.4.2 y 3.2.4.3 del contexto de uso, por medio del cual se establece como aspecto técnico de seguridad entre la máquina y el cliente el cifrado de datos y el uso de protocolos de seguridad. Por otro lado en **[67]** menciona que el usuario espera un cambio de http:// a https:// cuando se espera autenticación y cifrado de datos.
		SSS	O1- ¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?	La relación se establece a partir de los apartados 3.2.2, 3.2.4.2, 3.2.4.4 y 3.2.4.5 del contexto de uso referentes a las normas básicas de seguridad.
2	El sistema debe bloquear a los usuarios que superen el máximo número de intentos con la clave incorrecta.	**S**	S3- ¿El proceso de autenticación hace cumplir un límite de intentos de acceso no válidos consecutivos por un usuario?	Aunque la relación de este requerimiento y la sub-heurística es explicito se justifica también con el apartado 3.2.2 del contexto de uso.
3	Una vez el usuario ingrese al sistema, se le debe presentar una vista con las diferentes opciones que le permitan usar los servicios.	**SSS**	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	La relación se establece mediante los apartados 3.2.2 y 3.2.3.2 del contexto de uso, donde se establece la posibilidad de elección y la interactividad que ofrece el sistema.
4	La sección de ayuda relevante debe proporcionar explicaciones de las medidas empleadas para garantizar la seguridad.	**S**	U2- ¿La información de seguridad presentada en pantalla es relevante?	Se establece la relación a partir del apartado 3.2.3.1 del contexto de uso sobre información de seguridad.
		SS	U11- ¿La información relacionada con la seguridad es presentada de una manera coherente y estandarizada?	Se establece la relación a partir de los apartados 3.2.3.1 y 3.2.4.5 del contexto de uso sobre información de seguridad protección al cliente y apoyo.
		S	U19- ¿La información necesaria para tomar una buena decisión de seguridad, es adecuada y está disponible antes de que se adopte la medida?	Se establece la relación a partir del apartado 3.2.3.5 del contexto de uso sobre apoyo en toma de decisiones.
		S	U22- ¿La información proporcionada por la ayuda es relevante?	Se establece la relación a partir de la sección 3.2.2, 3.2.3.5 y 3.2.3.6 sobre apoyo, ayuda y responsabilidad hacia el usuario.
5	El sistema debe presentar la información más relevante en letra grande y/o resaltada. Además, el lenguaje que se presente	**S**	U9- ¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?	En **[70]** se menciona que para mejorar la usabilidad es indispensable hace uso del leguaje conversacional y evitar términos técnicos. Por otro lado **[75]** el sistema debe manejar un

	en él debe ser sencillo y conversacional.			lenguaje natural y familiar con un orden lógico.
6	Las medidas de seguridad implementadas por el sistema **no** deben ser excesivas ni molestas (contraseñas demasiado largas, varios códigos de acceso, preguntas de seguridad demasido complejas, etc.)	**S**	U8- ¿Las preguntas de seguridad son expresadas en un lenguaje claro y sencillo?	En **[70]** se menciona que para mejorar la usabilidad es indispensable hacer uso del leguaje conversacional y evitar términos técnicos.
		S	U9- ¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?	En **[70]** se menciona que para mejorar la usabilidad es indispensable hacer uso del leguaje conversacional y evitar términos técnicos.
		S	S8- ¿El sistema hace cumplir el nivel de complejidad de la contraseña, con los requisitos mínimos exigidos?	En **[68]** se plantea que a nivel de seguridad una entidad bancaria debe proponer una autenticación fuerte sin contraseñas complejas
		SSS	S10- Si es necesario realizar autenticación por multi-factor, ¿el uso de PIN es implementada, dándole libertad al usuario para decidir el número de dígitos?	En **[68]** se menciona que la autenticación multi-factor se ha convertido en un estándar con el fin de proporcionar autenticación fuerte sin ser necesidad de ser compleja.
		SS	A3- En un proceso de autenticación, ¿el sistema evita esfuerzo adicional?	En **[70]** se menciona el evitar el esfuerzo adicional en los procesos de autenticación como mecanismo para mejorar la usabilidad para los usuarios.
7	El sistema debe informar al usuario sobre medidas de seguridad y proporcionar unas políticas de seguridad.	**SSS**	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?	Aunque la relación es explicita, se justifica a través del apartado 3.2.4.5 de contexto de uso sobre protección del cliente y apoyo.
		S	S9- ¿El sistema posee políticas de privacidad para comercio o contenido del usuario?	Aunque la relación es explicita, se justifica a través del apartado 3.2.4.5 de contexto de uso sobre protección del cliente y apoyo.
8	El usuario debe poder iniciar sesión con un usuario y una contraseña que ha creado anteriormente y se ha guardado en la base de datos.	**SS**	A2-¿El sistema evita el uso de claves aleatorias para la etapa de registro o autenticación?	Se establece la relación a partir del apartado 3.2.2 del contexto de uso sobre autenticación.
9	Si el usuario se equivoca al ingresar el usuario o la contraseña, el sistema debe mostrar un mensaje de alerta de Usuario y/o contraseña incorrecta	**S**	U7-¿Las sentencias de alerta son simples, cortas y comprensibles?	En **[70]** se menciona que para mejorar la usabilidad es indispensable hace uso del leguaje conversacional y evitar términos técnicos.
		S	U15- ¿Los mensajes de error relacionados con la seguridad son significativos y sensibles al problema?	En **[75]** esta sub-heurística es usada en el reconocimiento, diagnóstico y recuperación de errores, lo cual se relaciona con este requerimiento.
		S	U16- ¿Los mensajes de error relacionados con la seguridad indican la acción que el usuario debe tomar para corregir el error?	En **[75]** menciona que los mensajes de error deben ser expresados en un lenguaje sencillo, entendible, no con códigos que el usuario no va a entender.

		SS	U17- ¿Los mensajes de error relacionados con la seguridad son adecuados al lenguaje del usuario?	En **[70]** se menciona que para mejorar la usabilidad es indispensable hace uso del leguaje conversacional y evitar términos técnicos.
		S	U18- ¿Los mensajes de error relacionados con la seguridad indican al usuario dónde obtener ayuda?	Se relacionan a partir del apartado 3.2.2 del contexto de uso sobre autenticación y solicitud de ayuda.
		SSS	O2- En un proceso de autenticación, ¿este tiene palabras adecuadas para desarrollar una acción en particular?	En **[70]** se menciona que para mejorar la usabilidad es indispensable hace uso del leguaje conversacional y evitar términos técnicos.
		SS	F3- Si el proceso de inicio de sesión falla, ¿el sistema evita indicarle al usuario qué parte del proceso es incorrecto?	Se establece la relación según el apartado 3.2.2 del contexto de uso sobre autenticación.
10	El cliente debe haber iniciado sesión para estar habilitado a hacer transacciones o transferencia de fondos	**S**	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?	Aunque la relación es explicita se justifica a partir del apartado 3.2.2 sobre autenticación.
11	El sistema debe ser explícito con los detalles de la información personal que será retenida, por qué y cómo será usada (e.g. El correo será usado para enviar publicidad).	**SSS**	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?	Se relacionan a partir del apartado 3.2.3.1 y 3.2.4.5 de contexto de uso, en lo referente a integridad, riesgos y beneficios.
		S	S2- Si el sistema utiliza "cookies informáticos", ¿la información sobre la privacidad del sistema describe con precisión el uso de estas cookies?	Se relacionan a partir del apartado 3.2.3.1 y 3.2.4.5 de contexto de uso, en lo referente a integridad, riesgos y beneficios.
		SS	S4- ¿Se presenta al usuario mensajes de notificación concernientes a la seguridad y privacidad antes de acceder al sistema?	Se relación por medio del apartado 3.2.4.5 del contexto de uso, sobre riesgos y beneficios del uso de sistemas e-Banking.
		S	S5- ¿La información de privacidad del sistema garantiza al usuario el derecho a optar por compartir información no crítica con terceros?	Se relacionan por medio del apartado 3.2.3.1 y 3.2.4.5 de contexto de uso, en lo referente a integridad, riesgos y beneficios.
		SS	S7- ¿El sistema describe cada opción de privacidad en detalle?	Se relacionan por medio del apartado 3.2.3.1 y 3.2.4.5 de contexto de uso, en lo referente a integridad, riesgos y beneficios.
		S	F2- ¿Está claramente establecido el propósito de utilizar la información personal del usuario?	Se relacionan por medio del apartado 3.2.3.1 y 3.2.4.5 de contexto de uso, en lo referente a integridad, riesgos y beneficios.
12	El sistema debe permitir a los usuarios controlar las acciones críticas e información crítica	**S**	S7- ¿La información de privacidad del sistema garantiza al usuario el derecho a optar por compartir información no crítica con terceros?	Se relacionan por medio del apartado 3.2.3.2 del contexto de uso en lo referente a la capacidad de elección del usuario.

13	El sistema debe tomar medidas para hacer frente a los riesgos, e inmediatamente informar a los usuarios acerca de estas medidas.	**S**	U24- ¿El sistema notifica a los usuarios si está interactuando con fuentes no confiables e interpone algún tipo de bloqueo que evita males mayores?	Se relacionan por medio de los apartados 3.2.4.2, 3.2.4.3, 3.2.4.4 del contexto de uso en lo referente a medidas de seguridad
		S	S6- ¿El sistema notifica y da posibles soluciones al usuario sobre vulnerabilidades asociados a incidentes de seguridad detectados?	Se relacionan por medio del apartado 3.2.4.4 del contexto de uso sobre medidas de seguridad del sistema.
14	Proporcionar autenticación usable (OTP, Tokens, Biométrica, Multi-factor)	**SS**	U12- En un proceso de autenticación por conocimiento, ¿el sistema permite minimizar la carga de memoria para los usuarios?	En **[70]** se menciona el evitar el esfuerzo adicional en los procesos de autenticación como mecanismo para mejorar la usabilidad para los usuarios.
		S	A1- ¿El sistema permite usar passwords gráficos para usuarios con dificultades de lectura?	En **[68]** se menciona que la autenticación multi-factor se ha convertido en un estándar con el fin de proporcionar autenticación fuerte sin ser necesidad de ser compleja.
		SS	A3- En un proceso de autenticación, ¿el sistema evita esfuerzo adicional?	En **[70]** se menciona el evitar el esfuerzo adicional en los procesos de autenticación como mecanismo para mejorar la usabilidad para los usuarios.
		SS	A4- ¿El sistema provee a los usuarios otras alternativas para autenticarse?	En **[68]** se menciona que la autenticación multi-factor se ha convertido en un estándar con el fin de proporcionar autenticación fuerte sin ser necesidad de ser compleja.
		SS	A5- ¿El método de autenticación sirve a usuarios nuevos y experimentados?	Aunque la relación es explicita se relacionan con base en **[70]** que menciona que se puede proporcionar usabilidad en procesos de autenticación sin necesidad de esfuerzo adicional
15	Las interfaces de usuario deben ser presentadas con una lógica clara y ser entendibles.	**SS**	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	Aunque la relación es explicita se justifica por medio del apartado 3.2.3.5 del contexto de uso sobre interactividad.
		SS	F1-¿La interfaz ayuda al usuario a tener una experiencia segura y satisfactoria con el sistema?	Aunque la relación es explicita se justifica por medio del apartado 3.2.3.5 del contexto de uso sobre interactividad.
16	El sistema en el proceso de autenticación debe hacer uso de criptografia fuerte o protocolos y funciones relacionadas, tales como, TripleDES, AES, RC4, IDEA, RSA, ECC, OATH y RFC 2104 HMAC.	**S**	U25- ¿El sistema muestra logos de seguridad?	Se establece la relación por medio de los apartados 3.2.3.1, 3.2.4.3 y 3.2.4.4 del contexto de uso sobre percepción, certificados y protocolos de seguridad.
		S	U26-¿El sistema tiene certificados de seguridad otorgados por entidades externas reconocidas?	Se establece la relación por medio de los apartados 3.2.4.3 y 3.2.4.4 del contexto de uso sobre certificados, protocolos y medidas de seguridad.
		SSS	O1-¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?	Se establece la relación según el apartado 3.2.2 del contexto de uso sobre autenticación.

17	El sistema debe incluir las respectivas instrucciones para una adecuada interacción del usuario, en el sitio web u otros medios de comunicación.	**S**	U21- ¿Hay una función de ayuda de seguridad visible?	Se establece la relación por medio de los apartados 3.2.2 y 3.2.3.5 del contexto de uso sobre sección de ayuda y cuidado del cliente
18	Después que un usuario se haya autenticado y obtenido acceso. El sistema debe asegurarse que el usuario pueda invocar únicamente la funciones que se le permiten (e.g. ver, escribir, ejecutar, modificar, crear y / o borrar datos).	**S**	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?	Se establece la relación por medio del apartado 3.2.2 del contexto de uso sobre autenticación y vista y modificación de cuenta.
19	El sistema debe implementar técnicas de prevención de errores.	**SS**	U13- ¿Los mensajes de error relacionados con la seguridad informan al usuario de la gravedad del error?	En **[75]** esta sub-heurística está directamente relacionada con el diagnostico, prevención y recuperación de errores.
		SS	U14- ¿El sistema facilita la posibilidad al usuario de solucionar problemas a posibles errores?	En **[75]** menciona que la prevención de errores es incluso mejor que un buen mensaje de error en un diseño cuidadoso que previene que el error ocurra en primer lugar.
		S	U15- ¿Los mensajes de error relacionados con la seguridad son significativos y sensibles al problema?	En **[75]** esta sub-heurística está directamente relacionada con el diagnostico, prevención y recuperación de errores.
		S	U16- ¿Los mensajes de error relacionados con la seguridad indican la acción que el usuario debe tomar para corregir el error?	En **[75]** menciona que los mensajes de error deben ser expresados en un lenguaje sencillo, entendible, no con códigos que el usuario no va a entender.
20	Claridad en los enlaces y en las etiquetas de los botones donde se sugiere la acción requerida.	**SS**	U3- ¿Los íconos de seguridad son identificables y diferenciables?	En **[67]** menciona que el usuario espera un cambio de http:// a https:// y la aparición de una llave de bloqueo cuando se espera autenticación y cifrado de datos.
		S	U4- ¿Las etiquetas de seguridad son sencillas, fáciles de entender y representativas?	Se relacionan por medio de **[71]** donde menciona que las etiquetas deben usar nombres que los usuarios entiendan y que se relación a la acción que ejecutan.
		S	U6- ¿El sistema está diseñado de manera que los botones con nombres similares, no desarrollen acciones de seguridad opuestas?	En **[75]** se considera importante que etiquetas coincidan con su acción, en lo que a estética y diseño minimalista hace referencia.
		S	U20- ¿Los iconos de seguridad poseen etiqueta?	En **[75]** en cuanto a visibilidad del estado del sistema, consistencia y estándares considera la claridad y la familiaridad de los íconos.

21	Las interfaces de usuario deben presentar y destacar la información relevante en el contexto y en el momento correcto.	**SS**	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	Se relacionan por medio de lo dicho en **[75]** donde expresa que el sistema debe mantener a los usuarios informados sobre lo que está pasando, a través de la retroalimentación adecuada en un tiempo razonable
22	El sistema debe implementar canales de soporte al cliente, mejores y más rápidos (e.g. El chat en línea para resolver los obstáculos bancarios).	**SS**	U23- ¿El sistema provee soporte técnico en línea para solucionar problemas de seguridad?	Se relacionan por medio de los apartados 3.2.2 y 3.2.3.5 en lo referente a ayuda y soporte en línea.
23	El sistema debe entregar retroalimentación (e.g. su dinero será transferido en 24 horas).	**SS**	U1- Después de que el usuario complete una acción de seguridad, ¿la realimentación indica que el siguiente grupo de acciones puede ser iniciado?	En **[75]** se menciona que el sistema debe mantener a los usuarios informados sobre lo que está pasando, a través de la retroalimentación adecuada en un tiempo razonable.

Tabla 6. Requerimiento, sub-heurísticas, grado de importancia y justificación

3.6 SOPORTE DE EXPERTOS Y PARTICIPACIÓN DE USUARIOS

La participación por parte de expertos en evaluaciones heurísticas o por criterios corresponde a evaluadores especializados en los principios establecidos en la áreas de estudio en las que se trabaje **[76]**. Esta sección constituye en gran medida la participación de expertos en las áreas de HCI y Seguridad de la Información, la finalidad, que bajo su criterio brinden el soporte necesario para la construcción de una herramienta (*modelo matemático*) que permita la medición de los atributos de seguridad y usabilidad en conjunto**.**

En la sección anterior se encuentran relacionadas las sub-heurísticas con cada requerimiento, sin embargo, antes de llevar a cabo la evaluación fue necesario preparar los aspectos que se deben considerar en el proceso. El primero de ellos, determinar una escala 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 auditores deberán diligenciar según el estudio de caso seleccionado.

3.6.1 Escala Adjetiva y Numérica

Contando con el apoyo de 10 expertos en Ciencias de la Computación nacionales e internacionales y a través de una encuesta (véase **Anexo A**), se logra determinar el rango de escala numérica correspondiente a un adjetivo calificativo para el cumplimiento las sub-heurísticas (véase **Tabla 7**).

Escala de Evaluación				
Muy pobre	**Pobre**	**Moderado**	**Bueno**	**Excelente**
[0,20)	[20,40)	[40,60)	[60,80)	[80,100]
Explicación - Escala de Evaluación				

Muy pobre:	El requerimiento presenta fallas severas y requiere atención inmediata de seguridad o usabilidad, según sea el caso, con respecto al principio asociado
Pobre:	El requerimiento presenta fallas severas de seguridad o usabilidad, según sea el caso, con respecto al principio asociado
Moderado:	El requerimiento presenta determinadas fallas de seguridad o usabilidad, según sea el caso, con respecto al principio asociado
Bueno:	El requerimiento presenta pocas fallas de seguridad o usabilidad, según sea el caso, con respecto al principio asociado
Excelente:	El requerimiento se encuentra en óptimas condiciones de seguridad o usabilidad, según sea el caso, con respecto al principio asociado

Tabla 7. Escala de calificación

Los 5 adjetivos que se presentan se toman con base en la literatura; la consideración de los rangos de la escala ($\mathbf{0}\ a\ \mathbf{100}$) únicamente tiene como finalidad facilitar al auditor el manejo de datos enteros, para no implicar el uso de calificaciones con datos decimales. El objetivo final, es generar un soporte cualitativo que permita al auditor seleccionar un valor cuantitativo para realizar la calificación.

3.6.2 Porcentaje de influencia de los atributos Seguridad y Usabilidad

Se evidencia que en la mayoría de requerimientos hay una mayor influencia de un atributo con respecto al otro, por tal motivo fue necesario contar con un nuevo grupo de expertos que bajo su criterio y mediante un formulario (véase **Anexo B**) definiera el porcentaje de influencia que implicaba cada uno de los atributos seguridad y usabilidad según el requerimiento. El número total de expertos que participaron en la encuesta fue seis (6), obteniéndose los resultados de la ***Tabla 8***.

	EXPERTO 1		EXPERTO 2		EXPERTO 3		EXPERTO 4		EXPERTO 5		EXPERTO 6		PROMEDIO	
REQ_ID	% USABILIDAD	% SEGURIDAD	% USABILIDAD	% SEGURIDAD	% USABILIDAD	% SEGURIDAD	% USABILIDAD	% SEGURIDAD	% USABILIDAD	% SEGURIDAD	% USABILIDAD	% SEGURIDAD	% USABILIDAD	% SEGURIDAD
1	50	50	30	70	0	100	10	90	0	100	20	80	18,33	81,67
2	10	90	25	75	0	100	40	60	0	100	30	70	17,50	82,50
3	90	10	10	90	100	0	90	10	100	0	70	30	76,67	23,33
4	100	0	60	40	50	50	80	20	80	20	70	30	73,33	26,67
5	90	10	80	20	100	0	75	25	80	20	90	10	85,83	14,17
6	90	10	25	75	30	70	50	50	80	20	70	30	57,50	42,50
7	50	50	20	80	0	100	40	60	20	80	20	80	25,00	75,00
8	50	50	20	80	0	100	30	70	50	50	90	10	40,00	60,00
9	80	20	40	60	50	50	50	50	50	50	90	10	60,00	40,00
10	0	100	0	100	0	100	70	30	30	70	30	70	21,67	78,33
11	0	100	70	30	0	100	50	50	30	70	40	60	31,67	68,33
12	0	100	20	80	50	50	40	60	30	70	80	20	36,67	63,33
13	100	0	20	80	0	100	70	30	30	70	80	20	50,00	50,00

14	90	10	30	70	0	100	50	50	70	30	60	40	50,00	50,00
15	100	0	90	10	100	0	90	10	80	20	90	10	91,67	8,33
16	0	100	0	100	0	100	0	100	20	80	0	100	3,33	96,67
17	100	0	85	15	100	0	90	10	80	20	90	10	90,83	9,17
18	0	100	25	75	0	100	80	20	80	20	70	30	42,50	57,50
19	90	10	30	70	50	50	80	20	80	20	80	20	68,33	31,67
20	100	0	100	0	100	0	80	20	80	20	90	10	91,67	8,33
21	100	0	85	15	100	0	90	10	80	20	90	10	90,83	9,17
22	100	0	75	25	60	40	50	50	80	20	90	10	75,83	24,17
23	100	0	80	20	50	50	60	40	20	80	90	10	66,67	33,33

Tabla 8. Porcentaje de influencia de los atributos seguridad y usabilidad

Como es posible observar, cada experto asignó un porcentaje a los atributos de seguridad y usabilidad para cada uno de los requerimientos, finalmente, se promedia cada una de las consideraciones obteniéndose los porcentajes de la última columna de la *tabla*, los cuales serán utilizados en el cálculo de la USec del sistema e-Banking del estudio de caso.

Nota: Los porcentajes correspondientes a la columna del promedio fueron redondeados a dos cifras significativas. Los valores más precisos pueden ser encontrados en el anexo correspondiente al ajuste realizado por los expertos (véase **Anexo B**).

3.6.3 Grado de importancia de las sub-heurísticas

En la sección 3.5, se destacó una escala de importancia que compone a cada una de las sub-heurísticas, esta fue considerada para permitir mayor precisión en el resultado del cálculo de la USec. Considerando los tres niveles de importancia de las sub-heurísticas, se procede a asignar un valor numérico de $1\,a\,3$ a cada uno de ellos, donde el valor 3 es asignado a las sub-heurísticas de grado S, 2 a las sub-heurísticas de grado SS y el valor 1 a las sub-heurísticas de grado SSS (véase **Tabla 9**), generando esta analogía, será posible distribuir un valor porcentual a cada sub-heurística. Algunos ejemplos son ilustrados en la ***Tabla 10***.

Grado de Importancia Sub-Heurísticas	
Cualitativo	**Numérico**
S	3
SS	2
SSS	1

Tabla 9. Grado de importancia numérico de las sub-heurísticas

A continuación en la columna 'Importancia Numérica' se aprecia el cálculo del porcentaje de importancia asignado a cada sub-heurística.

REQ _ID	Requerimiento	Sub-Heurística asociada	Importancia Cualitativa	Importancia Numérica
1	El sistema debe establecer una sesión segura entre la máquina del cliente y	S11- El sistema soporta y hace uso por defecto del protocolo HTTPS?	**S**	$\frac{100\%}{(S+SSS)} * S = \frac{100\%}{(3+1)} * 3 = 75\%$

	el servidor del banco, con cifrado de datos.	O1- ¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?	**SSS**	$\frac{100\%}{(S+SSS)} * SSS = \frac{100\%}{(3+1)} * 1 = 25\%$
4	La sección de ayuda relevante debe proporcionar explicaciones de las medidas empleadas para garantizar la seguridad.	U2- ¿La información de seguridad presentada en pantalla es relevante?	**S**	$\frac{100\%}{(S+SS+S+S)} * S = \frac{100\%}{(3+2+3+3)} * 3 = 27.27\%$
		U11- ¿La información relacionada con la seguridad es presentada de una manera coherente y estandarizada?	**SS**	$\frac{100\%}{(S+SS+S+S)} * SS = \frac{100\%}{(3+2+3+3)} * 2 = 18.18\%$
		U19- ¿La información necesaria para tomar una buena decisión de seguridad, es adecuada y está disponible antes de que se adopte la medida?	**S**	$\frac{100\%}{(S+SS+S+S)} * S = \frac{100\%}{(3+2+3+3)} * 3 = 27.27\%$
		U22- ¿La información proporcionada por la ayuda es relevante?	**S**	$\frac{100\%}{(S+SS+S+S)} * S = \frac{100\%}{(3+2+3+3)} * 3 = 27.27\%$

Tabla 10. Ejemplo del proceso de cálculo del grado de importancia de las sub-heurísticas

Nota: Para la realización del cálculo de la importancia, es necesario destacar que las sub-heurísticas del estudio **[73]** contaban con un valor adjetivo de importancia, el cual por sus condiciones cualitativas, no permite ser integrado al modelo matemático que se desarrollará en el siguiente capítulo (véase **Capítulo 4**), por esta razón, surge la necesidad de asociar un valor cuantitativo a la denominación adjetiva ya existente, por lo tanto, el valor cuantitativo ajustado corresponde a la aplicación de un cálculo basado en regla de tres simple, sin embargo, los valores cuantitativos de importancia obtenidos en esta sección no han sido sometidos a criterio de expertos.

Capítulo 4

Modelo Matemático para la medición de la USec en sistemas e-Banking

Los artefactos generados en este capítulo, pueden ser evidenciados en el Sprint 4 de la metodología (véase **Anexo L**).

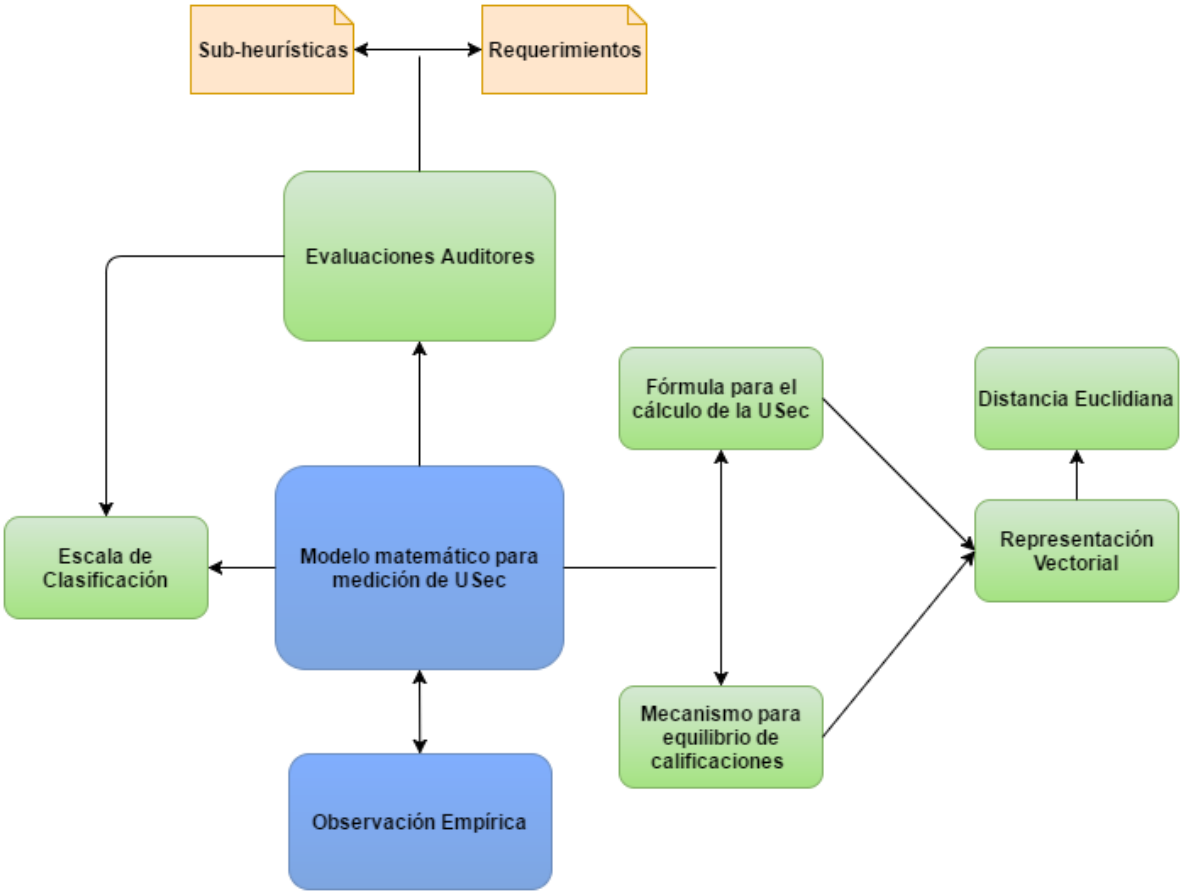

Figura 2. Esquema Conceptual del Modelo Matemático (Creación Propia)

En el esquema anterior (véase **Figura 2**), se presentan los componentes del modelo matemático generado en este trabajo de investigación, el cual surge a través del método de observación empírica **[92]** con el cual se logra establecer los diversos atributos que intervienen para lograr el cálculo del valor de Seguridad Usable (USec). 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 formulas 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.

Partiendo de la literatura, y siendo conscientes de los debates que a diario son generados debido a las recomendaciones de diseño de sistemas seguros y usables. Esta investigación ha considerado indagar de manera profunda la relación establecida entre los aspectos de seguridad y usabilidad con el fin de generar un acercamiento que permita afianzar estos dos atributos en el diseño de los sistemas.

4.1. RELACIÓN ENTRE LOS ATRIBUTOS SEGURIDAD Y USABILIDAD

Inicialmente, la seguridad y la usabilidad eran tratadas como dos dominios completamente separados y sin relación en los sistemas computacionales **[79]** esto debido a la dificultad que se presentaba para la creación de contenido altamente seguro y usable, que hoy en día, a pesar del exigente trabajo presentado en ambas áreas, escasamente se ha logrado contrarrestar.

A favor de la investigación, no muchos estudios han sido conducidos en orden de entender la relación entre seguridad y usabilidad, sin embargo, se pueden encontrar algunos dirigidos al área de los sistemas computacionales. Los cuáles serán mencionados en la siguiente *tabla*.

Trabajo	Descripción	Entorno
"Designing a Trade-off between Usability and Security: A Metrics Based-Model"[80]	Modelo de diseño basado en un método de inspección de usabilidad en máquinas de autómatas.	Máquinas de autómatas
"Relationship between security and usability – authentication case study"[81]	Método matemático empleado para vulnerar contraseñas el cual es analizado teniendo en cuenta el atributo 'Usabilidad'.	Métodos de autenticación
"Tradeoffs between Usability and Security"[79]	Recopilación de principios de diseño para interfaces seguras.	Diseño de interfaces
"Understanding Visual Perceptions of Usability and Security of Android's Graphical Password Pattern"[82]	Estudio de los patrones de contraseñas empleados en dispositivos Android.	Dispositivos Android

"Development of a Model for Security and Usability"[83]	Desarrollo de modelo para la seguridad y usabilidad en productos software	Aplicativos software

Tabla 11. Trabajos que contemplan la relación entre seguridad y usabilidad

4.1.1 Tipo de correlación entre los atributos Seguridad y Usabilidad

Zapata **[83]** despliega una lista de los diferentes tipos de relaciones que se presentan entre seguridad y usabilidad, recopilando el trabajo determinado por diferentes autores en sus estudios, las relaciones son explicadas a continuación.

- **Relación Inversa:** El aumento o disminución de la usabilidad tiene el efecto inverso o recíproco sobre la seguridad y viceversa.
- **Relación Directa:** El aumento o disminución de la usabilidad tiene el mismo efecto en la seguridad y viceversa.
- **Sin Relación:** Los dos factores no están relacionados, por lo que aumentar o disminuir la usabilidad no tiene efecto sobre la seguridad y viceversa.
- **Relación Inversa Unidireccional:** Existe una relación inversa entre los dos factores, siempre que no se cambie el orden.
- **Relación Relativa o Dependiente:** La relación depende de alguna característica y podría ser directa en algunos casos e inversa en otros.

Cabe destacar que en su investigación, resalta que incrementar o disminuir uno de los dos atributos no necesariamente afectará de manera proporcional al otro.

4.1.2 Taxonomía – Tipo Correlación

En este apartado, se presenta una taxonomía donde se sitúan autores que han contribuido con sus investigaciones en el entendimiento de los tipos de relación entre seguridad y usabilidad.

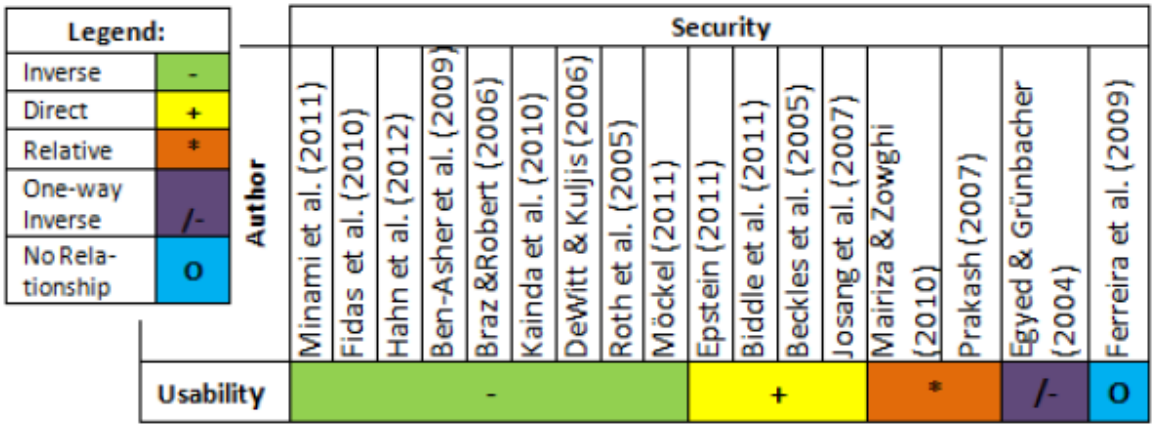

Figura 3. Taxonomía de correlación. (Tomada de [83])

4.2. MODELOS DE MEDICIÓN PARA LA USec

A través de esta investigación, se ha corroborado la existencia de la correlación implícita entre los atributos de seguridad y usabilidad inmersos diariamente en el contexto de sistemas computacionales y aplicaciones. Luego de identificada esta gran brecha, el interés de esta investigación se ha centrado en la búsqueda de herramientas que permitan la medición de la USec (véase **Apartado 2.1.4**).

En el detallado proceso de búsqueda de literatura, se identificaron pocas propuestas que permitan la medición de la USec, además, estas presentan un grado alto de complejidad, por esta razón, surge la motivación de enfrentar el reto del conocimiento con el propósito de generar un modelo que permita evaluar los atributos de seguridad y usabilidad, y, del mismo modo, reducir la subjetividad que se exhibe en la fase evaluativa.

4.2.1 Taxonomía – Aproximaciones

A continuación, se identifican algunas investigaciones que han centrado sus estudios en la evaluación de la USec, no obstante, es relevante mencionar que cuatro (4) de las cinco (5) investigaciones están sujetas únicamente a escalas de evaluación sometidas a criterio de expertos, además, en las cuatro (4) investigaciones mencionadas anteriormente los atributos son asumidos de forma conjunta desde el proceso inicial, lo cual prioriza la subjetividad, característica apreciable durante la fase evaluativa.

Trabajo	Descripción	Entorno
"Usable Security using GOMS: A Study to Evaluate and Compare the Usability of User Accounts on e-Government Websites"[84]	Método para evaluar la usabilidad en el diseño de interfaces de usuario en e-Government.	e-Government
"A Framework to Evaluate Usable Security in Online Social Networking"[85]	Framework para evaluar la USec a través de heurísticas de seguridad y usabilidad en redes sociales.	Redes Sociales
"Heuristics for Evaluating IT Security Management Tools"[86]	Propuesta de heurísticas para la evaluación y búsqueda de problemas de usabilidad en herramientas para la gestión de la seguridad de la tecnología de la información.	Herramientas para la Gestión de la Seguridad de la Tecnología de la Información.
"Using Human Computer Interaction Principles to Promote Usable Security"[30]	Propuesta de directrices de HCISec evaluadas usando productos software reconocidos.	Aplicativos Software
"A Conceptual Framework for Evaluating Usable Security in Authentication Mechanisms – Usability Perspectives"[87]	Propuesta matemática para la evaluación de la USec en mecanismos de autenticación.	Mecanismos de autenticación

Tabla 12. Trabajos centrados en la USec

Mihajlov et al. **[87]** centran su investigación en la medición de la USec en mecanismos de autenticación. Esta propuesta ha sido relevante ya que considera los atributos de forma independiente y, a través de una consideración matemática logra relacionar la seguridad y la usabilidad, permitiendo reducir la característica de subjetividad.

4.3. CONCEPTOS ASOCIADOS

El desarrollo de este capítulo, se ha de centrar arduamente en dar cumplimiento al objetivo específico número dos (2) (véase **Apartado 1.4**), que, como se ha expuesto en las anteriores secciones, abre una gran brecha hacía la construcción del conocimiento en el área de HCISec.

Inicialmente, es necesario destacar que el proceso llevado a cabo durante esta investigación ha dependido de la participación de diferentes áreas afines a la seguridad y usabilidad, por esta razón, todos los argumentos que en este apartado se expongan centran sus bases en la literatura, del mismo modo, han sido revisados por expertos en seguridad, usabilidad y matemáticas.

Acto seguido, es importante aclarar que el modelo ha sido validado con los requerimientos y principios expuestos en el ***Capítulo 3***.

Para el desarrollo de la propuesta matemática se toma como punto de inicio la premisa expuesta sobre el tipo de relación entre seguridad y usabilidad (véase **Apartado 4.1**), por lo tanto, toda condición de seguridad o usabilidad que sea implementada en sistemas que consideren estos atributos puede ser evaluada teniendo en cuenta la ***correlación estadística*** entre variables.

4.3.1 Variables Independientes

Los atributos de seguridad y usabilidad son expuestos de forma autónoma (véase **Anexo C**), lo que permitirá al auditor evaluar los atributos independientemente, reduciendo la subjetividad de la evaluación al evitar la mezcla de conceptos que en algunos casos suelen ser interpretados de manera inadecuada. Por consiguiente, surge la analogía de variables independientes, que apoyará el uso de la correlación estadística, base de este modelo.

4.3.2 Representación Vectorial

La inclusión de sub-heurísticas asociadas a requerimientos (véase **Capitulo 3**) permite identificar una representación vectorial inherente. Cada requerimiento cuenta con un número determinado de sub-heurísticas, el número de sub-heurísticas asociadas permitirá conocer la dimensión del vector (véase **Figura 4**). Es de gran importancia destacar que las sub-heurísticas asociadas a un requerimiento no son truncadas por limites, es decir, el modelo permite asociar desde una (1) sub-heurística hasta $\boldsymbol{n}$ sub-heurísticas a un requerimiento, asimismo, la dimensión en el plano o en el espacio estará estrictamente ligada al número de sub-heurísticas asociadas a dicho requerimiento.

Justificación Matemática

Sea $\boldsymbol{A} = \{s, u\}$ el conjunto de los atributos asociados a un sistema e-Banking, donde s es Seguridad y u Usabilidad, sea $\boldsymbol{R} = \{r1, r2, r3, r4, \dots, rn\}$ el conjunto de los requerimientos

asociados a un sistema e-Banking, sea H_r el número de sub-heurísticas asociadas al requerimiento $\boldsymbol{r_i}$ y $\mathbb{R}^{H_r}$ la representación dimensional en el plano o en el espacio tal que,

- (i) Si $H_r = x$, entonces, la representación dimensional en el plano o en el espacio es $\mathbb{R}^{\boldsymbol{x}}$ para el requerimiento $\boldsymbol{r_i}$.

Por lo tanto, la representación vectorial del sistema en cuestión estará estrictamente ligada a $\boldsymbol{x}$ y al atributo evaluado $(\boldsymbol{s} \vee \boldsymbol{u}) \epsilon \boldsymbol{A}$, y será representada de la siguiente manera,

$\boldsymbol{v_s} = (a1, a2, a3, \ldots, ax) \vee \boldsymbol{v_u} = (a1, a2, a3, \ldots, ax)$, donde $\boldsymbol{v} \epsilon \mathbb{R}^{\boldsymbol{x}}$, $ai \epsilon R^+$ y los componentes del vector $\boldsymbol{a_i}$ constituyen el valor de evaluación proporcionado por el auditor para cada sub-heurística del requerimiento $\boldsymbol{r_i}$.

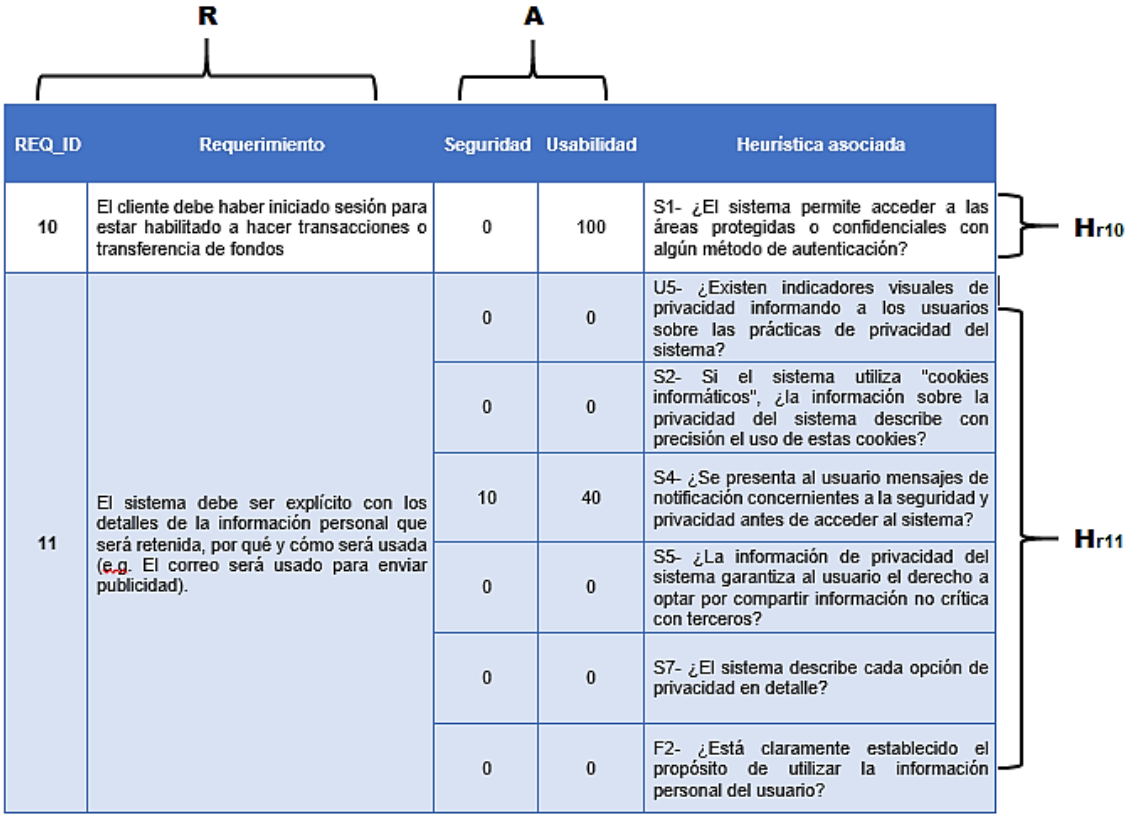

Figura 4. Distribución gráfica – Representación Vectorial

Por ejemplo, se probará la *justificación matemática* teniendo en cuenta la representación inmediatamente anterior (véase **Figura 4**), con respecto a la evaluación del atributo seguridad (véase **Apartado 4.3.1**) determinada para el requerimiento número 11.

$$s : atributo\ seguridad$$

$$r11 : requerimiento\ número\ 11$$

$$H_{r11} = 6 : número\ de\ sub - heurísticas\ asociadas\ a\ r11$$

$$\mathbb{R}^6 : Dimensión\ espacial$$

Finalmente, la representación vectorial de la seguridad correspondiente al ejemplo, estará constituida de la siguiente manera,

$\boldsymbol{v_s} = (a1, a2, a3, a4, a5, a6)$, donde $\boldsymbol{v_s} \epsilon \mathbb{R}^{\mathbf{6}}$

4.3.3 Distancia Euclidiana y Producto Punto

Logrando la analogía vectorial (véase **Apartado 4.3.2**) es adecuado tener en cuenta las operaciones que se pueden realizar sobre vectores para lograr un acercamiento hacía la medición de la USec, por lo tanto, al considerar el vector seguridad, independiente del vector usabilidad (véase **Apartado 4.3.1**), es posible hallar la relación de los mismos haciendo uso de la distancia euclidiana o del producto escalar entre vectores, no obstante, se debe reconocer que existen diferentes artefactos matemáticos que permiten la medición de la correlación entre vectores, pero la literatura ha permitido abalanzarse por el método de la distancia euclidiana evidenciado y empleado en plataformas referentes a la USec expuesto en **[87]**, que, complementado junto con la operación del producto escalar entre vectores, integran una gran herramienta que ha permitido solucionar problemas de diferente índole en áreas subyacentes de la tecnología y sistemas computacionales **[88] [89] [90] [91]**.

El uso de los métodos empleados ha sido continuamente expuesto a criterio y revisión de un doctor en matemáticas, que ha acompañado la construcción del modelo propuesto desde la etapa inicial (véase **Anexo D**).

Justificación matemática

Premisa #1

Los componentes de los vectores seguridad y usabilidad $\boldsymbol{C_s} = \{a_s1, a_s2, a_s3, \dots, a_sn\}$ y $\boldsymbol{C_u} = \{a_u1, a_u2, a_u3, \dots, a_un\}$, representan análogamente la condición de puntos en el plano o en el espacio, dependiendo del número de sus componentes.

Sea $\boldsymbol{R} = \{r1, r2, r3, r4, \dots, rn\}$ el conjunto de los requerimientos asociados a un sistema e-Banking, sea $\boldsymbol{v_s}$ y $\boldsymbol{v_u}$ los vectores asociados a un requerimiento de un sistema e-Banking que involucra a $\boldsymbol{r_i}$ y $\boldsymbol{C_s} = \{a_s1, a_s2, a_s3, \dots, a_sn\}$, $\boldsymbol{C_u} = \{a_u1, a_u2, a_u3, \dots, a_un\}$, los componentes de los vectores $\boldsymbol{v_s}$ y $\boldsymbol{v_u}$ respectivamente, por lo tanto,

Haciendo uso de la premisa # 1,

$\boldsymbol{C_s} = \{a_s1, a_s2, a_s3, \dots, a_sn\}, \equiv \boldsymbol{P_s} = (a_s1, a_s2, a_s3, \dots, a_sn)$, donde el punto $\boldsymbol{P_s} \epsilon \mathbb{R}^n$ y $n \epsilon \mathbb{Z}^+$

$\boldsymbol{C_u} = \{a_u1, a_u2, a_u3, \dots, a_un\} \equiv \boldsymbol{P}_u = (a_u1, a_u2, a_u3, \dots, a_un)$, donde el punto $\boldsymbol{P}_u \in \mathbb{R}^n$ y $n \in \mathbb{Z}^+$

Posteriormente, al obtener la representación de puntos en el plano o en el espacio, se puede recurrir a la fórmula de la distancia euclidiana, definida por la siguiente ecuación,

$$d_E(\boldsymbol{P_s}, \boldsymbol{P_u}) = \sqrt{(a_s1 - a_u1) + (a_s2 - a_u2) + \cdots + (a_sn - a_un)}$$

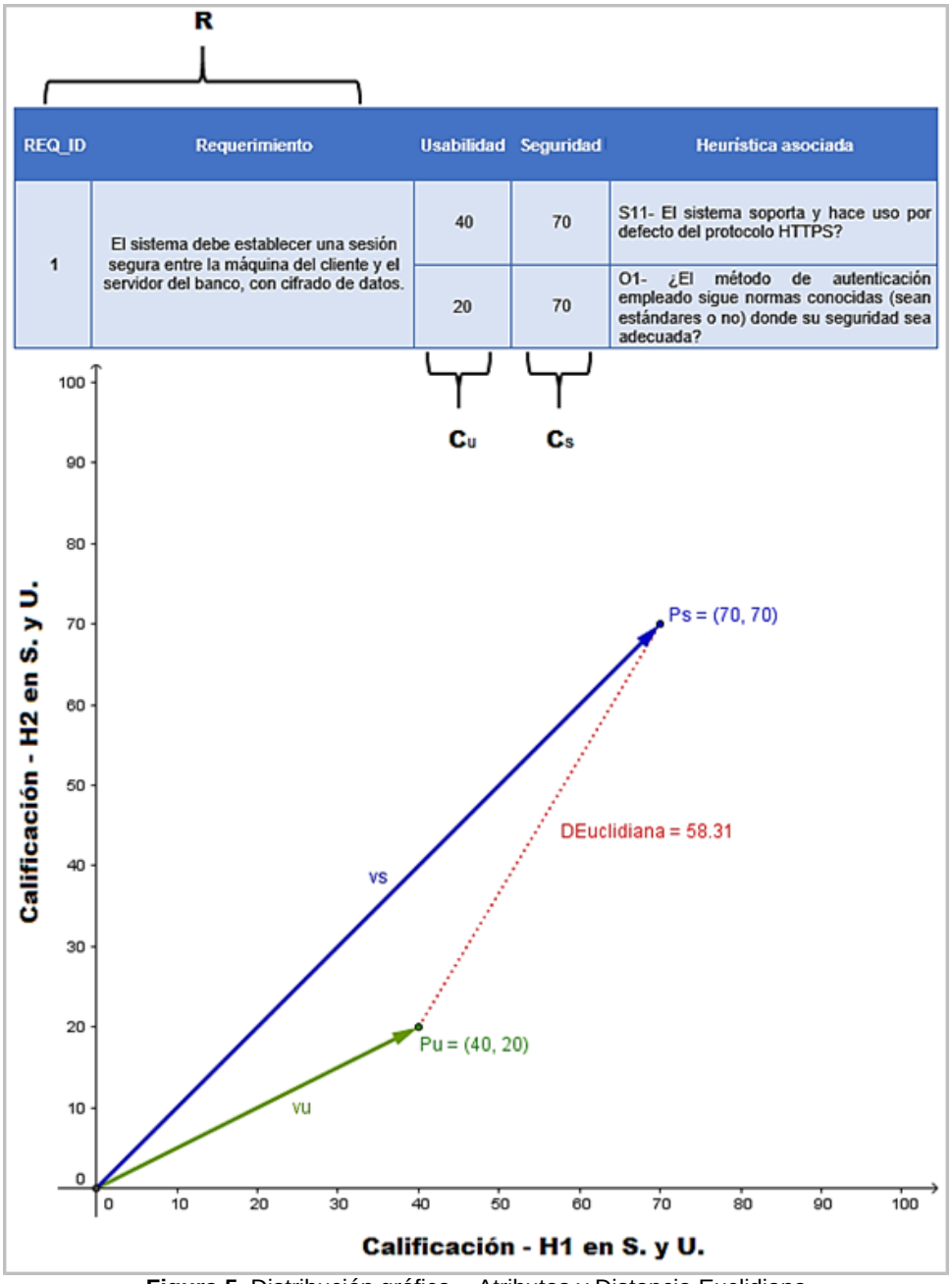

Figura 5. Distribución gráfica – Atributos y Distancia Euclidiana

Se probará la *justificación matemática* teniendo en cuenta la representación inmediatamente anterior (véase **Figura 5**), con respecto a los vectores $\boldsymbol{v_s} = (70, 70)$, $\boldsymbol{v_u} = (40, 20)$, que generan dos puntos en el plano con coordenadas $\boldsymbol{P_s} = (70, 70)$ y $\boldsymbol{P_u} = (40, 20)$.

$$d_E(\boldsymbol{P_s}, \boldsymbol{P_u}) = \sqrt{(a_s1 - a_u1)^2 + (a_s2 - a_u2)^2} = \sqrt{(70 - 40)^2 + (70 - 20)^2}$$

$$d_E(\boldsymbol{P_s}, \boldsymbol{P_u}) = 58.3095189$$

4.4. FORMULA PARA EL CÁLCULO DE LA USec

Luego de considerar los conceptos matemáticos asociados anteriormente (véase **Apartado 4.3**), y con base en la literatura, se identificó que los requerimientos de e-Banking que asocian seguridad y usabilidad, en muchas ocasiones se inclinaban con mayor elocuencia hacía uno de los dos atributos, es decir, para algunos requerimientos la seguridad primaba sobre la usabilidad, lo que implica substancialmente una disminución por el favoritismo hacía la usabilidad y viceversa (véase **Anexo B**), este hecho se encuentra fundamentado específicamente en las características de los requerimientos, pues no es posible desconocer la naturaleza del contexto de los mismos, y de ser obviada, el resultado de la USec podrá ser indebido. Esta característica inherente de los requerimientos fue tenida en cuenta para la realización de los ajustes del modelo (véase **Apartado 3.6.2**).

Un ejemplo ilustrativo del caso anterior, centra la atención en un requerimiento que implique el inicio de sesión a una plataforma que maneje información sensible, como lo son datos personales y dinero. Generalmente, estas plataformas son muy atractivas para los delincuentes informáticos por los tipos de datos y las grandes cifras que fluyen a diario. Suponga que usted es un usuario de esta plataforma, todos sus datos personales e información de contacto se encuentran en ella, además, opera frecuentemente con dinero. Se pone a consideración del lector la siguiente pregunta, ¿Qué tipo de contraseña prefiere, una con valores alfanuméricos y caracteres especiales o una cuya intención sea fácil de recordar, y que por ende no considera caracteres especiales y se encuentra ajustada a una longitud predeterminada de no más de 8 valores alfanuméricos?

Del mismo modo, el modelo propuesto considera el factor correspondiente al grado de importancia de cada sub-heurística (véase **Apartado 3.6.3**). Lo que permitió fortalecer la sinergia con la literatura.

Teniendo en cuenta la condición de variables independientes (véase **Apartado 4.3.1**) se definió un rango de valores numéricos ($\mathbf{0}\ a\ \mathbf{100}$) con el cual los atributos de seguridad y usabilidad pudieran ser calificados por los auditores evitando confusiones de cualquier tipo (véase **Anexo C**), asimismo, la elección del rango definido únicamente se encuentra ligada al soporte y comodidad de la etapa evaluativa que realizará el auditor, por esta razón, el intervalo puede ser modificado sin afectar el modelo.

Se determinó que a través del empleo de la fórmula de la distancia euclidiana (véase **Apartado 4.3.3**), se presentaba una ambigüedad (véase **Figura 6**) que debía ser

despejada, ya que, el resultado podía ser el mismo para distintos tipos de evaluación e implicaría inconsistencias en el cálculo de la USec.

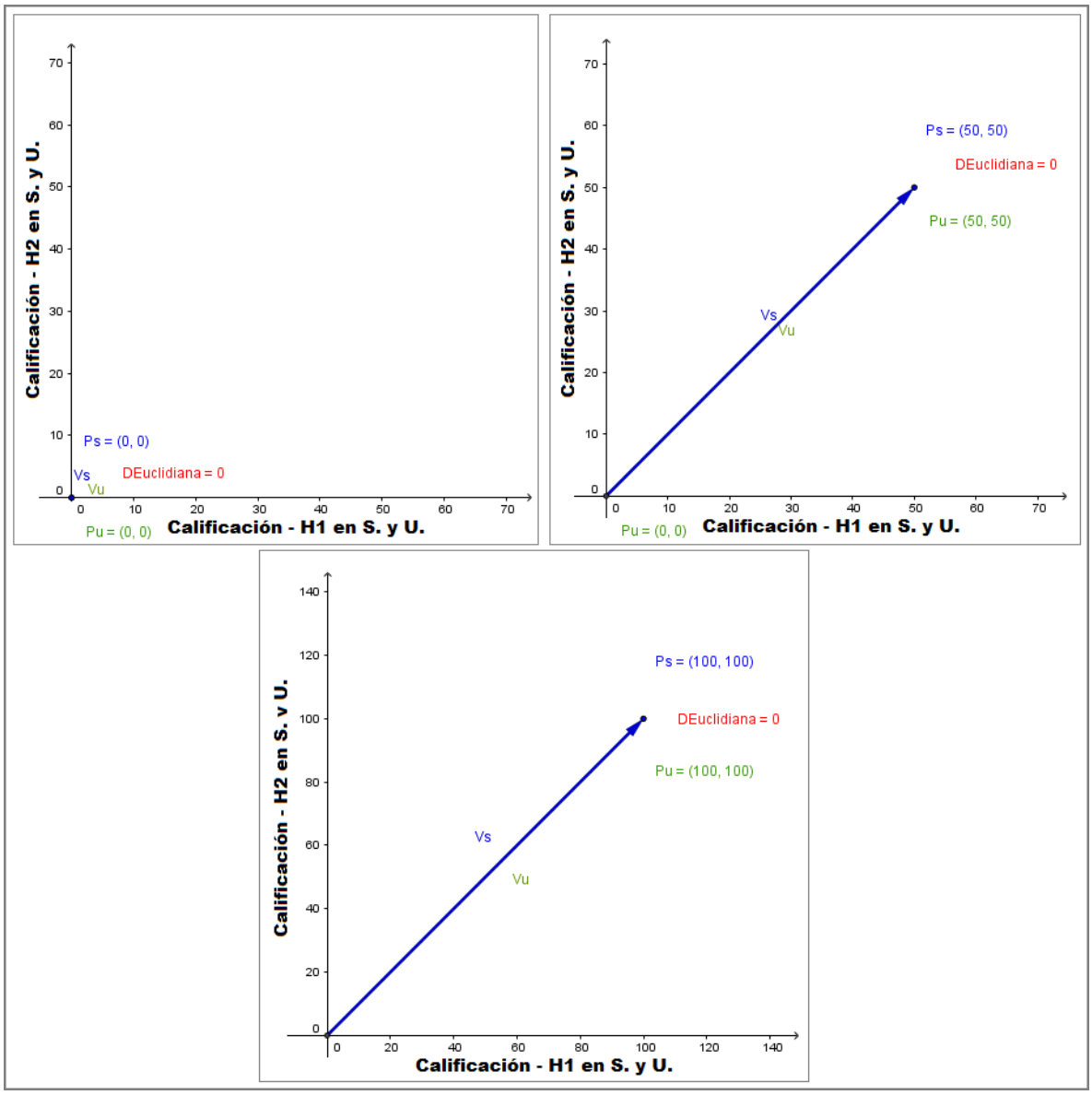

Figura 6. Ambigüedad presentada de acuerdo a calificaciones

Como es posible evidenciar en la figura inmediatamente anterior, el resultado de la distancia euclidiana para los tres casos expuestos resulta siendo el mismo, por lo que fue estrictamente necesario añadir un *factor* que permitiera la distinción de los mismos sin afectar el resultado de la USec (véase **Figura 7**), por consiguiente, la operación que permite el cálculo de la USec queda sujeta a los valores calificados por el auditor (véase **Anexo C**).

Nota: El ejemplo presentado en la figura anterior (véase **Figura 6**), puede presentarse para distintos valores, por lo tanto, los casos expuestos en la figura no son los únicos para ser considerados.

Un ejemplo ilustrativo de la aclaración anterior, podrá ser visualizado en la siguiente figura,

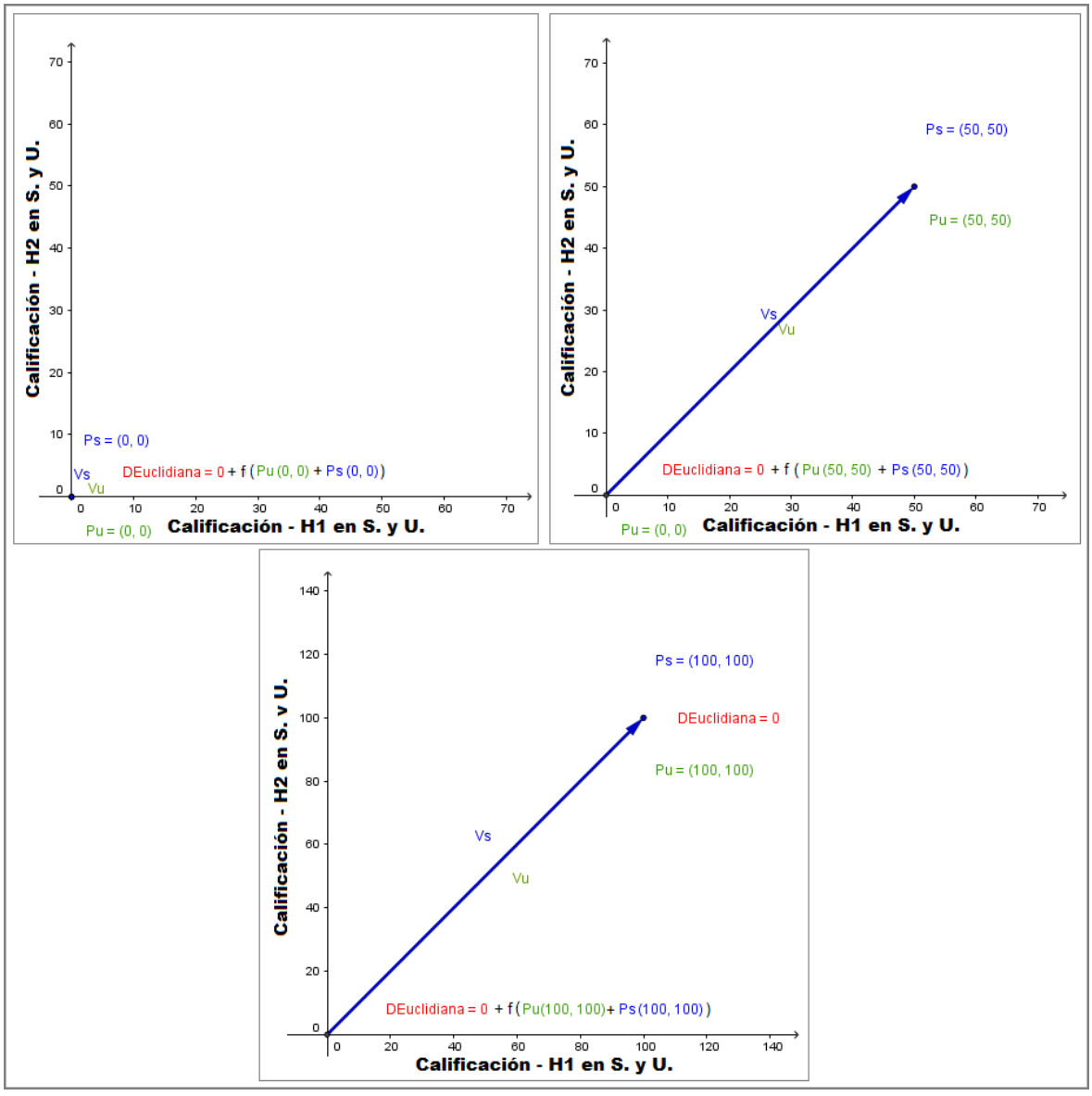

Figura 7. Anulación de ambigüedad

4.4.1 ¿Seguridad o Usabilidad?

Teniendo en cuenta el esquema de evaluación planteado, es fundamental tener en cuenta la composición del requerimiento de acuerdo a sus atributos (véase **Apartado 3.6.2**), en

estos casos el valor de la distancia euclidiana se verá afectada, ya que los valores del atributo que prime en el requerimiento determinarán con mayor influencia en el resultado del cálculo. Un ejemplo ilustrativo tomado de la herramienta de ajuste de atributos a cargo de expertos (véase **Anexo B**) se revela a continuación.

REQ_ID	Requerimiento	% Usabilidad	% Seguridad
16	El sistema en el proceso de autenticación debe hacer uso de criptografía fuerte o protocolos y funciones relacionadas, tales como, TripleDES, AES, RC4, IDEA, RSA, ECC, OATH y RFC 2104 HMAC.	3,33	96,67

Tabla 13. Ejemplo - Requerimiento de mayor influencia.

Con el ejemplo inmediatamente anterior (véase **Tabla 13**), se pone a consideración del lector la siguiente pregunta, ¿El valor de la USec debería verse afectado drásticamente si se obtiene una baja calificación en el atributo usabilidad?

Con el fin de dar solución a este inconveniente, se recurre a definir un mecanismo que permita equilibrar las calificaciones, teniendo en cuenta el porcentaje definido por los expertos para los atributos de seguridad y usabilidad de cada uno de los requerimientos (véase **Anexo B**), que permita contrastar adecuadamente los porcentajes definidos, con la incidencia de cada atributo sobre el requerimiento. Para ello, fue necesario recurrir a uno de los entes geométricos fundamentales denominado recta.

4.4.2 Mecanismo para el equilibrio de calificaciones

A través del método de observación empírica **[92]** fijado en el comportamiento de los vectores seguridad y usabilidad, bajo la influencia del porcentaje definido por los expertos (véase **Anexo B)**, es posible afirmar que, la distancia euclidiana no evidencia dichos porcentajes, por esta razón, se emplea un mecanismo para contrarrestar dicha característica, el cual se fundamenta en la ecuación general de la recta **[93]** y cumple con la condición de acercar o alejar un atributo del otro según la calificación otorgada por el auditor. El mecanismo se encuentra estrictamente sujeto a los porcentajes definidos por los expertos (véase **Anexo B)** y a las calificaciones realizadas por los auditores.

Es importante resaltar que el mecanismo definido tomará la característica de una *recta parametrizada que pasa por el vector resta (distancia euclidiana)* en el plano (ver **Apartado 4.5.1**), lo que implica que pueda ser exhibido como una fórmula matemática, que ha sido construida a través del método de observación empírica anteriormente mencionado, con el soporte y acompañamiento de un doctor en matemáticas, quien ha estado presente en la construcción del modelo propuesto desde la etapa inicial del proceso (véase **Anexo D**).

La explicación de la formula, está sujeta al comportamiento de los atributos, por lo tanto, los siguientes ejemplos (véase **Figura 8**) serán citados con el fin de justificar la experiencia del uso del método de observación empírica.

REQ_ID	Requerimiento	Usabilidad 18.33%	Seguridad 81.67%	Heurística asociada
1	El sistema debe establecer una sesión segura entre la máquina del cliente y el servidor del banco, con cifrado de datos.	0	100	S11- El sistema soporta y hace uso por defecto del protocolo HTTPS?
		20	100	O1- ¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?

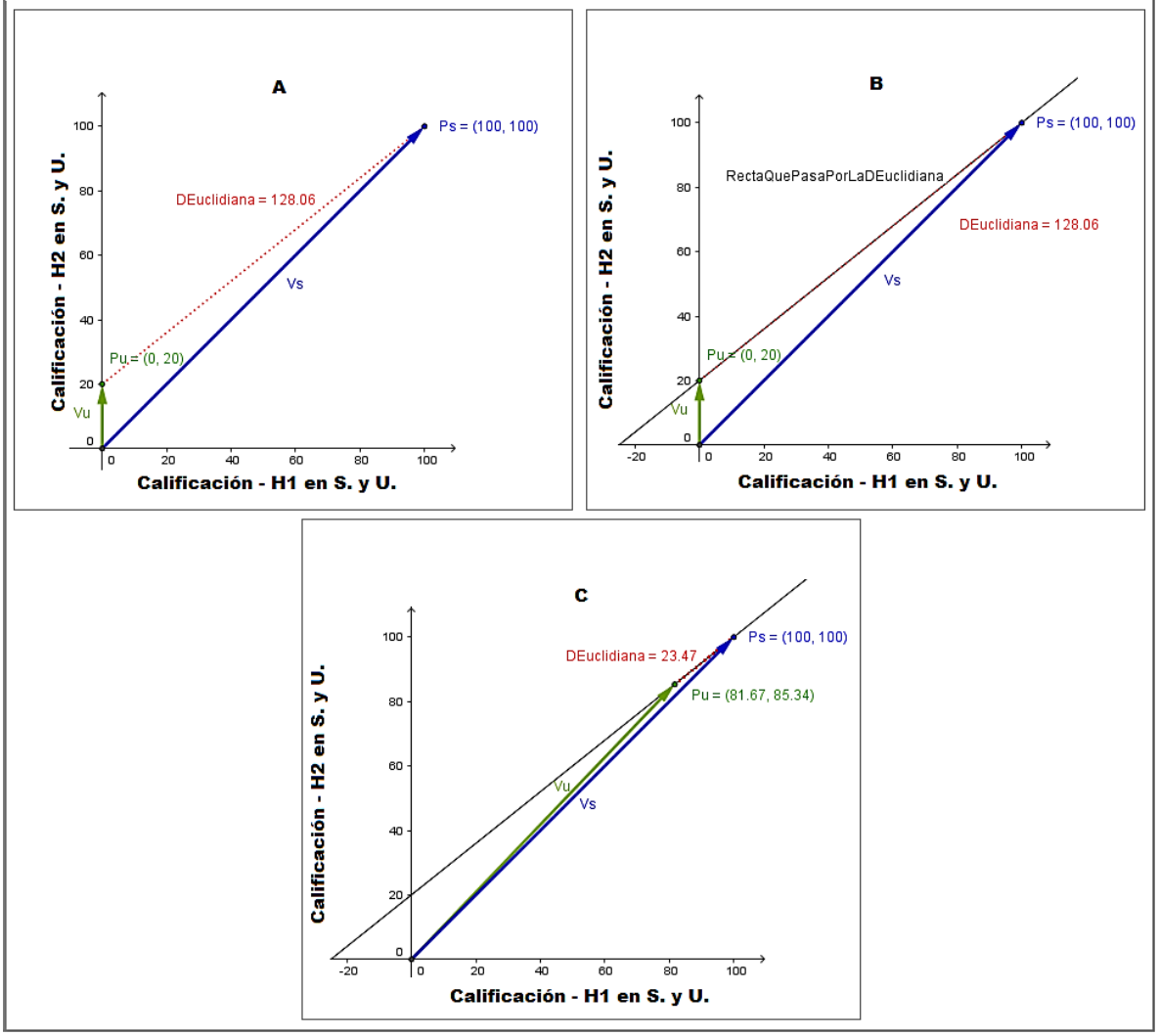

Figura 8. Comportamiento de los vectores aplicando el mecanismo para el equilibrio de calificaciones

En **A** se encuentra representada gráficamente el valor de la *distancia euclidiana* con respecto a los puntos $\boldsymbol{P_s}$ y $\boldsymbol{P_u}$, y no son considerados los porcentajes de los atributos definidos por los expertos (18.33% *Usabilidad*, 81.67% *Seguridad*).

En **B** se encuentra representada la recta parametrizada que pasa a través de la distancia euclidiana.

En **C** se encuentra representada gráficamente el valor de la distancia euclidiana con respecto a los puntos $\boldsymbol{P_s}$ y $\boldsymbol{P_u}$, considerando los porcentajes de los atributos definidos por expertos (18.33% *Usabilidad*, 81.67% *Seguridad*). Se puede contemplar un desplazamiento del punto $\boldsymbol{P_u}$, a través de la recta, que ha permitido en este caso, reducir la distancia euclidiana, y a su vez, influenciar en el resultado de la USec.

Nota: En el ejemplo anterior, es claro evidenciar que el resultado de la USec será favorecido por el acercamiento del punto $\boldsymbol{P_u}$, al punto $\boldsymbol{P_s}$, sin embargo, en algunas ocasiones podrán presentarse casos en los que se evidencie un alejamiento de los puntos, lo cual será desfavorable para el resultado de la USec, que como se ha mencionado queda estrictamente sujeto a los porcentajes definidos por los expertos (véase **Anexo B)** y a las calificaciones realizadas por los auditores.

4.4.3 Transformación de calificaciones

En la mayoría de los requerimientos referentes a esta investigación, la importancia de los atributos de seguridad y usabilidad varía según la naturalidad del requerimiento (véase **Anexo B**). Esto implica que la atención de un auditor estará fijada en el atributo que presente mayor influencia sobre el requerimiento, por consiguiente, las sub-heurísticas de un requerimiento serán calificadas con mayor exigencia en el atributo que predomine sobre el mismo, por esta razón, la calificación de las sub-heurísticas en el atributo con menor influencia demandarán menor atención, de ahí, que la calificación correspondiente al atributo pueda ser inferior comparado con el atributo que requiere mayor atención, para considerables casos.

Para mitigar las consecuencias de este hecho que ya ha sido expuesto en el anterior apartado (véase **Apartado 4.4.2**, **Figura 8**), las calificaciones originales de los auditores en los atributos de menor porcentaje correspondientes a cada uno de los requerimientos, serán transformadas haciendo uso de la *fórmula matemática* anteriormente introducida (véase **Apartado 4.4.2**, **Figura 8**).

4.4.4 Escala para la medición de la USec

Para reflejar el resultado de la USec, fue necesario trabajar en la construcción de una escala (véase **Tabla 14**). La escala se encuentra ligada a la distancia euclidiana y a la calificación del auditor (véase **Apartado 4.4.2**). Es necesario resaltar, que la construcción de los rangos numéricos fue equitativo, ya que se observó el comportamiento de la escala definida por expertos en Ciencias de la Computación (véase **Apartado 3.6**) y se tuvo en cuenta las apreciaciones y sugerencias hechas por el matemático, además, los respectivos valores cualitativos fueron tomados de la investigación realizada por Yeratziotis **[85]**.

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.

Tabla 14. Escala USec

La fórmula que permite la clasificación en la escala, se presenta a continuación,

$$\boldsymbol{USec} = \left(\sum \boldsymbol{u} + \sum \boldsymbol{s}\right) * (\mathbf{1} - \boldsymbol{DE'})$$

Donde,

$\sum \boldsymbol{u}$: Son los valores calificados por el auditor en las sub-heurísticas correspondientes al atributo usabilidad.
$\sum \boldsymbol{s}$: Son los valores calificados por el auditor en las sub-heurísticas correspondientes al atributo seguridad.
$\boldsymbol{DE'}$: Es la distancia euclidiana normalizada teniendo en cuenta el mayor valor de calificación.

La fórmula anteriormente expuesta, considera el *factor* que permite la *anulación de la ambigüedad* presentada en este apartado (véase **Figura 7**), asimismo, considera la *distancia euclidiana* aludida a lo largo de este capítulo.

La fórmula queda sujeta al método de observación empírica **[92]**, base fundamental para la construcción del modelo matemático.

Es importante destacar que la formula puede ser adaptada según los parámetros (Escalas de evaluación) que se consideren en futuros trabajos.

4.5. REPRESENTACIÓN MATEMÁTICA

A continuación se presenta la estructura general que abarca el proceso desarrollado en este capítulo. Se presentan dos casos para la obtención del resultado de la USec.

4.5.1 Primer caso

Utilización de la fórmula que permite compensar el porcentaje de influencia de los atributos.

			Atributo P_u	Atributo P_s
			P_u	P_s
Requerimiento(R)	Sub-Heurística(h)	Importancia Sub-Heurística(Ih)	Usabilidad(u)	Seguridad(s)
r_i	h_1	Ih_1	x_1	x_2
	h_2	Ih_2	y_1	y_2
	...	...	...	...
	h_{n-1}	Ih_{n-1}	w_1	w_2
	h_n	Ih_n	z_1	z_2

Tabla 15. Representación general de las características presentes en la valoración inicial

En la t*abla*, se ilustra una situación general de evaluación heurística según lo planteado.

Donde,

$\boldsymbol{r_i}$: Es el requerimiento a considerar.
$\boldsymbol{h_n}$: La sub-heurística a evaluar según $\boldsymbol{r_i}$.
$\boldsymbol{Ih_n}$: Es la importancia de la sub-heurística a evaluar expresada en porcentaje (véase **Apartado 3.6.3)** donde,

$$\sum_{i=1}^{n} \boldsymbol{Ih\ i} = \mathbf{1}$$

$\boldsymbol{x, y, \ldots, w, z}$: Son las calificaciones entregadas por los auditores.
$\boldsymbol{P_u}$, $\boldsymbol{P_s}$: El porcentaje de influencia de cada atributo (seguridad y usabilidad) (véase **Apartado 3.6.2)** donde,

$$\boldsymbol{P_u} + \boldsymbol{P_s} = \mathbf{1}$$

- **Primer Paso,**

Para lograr un equilibrio en el factor de influencia de los atributos, se introduce la siguiente formula, (véase **Apartado 4.4)**

$$\boldsymbol{A_i * Ih_i = F_{em} * (Val_{max} - Val_{act}) + Val_{act}}$$

Donde,

$\boldsymbol{A_i * Ih_i}$: Son los nuevos valores a obtener en el atributo que espera ser mejorado, es decir, la transformación de los componentes del atributo que presenta menor porcentaje de influencia.
$\boldsymbol{F_{em}}$: Es el mayor porcentaje de influencia ($\boldsymbol{P_u} \vee \boldsymbol{P_s}$).
$\boldsymbol{Val_{max}}$: Es el valor máximo que un experto puede dar a la heurística según el atributo. El valor ha sido ajustado a $\mathbf{100}$.

$\boldsymbol{Val_{act}}$: Es el valor calificado por el experto en la sub-heurística según el atributo.

La fórmula debe ser aplicada a cada una de las calificaciones proveídas por el auditor en el atributo con menor porcentaje de influencia.

- **Segundo Paso,**

Obtener los **nuevos** valores en $\boldsymbol{u} \vee \boldsymbol{s}$

- **Tercer Paso,**

Multiplicar los $\boldsymbol{Ih}$ de cada heurística por los valores de $\boldsymbol{u} \wedge \boldsymbol{s}$, la representación se ilustra en la siguiente *tabla*,

R	h	Ih	u'	s'
r_i	h_1	Ih_1	$x'_1 = Ih_1 * x_1$	$x'_2 = Ih_1 * x_2$
	h_2	Ih_2	$y'_1 = Ih_2 * y_1$	$y'_2 = Ih_2 * y_2$
	...	...	...	...
	h_{n-1}	Ih_{n-1}	$w'_1 = Ih_{n-1} * w_1$	$w'_2 = Ih_{n-1} * w_2$
	h_n	Ih_n	$z'_1 = Ih_n * z_1$	$z'_2 = Ih_n * z_2$

Tabla 16. Representación general de las características ajustadas

- **Cuarto Paso,**

Calcular la distancia euclidiana para los puntos $\boldsymbol{u}'(x'^1, y'^1, \dots, w'^1, z'^1) \wedge \boldsymbol{s}'(x'^2, y'^2, \dots, w'^2, z'^2)$

$$\boldsymbol{DE} = \sqrt{((x'^1 - x'^2) + (y'^1 - y'^2) + \cdots + (w'^1 - w'^2) + (z'^1 - z'^2))^2}$$

- **Quinto Paso,**

Normalizar la distancia euclidiana teniendo en cuenta el mayor valor de evaluación (véase **Apartado 4.4**).

$$\boldsymbol{DE'} = \frac{\boldsymbol{DE}}{\boldsymbol{valmax}}$$

- **Sexto Paso,**

Obtener el valor de USec haciendo uso de la siguiente formula (véase **Apartado 4.4.3**):

$$\boldsymbol{USec} = \left(\sum \boldsymbol{u'} + \sum \boldsymbol{s'}\right) * (\mathbf{1} - \boldsymbol{DE'})$$

Donde,

$\sum \boldsymbol{u'}$: Son los valores calificados por el auditor 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.
DE' : Es la distancia euclidiana normalizada teniendo en cuenta el mayor valor de calificación.

4.5.2 Segundo caso

La fórmula que permite compensar el porcentaje de influencia de los atributos *no es considerada*, ya que estos se encuentran en igualdad de condiciones. Se debe seguir el proceso anterior, obviando ***Primer y Segundo Paso*** (véase **Apartado 4.5.1**).

4.5.3 Ejemplos Ilustrativo

4.5.3.1 Ejemplo #1

A continuación, se introduce un ejemplo alusivo al ***Primer Caso*** (véase **Apartado 4.5.1**).

Sea un requerimiento evaluado por dos o más sub-heurísticas como se aprecia en la ***Tabla 17***, el porcentaje de influencia de los atributos (P_u y P_s) diferente.

			Atributo	
			P_u	P_s
			0,6	0,4
R	h	Ih	u	s
r_i	h_1	0,35	80	60
	h_2	0,35	75	55
	h_3	0,3	90	60

Tabla 17. Ejemplo#1 Ilustrativo – Primer Caso

- **Primer Paso,**

Aplicar la formula correspondiente al equilibrio en el factor de influencia de los atributos. En este caso el porcentaje de seguridad presenta un desequilibrio, por lo tanto.

$$A_i * Ih_i = F_{em} * (Val_{max} - Val_{act}) + Val_{act}$$

Donde,

$s_1 * Ih_1 = 0{,}6 * (100 - 60) + 60 = \mathbf{84}$
$s_2 * Ih_2 = 0{,}6 * (100 - 55) + 55 = \mathbf{82}$
$s_3 * Ih_3 = 0{,}6 * (100 - 60) + 60 = \mathbf{84}$

$F_{em} = 0{,}6$
$Val_{max} = 100$
$Val_{act} = (60, 55, 60).$

- **Segundo Paso,**

Registrar **nuevos** valores en $\boldsymbol{s}$,

R	h	Ih	u	s
$\boldsymbol{r_i}$	$\boldsymbol{h_1}$	0,35	80	**84**
	$\boldsymbol{h_2}$	0,35	75	**82**
	$\boldsymbol{h_3}$	0,3	90	**84**

Tabla 18. Ejemplo #1 – Nuevos valores de *s*

- **Tercer Paso,**

Multiplicar los $\boldsymbol{Ih}$ de cada heurística por los valores de $\boldsymbol{u} \wedge \boldsymbol{s}$, la representación se ilustra en la siguiente *tabla*,

R	h	Ih	u'	s'
$\boldsymbol{r_i}$	h_1	0,35	$x'_1 = 0{,}35 * 80 = \mathbf{28}$	$x'_2 = 0{,}35 * 84 = \mathbf{29.4}$
	h_2	0,35	$y'_1 = 0{,}35 * 75 = \mathbf{26.25}$	$y'_2 = 0{,}35 * 82 = \mathbf{28.7}$
	h_3	0,30	$z'_1 = 0{,}30 * 90 = \mathbf{27}$	$z'_2 = 0{,}30 * 84 = \mathbf{25.2}$

Tabla 19. Ejemplo #1 – Multiplicación *Ih*

- **Cuarto Paso,**

Calcular la distancia euclidiana para los puntos $\boldsymbol{u}'(28, 26.25, 27) \wedge \boldsymbol{s}'(29.4, 28.7, 25.2)$

$$\boldsymbol{DE} = \sqrt{(28 - 29.40)^2 + (26.25 - 28.70)^2 + (27 - 25.20)^2}$$

$$\boldsymbol{DE} = \mathbf{3.34701359424}$$

- **Quinto Paso,**

Normalizar la distancia euclidiana teniendo en cuenta el mayor valor de evaluación.

$$\boldsymbol{DE'} = \frac{DE}{100} = \mathbf{0.03347013594}$$

- **Sexto Paso,**

Aplicar la fórmula para obtener el valor de USec,

$$\boldsymbol{USec} = \left(\sum \boldsymbol{u'} + \sum \boldsymbol{s'}\right) * (\mathbf{1} - \boldsymbol{DE'})$$

Donde,

$\sum \boldsymbol{u'} = (28 + 26.25 + 27) = \mathbf{81.25}$
$\sum \boldsymbol{s'} = (29.40 + 28.70 + 25.20) = \mathbf{83.3}$

$$DE' = 0.03347013594$$

$$USec = (81.25 + 83.3) * (1 - 0.03347013594)$$

$$USec = 159.042489131$$

Por medio del resultado de USec, es posible hallar la calificación cualitativa del requerimiento referenciado haciendo uso de la escala para la medición de la USec (véase **Apartado 4.4.4**).

Valor Cuantitativo	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.

Tabla 20. Ejemplo #1 – Calificación USec

Finalmente, es posible concluir que es un requerimiento que no presenta un índice de riesgo alto, sin embargo, debe ser tratado dándole una prioridad baja.

4.5.3.2 Ejemplo #2

A continuación, se introduce un ejemplo alusivo al ***Primer Caso*** (véase **Apartado 4.5.1**).

Sea un requerimiento evaluado por dos o más sub-heurísticas como se aprecia en la ***Tabla 21***, el porcentaje de influencia de los atributos (P_u y P_s) diferente.

			Atributo	
			P_u	P_s
			0,35	0,65
R	h	Ih	u	s
r_i	h_1	0,30	80	70
	h_2	0,35	84	75
	h_3	0,35	70	60

Tabla 21. Ejemplo#2 Ilustrativo – Primer Caso

❖ **Primer Paso,**

Aplicar la formula correspondiente al equilibrio en el factor de influencia de los atributos. En este caso el porcentaje de seguridad presenta un desequilibrio, por lo tanto.

$$\boldsymbol{A_i * Ih_i = F_{em} * (Val_{max} - Val_{act}) + Val_{act}}$$

Donde,

$\boldsymbol{u_1 * Ih_1} = 0{,}65 * (100 - 80) + 80 = \mathbf{93}$
$\boldsymbol{u_2 * Ih_2} = 0{,}65 * (100 - 84) + 84 = \mathbf{94.4}$
$\boldsymbol{u_3 * Ih_3} = 0{,}65 * (100 - 70) + 70 = \mathbf{89.5}$

$\boldsymbol{F_{em}} = 0{,}6$
$\boldsymbol{Val_{max}} = 100$
$\boldsymbol{Val_{act}} = (60, 55, 60).$

❖ **Segundo Paso,**

Registrar **nuevos** valores en $\boldsymbol{s}$,

R	h	Ih	u	s
r_i	h_1	0,30	**93**	70
	h_2	0,35	**94.4**	75
	h_3	0,35	**89.5**	60

Tabla 22. Ejemplo #2 – Nuevos valores de *s*

❖ **Tercer Paso,**

Multiplicar los $\boldsymbol{Ih}$ de cada heurística por los valores de $\boldsymbol{u} \wedge \boldsymbol{s}$, la representación se ilustra en la siguiente *tabla*,

R	h	Ih	u'	s'
r_i	h_1	0,35	$x'_1 = 0{,}30 * 93 = \mathbf{27.9}$	$x'_2 = 0{,}30 * 70 = \mathbf{21}$
	h_2	0,35	$y'_1 = 0{,}35 * 94.4 = \mathbf{33.04}$	$y'_2 = 0{,}35 * 75 = \mathbf{26.25}$
	h_3	0,30	$z'_1 = 0{,}35 * 89.5 = \mathbf{31.325}$	$z'_2 = 0{,}35 * 60 = \mathbf{21}$

Tabla 23. Ejemplo #2 – Multiplicación *Ih*

❖ **Cuarto Paso,**

Calcular la distancia euclidiana para los puntos $\boldsymbol{u}'(27.9, 33.04, 31.325) \wedge \boldsymbol{s}'(21, 26.25, 21)$

$$\boldsymbol{DE} = \sqrt{(27.90 - 21.00)^2 + (33.04 - 26.25)^2 + (31.325 - 21.00)^2}$$

$$\boldsymbol{DE = 14.1534350954}$$

- **Quinto Paso,**

Normalizar la distancia euclidiana teniendo en cuenta el mayor valor de evaluación.

$$\boldsymbol{DE'} = \frac{DE}{100} = \mathbf{0.141534350954}$$

- **Sexto Paso,**

Aplicar la fórmula para obtener el valor de USec,

$$\boldsymbol{USec} = \left(\sum \boldsymbol{u'} + \sum \boldsymbol{s'}\right) * (\mathbf{1} - \boldsymbol{DE'})$$

Donde,

$\sum \boldsymbol{u'} = (27.9 + 33.04 + 31.325) = \mathbf{92.265}$
$\sum \boldsymbol{s'} = (21 + 26.25 + 21) = \mathbf{68.25}$
$\boldsymbol{DE'} = \mathbf{0.141534350954}$

$$\boldsymbol{USec} = (\mathbf{92.265} + \mathbf{68.25}) * (1 - \mathbf{0.141534350954})$$

$$\boldsymbol{USec} = \mathbf{137.796613657}$$

Por medio del resultado de USec, es posible hallar la calificación cualitativa del requerimiento referenciado haciendo uso de la escala para la medición de la USec (véase **Apartado 4.4.4**).

Valor Cuantitativo	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.

Tabla 24. Ejemplo #2 – Calificación USec

Finalmente, es posible concluir que es un requerimiento que no presenta un índice de riesgo alto, sin embargo, debe ser tratado dándole una prioridad baja.

4.5.3.3 Ejemplo #3

A continuación, se introduce un ejemplo alusivo al ***Segundo Caso*** (véase **Apartado 4.5.2**).

Sea un requerimiento evaluado por dos o más sub-heurísticas como se aprecia en la ***Tabla 25***, el porcentaje de influencia de los atributos ($\boldsymbol{P_u}$ y $\boldsymbol{P_s}$) no presenta desigualdad.

			Atributo	
			$\boldsymbol{P_u}$	$\boldsymbol{P_s}$
			0,50	0,50
R	$\boldsymbol{h}$	$\boldsymbol{Ih}$	$\boldsymbol{u}$	$\boldsymbol{s}$
$\boldsymbol{r_i}$	$\boldsymbol{h_1}$	0,30	80	70
	$\boldsymbol{h_2}$	0,35	84	75
	$\boldsymbol{h_3}$	0,35	70	60

Tabla 25. Ejemplo#3 Ilustrativo – Segundo caso

Primer y Segundo Paso son obviados.

- **Tercer Paso,**

Multiplicar los $\boldsymbol{Ih}$ de cada heurística por los valores de $\boldsymbol{u} \wedge \boldsymbol{s}$, la representación se ilustra en la siguiente *tabla*,

R	$\boldsymbol{h}$	$\boldsymbol{Ih}$	$\boldsymbol{u'}$	$\boldsymbol{s'}$
$\boldsymbol{r_i}$	h_1	0,35	$x'_1 = 0{,}30 * 80 = \mathbf{24}$	$x'_2 = 0{,}30 * 70 = \mathbf{21}$
	h_2	0,35	$y'_1 = 0{,}35 * 84 = \mathbf{29.04}$	$y'_2 = 0{,}35 * 75 = \mathbf{26.25}$
	h_3	0,30	$z'_1 = 0{,}35 * 70 = \mathbf{24.5}$	$z'_2 = 0{,}35 * 60 = \mathbf{21}$

Tabla 26. Ejemplo #3 – Multiplicación *Ih*

- **Cuarto Paso,**

Calcular la distancia euclidiana para los puntos $\boldsymbol{u}'(24, 29.04, 24.5) \wedge \boldsymbol{s}'(21, 26.25, 21)$

$$\boldsymbol{DE} = \sqrt{(24 - 21.00)^2 + (29.04 - 26.25)^2 + (24.5 - 21.00)^2}$$

$$\boldsymbol{DE} = \mathbf{5.38832998247}$$

- **Quinto Paso,**

Normalizar la distancia euclidiana teniendo en cuenta el mayor valor de evaluación.

$$\boldsymbol{DE'} = \frac{DE}{100} = \mathbf{0.05388329982}$$

- **Sexto Paso,**

Aplicar la fórmula para obtener el valor de USec,

$$\boldsymbol{USec} = \left(\sum \boldsymbol{u'} + \sum \boldsymbol{s'}\right) * (\mathbf{1} - \boldsymbol{DE'})$$

Donde,

$\sum \boldsymbol{u'} = (24 + 29.04 + 24.5) = \mathbf{77.54}$
$\sum \boldsymbol{s'} = (21 + 26.25 + 21) = \mathbf{68.25}$
$\boldsymbol{DE'} = \mathbf{0.05388329982}$

$$\boldsymbol{USec} = (\mathbf{77.54} + \mathbf{68.25}) * (1 - \mathbf{0.05388329982})$$

$$\boldsymbol{USec} = \mathbf{137.934353719}$$

Por medio del resultado de USec, es posible hallar la calificación cualitativa del requerimiento referenciado haciendo uso de la escala para la medición de la USec (véase **Apartado 4.4.4**).

Valor Cuantitativo	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.

Tabla 27. Ejemplo #3 – Calificación USec

Finalmente, es posible concluir que es un requerimiento que no presenta un índice de riesgo alto, sin embargo, debe ser tratado dándole una prioridad baja.

4.5.3.4 Ejemplo #4

A continuación, se introduce un ejemplo alusivo al ***Segundo Caso*** (véase **Apartado 4.5.2**).

Sea un requerimiento evaluado una sub-heurística como se aprecia en la ***Tabla 28***, el porcentaje de influencia de los atributos ($\boldsymbol{P_u}$ y $\boldsymbol{P_s}$) no presenta desigualdad.

			Atributo	
			P_u	P_s
			0,50	0,50
R	h	Ih	u	s
r_i	h_1	1	80	90

Tabla 28. Ejemplo#4 Ilustrativo – Segundo caso

Primer y Segundo Paso son obviados.

- **Tercer Paso,**

Multiplicar los Ih de cada heurística por los valores de $u \wedge s$, la representación se ilustra en la siguiente *tabla*,

R	h	Ih	u'	s'
r_i	h_1	1	$x'_1 = 1 * 80 = \mathbf{80}$	$x'_2 = 1 * 90 = \mathbf{90}$

Tabla 29. Ejemplo #4 – Multiplicación *Ih*

- **Cuarto Paso,**

Calcular la distancia euclidiana para los puntos $u'(80) \wedge s'(90)$

$$DE = \sqrt{(80 - 90)^2}$$

$$DE = \mathbf{10}$$

- **Quinto Paso,**

Normalizar la distancia euclidiana teniendo en cuenta el mayor valor de evaluación.

$$DE' = \frac{DE}{100} = \mathbf{0.1}$$

- **Sexto Paso,**

Aplicar la fórmula para obtener el valor de USec,

$$USec = \left(\sum u' + \sum s'\right) * (1 - DE')$$

Donde,

$\sum u' = (80) = \mathbf{80}$
$\sum s' = (90) = \mathbf{90}$

$$\boldsymbol{DE' = 0.1}$$

$$\boldsymbol{USec = (80 + 90) * (1 - 0.1)}$$

$$\boldsymbol{USec = 153}$$

Por medio del resultado de USec, es posible hallar la calificación cualitativa del requerimiento referenciado haciendo uso de la escala para la medición de la USec (véase **Apartado 4.4.4**).

Valor Cuantitativo	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.

Tabla 30. Ejemplo #4 – Calificación USec

Finalmente, es posible concluir que es un requerimiento que no presenta un índice de riesgo alto, sin embargo, debe ser tratado dándole una prioridad baja.

Capítulo 5

Estudio de caso y análisis de resultados

Los artefactos generados en este capítulo, pueden ser evidenciados en el Sprint 5 de la metodología (véase **Anexo L**).

Desde el inicio de esta investigación, 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 en el **Capítulo 3** y **Capítulo 4**, serán validados mediante un estudio de caso que contempla una plataforma e-Banking de una entidad financiera.

5.1 ESTUDIO DE CASO

Inicialmente, se consideró trabajar con plataformas de entidades bancarias colombianas, pues en estas se podrían identificar los requerimientos de un sistema e-Banking (véase **Apartado 3.3**). La idea fue rápidamente descartada, debido a la dificultad que se presentaba al encontrar auditores, expertos y usuarios que pertenecieran a la misma entidad bancaria.

El proceso llevado a cabo para la realización del estudio de caso se puede evidenciar en la siguiente figura (véase **Figura 9**)

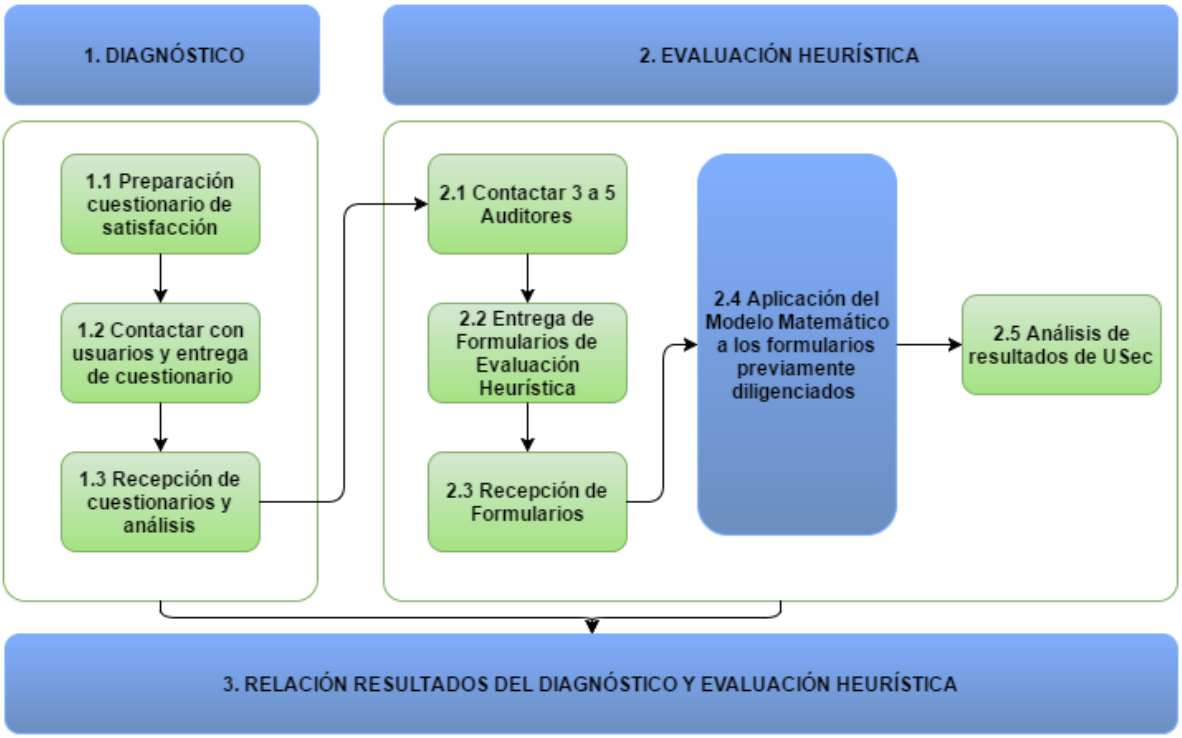

Figura 9. Proceso para llevar a cabo el estudio de caso

Se inicia con un proceso de diagnóstico por medio de un cuestionario de satisfacción, el cual se lleva a cabo en tres fases: *Fase 1 – marco 1.1*, Preparación del cuestionario, Fase 2 – *marco 1.2*, Contactar usuarios participantes para la entrega de los cuestionarios, Fase 3 – *marco 1.3*, Consolidar y analizar los resultados obtenidos en los cuestionarios.
Finalizada la primera etapa se procede a llevar a cabo la aplicación de la evaluación heurística a la plataforma e-Banking del estudio de caso. En primer lugar se contacta con los auditores expertos, entre 3 y 5 de ellos, que manejen las áreas de Seguridad y Usabilidad, además deben disponer de una cuenta para acceder al aplicativo e-Banking del estudio de caso – *marco 2.1*, seguido, a cada uno de los auditores se les hace entrega del formulario de evaluación heurística y firman carta de consentimiento informado – *marco 2.2*, los auditores proceden a realizar la evaluación, posteriormente, con la recolección de datos obtenidos – *marco 2.3*, se procede a aplicar el modelo matemático como herramienta para calcular el USec de la plataforma e-Banking – *marco 2.4*, se concluye esta etapa con el análisis de los resultados USec obtenidos por medio del modelo matemático – *marco 2.5*. Finalmente se contrastan los resultados obtenidos en el diagnóstico con los resultados obtenidos en la evaluación heurística y se generan las conclusiones.

5.1.1 Entidad Financiera

La Universidad del Cauca, cuenta con una entidad financiera llamada *Fondo de Profesores de la Universidad del Cauca* – ***FONDUC***. 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*** (véase **Anexo E**). Luego, la gerencia a cargo del *Esp. Juan Felipe Vallejo Matus*, decidió citar a los implicados de la investigación a una reunión presencial, la cual resultó con el 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 auditores, expertos y usuarios que pertenecieran a la misma entidad, ya que todos los actores implicados en esta investigación estarían vinculados a la entidad.

5.1.2 Propuesta

Contando con los artefactos producto de esta investigación, se desarrolló una propuesta que fue presentada y aprobada por la administración del **FONDUC** (véase **Anexo F**).

5.1.3 Acuerdo de confidencialidad

Para desarrollar la propuesta presentada anteriormente, fue necesario, radicar un acuerdo de confidencialidad entre las partes, asegurándose de la protección de los datos del sistema, el acuerdo fue suscripto por la gerencia del *Fondo de Profesores de la Universidad del Cauca* – ***FONDUC*** y el líder del Grupo de Investigación y Desarrollo en Ingeniería de Software – ***IDIS*** (véase **Anexo G**).

5.1.4 Alcance del estudio de caso

Para validar el estudio de caso, es necesario resaltar las altas medidas de seguridad que implican llevar a cabo estudios de caso con entidades bancarias, las grandes cifras de dinero y exposición de datos sensibles son consecuencia de dichas medidas. La entidad **FONDUC** ha expresado su continua preocupación por el manejo inapropiado de los datos que pueda implicar la realización de esta investigación, además, ha sido muy específica en las autorizaciones delegadas al grupo de investigación **IDIS**. El incumplimiento de cualquier cláusula del acuerdo de confidencialidad (véase **Apartado 5.1.3**) implicará acciones legales sobre el grupo de investigación **IDIS**.

A pesar, de tener las intenciones de llevar a cabo un análisis de riesgos aplicando metodologías como **OWASP** (The Open Web Application Security Project) **[96]** o estándares como **ISO/IEC 27005 [97]**, resulta imposible por lo legalmente pactado en el acuerdo de confidencialidad (véase **Anexo G**), por consiguiente, el estudio de caso queda

limitado a la realización de una evaluación heurística por parte de auditores que pertenecen a la entidad **FONDUC**.

Finalmente, esta investigación corrobora la dificultad para hallar una entidad financiera que cuente con un aplicativo e-Banking y permita realizar investigaciones con fines académicos, ya que en muchos de los casos, no representa beneficio alguno para ellos, por el contrario, pone en riesgo la credibilidad de la institución financiera.

5.2 ANÁLISIS DE RESULTADOS

Considerando la propuesta presentada al **FONDUC** (véase **Apartado 5.1.2**), se sigue el orden de ideas para presentar los resultados de esta investigación.

5.2.1 Encuesta de Satisfacción

Considerando los elementos incluidos en la usabilidad y seguridad se realiza una encuesta de satisfacción (véase **Anexo H**) a un grupo de 10 usuarios recurrentes del sistema e-Banking **FONDUC** (Fondo de Profesores de la Universidad de Cauca), cuyo perfil profesional oscila entre ingenieros electrónicos y de sistemas y en consecuencia, con amplios conocimientos en el manejo de aplicativos virtuales. Aunque a simple vista parece un número reducido, según **[94]** esta cifra resulta ser aceptable para obtener conclusiones considerables, a fin de determinar qué tan apropiados y fáciles de comprender son algunos componentes del sistema. El mismo autor expone que la encuesta fue elaborada utilizando una escala basada en el sistema SUS (*System Usability Scale*). Una pregunta consta de 5 opciones de respuesta, con valores comprendidos de uno (1) a cinco (5), donde, uno (1) es la calificación mínima, por lo tanto, se reprueba y cinco (5) la calificación máxima que aprueba positivamente la característica que se evalúa. Para esta investigación se realizan algunas modificaciones, de tal manera que se ajuste al estudio de caso planteado.

Para el desarrollo de esta actividad, se consideraron 3 fases:

5.2.1.1 Fase 1

Basándose en la encuesta de referencia se proceden a hacer los ajustes y preparar el formulario con el que se evalúa la satisfacción del usuario, el formulario evalúa el desempeño de una lista de seis (6) tareas (véase **Anexo H**), las cuales a través de la literatura se identifican como posibles tareas que se realizan con mayor frecuencia en plataformas e-Banking, es necesario aclarar que se evitó plantear tareas que alteraran el estado financiero del usuario participante, considerando las sugerencias realizadas por la administración del **FONDUC.**

A partir de la realización de las tareas, el usuario continuaría con dar respuesta a un post-test que consta de 10 preguntas (véase **Anexo H**), que se responden según la especificación de la escala SUS, ya mencionada.

5.2.1.2 Fase 2

En esta fase de la encuesta fue necesario ponerse en contacto con docentes de planta de la Universidad del Cauca, que contaran con una cuenta en el **FONDUC**, y que además hicieran uso frecuente de la plataforma virtual, para ello fue necesario concordar una reunión con cada uno de los docentes dispuestos a colaborar, con el propósito de explicar el motivo de la encuesta y asegurar su participación.

5.2.1.3 Fase 3

Finalmente, se presentan los resultados obtenidos de los formularios diligenciados, producto de la participación de los usuarios.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Usuario 1	2	3	2	2	3	2	3	2	2	3
Usuario 2	4	4	4	4	4	4	4	4	3	4
Usuario 3	4	4	4	4	4	4	4	4	3	4
Usuario 4	4	4	3	4	4	4	4	4	3	4
Usuario 5	3	3	3	3	3	3	3	3	3	3
Usuario 6	3	2	2	2	2	2	5	2	3	3
Usuario 7	4	4	5	5	4	4	5	4	3	4
Usuario 8	4	3	3	3	3	4	4	4	3	3
Usuario 9	2	4	4	3	3	4	3	3	3	3
Usuario 10	4	3	4	3	4	4	3	4	3	3

Tabla 31. Resultados encuesta de satisfacción

Las **columnas** $\boldsymbol{Q1, Q2, \dots, Q10}$: Son las preguntas realizadas en la fase 2 (post-test).
Las **filas** $\boldsymbol{Usuario1, Usuario2, \dots, Usuario\ 10}$: Son los 10 usuarios que participaron de la encuesta de satisfacción.
Los **valores** registrados por fila, son las respuestas de cada uno de los usuarios a determinada pregunta.

Para tener una perspectiva de la simetría de la distribución de los datos, se expone la siguiente (véase **Figura 10**), correspondiente a un Diagrama de caja y bigotes, para luego explicar de forma detallada los resultados de cada pregunta.

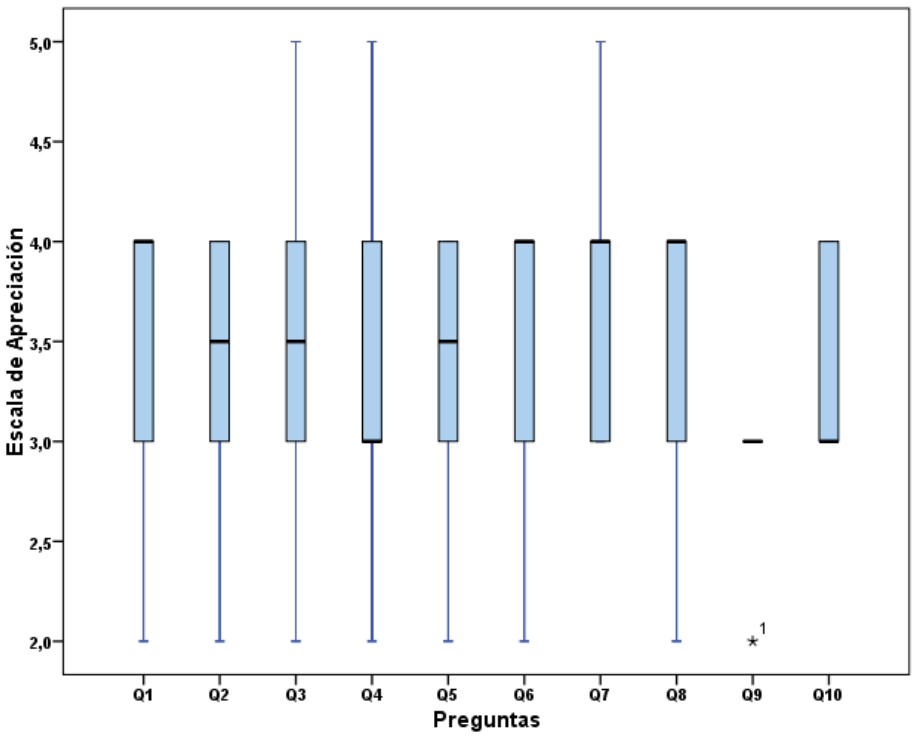

Figura 10. Distribución de los datos

Q1		
Apreciaciones	**Frecuencia**	**Porcentaje**
2	2	20%
3	2	20%
4	6	60%
Total	10	100%

Tabla 32. Frecuencias Q1

Para la pregunta Q1, como se evidencia en la ***Tabla 32***, se puede observar que el 20% de los usuarios calificó con apreciación 2, siendo equivalente a que difícilmente logró completar la totalidad de las tareas, otro 20% se posicionó neutral con apreciación 3, y el 60% restante calificó con apreciación 4, ya que consideró haber completado todas las tareas fácilmente.

Q2		
Apreciaciones	**Frecuencia**	**Porcentaje**
2	1	10%
3	4	40%
4	5	50%
Total	10	100%

Tabla 33. Frecuencias Q2

Para la pregunta Q2, como se evidencia en la ***Tabla 33***, se puede observar que el 10% de los usuarios calificó con apreciación 2, siendo equivalente a que fue difícilmente logró comprender la información requerida para esta encuesta, otro 40% se posicionó neutral con apreciación 3, y el 50% restante califico con apreciación 4, ya que fácilmente comprendió la información requerida.

Q3		
Apreciaciones	**Frecuencia**	**Porcentaje**
2	2	20%
3	3	30%
4	4	40%
5	1	10%
Total	10	100%

Tabla 34. Frecuencias Q3

Para la pregunta Q3, como se evidencia ver en la ***Tabla 34***, se puede observar que el 20% de los usuarios calificó con apreciación 2, siendo equivalente a que la información del aplicativo virtual es muy difusa, otro 30% se posicionó neutral con apreciación 3, el 40% calificó con apreciación 4, la información fue clara, y el 50% restante calificó con apreciación 5, valorando la información del aplicativo como muy clara.

Q4		
Apreciaciones	**Frecuencia**	**Porcentaje**
2	2	20%
3	4	40%
4	3	30%
5	1	10%
Total	10	100%

Tabla 35. Frecuencias Q4

Para la pregunta Q4, como se evidencia en la ***Tabla 35***, se puede observar que el 20% de los usuarios calificó con apreciación 2, siendo equivalente a que la navegación en el sitio web es difícil, un 40% se posicionó neutral con apreciación 3, el 30% restante califico con apreciación 4, considerando la navegación fácil, y el 10% restante calificó con apreciación 5, siendo muy fácil.

Q5		
Apreciaciones	**Frecuencia**	**Porcentaje**
2	1	10%
3	4	40%

4	5	50%
Total	10	100%

Tabla 36. Frecuencias Q5

Para la pregunta Q5, como se evidencia en la ***Tabla 36***, se puede observar que el 10% de los usuarios calificó con apreciación 2, estando en desacuerdo sobre la facilidad para entender la información requerida en la prueba, el 40% se posicionó neutral con apreciación 3, y el 50% restante califico con apreciación 4, estando de acuerdo con que la información fue fácil de entender.

Q6		
Apreciaciones	**Frecuencia**	**Porcentaje**
2	2	20%
3	1	10%
4	7	70%
Total	10	100%

Tabla 37. Frecuencias Q6

Para la pregunta Q6, como se evidencia en la ***Tabla 37***, se puede observar que el 20% de los usuarios calificó con apreciación 2, estando en desacuerdo en que se sintieron bien informados y orientados en el sitio web, el 10% se posicionó neutral con apreciación 3, y el 70% restante calificó con apreciación 4, estando de acuerdo en que se sintieron bien informados y orientados en el sitio web.

Q7		
Apreciaciones	**Frecuencia**	**Porcentaje**
3	4	40%
4	4	40%
5	2	20%
Total	10	100%

Tabla 38. Frecuencias Q7

Para la pregunta Q7, como se evidencia en la ***Tabla 38***, se puede observar que el 40% de los usuarios calificó con apreciación 3, considerándose neutrales en cuanto al nivel de confianza que inspira realizar movimientos en el sitio, otro 40% calificó con apreciación 4, estando de acuerdo con que la plataforma inspira confianza y el 20% restante califico con apreciación 5, estando completamente de acuerdo con que la plataforma inspira confianza.

Q8		
Apreciaciones	**Frecuencia**	**Porcentaje**
2	2	20%
3	2	20%
4	6	60%
Total	10	100%

Tabla 39. Frecuencias Q8

Para la pregunta Q8, como se evidencia en la ***Tabla 39***, se puede observar que el 20% de los usuarios calificó con apreciación 2, considerando el sitio web poco satisfactorio, otro 20% se posicionó neutral con apreciación 3, y el 60% restante califico con apreciación 4, considerando el sitio satisfactorio.

Q9		
Apreciaciones	**Frecuencia**	**Porcentaje**
2	1	10%
3	8	90%
Total	10	100%

Tabla 40. Frecuencias Q9

Para la pregunta Q9, como se evidencia en la ***Tabla 40***, se puede observar que el 10% de los usuarios califico con apreciación 2, considerando la experiencia con el sitio de **FONDUC** peor comparado a otros sitios. El 90% restante se posicionó neutral ante la pregunta con apreciación 3.

Q10		
Apreciaciones	**Frecuencia**	**Porcentaje**
3	6	60%
4	4	40%
Total	10	100%

Tabla 41. Frecuencias Q10

Para la pregunta Q10, como se evidencia en la ***Tabla 41***, se puede observar que el 60% de los usuarios califico con apreciación 3, considerándose neutrales respecto a su experiencia como colaborador de la prueba. El 40% restante califico con apreciación 4, al considerar agradable su experiencia.

En resumen, la encuesta muestra resultados un poco variables entre los usuarios, además, es posible notar que ninguno de los promedios superó en valor a 4, siendo el peor de los casos 2.90 y el mejor 3.50, considerándose la mayoría de los usuarios, neutrales a las preguntas de la encuesta. Entre los comentarios que hicieron los usuarios (véase **Anexo I**), algunos mencionaron que el sistema no contaba con logos ni recomendaciones de seguridad, y que en algún apartado presentaba fallas ortográficas, evidenciándose que

existen muchas mejoras que pueden hacerse a la plataforma del **FONDUC** en materia de seguridad y usabilidad.

5.2.2 Análisis de desempeño de la Evaluación Heurística a cargo de Auditores

El método de evaluación determinado en esta investigación ha sido el método de evaluación heurística que ha sido determinado a través de la literatura. Moallem. **[95]** permite evidenciar las ventajas de este método, destacando su rápida aplicabilidad y bajos costos operacionales.

Una vez realizada la evaluación por parte de los auditores, quienes bajo su criterio evaluaron la plataforma del **FONDUC** con las sub-heurísticas propuestas en esta investigación. A continuación, se muestra el grado de USec obtenido en cada requerimiento por cada una de las evaluaciones, diligenciadas por tres (3) auditores.

Cuando se llevan a cabo evaluaciones por criterios de un sitio web, un número de tres a cinco auditores es suficiente, pero este número puede ser incrementado si la usabilidad es un criterio prioritario a evaluar **[76]**, para este estudio de caso se busca evaluar seguridad y usabilidad en conjunto por lo cual se opta por solicitar la colaboración de sólo tres de ellos.

La evaluación heurística contó con una duración de dos (2) a tres (3) horas, ya que los auditores 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 (véase **Anexo C**).

Una vez hecha la recolección de datos, se procede a realizar los cálculos a través del modelo matemático expuesto a lo largo del **Capítulo 4**. Seguidamente, se obtienen los resultados para la USec expresados en la siguiente *tabla*.

REQ_ID	AUDITOR 1		AUDITOR 2		AUDITOR 3	
	USec	Cualitativo	USec	Cualitativo	USec	Cualitativo
1	156,60	Violación Menor	165,87	Violación Menor	43,11	Catástrofe
2	159,96	Violación Menor	179,49	Violación Insignificante	14,44	Catástrofe
3	172,87	Violación Insignificante	17,89	Catástrofe	17,89	Catástrofe
4	62,37	Violación Mayor	89,45	Violación Moderada	121,31	Violación Menor
5	159,51	Violación Menor	167,28	Violación Insignificante	200,00	Violación Insignificante
6	126,87	Violación Menor	133,97	Violación Menor	116,33	Violación Moderada
7	40,92	Violación Mayor	52,57	Violación Mayor	30,53	Catástrofe
8	149,76	Violación Menor	60,76	Violación Mayor	24,00	Catástrofe
9	66,02	Violación Mayor	135,69	Violación Menor	52,26	Violación Mayor

10	139,69	Violación Menor	139,69	Violación Menor	200,00	Violación Insignificante
11	49,23	Violación Mayor	95,86	Violación Moderada	89,39	Violación Moderada
12	119,22	Violación Moderada	0,00	Catástrofe	150,80	Violación Menor
13	4,75	Catástrofe	33,07	Catástrofe	100,00	Violación Moderada
14	15,46	Catástrofe	68,67	Violación Mayor	0,00	Catástrofe
15	78,05	Violación Mayor	99,41	Violación Moderada	32,25	Catástrofe
16	173,76	Violación Insignificante	38,59	Catástrofe	38,48	Catástrofe
17	8,33	Catástrofe	8,33	Catástrofe	8,33	Catástrofe
18	106,56	Violación Moderada	90,56	Violación Moderada	90,56	Violación Moderada
19	74,82	Violación Mayor	49,01	Violación Mayor	49,01	Violación Mayor
20	79,99	Violación Mayor	192,03	Violación Insignificante	192,03	Violación Insignificante
21	30,80	Catástrofe	178,54	Violación Insignificante	178,54	Violación Insignificante
22	29,33	Catástrofe	0,00	Catástrofe	0,00	Catástrofe
23	78,22	Violación Mayor	127,11	Violación Menor	127,11	Violación Menor

Tabla 42. Resultados USec - FONDUC

Es necesario aclarar, que en esta investigación antes de evaluar la plataforma del **FONDUC**, uno de los objetivos principales se centraba en evaluar el desempeño de los principios de USec y el modelo matemático propuestos. Para ello fue necesario determinar qué tan relacionados se encontraban los resultados obtenidos por cada auditor.

Entonces, continuando con el concepto del espacio dimensional considerado a partir de la literatura en el modelo matemático, es posible establecer un grado de relación en el resultado de las tres (3) evaluaciones, según como se indica a continuación:

- Si se toma el número 23 (número de requerimientos) como el número de dimensiones del espacio euclidiano, se puede definir cada calificación de los auditores como un punto en dicho espacio, a través de lo mencionado, es posible realizar el cálculo de la distancia euclidiana.

- Sea $\boldsymbol{P1}(\boldsymbol{USec_1}, \boldsymbol{USec_2}, \dots, \boldsymbol{USec_{23}})$ los resultados de la evaluación del auditor 1, $\boldsymbol{P2}(\boldsymbol{USec_1}, \boldsymbol{USec_2}, \dots, \boldsymbol{USec_{23}})$ los resultados de la evaluación del auditor 2 y $\boldsymbol{P3}(\boldsymbol{USec_1}, \boldsymbol{USec_2}, \dots, \boldsymbol{USec_{23}})$ los resultados de la evaluación del auditor 3.

- Cuanto menor sea la distancia euclidiana entre los puntos respecto al peor de los casos, se puede concluir que las evaluaciones en conjunto tienden a presentar mayor grado de similitud.

- Para determinar el peor de los casos se parte de que los valores de USec varían entre 0 y 200 según la escala establecida (véase **Apartado 4.4.4**), con lo cual el mayor valor de la distancia euclidiana que se puede presentar entre dos puntos está

indicado por el escenario en que uno de los puntos se encuentre en el origen cuyos valores de USec sean 0 y el otro punto se encuentre en el otro extremo, es decir con todos los valores de USec en 200, por lo tanto, la distancia euclidiana en el peor de los casos estaría dada por:

$$\boldsymbol{DE} = \sqrt{(200-0)^2 * 23}$$
$$\boldsymbol{DE} = 959.1663047$$

- A partir de este valor se puede establecer un grado de relación entre los tres puntos $\boldsymbol{P1, P2\ y\ P3}$, y se procede a calcular la distancia euclidiana entre $\boldsymbol{P1}$ y $\boldsymbol{P2}$, $\boldsymbol{P1}$ y $\boldsymbol{P3}$, $\boldsymbol{P2}$ y $\boldsymbol{P3}$, presentándose los siguientes resultados:

	Valor	Porcentaje respecto al peor de los casos (959.1663047)	Porcentaje de similitud entre evaluaciones	Variación entre porcentajes de similitud
$DE_{P1,P2}$	339,91	35,44%	64,56%	No mayor a 9%
$DE_{P1,P3}$	305,99	40,90%	59,10%	
$DE_{P2,P3}$	392,33	31,90%	68,10%	

Tabla 43. Comparación calificaciones auditores

Como se puede observar, las distancias euclidianas en la tabla anterior (véase **Tabla 43**) al ser comparadas con el peor de los casos, representan pequeños porcentajes, pudiéndose determinar que existe una cercanía considerable entre los tres puntos, por lo tanto, es posible concluir que los auditores 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 en el **Capítulo 4**.

5.2.3 Resultados referentes a la plataforma virtual – FONDUC

En cuanto al desempeño de la plataforma se refiere, primero se procede a obtener los promedios de los valores de USec de cada auditor por cada requerimiento, a fin de obtener una valoración y conclusión a nivel general correspondiente a la evaluación heurística, los resultados son presentados en al siguiente *tabla*.

REQ_ID	EVALUADOR 1	EVALUADOR 2	EVALUADOR 3	Promedios	
	USec	USec	USec	Usec	Cualitativo
1	156,6	165,87	43,11	121,86	Violación Menor
2	159,96	179,49	14,44	117,96	Violación Moderada
3	172,87	17,89	17,89	69,55	Violación Mayor
4	62,37	89,45	121,31	91,04	Violación Moderada
5	159,51	167,28	200	175,6	Violación Insignificante
6	126,87	133,97	116,33	125,72	Violación Menor

7	40,92	52,57	30,53	41,34	Violación Mayor
8	149,76	60,76	24	78,17	Violación Mayor
9	66,02	135,69	52,26	84,66	Violación Moderada
10	139,69	139,69	200	159,79	Violación Menor
11	49,23	95,86	89,39	78,16	Violación Mayor
12	119,22	0	150,8	90,01	Violación Moderada
13	4,75	33,07	100	45,94	Violación Mayor
14	15,46	68,67	0	28,04	Catástrofe
15	78,05	99,41	32,25	69,9	Violación Mayor
16	173,76	38,59	38,48	83,61	Violación Moderada
17	8,33	8,33	8,33	8,33	Catástrofe
18	106,56	90,56	90,56	95,89	Violación Moderada
19	74,82	49,01	49,01	57,61	Violación Mayor
20	79,99	192,03	192,03	154,68	Violación Menor
21	30,8	178,54	178,54	129,29	Violación Menor
22	29,33	0	0	9,78	Catástrofe
23	78,22	127,11	127,11	110,81	Violación Moderada

Tabla 44. Calificación general del sistema

Con base en la columna promedios de la ***Tabla 44***, continuación se presenta una síntesis de los resultados obtenidos (véase **Tabla 45**).

Cualitativo	Numero de Requerimientos	REQ_ID	Valoración
Catástrofe	3	14,17,22	Para estos requerimientos el potencial de impacto es SEVERO, por lo tanto, es imperativo solucionar los problemas que se presentan de manera inmediata
Violación Mayor	7	3, 7, 8, 11, 13, 15, 19	Para estos requerimientos el potencial de impacto es ALTO, por lo tanto, es importante solucionar los problemas dándoles una prioridad alta.
Violación Moderada	7	2, 4, 9, 12, 16, 18, 23	Para esto requerimientos el potencial de impacto es MODERADO, por lo tanto, los problemas que se presenten pueden ser solucionados dándoles una prioridad media.
Violación Menor	5	1, 6, 10, 20, 21	Para esto requerimientos el potencial de impacto es BAJO, por lo tanto, los problemas que se presenten pueden ser solucionados dándoles una prioridad baja.
Violación Insignificante	1	5	Para estos requerimientos el potencial de impacto es MUY BAJO, los inconvenientes que se presenten pueden ser solucionados dándoles una prioridad muy baja.

Tabla 45. Síntesis calificación general

A partir de la ***Tabla 45***, la plataforma del **FONDUC** requiere mejoras considerables. En promedio 14 de los 23 requerimientos, se encuentran clasificados en categorías cualitativas que comprometen significativamente la seguridad y usabilidad del sistema, por lo tanto, es

trascendental considerar las sub-heurísticas asociadas a los requerimientos, para realizar las mejoras pertinentes que permitan un cumplimiento más adecuado de los requerimientos en cuestión y minimicen los riesgos que implican.

	Promedios	Cualitativo	Valoración General de la Plataforma
USec Auditor 1	90,5691304	Violación Moderada	En promedio el potencial de impacto en cuanto a desempeño de la plataforma es MODERADO, por lo tanto, los problemas que se presenten, en su mayoría, pueden ser solucionados dándoles una prioridad media.
USec Auditor 2	92,3408696	Violación Moderada	
USec Auditor 3	81,5813043	Violación Moderada	
Promedio USec	88,1626087	Violación Moderada	

Tabla 46. Resultado final, USec general

Ahora bien, calculando a través de un promedio el valor USec general obtenido por cada auditor como se muestra en la ***Tabla 46***, se puede notar una similitud entre cada uno de ellos, incluyendo los promedios generales de la última columna de la ***Tabla 44***, por lo tanto, se puede 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.

Finalmente, en vista de los resultados obtenidos en el cuestionario de satisfacción (véase **Apartado 5.2.1**), donde se evidencia que los usuarios a pesar de tener amplios conocimientos en el uso de estos sistemas debido a su perfil profesional (véase **Apartado 5.1.2**), no se encuentran totalmente satisfechos y manifiestan que han tenido mejor experiencia en el manejo de las plataformas de otras entidades bancarias en comparación con la del **FONDUC**. Se pone en evidencia que el sistema en cuestión requiere atención en seguridad y usabilidad, de manera que se garantice una mejor experiencia de usuario. En este punto es donde la evaluación heurística de Seguridad Usable juega un papel fundamental al momento de decidir qué características y funciones deben ser intervenidas en el aplicativo **FONDUC**, ya que al obtener los resultados de la evaluación de un listado de requerimientos específicos, es posible determinar la prioridad con la estos deben ser atendidos, si es necesario. Inicialmente, los principales autores de esta investigación se han comprometido a entregar un *documento*[2] que contenga las recomendaciones a la plataforma FUNDUC, producto de los resultados de esta investigación. Será el encargado de los aspectos técnicos y funcionales de la plataforma quien realice un informe basándose en el *documento de recomendaciones*, al gerente de la entidad **FONDUC**, con la intención de que se tomen los correctivos necesarios, si así lo consideran.

[2] El documento es confidencial, por esta razón, no puede ser evidenciado en los anexos.

5.3 RECOMENDACIONES PARA APLICACIÓN FUTURA

A manera general, si alguna organización bancaria decide optar por realizar pruebas piloto tomando como referencia esta investigación, es necesario aclarar que se cuenta con un componente de percepción de satisfacción (véase **Anexo H**) que adquirirá una relevancia importante, pues permitirá identificar algunas falencias, si se presentan, en el aplicativo e-Banking, luego, al someter el aplicativo a las calificaciones del número de auditores recomendados por esta investigación y obtener los valores de USec para cada requerimiento, será necesario presentar un informe a la entidad que argumente los valores obtenidos, contrastándolos con el componente de la satisfacción del usuario, y así, los entes encargados de la toma de decisiones, junto al analista de sistemas de información, se encontrarán en potestad de tomar correctivos frente a los requerimientos que presenten una debilidad de seguridad o usabilidad, si lo consideran pertinente.

Capítulo 6

Conclusiones, limitaciones y trabajo futuro

Los artefactos generados en este capítulo, pueden ser evidenciados en el Sprint 6, de la metodología (véase **Anexo L**).

Este capítulo presenta las conclusiones a las que se ha llegado mediante el desarrollo del presente trabajo de investigación y del cumplimiento de sus objetivos. Posteriormente se presentan las limitaciones y trabajos futuros caracterizados por ser oportunidades para afianzar y potencializar la investigación que hasta el momento se ha desarrollado.

6.1 CONCLUSIONES

En esta sección se presentan las conclusiones del presente trabajo de Investigación. Estas se irán desarrollando en orden de importancia. Para la construcción de estas conclusiones se realizó un análisis por cada capítulo recopilando las deducciones más importantes que surgieron en el desarrollo de los mismos. Las conclusiones finales se presentan a continuación.

1. El área de investigación HCISec se proyecta a futuro como un campo investigativo que a través de sus propuestas, logrará minimizar los inconvenientes que se presentan al exponer dos atributos que en algunas ocasiones resultan siendo contradictorios.
2. De los resultados obtenidos es posible afirmar que se manifiestan de manera apropiada, teniendo en cuenta que se trata de una primera propuesta, y concluyendo que, el conjunto de sub-heurísticas puede ser aplicado para realizar la evaluación de otros sistemas e-Banking.
3. A través de esta investigación, se logra validar requerimientos fundamentales de e-Banking, al ser sometidos a criterio de expertos para ajustar sus porcentajes de influencia sobre cada uno de los requerimientos.
4. El modelo matemático empleado en esta investigación, reúne conceptos que son aplicados en muchas técnicas referentes al área tecnológica, además, ha sido construido con el apoyo de un matemático, razón por la cual, se puede considerar un atractivo punto de inicio para desarrollar mayores investigaciones en el campo de HCISec.

5. El modelo matemático ha arrojado resultados con gran similitud durante su validación realizada por parte de auditores, es prioritario tener en cuenta que los resultados generales presentan una incertidumbre menor al 10%. Teniendo en cuenta los factores de subjetividad que se manejan en el campo de la USec, se puede concluir que con una incertidumbre menor al 10% con respecto a las calificaciones generales de USec el modelo parece ser confiable.
6. Por medio del modelo matemático, es posible validar sub-heurísticas que estén presentes en el contexto de e-Banking, sin embargo, esta validación depende de una gran cantidad de interesados (Expertos, Auditores, Usuarios).
7. El modelo matemático que surge de esta investigación, puede resultar difícil de comprender por los conceptos que se asocian, en muchas ocasiones es recomendable estudiar los ejemplos más de una vez para despejar las dudas, además, implica determinar considerables factores para lograr una adecuada precisión.
8. Las propuestas para la medición de la USec encontradas en la literatura conservan la característica de subjetividad, sin embargo, algunas propuestas que intenta reducir dicha características, no han sido validadas o son demasiado complejas.
9. La propuesta de investigación, logra reducir la subjetividad que se presenta al evaluar los atributos de seguridad y usabilidad, ya que provee herramientas a los auditores o evaluadores, que permiten diferenciar los atributos de manera singular.

6.2 LIMITACIONES

1. Se añade alto grado de dificultad al momento de hallar auditores, que sean expertos en las áreas de seguridad y/o usabilidad, y que a su vez, sean usuarios de una misma entidad financiera que preste el servicio de e-Banking.
2. Cuando se pretende evaluar sistemas e-Banking, poder acceder a la plataforma con un permiso adecuado que sea otorgado por la administración de la entidad financiera, en ocasiones parecerá imposible, debido a las grandes cifras de dinero y exposición a datos sensibles.
3. La exposición a datos sensibles y a grandes cifras de dinero, crean una percepción negativa en los usuarios cuando son cuestionados para llevar a cabo una participación voluntaria que implique a su entidad financiera, por esta razón, muchos de los usuarios tienden a rechazar las invitaciones que impliquen su información personal y financiera.
4. El proceso para analizar los resultados referentes al modelo matemático empleado para el cálculo de la USec, puede demandar una cantidad de tiempo considerable.
5. Es necesario destacar que esta investigación ha dependido netamente de la colaboración de personas afines a las áreas de seguridad y usabilidad, además de la disposición de un gran número de personas para llevar a cabo la realización de todos los artefactos, por lo tanto, la investigación en el campo de HCISec para

resolver problemas con respecto a los atributos seguridad y usabilidad de sistemas e-Banking, podría llegar a ser extenuante debido a que los implicados de la realización de trabajos de investigación en esta área, dependen de la colaboración de diferentes disciplinas y la disponibilidad del tiempo de los participantes y en muchas ocasiones resultan esperas bastante prolongadas que pueden retrasar el trabajo en cuestión.

6.3 TRABAJO FUTURO

1. Generar un análisis de riesgos a partir de los atributos que se exponen en el modelo matemático.
2. Someter el valor de la importancia de las sub-heurísticas a criterio de expertos para hallar valores cuantitativos más precisos.
3. Validar el modelo matemático con aplicaciones e-Banking.
4. Validar el modelo a través de la consideración de aplicaciones e-Commerce.
5. Añadir más atributos al modelo matemático con el propósito de mejorar la precisión que se obtiene en los resultados.
6. Generar un semillero de investigación para trabajar en mutuo beneficio con la colaboración de futuros matemáticos e ingenieros.
7. Adecuar el modelo matemático para que sea más sencillo de usar.
8. Contar con evaluadores que manejen las dos áreas seguridad y usabilidad simultáneamente.

REFERENCIAS BIBLIOGRAFICAS

[1] C. Altin Gumussoy, “Usability guideline for banking software design,” Comput. Human Behav. vol. 62, pp. 277–285, 2016.

[2] M. Ramachandran, “Software security requirements management as an emerging cloud computing service,” Int. J. Inf. Manage., vol. 36, no. 4, pp. 580–590, 2016.

[3] G. Dhillon, T. Oliveira, S. Susarapu, and M. Caldeira, “Deciding between information security and usability: Developing value based objectives,” Comput. Human Behav. vol. 61, pp. 656–666, 2016.

[4] A. Whitten and J. D. Tygar, “Usability of Security : A Case Study,” Science. no. 102590, 1998.

[5] S. L. Garfinkel, “Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable by. Gene, 31, 1987, 13-40 (Chapter 1, Chapter 2).

[6] R. Kainda, I. Flechais, and a. W. Roscoe, “Security and usability: Analysis and evaluation,” ARES 2010 - 5th International Conference on Availability, Reliability, and Security, 2010, 275–282.

[7] J. Johnston, J. H. P. Eloff, and L. Labuschagne, “Security and human computer interfaces,” Computers & Security, 22(8), 675–684.

[8] S. Chiasson, P. van Oorschot, and R. Biddle, “Even experts deserve usable security: Design guidelines for security management systems,” SOUPS Workshop on Usable IT Security Management, (July), 7–10.

[9] C. a. Fidas, A. G. Voyiatzis, and N. M. Avouris, “When security meets usability: A user-centric approach on a crossroads priority problem,” Proceedings - 14th Panhellenic Conference on Informatics, PCI 2010, 112–117.

[10] W. Chaouali, I. Ben Yahia, and N. Souiden, “The interplay of counter-conformity motivation, social influence, and trust in customers’ intention to adopt Internet banking services: The case of an emerging country,” Journal of Retailing and Consumer Services, 28, 209–218.

[11] M. Hertzum, “Usable security and e-banking: ease of use vis-à-vis security,” (December), 52–65.

[12] C. Möckel, “Usability and security in EU e-banking systems - Towards an integrated evaluation framework,” Proceedings - 11th IEEE/IPSJ International Symposium on Applications and the Internet, SAINT 2011, 230–233.

[13] C. Möckel, “Human-Computer Interaction for Security Research: The Case of EU E-Banking Systems 1 The Role of Security and Usability in Current EU E-Banking,” Ifip International Federation For Information Processing, 2012, 406–409.

[14] M. Mujinga, M. M. Eloff, and J. H. Kroeze, “Towards a heuristic model for usable and secure online banking,” in Hepu Deng and Craig Standing (ed.) ACIS 2013: Information systems: Transforming the Future: Proceedings of the 24th Australasian Conference on Information Systems, Melbourne, Australia, 4-6 December, 2013, pp. 1-12.

[15] M. Sasse, “Usability and trust in information systems,” Trust and Crime in Information Societies, 2005, 319–348.

[16] A. Adams, “Shouldn’t All Security Be Usable?,” Test, April 2011 doi:10.1109/MSP.2011.30.

[17] M. E. Zurko and R. T. Simon, “User-centered security,” Proceedings of the 1996 Workshop on New Security Paradigms - NSPW ’96, 1996, 27–33.
[18] B. Shackel, “Applied Ergonomics Handbook,” Guildford: IPC Science and Technology Press. ISBN 0902852388, 1975, 101-122 (Chapter 14, Chapter 15)
[19] T. Ibrahim, S. Furnell, M. Papadaki, and N. Clarke, “Assessing the usability of personal internet security tools" in 8th European Conference on Information Warfare and Security, 2009.
[20] M. Mannan and P. C. Van Oorschot, “Security and Usability : The Gap in Real-World Online Banking,” Proceeding NSPW ’07 Proceedings of the 2007 Workshop on New Security Paradigms, 2008, 1–14.
[21] J. R. C. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, “Guidelines for usable cybersecurity: Past and present,” Proceedings - 2011 3rd International Workshop on Cyberspace Safety and Security, 2011, 21–26.
[22] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, “Usable security: User preferences for authentication methods in eBanking and the effects of experience,” Interacting with Computers, 22(3), 2010, 153–164.
[23] B. Shneiderman, “Designing the User Interface: Strategies for Efective Human-Computer Interaction,” J. Dubau and A. Willner, Eds. Addison-Wesley Publishing Company, 1998.
[24] J. Nielsen, “Introduction to usability,” Nielsen Norman Group. [Online]. Available: http://www.nngroup.com/articles/usability-101-introduction-to-usability/, [Accessed: 05- Feb- 2016].
[25] A. Dix, J. Finlay, G. Abowd, and R. Beale, “Human-Computer Interaction,” 3rd ed. ISBN-10: 0-13-046109-1. Prentice-Hall, 2004. 258-287.
[26] Y. Rogers, H. Sharp, and J. Preece, “Interaction Design: Beyond Human-Computer Interaction,” J. W. Sons, Ed. Rogers Sharp ISBN 0-471-49278-7, 2011. 1-160.
[27] K. Yee, “User interaction design for secure systems,” May 2002, 278–290.
[28] 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, 394-407.
[29] J. Saltzer and M. Schroeder, “The protection of information in computer systems," in Security and Privacy on the Internet. ACM, 2000.
[30] D. Katsabas, S. Furnell, and P. Dowland, “Using human computer interaction principles to promote usable security," in 5th International Network Conference, 2005.
[31] A. Zhou, J. Blustein, and N. Zincir-Heywood, “Improving intrusion detection systems through heuristic evaluation," in Canadian Conference on Electrical and Computer Engineering, vol. 3. IEEE, May 2004, 1641-1644.
[32] 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.
[33] S. Furnell, “Security usability challenges for end-users,” in Social and Human Elements of Information Security: Emerging Trends and Countermeasures. IGI Global, 2009. ISBN 978-1-60566-037-0, 179–195.
[34] S. Furnell, “Security usability challenges for end-users,” in Social and Human Elements of Information Security: Emerging Trends and Countermeasures. IGI Global, 2009. ISBN 978-1-60566-037-0, 196–219.

[35] Oxford Dictionary. "Oxford English Dictionary Online," Oxford University Press. http://www.oxforddictionaries.com/definition/english/heuristic, [Accessed: 06- Feb- 2016].
[36] M. Bishop, "Security and Usability: Designing Secure Systems that People Can Use," Psychological acceptability revisited. In L. F. Cranor & S. L. Garfinkel Eds., Sebastopol, CA: O'Reilly Media, ISBN: 9780596008277, Inc., 2005, 1-13.
[37] L. Bonastre and T. Granollers, "A Set Of Heuristics for User Experience Evaluation in E-commerce Websites," ACHI 2014: The Seventh International Conference on Advances in Computer-Human Interactions, (c), 2014, 27–34.
[38] P. Runeson and M. Höst, "Guidelines for conducting and reporting case study research in software engineering," Empirical Software, Engineering, 2009.
[39] M. Hicks, J.S. Foster, "Adapting Scrum to Managing a Research Group, ", 2008
[40] K. Schwaber and M. Beedle, "Agile Software Development with Scrum," 1st ed., ISBN 0130676349, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2001, 1-135.
[41] B. Tognazzini, "Security and Usability: Designing Secure Systems that People Can Use," Psychological acceptability revisited. In L. F. Cranor & S. L. Garfinkel Eds., Sebastopol, CA: O'Reilly Media, ISBN: 9780596008277, Inc., 2005, 31-46.
[42] A. Adams and M. A. Sasse, "Users Are Not the Enemy," Communications of the ACM, vol. 42, ACM Press, 1999, 40–46.
[43] I. Flechais and M. A. Sasse, "Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science," Int. J. Hum. Comput. Stud., vol. 67, no. 4, pp. 281–296, 2009
[44] M. L. Unda "Sistema de internet banking para el banco de Guayaquil," Repositorio de Espol – Escuela Superior Politécnica del Litoral, 2001. Available: http://www.dspace.espol.edu.ec/xmlui/handle/123456789/3198, [Accessed: 19- May- 2016].
[45] J. Iyengar and M. Belvalkar, "Case study of online banking in India: User behaviors and design guidelines," IFIP Adv. Inf. Commun. Technol., vol. 316, pp. 180–188, 2010.
[46] F. S. AlAbdullah, F. H. Alshammari, R. Alnaqeib, H. A. Jalab, A. A. Zaidan, and B. B. Zaidan, "Analytical Study on Internet Banking System," vol. 2, no. 6, pp. 140–146, 2010.
[47] B. J. Fajfr, "Design and implementation of online banking system for near future," Czech Technical University in Prague, 2012, Available: https://dip.felk.cvut.cz/browse/pdfcache/fajfrjan_2012dipl.pdf, [Accessed: 19- May- 2016].
[48] A. Babatunde "DESIGN AND IMPLEMENTATION OF ONLINE BANKING SYSTEM, (A CASE STUDY OF MAY FRESH SAVINGS AND LOANS BANK CARITAS UNIVERSITY, ENUGU)," Caritas University, 2012, Available: http://pubs.caritasuni.edu.ng/download.php?file=projects/2011-2012%20Projects/Computer%20Engineering/DESIGN_AND_IMPLEMENTATION_OF_ONLINE_BANKING_SYSTEM.pdf, [Accessed: 19- May- 2016].
[49] D. Abrazhevich, P. Markopoulos, and M. Rauterberg, "Designing Internet-Based Payment Systems: Guidelines and Empirical Basis," Human-Computer Interact, vol. 24, no. 4, pp. 408–443, 2009.
[50] Monetary Authority of Singapore, "INTERNET BANKING AND TECHNOLOGY RISK MAGAMENT GUIDELINES," vol. 3, pp. 1-43, 2008, Available: http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stabilit

y/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/IBTRMV3.ashx, [Accessed: 23- May- 2016].

[51] J. P. Carvallo, X. Franch, C. Quer, "Calidad del producto y proceso software", RA-MA S.A. Editorial y Publicaciones, ISBN: 9788478979615, pp. 287-313, 2010.

[52] W. Sanchez, "La usabilidad en Ingeniería de Software: definición y características," Agesic, pp. 7–21, 2011.

[53] Systems and software engineering — Systems and software quality requirements and evaluation (SQuaRE) — Measurement of quality in use, ISO/IEC 25022:2016.

[54] Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability, ISO 9241-11:1998.

[55] J. Ferrer and J. Fernandez, "Seguridad informática y software libre," Hispalinux. Available: http://es.tldp.org/Informes/informe-seguridad-SL/informe-seguridad-SL.pdf, [Accessed: 04- Mar- 2016].

[56] Ergonomics of human-system interaction. Part 171: Guidance on software accessibility, ISO 9241-171:2008.

[57] C.I.D.A.T, "accesibilidad de páginas web, " 2013, Available: ftp://ftp.once.es/pub/utt/bibliotecnia/Accesibilidad/webs/AccesibilidadWeb2013.pdf, [Accessed: 04- Mar- 2016]

[58] M. F. Bertoa, J. M. Troya, and A. Vallecillo, "Measuring the usability of software components," J. Syst. Softw., vol. 79, no. 3, pp. 427–439, 2006.

[59] Ergonomics of human-system interaction. Part 110: Dialogue principles, ISO 9241-110:2006.

[60] H. Pham, "System Software Reliability, " British Library Cataloguing in Publiction Data, ISBN: 978-1-84628-295-9, pp. 1-16, 2008.

[61] J. Nielsen, "Usability inspection methods," Conf. companion Hum. factors Comput. Syst. - CHI '94, vol. 25, no. 1, pp. 413–414, 1994.

[62] S. Mtimkulu, J. Biljon and T. Dyk, "Designing for the Functionality South African Internet Banking Websites should provide to address the Needs of Generation-Y users," no. July, p. 313, 2014.

[63] M. Maguire, "Context of Use within usability activities," *Int. J. Hum. Comput. Stud.*, vol. 55, no. 4, pp. 453–483, 2001.

[64] R. K. Srivastava, "Customer's perception on usage of internet banking", *Innovative Marketing* ., vol. 3, no. 4, pp. 67–73, 2007.

[65] F. S. AlAbdullah, F. H. Alshammari, R. Alnaqeib, H. A. Jalab, A. A. Zaidan, and B. B. Zaidan, "Analytical Study on Internet Banking System," vol. 2, no. 6, pp. 140–146, 2010.

[66] H. H. Bauer, M. Hammerschmidt, and T. Falk, "Measuring the quality of e-banking portals," *Int. J. Bank Mark.*, vol. 23, no. 2, pp. 153–175, 2005.

[67] Authority Monetary of Singapore, "Technology Risk Management Guidelines," no. June, 2013.

[68] J. Fajfr, "Design and implementation of online banking system for near future", *Czech Technical University in Prague - Department of Computer Science and Engineering*, 2012.

[69] A. B. Oluwayomi, "design and implementation of online banking system, (a case study of may fresh savings and loans bank caritas university, enugu)" - Caritas University/Department Of Computer Engineering, 2012.

[70] D. Abrazhevich, P. Markopoulos, and M. Rauterberg, "Designing Internet-Based Payment Systems: Guidelines and Empirical Basis," *Human-Computer Interact.*, vol.

24, no. 4, pp. 408–443, 2009.
[71] J. Iyengar and M. Belvalkar, “Case study of online banking in India: User behaviors and design guidelines,” *IFIP Adv. Inf. Commun. Technol.*, vol. 316, pp. 180–188, 2010.
[72] Monetary Authority of Singapore, "Internet Banking And Technology Risk Management Guidelines” no. June, 2008.
[73] P. C. Realpe, C. A. Collazos, and T. Granollers, “A Set of Heuristics for Usable Security and User Authentication.”, no. September, 2016
[74] P. C. Realpe, C. A. Collazos, J. Hurtado, T. Granollers, and J. V. Medina, “An Integration of Usable Security and User Authentication into the ISO 9241-210 and ISO/IEC 25010:2011,” pp. 65–76, 2016.
[75] C. Altin Gumussoy, “Usability guideline for banking software design,” *Comput. Human Behav.*, vol. 62, pp. 277–285, 2016.
[76] H. M. G. Rene Pulido Granados, “a Model for ,Easuring and Evaluating the Usability of Web Sites in Colombia Virtual Banking Services,” *Eng. Uiversity*, vol. 12, no. 1, pp. 81–102, 2008.
[77] Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models, ISO/IEC 25010:2011.
[78] J. M. Marete, H. P. Gommans, and G. E. George, “An Evaluation of EBanking Services on Customer Satisfaction : Case of National Bank of Kenya,” vol. 6, no. 22, pp. 228–239, 2014.
[79] F. Sahar, “Tradeoffs between Usability and Security,” *Int. J. Eng. Technol.*, vol. v 5, n 4, no. 4, 2013.
[80] C. Braz, A. Seffah, and D. M. Raihi, “Designing a Trade-Off Between Usability and Security: A Metrics Based-Model,” *Lect. Notes Comput. Sci.*, vol. 4663, pp. 114–126, 2007.
[81] M. Hub, J. Čapek, R. Myšková, and A. G. Principle, “Relationship between security and usability – authentication case study,” *Nternational J. Comput. Commun.*, vol. 5, no. 1, pp. 1–8, 2011.
[82] A. J. Aviv and D. Fichter, “Understanding visual perceptions of usability and security of Android’s graphical password pattern,” *Proc. 30th Annu. Comput. Secur. Appl. Conf. - ACSAC ’14*, pp. 286–295, 2014.
[83] L. Z. Aspiazu, “Development of a Model for Security and Usability,” no. July, pp. 1–74, 2013.
[84] A. Din, “Usable Security using GOMS: A Study to Evaluate and Compare the Usability of User Accounts on E-Government Websites,” *ProQuest Diss. Theses*, no. 45, 2015.
[85] A. Yeratziotis, “A FRAMEWORK TO EVALUATE USABLE SECURITY IN ONLINE SOCIAL NETWORKING,", *Nelson Mandela Metropolitan University - Faculty of Engineering, the Built Environment and Information Technology*, 2011.
[86] P. Jaferian, K. Hawkey, A. Sotirakopoulos, M. Velez-Rojas, and K. Beznosov, “Heuristics for Evaluating IT Security Management Tools,” *SOUPS ’11 Proc. Seventh Symp. Usable Priv. Secur.*, vol. 0024, no. June 2016, pp. 1–20, 2011.
[87] M. Mihajlov, “A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives,” *(NSS), 2011 5th,* pp. 332–336, 2011.
[88] M. Johnson, D. Paulusma, and E. J. van Leeuwen, “Algorithms for diversity and

clustering in social networks through dot product graphs," *Soc. Networks*, vol. 41, pp. 48–55, 2015.

[89] N. vom Stein, N. Sick, and J. Leker, "How to measure technological distance in collaborations - The case of electric mobility," *Technol. Forecast. Soc. Change*, vol. 97, pp. 154–167, 2015.

[90] E. Richard, B. Mead, E. Zlotnikov, H. Park, N. J. Us, D. Haders, and S. Nj, "(12) United States Patent," vol. 2, no. 12, pp. 19–35, 2011.

[91] Y. Kanellopoulos, P. Antonellis, C. Tjortjis, and C. Makris, "k-Attractors: A Clustering Algorithm for Software Measurement Data Analysis," *IEEE Int. Conf. Tools with Artif. Intell. 2007)*, pp. 358–365, 2007.

[92] G. Marion, "An Introduction to Mathematical Modelling," *University of Bristol - School of Mathematics*, 2008. Available: http://www.maths.bris.ac.uk/~madjl/course_text.pdf, [Accessed: 07-Jul- 2016].

[93] MathCentre, "Equations of straight lines," *Loughborough University - mathcentre*, pp. 1–11, 2009. Available: http://www.mathcentre.ac.uk/resources/uploaded/mc-ty-strtlines-2009-1.pdf, [Accessed: 07-Jul- 2016].

[94] A. Solano, "Metodología para la evaluación colaborativa de la usabilidad de sistemas software interactivos," [Ph.D. thesis], *Departamento de Sistemas, Universidad del Cauca, Popayán, Colombia,* 2015.

[95] A. Moallen, "Methods for Evaluating User Interfaces - Cognitive Walkthrough and Heuristics Evaluation,", *Computer Engineering Department, Santa Clara University, San José, United States,* 2004, Available: http://www.cse.scu.edu/~amoallem/archive/handouts/Session_7_MEUI.doc, [Accessed: 21-Oct- 2016]

[96] Open Web Security Project, "OWASP Top 10-2013", 2013, Available: https://www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf, [Accessed: 21-Oct- 2016].

[97] Information technology — Security techniques — Information security risk management, ISO/IEC 27005:2011