Evaluación Heurística de Seguridad Usable Aplicada en Sistemas e-Banking

Anexos

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

ANEXO A: Escala de clasificación adjetiva y numérica

Escala de clasificación ADJETIVA Y NUMÉRICA

En esta encuesta se pretende obtener una clasificación adjetiva y numérica de algunos atributos de la ISO/IEC 25010:2011 para sistemas donde sea necesario la usabilidad, seguridad, accesibilidad, desempeño, fiabilidad y operabilidad en el contexto de seguridad usable y autenticación de usuario

*Obligatorio

Perfil

Por favor ingrese los siguientes datos sobre su perfil.

¿Cuál es su ocupación actual? *

- ◯ Profesor
- ◯ Estudiante
- ◯ Otra: _____

¿Cuál es su grado académico actual? *

- ◯ PhD
- ◯ Maestría
- ◯ Universitario
- ◯ Otra: _____

¿Cuál es su linea de investigación? *

- ◯ UX
- ◯ Seguridad informática
- ◯ UX y Seguridad informática
- ◯ Otra: _____

Escala de clasificación ADJETIVA Y NUMÉRICA

*Obligatorio

Escala de clasificación ADJETIVA Y NUMÉRICA

En una evaluación adecuada el significado de una puntuación numérica es importante en todo proceso de medida. Aunque existen trabajos donde se presenta una escala de clasificación adjetiva y numérica para la usabilidad de un producto (e.g. System Usability Scale presenta un rango dentro de 0 a 100, donde 100 es el mejor absoluto y 0 es lo peor), es necesario también encontrar métricas más intuitiva sin ningún tipo de interpretación especial para un conjunto más amplio de atributos.
A partir del estado del arte se determinó 5 categorías para decidir el grado de calidad o estimación de un sistema a partir de los atributos presentados en la primera sección.

1. Excelente
2. Bueno
3. Moderado
4. Pobre
5. Muy pobre

Cada grado anterior representa un intervalo el cual debe estar dentro del rango entre 0 y 100. Por lo tanto, es importante aclarar que la escala de clasificación anterior debe cubrir todo el intervalo [0, 100] y cumplirse que 'Excelente' es el máximo superior del intervalo y 'Muy pobre' el mínimo inferior.
Por ejemplo, Muy pobre = [0 , 10), Pobre = [10, 40), Moderado = [40, 60), Bueno = [60, 90) y Excelente = [90, 100], donde '[' representa intervalo cerrado y ')' representa intervalo abierto (nota: este mismo ejemplo se puede aplicar para las siguientes secciones).

¿Cuál intervalo considera que debería estar el adjetivo 'Excelente' para cada uno de los atributos mencionados en la primera sección? *

Tu respuesta

¿Cuál intervalo considera que debería estar el adjetivo 'Bueno' para cada uno de los atributos mencionados en la primera sección? *

Tu respuesta

¿Cuál intervalo considera que debería estar el adjetivo 'Moderado' para cada uno de los atributos mencionados en la primera sección? *

Tu respuesta

¿Cuál intervalo considera que debería estar el adjetivo 'Pobre' para cada uno de los atributos mencionados en la primera sección? *

Tu respuesta

¿Cuál intervalo considera que debería estar el adjetivo 'Muy Pobre' para cada uno de los atributos mencionados en la primera sección? *

Tu respuesta

ANEXO B: Porcentaje de Influencia – Expertos

	PORCENTAJE DE INFLUENCIA											
	Experto 1		Experto 2		Experto 3		Experto 4		Experto 5		Experto 6	
REQ_ID	% U.	% S.	% U.	% S.	% U.	% S.	% U.	% S.	% U.	% .S	% U.	% S.
1	50	50	30	70	0	100	10	90	0	100	20	80
2	10	90	25	75	0	100	40	60	0	100	30	70
3	90	10	10	90	100	0	90	10	100	0	70	30
4	100	0	60	40	50	50	80	20	80	20	70	30
5	90	10	80	20	100	0	75	25	80	20	90	10
6	90	10	25	75	30	70	50	50	80	20	70	30
7	50	50	20	80	0	100	40	60	20	80	20	80
8	50	50	20	80	0	100	30	70	50	50	90	10
9	80	20	40	60	50	50	50	50	50	50	90	10
10	0	100	0	100	0	100	70	30	30	70	30	70
11	0	100	70	30	0	100	50	50	30	70	40	60
12	0	100	20	80	50	50	40	60	30	70	80	20
13	100	0	20	80	0	100	70	30	30	70	80	20
14	90	10	30	70	0	100	50	50	70	30	60	40

15	100	0	90	10	100	0	90	10	80	20	90	10
16	0	100	0	100	0	100	0	100	20	80	0	100
17	100	0	85	15	100	0	90	10	80	20	90	10
18	0	100	25	75	0	100	80	20	80	20	70	30
19	90	10	30	70	50	50	80	20	80	20	80	20
20	100	0	100	0	100	0	80	20	80	20	90	10
21	100	0	85	15	100	0	90	10	80	20	90	10
22	100	0	75	25	60	40	50	50	80	20	90	10
23	100	0	80	20	50	50	60	40	20	80	90	10

ANEXO C: Formulario de Evaluación – Auditores

C.1 Información

ORGANIZACIÓN HEURÍSTICA	
Las sub-heurísticas presentadas en este documento estan agrupadas teniendo en cuenta algunas facetas y atributos de la ISO/IEC 25010:2011. Estas sub-heurísticas se basan en seguridad usable y autenticación de usuario.	
FACETA	**DESCRIPCIÓN**
1. USABILIDAD	La faceta de usabilidad esta basado en las 10 reglas heurísticas de Nielsen y el principio transmitir características de Johnston et al. El principio de transmitir características informa al usuario de las características de seguridad disponibles, a diferencia del criterio de visibilidad del estado del sistema el cual le permite al usuario "ver" si estas características estan activas y están siendo usadas (para mayor información consultar el paper *Security and human computer interface*).
2. SEGURIDAD	El sistema tiene en cuenta 5 atributos importantes en cuanto a esta faceta: integridad, autenticidad, confidencialidad, registro y no repudio. Los aspectos anteriores estan basados en la ISO/IEC 25010:2011. En esta faceta tambien se tiene en cuenta los aspectos de privacidad.
3. OPERABILIDAD	Hace referencia a la cantidad de esfuerzo necesario para operar o controlar un método de autenticacion.
4. ACCESIBILIDAD	La accesibilidad asegura que sin importar la parte cognitiva, la movilidad y las habilidades sensoriales, puede utilizar un mecanismo de autenticación. Esto incluye discapacidades como el oído, la vista, la movilidad, el aprendizaje y el color, que son pertinentes en un contexto de autenticación.

5. FIABILIDAD	La fiabilidad indica la capacidad de realizar funciones específicas que permitan llevar a cabo una autenticación satisfactoria. En este aspecto también es importante tener en cuenta algunos aspectos de seguridad (integridad y confidencialidad), mantenimiento y soporte técnico.

C.2 Datos Evaluador

DATOS GENERALES DEL EVALUADOR	
Nombre del evaluador:	
Nivel de Estudios:	
Linea de investigación:	
Años de experiencia:	
Fecha de eval. (dd/mm/aa):	

C.3 Escala de evaluación e información de evaluación

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

Explicación de Evaluación
En las columnas *Usabilidad* y *Seguridad* que se encuentran en la hoja 'Formulario', se debe especificar un valor frente a cada heurística entre 0 y 100, teniendo en cuenta la escala expuesta, su explicación y su criterio como evaluador.

C.4 Formulario de Evaluación

Sub-heuristicas según Requerimiento				Valores	
REQ_ID	**Requerimiento**	**Atributo**	**Heurística asociada**	**U.**	**S.**
1	El sistema debe establecer una sesión segura entre la máquina del cliente y el servidor del banco, con cifrado de datos.	**Seguridad**	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?		
2	El sistema debe bloquear a los usuarios que superen el máximo número de intentos con la clave incorrecta.	**Seguridad**	S3- ¿El proceso de autenticación hace cumplir un límite de intentos de acceso no válidos consecutivos por un usuario?		
3	Una vez el usuario ingrese al sistema, se le debe presentar una vista con las diferentes opciones que le permitan usar los servicios.	**Usabilidad**	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?		
4	La sección de ayuda relevante debe proporcionar explicaciones de las medidas empleadas para garantizar la seguridad.	**Usabilidad**	U2- ¿La información de seguridad presentada en pantalla es relevante?		
			U11- ¿La información relacionada con la seguridad es presentada de una manera coherente y estandarizada?		
			U19- ¿La información necesaria para tomar una buena decisión de seguridad, es adecuada y está disponible antes de que se adopte la medida?		

			U22- ¿La información proporcionada por la ayuda es relevante?		
5	El sistema debe presentar la información mas relevante en letra grande y/o resaltada. Además, el lenguaje que se presente en él debe ser sencillo y conversacional.	**Usabilidad**	U9- ¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?		
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.)	**Usabilidad**	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?		
		Seguridad	S8- ¿El sistema hace cumplir el nivel de complejidad de la contraseña, con los requisitos mínimos exigidos?		
			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?		
		Accesibilidad	A3- En un proceso de autenticación, ¿el sistema evita esfuerzo adicional?		
7	El sistema debe informar al usuario sobre medidas de seguridad y proporcionar unas políticas de seguridad.	**Usabilidad**	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?		
		Seguridad	S9- ¿El sistema posee políticas de privacidad para comercio o contenido del usuario?		
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.	**Accesibilidad**	A2-¿El sistema evita el uso de claves aleatorias para la etapa de registro o autenticación?		
9	Si el usuario se equivoca al ingresar el usuario o la contraseña, el sistema debe mostrar un mensaje de	**Usabilidad**	U7-¿Las sentencias de alerta son simples, cortas y comprensibles?		

	alerta de Usuario y/o contraseña incorrecta		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?		
		Operabilidad	O2- En un proceso de autenticación, ¿este tiene palabras adecuadas para desarrollar una acción en particular?		
		Fiabilidad	F3- Si el proceso de inicio de sesión falla, ¿el sistema evita indicarle al usuario qué parte del proceso es incorrecto?		
10	El cliente debe haber iniciado sesión para estar habilitado a hacer transacciones o transferencia de fondos	**Seguridad**	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de 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).	**Usabilidad**	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?		
		Seguridad	S2- Si el sistema utiliza "cookies informáticos", ¿la información sobre la privacidad del sistema describe con precisión el uso de estas cookies?		
			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?		

			S7- ¿El sistema describe cada opción de privacidad en detalle?		
		Fiabilidad	F2- ¿Está claramente establecido el propósito de utilizar la información personal del usuario?		
12	El sistema debe permitir a los usuarios controlar las acciones críticas e información crítica	**Seguridad**	S5- ¿La información de privacidad del sistema garantiza al usuario el derecho a optar por compartir información no crítica con terceros?		
13	El sistema debe tomar medidas para hacer frente a los riesgos, e inmediatamente informar a los usuarios acerca de estas medidas.	**Usabilidad**	U24- ¿El sistema notifica a los usuarios si está interactuando con fuentes no confiables e interpone algún tipo de bloqueo que evita males mayores?		
		Seguridad	S6- ¿El sistema notifica y da posibles soluciones al usuario sobre vulnerabilidades asociados a incidentes de seguridad detectados?		
14	Proporcionar autenticación usable (OTP, Tokens, Biométrica, Multi-factor)	**Usabilidad**	U12- En un proceso de autenticación por conocimiento, ¿el sistema permite minimizar la carga de memoria para los usuarios?		
		Accesibilidad	A1- ¿El sistema permite usar passwords gráficos para usuarios con dificultades de lectura?		
			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?		
15	Las interfaces de usuario deben ser presentadas con una lógica clara y ser entendibles.	**Usabilidad**	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?		
		Fiabilidad	F1- ¿La interfaz ayuda al usuario a tener una experiencia segura y satisfactoria con el sistema?		

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.	**Usabilidad**	U25- ¿El sistema muestra logos de seguridad?		
			U26- ¿El sistema tiene certificados de seguridad otorgados por entidades externas reconocidas?		
		Operabilidad	O1- ¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?		
17	El sistema debe incluir las respectivas instrucciones para una adecuada interacción del usuario, en el sitio web u otros medios de comunicación.	**Usabilidad**	U21- ¿Hay una función de ayuda de seguridad visible?		
18	Después que un usuario se haya autenticado y obtenido acceso. El sistema debe asegurarse que el usuario pueda invocar unicamente la funciones que se le permiten (e.g. ver, escribir, ejecutar, modificar, crear y / o borrar datos).	**Seguridad**	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?		
19	El sistema debe implementar técnicas de prevención de errores.	**Usabilidad**	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?		
20	Claridad en los enlaces y en las etiquetas de los botones donde se sugiere la acción requerida.	**Usabilidad**	U3- ¿Los íconos de seguridad son identificables y diferenciables?		
			U4- ¿Las etiquetas de seguridad son sencillas, fáciles de entender y representativas?		

			U6- ¿El sistema está diseñado de manera que los botones con nombres similares, no desarrollen acciones de seguridad opuesto?		
			U20- ¿Los iconos de seguridad poseen etiqueta?		
21	Las interfaces de usuario deben presentar y destacar la información relevante en el contexto y en el momento correcto.	**Usabilidad**	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?		
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).	**Usabilidad**	U23- ¿El sistema provee soporte técnico en línea para solucionar problemas de seguridad?		
23	El sistema debe entragar retroalimentación (e.g. su dinero será transferido en 24 horas).	**Usabilidad**	U1- Después de que el usuario complete una acción de seguridad, ¿la realimentación indica que el siguiente grupo de acciones puede ser iniciado?		

C.5 Comentarios Generales

COMENTARIOS GENERALES	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

ANEXO D: Carta de Acompañamiento - Matemático

Popayán, Cauca, Colombia 03 de noviembre de 2016

A quien interese,

Yo Carlos Alberto Trujillo Solarte identificado con cédula de ciudadanía No. 10.532.448 de Popayán, en mi calidad de Licenciado en Matemáticas de la Universidad del Cauca, Magíster en Matemáticas de la Universidad del Valle y Doctor en Matemáticas de la Universidad Politécnica de Madrid, España, certifico el acompañamiento que he brindado al proceso de desarrollo referente al modelo matemático del estudio titulado "Evaluación Heurística de Seguridad Usable Aplicada en Sistemas e-Banking" perteneciente a los estudiantes, Andrés Felipe Gómez Daza y Andrés Felipe Orozco Orozco, apoyados de su director Ph.D(c). Paulo César Realpe Muñoz y codirector Ph.D. César Alberto Collazos Ordóñez, miembros del grupo de Investigación y Desarrollo en Ingeniería de Software - IDIS de la Universidad del Cauca – Popayán – Facultad Ingeniería Electrónica y Telecomunicaciones FIET.

Para constancia se firma en Popayán a los tres (03) días del mes de noviembre del año 2016

Carlos Alberto Trujillo Solarte
C.C No. 10.532.448 de Popayán

ANEXO E: Colaboración de Beneficio Mutuo – FONDUC

Colaboración de Beneficio Mutuo Recibidos x

Julio Ariel Hurtado Alegria <ahurtado@unicauca.edu.co> 16 may.

para Juan, mí, ANDRÉS

Apreciado Dr Vallejo,

Nos dirigimos a usted a través de este medio con la intención de establecer un puente de comunicación entre el grupo de investigación IDIS y el FONDUC que nos permita realizar algún trabajo conjunto y beneficioso para las partes.

Actualmente nuestro grupo viene desarrollando una propuesta para la "*Evaluación Heurística de Seguridad Usable Aplicada en Sistemas e-Banking*" y creemos que una evalaución a la solución virtual del fondo de profesores de la Universidad del Cauca (FONDUC) sería un escenario perfecto para validar nuestro enfoque y los resultados le resultarían útiles para mejorar las soluciones a través de su proveedor.

Estamos estableciendo, con los tesistas Andrés Orozco y Andrés Gómez, un trabajo que implica los aspectos de Seguridad y Usabilidad, aspectos que se encuentran presentes en las aplicaciones de banca electrónica, para el cual buscamos definir y evaluar un conjunto de heurísticas de seguridad usable en el contexto de e-Banking que permita contribuir en el diseño del sistema con respecto a su seguridad sin que se pierdan los aspectos de usabilidad.

La evaluación será realizada con una herramienta que habrá sido previamente diseñada para la evaluación de las reglas o heurísticas que también habrán sido seleccionadas previamente y no es invasiva en su sistema, por lo que no se tiene que exponer información confidencial.

Esperamos nos pueda atender para contarle más de la propuesta y ver como podemos dar inicio a alguna colaboración, si es de su interés el trabajo.

Cordialmente,

Julio Ariel Hurtado Alegría
Profesor Departamento de Sistemas
Investigador Grupo IDIS

Universidad del Cauca: Comprometidos con la calidad.

ANEXO F: Propuesta– FONDUC

Propuesta FONDUC

Evaluación Heurística de Seguridad Usable Aplicada en Sistemas e-Banking

Fecha: [19/08/2016]

Historial de Versiones

Fecha	Versión	Autor	Organización	Descripción
19/08/16	03	Orozco-Gómez	FIET- IDIS – UNICAUCA	Entregable

Información del Proyecto

Empresa / Organización	IDIS
Proyecto	Evaluación Heurística de Seguridad Usable Aplicada en Sistemas e-Banking
Fecha de preparación	
Cliente	FONDUC
Gerente / Líder de Proyecto	Andrés F. Orozco – Andrés F. Gómez

Resumen Ejecutivo

La siguiente propuesta tiene como intención establecer un puente de comunicación entre el grupo de investigación IDIS (Investigación y Desarrollo en Ingeniería de Software) y el FONDUC (Fondo de Profesores de la Universidad del Cauca) que permita realizar un trabajo conjunto y beneficioso para ambas partes.

Andrés Felipe Orozco Orozco y **Andrés Felipe Gómez Daza**, estudiantes pertenecientes a la FIET (Facultad de Ingeniería Electrónica y Telecomunicaciones) que actualmente cursan décimo semestre, se encuentran realizando un proyecto de grado que implica los aspectos de Seguridad y Usabilidad, aspectos que están presentes en las aplicaciones de Banca Electrónica, para las cuales se busca proponer y evaluar un conjunto de principios de Seguridad Usable que permita contribuir en el diseño de los sistemas con respecto a su Seguridad sin que se vean afectados los aspectos de Usabilidad.

A través del siguiente proyecto, se pondrán a prueba algunos hitos de la Banca Electrónica, buscando esclarecer los aspectos de Seguridad y Usabilidad presentes. Por tal motivo, es pertinente aclarar que en **NINGÚN** momento será necesario acceder a información confidencial de la institución o de los involucrados en el proyecto y que las pruebas que ahí se realicen **SÓLO** serán diligenciadas de **MANERA INDIVIDUAL** por el involucrado **SIN** acompañamiento. Luego de terminada la ejecución del proyecto, quedará a disposición del FONDUC las recomendaciones de Seguridad y Usabilidad, los resultados estadísticos obtenidos de la evaluación por parte de los expertos y el grado de satisfacción de los usuarios.

Este proyecto de investigación pretende apoyar a cualquier involucrado de los sistemas de Banca Electrónica y contribuir a la comunidad científica, al permitir la evaluación de la Seguridad y Usabilidad en estos sistemas.

Nuestro entendimiento

Teniendo en cuenta la necesidad de esclarecer los términos[1] que involucra esta propuesta, nos permitimos hacer mención de las definiciones de algunos de ellos:

Seguridad Informática

"El estado de estar protegido contra el uso delictivo o no autorizado de los datos electrónicos, o las medidas adoptadas para lograr esto."

Usabilidad

"El grado en que algo puede ser apto o no apto para su utilización."

Heurística

"Permite a una persona descubrir o aprender algo para sí mismos." Las heurísticas son generalmente usadas para representar características o aspectos del mundo real, facilitan la comprensión del problema en cuestión. (Sistemas de Banca Electrónica Seguros y Usables).

[1] : La evidencia de las definiciones anteriores se puede constatar en el diccionario en línea de Oxford [http://www.oxforddictionaries.com/].

Objetivos

Los objetivos que en esta sección se presentan, son los objetivos que cobijan el proyecto de grado denominado "*Evaluación Heurística de Seguridad Usable Aplicada en Sistemas e-Banking*". Se debe resaltar que ya se encuentran elaborados los objetivos específicos 1 y 2 que se encuentran expuestos posteriormente, y que el desarrollo de este proyecto cursa actualmente su fase final. La parte experimental que se llevará a cabo en el FONDUC contempla únicamente el objetivo específico 3.

Objetivo General

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

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.

Alcance

El presente proyecto contempla evaluar un conjunto de 46 sub-heurísticas a través de una herramienta de evaluación en un sistema de Banca Electrónica. Constará de 6 fases que se describen a continuación.

- Inspección de las características del sistema de Banca Electrónica del FONDUC
- Elaboración de la guía donde los auditores evaluaran las respectivas sub-heurísticas
- Elaboración de la guía donde se evaluará la satisfacción de la aplicación por parte de los usuarios seleccionados para desarrollar el experimento y que disponen de una cuenta en el FONDUC
- Evaluación de las sub-heurísticas por parte de auditores
- Evaluación de la satisfacción por parte de los usuarios seleccionados para desarrollar el experimento y disponen de una cuenta en el FONDUC
- Generación de resultados y conclusiones

Entregables

Documento

Recomendaciones de Seguridad y Usabilidad
Resultados estadísticos obtenidos de la evaluación por parte de los auditores
Grado de satisfacción de los Usuarios

Charla

Espacio de socialización que aborda el contenido del documento.

Personal y recursos

Andrés Felipe Orozco Orozco - Organizador

Andrés Felipe Gómez Daza - Organizador

Paulo Cesar Realpe Muñoz - Organizador

Afirmaciones

1. Para la adecuada ejecución de los puntos descritos en el alcance, los organizadores realizarán el respectivo contacto con los expertos y usuarios del fondo, excluyendo así, a la firma FONDUC de esta labor.
2. En el presente espacio, es conveniente aclarar que bajo **NINGÚN** motivo se solicitará a la firma FONDUC la prestación de recursos físicos o acompañamiento de personal durante la ejecución de lo plasmado en el alcance.

Premisas y consideraciones

- Disponibilidad del sitio web y aplicación de sistema de banca electrónica

Metodología, Herramienta, Sub-Heurísticas y Requerimientos

Metodología

Método de inspección: Expertos en Seguridad y Usabilidad

Los participantes del proceso de evaluación son los siguientes.

- Organizadores
- Expertos
- Usuarios del FONDUC

Actividades que conforman la etapa de planeación con expertos

1. Definir el sistema a evaluar
2. Elaborar presentación general del sistema
3. Revisar la presentación general del sistema a evaluar
4. Identificar los posibles auditores a participar
5. Seleccionar los auditores que van a participar de la evaluación de Seguridad Usable
6. Elaborar el documento guía para la evaluación
7. Proveer a los auditores la información general del sistema y el documento guía de la evaluación
8. Solucionar preguntas a los auditores

Actividades que conforman la etapa de ejecución con expertos

9. Evaluación individual del sistema
10. Creación de la lista integrada de problemas
11. Calificación individual de problemas

Actividades que conforman la etapa de planeación con usuarios

12. Identificar los posibles usuarios con cuenta FONDUC a participar
13. Seleccionar los usuarios que van a participar de la encuesta de satisfacción
14. Elaborar el documento guía para la satisfacción de la aplicación
15. Proveer a los usuarios la información general del sistema y el documento guía de satisfacción de la aplicación
16. Solucionar preguntas a los usuarios

Actividades que conforman la etapa de ejecución con usuarios

17. Aplicación individual de la encuesta de satisfacción de la aplicación

Actividades que conforman la etapa de análisis de resultados

18. Aplicación de la herramienta de evaluación propuesta a partir de las calificaciones de los auditores
19. Generar una clasificación de problemas a partir de la herramienta de evaluación
20. Análisis e interpretación de resultados
21. Identificar elementos positivos en el sistema
22. Elaborar informe final de evaluación

Herramienta

La herramienta será empleada únicamente en la etapa de análisis de resultados y no implica **NINGUNA** participación en la plataforma virtual del FONDUC.

Sub-Heurísticas

1. Usabilidad **1.1. Visibilidad del estado del sistema**	
U1- Después de que el usuario complete una acción de seguridad, ¿la realimentación indica que el siguiente grupo de acciones puede ser iniciado?	A partir de mensajes que visualicen el inicio para el desarrollo de acciones posteriores (e.g. diseñar un proceso controlado por el sistema que avance paso a paso hasta que se haya completado la seguridad e iniciar, si el proceso de seguridad es satisfactorio, el inicio de las acciones posteriores).
1.2. Estética y mínimo diseño	
U2- ¿La información de seguridad presentada en pantalla es relevante?	Es necesario presentar en pantalla información de seguridad relevante y no aspectos técnicos.
U3- ¿Los íconos de seguridad son identificables y diferenciables?	Los iconos de seguridad deben ser fácilmente visualizados y distinguibles.
U4- ¿Las etiquetas de seguridad son sencillas, fáciles de entender y representativas?	Las etiquetas de seguridad no deben tener términos técnicos abstractos y ser visualizados adecuadamente.
U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?	El sistema puede tener elementos visuales que permitan al usuario conocer políticas de privacidad sobre el uso del sistema.
1.3. Control y libertad de usuario	
U6- ¿El sistema está diseñado de manera que los botones con nombres similares, no desarrollen acciones de seguridad opuesto?	Si los botones tienen etiquetas similares, estos deben cumplir funciones de seguridad adecuado sin ejecutar procedimientos opuestos. Se debe tener cuidado de las etiquetas ya que puede afectar la usabilidad, si el sistema tiene botones con nombres similares, puede causar un gran problema de entendimiento por parte del usuario.

1.4. Utilización del lenguaje del usuario	
U7- ¿Las sentencias de alerta son simples, cortas y comprensibles?	Toda la información de seguridad que es presentada por el sistema debe ser concisa y sencilla de entender.
U8- ¿Las preguntas de seguridad son expresadas en un lenguaje claro y sencillo?	Las preguntas de seguridad que permiten mitigar amenazas, son comprensibles por el usuario.
U9- ¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?	Los términos técnicos o avanzados relacionados con el manejo de las políticas de seguridad y privacidad deben ser evitados.
1.5. Minimizar carga de memoria	
U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	Los elementos de seguridad de los menús en la interfaz son claros para el usuario.
U11- ¿La información relacionada con la seguridad es presentada de una manera coherente y estandarizada?	Información coherente y basada en estándares es más fácil de aprender y recordar.
U12- En un proceso de autenticación por conocimiento, ¿el sistema permite minimizar la carga de memoria para los usuarios?	Sin memorizar datos extensos, complicados procedimientos o realizar actividades cognitivas complejas.
1.6. Reconocer, diagnosticar y recuperarse de errores	
U13- ¿Los mensajes de error relacionados con la seguridad informan al usuario de la gravedad del error?	Conocer el nivel de seriedad del error ayuda a tomar acciones adecuadas.
U14- ¿El sistema facilita la posibilidad al usuario de solucionar problemas a posibles errores?	Cuando existe una amenaza de seguridad el sistema puede presentar fallas (e.g. bloqueo), por lo tanto es necesario que el sistema informe claramente la forma de solucionar los errores que dejó la amenaza.
U15- ¿Los mensajes de error relacionados con la seguridad son significativos y sensibles al problema?	En algunos casos los mensajes de error debe proporcionar la causa del error de seguridad y de una forma que el usuario pueda entenderlo.
U16- ¿Los mensajes de error relacionados con la seguridad indican la acción que el usuario debe tomar para corregir el error?	Es necesario que el sistema recomiende acciones de acuerdo a errores de seguridad específicos.
U17- ¿Los mensajes de error relacionados con la seguridad son adecuados al lenguaje del usuario?	Los mensajes de error deben tener un lenguaje sencillo que los usuarios puedan entender y tomar decisiones.
U18- ¿Los mensajes de error relacionados con la seguridad indican al usuario dónde obtener ayuda?	Si el usuario no comprende el mensaje de error, este debe proporcionar ayuda para solucionarlo.
1.7. Prevención de errores	

U19- ¿La información necesaria para tomar una buena decisión de seguridad, es adecuada y está disponible antes de que se adopte la medida?	Por desconocimiento, los usuarios pueden realizan tareas sin darse cuenta de las consecuencias que pueden tener (e.g. Hacer que sus imágenes sean accesible para todos los usuarios).
1.8. Consistencia y estándares	
U20- ¿Los iconos de seguridad poseen etiqueta?	La etiqueta en los iconos de seguridad permite al usuario conocer su función.
1.9. Documentación y ayuda	
U21- ¿Hay una función de ayuda de seguridad visible?	La función de ayuda debe ser visible e identificable por el usuario.
U22- ¿La información proporcionada por la ayuda es relevante?	La información de seguridad debe ser significativo con respecto a las necesidades del usuario.
U23- ¿El sistema provee soporte técnico en línea para solucionar problemas de seguridad?	Es importante que exista ayuda técnica en línea a situaciones complejas de seguridad. Sin embargo, se debe tener precaución con ataques de ingeniería social.
1.10. Transmitir características	
U24- ¿El sistema notifica a los usuarios si está interactuando con fuentes no confiables e interpone algún tipo de bloqueo que evita males mayores?	La fuente no confiable representa algo que no tiene información sobre su identidad, si esto llega a presentarse, el sistema notifica al usuario que puede existir algún tipo de vulnerabilidad e interpone algún tipo de bloque para evitar un riesgo mayor.
U25- ¿El sistema muestra logos de seguridad?	El logo en función del tipo de interfaz de seguridad transmite confianza (e.g. Symantec).
U26- ¿El sistema tiene certificados de seguridad otorgados por entidades externas reconocidas?	Es importante conseguir que los usuarios conozcan sus funciones (e.g., VeriSign, ControlScan o SSL).

Requerimientos y Sub-Heurísticas Asociadas

REQ_ID	Requerimiento	Sub-Heurística asociada
1	El sistema debe establecer una sesión segura entre la máquina del cliente y el servidor del banco, con cifrado de datos.	S11- El sistema soporta y hace uso por defecto del protocolo HTTPS?
		O1- ¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?
2	El sistema debe bloquear a los usuarios que superen el máximo número de intentos con la clave incorrecta.	S3- ¿El proceso de autenticación hace cumplir un límite de intentos de acceso no válidos consecutivos por un usuario?

3	Una vez el usuario ingrese al sistema, se le debe presentar una vista con las diferentes opciones que le permitan usar los servicios.	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?
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?
		U11- ¿La información relacionada con la seguridad es presentada de una manera coherente y estandarizada?
		U19- ¿La información necesaria para tomar una buena decisión de seguridad, es adecuada y está disponible antes de que se adopte la medida?
		U22- ¿La información proporcionada por la ayuda es relevante?
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.	U9- ¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?
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.)	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?
		S8- ¿El sistema hace cumplir el nivel de complejidad de la contraseña, con los requisitos mínimos exigidos?
		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?
		A3- En un proceso de autenticación, ¿el sistema evita esfuerzo adicional?
7	El sistema debe informar al usuario sobre medidas de seguridad y proporcionar unas políticas de seguridad.	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?
		S9- ¿El sistema posee políticas de privacidad para comercio o contenido del usuario?

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.	A2-¿El sistema evita el uso de claves aleatorias para la etapa de registro o 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	U7-¿Las sentencias de alerta son simples, cortas y comprensibles?
		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?
		O2- En un proceso de autenticación, ¿este tiene palabras adecuadas para desarrollar una acción en particular?
		F3- Si el proceso de inicio de sesión falla, ¿el sistema evita indicarle al usuario qué parte del proceso es incorrecto?
10	El cliente debe haber iniciado sesión para estar habilitado a hacer transacciones o transferencia de fondos	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de 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).	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?
		S2- Si el sistema utiliza "cookies informáticos", ¿la información sobre la privacidad del sistema describe con precisión el uso de estas cookies?
		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?
		S7- ¿El sistema describe cada opción de privacidad en detalle?
		F2- ¿Está claramente establecido el propósito de utilizar la información personal del usuario?
12	El sistema debe permitir a los usuarios controlar las acciones críticas e información crítica	S7- ¿La información de privacidad del sistema garantiza al usuario el derecho a optar por compartir información no crítica con terceros?
13	El sistema debe tomar medidas para hacer frente a los riesgos, e inmediatamente informar a los usuarios acerca de estas medidas.	U24- ¿El sistema notifica a los usuarios si está interactuando con fuentes no confiables e interpone algún tipo de bloqueo que evita males mayores?
		S6- ¿El sistema notifica y da posibles soluciones al usuario sobre vulnerabilidades asociados a incidentes de seguridad detectados?
14	Proporcionar autenticación usable (OTP, Tokens, Biométrica, Multi-factor)	U12- En un proceso de autenticación por conocimiento, ¿el sistema permite minimizar la carga de memoria para los usuarios?
		A1- ¿El sistema permite usar passwords gráficos para usuarios con dificultades de lectura?
		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?
15	Las interfaces de usuario deben ser presentadas con una lógica clara y ser entendibles.	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?
		F1-¿La interfaz ayuda al usuario a tener una

		experiencia segura y satisfactoria con el sistema?
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.	U25- ¿El sistema muestra logos de seguridad?
		U26-¿El sistema tiene certificados de seguridad otorgados por entidades externas reconocidas?
		O1-¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?
17	El sistema debe incluir las respectivas instrucciones para una adecuada interacción del usuario, en el sitio web u otros medios de comunicación.	U21- ¿Hay una función de ayuda de seguridad visible?
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).	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?
19	El sistema debe implementar técnicas de prevención de errores.	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?
20	Claridad en los enlaces y en las etiquetas de los botones donde se sugiere la acción requerida.	U3- ¿Los íconos de seguridad son identificables y diferenciables?
		U4- ¿Las etiquetas de seguridad son sencillas, fáciles de entender y representativas?
		U6- ¿El sistema está diseñado de manera que los botones con nombres similares, no desarrollen acciones de seguridad opuestas?
		U20- ¿Los iconos de seguridad poseen etiqueta?

21	Las interfaces de usuario deben presentar y destacar la información relevante en el contexto y en el momento correcto.	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?
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).	U23- ¿El sistema provee soporte técnico en línea para solucionar problemas de seguridad?
23	El sistema debe entregar retroalimentación (e.g. su dinero será transferido en 24 horas).	U1- Después de que el usuario complete una acción de seguridad, ¿la realimentación indica que el siguiente grupo de acciones puede ser iniciado?

Información Personal y Capacidades Técnicas

ANDRÉS FELIPE OROZCO OROZCO
C.C. 1.061.767.301 de Popayán, Cauca.

Dirección: Calle 9 Norte No. 6B – 35
B/Belalcázar
Teléfono: 836 1787
Móvil: 318 522 2446
Email: andfelorozco@unicauca.edu.co

PERFIL PROFESIONAL

Estudiante de décimo semestre de Ingeniería de Sistemas capaz de brindar soluciones software a problemas de diferente índole, capacitado para innovar, diseñar, construir y mantener sistemas computacionales e informáticos, capacidad de fácil adaptación frente a cambios tecnológicos o sociales, fuertemente ligado al trabajo colaborativo, liderazgo y gestión de proyectos.

- Habilidades en desarrollo de Software en Java, JavaServer Faces (JSF), C, C++, C#, Python, Android, Php.
- Manejo de Patrones de Diseño en arquitectura del Software.
- Manejo de Bases de Datos: SQL, Oracle, MySql.
- Manejo de equipos de desarrollo de Software.
- Manejo de tecnologías de desarrollo ágil, Scrum, XP, Scrum+XP.
- Manejo de redes computacionales.
- Facilidad para el aprendizaje de nuevas herramientas y tecnologías de información.
- Buenas relaciones interpersonales.

ANDRÉS FELIPE GÓMEZ DAZA
C.C. 1.085.296.180 de Pasto, Nariño.

Dirección: Calle 9 Norte No. 6B – 35
B/Belalcázar
Móvil: 312 821 5876
Email: gomezdaza@unicauca.edu.co

PERFIL PROFESIONAL

Estudiante de 10° semestre de Ingeniería de Sistemas de la Universidad del Cauca.

Me considero una persona con mucha iniciativa, responsable en cualquier actividad, asumo con confianza y liderazgo cualquier reto laboral que se me proponga ya que puedo resolver problemas con mucha facilidad y pongo en evidencia mis conocimientos ante cualquier situación; me desenvuelvo muy bien trabajando en equipo y en condiciones de alta presión.

- Poseo conocimientos en redes, bases de datos, seguridad informática y cuentas contables.
- Tengo muy buen dominio del inglés.
- Participo en el semillero de investigación IRIS y semillero de emprendimiento StarTic, ambos de la universidad del Cauca.

PAULO CESAR REALPE MUÑOZ
C.C. 76.331.501 de Popayán, Cauca.

Dirección: Calle 8 Norte No. 6A – 138
B/Belalcázar
Móvil: 310 399 5514
Email: prealpe@hotmail.com

PERFIL PROFESIONAL

Ingeniero Físico de la Universidad del Cauca (2004), M.Sc en Ingeniería Electrónica de la Universidad del Valle (2009) y PhD (c) en ciencias electrónicas de la Universidad del Cauca. Miembro del grupo de investigación de Bionanoelectrónica de la Universidad del Valle y del grupo de Investigación y Desarrollo en Ingeniería de Software (IDIS) de la Universidad del Cauca. Áreas de investigación: Criptografía, diseño e implementación de sistemas digitales avanzados en FPGA, DSP y de seguridad usable.

- Habilidades en: Maple, C/C++, Labview, Matlab, simulación de circuitos electrónicos y eléctricos (CADs), Java, VHDL, Quartus II de Altera y ensamblador.
- Conocimientos en física mecánica y electromagnetismo, electrónica análoga, diseño e implementación de sistemas de control electrónicos basados en microcontroladores para diferentes procesos, procesamiento digital de señales, Instrumentación electrónica, electrónica digital avanzada, arquitectura de computadores, diseño e implementación de procesadores digitales sobre CPLD/FPGA, manejo de interfaces electrónicas y de adquisición de datos.
- Facilidad para el aprendizaje de nuevas herramientas y tecnologías de información.
- Buenas relaciones interpersonales.

ANEXO G: Acuerdo de Confidencialidad – FONDUC

ACUERDO DE CONFIDENCIALIDAD

PRIMERA.- OBJETO: El Acuerdo tiene por objeto establecer los términos que regirán el Uso de la Información Confidencial que **EL FONDUC** proporcionará a **Investigación y Desarrollo en Ingeniería de Software - IDIS**, para la Evaluación Heurística de Seguridad Usable Aplicada en Sistemas e-Banking del FONDUC.

SEGUNDA.- INFORMACION CONFIDENCIAL: Se entiende por Información Confidencial en los términos de este Acuerdo, toda la información de seguridad, técnica, financiera, comercial, jurídica y en general cualquier información que revele **EL FONDUC** a **Investigación y Desarrollo en Ingeniería de Software - IDIS**, relacionada con sus actividades y/o negocios, bien sea en forma escrita, oral, impresa, medio magnético, bases de datos o por cualquier otro medio que se transmita.

TERCERA.- OBLIGACIONES DE Investigación y Desarrollo en Ingeniería de Software - IDIS. Investigación y Desarrollo en Ingeniería de Software - IDIS se compromete a:

a) Mantener bajo confidencialidad y reserva todos los datos de informaciones, procedimientos, ideas, precios, estrategias y detalles relacionados con las actividades de **EL FONDUC** en desarrollo de los servicios que le preste a sus asociados.
b) No utilizar la información confidencial para el beneficio directo o indirecto de ninguna persona, entidad o compañía sin autorización previa y expresa de **EL FONDUC**.
c) Abstenerse de fotocopiar y/o sacarle copia a la información que en virtud de este acuerdo, reciba de **EL FONDUC**, salvo las copias que requiera el consultor para el desarrollo de su trabajo, entendiéndose que el manejo que **Investigación y Desarrollo en Ingeniería de Software - IDIS** de a tales copias está cobijado por los términos del presente acuerdo de confidencialidad.
d) No usar la información para ningún propósito distinto al relacionado con el objeto previsto en el contrato.
e) Instruir a cada uno de los integrantes del Grupo **Investigación y Desarrollo en Ingeniería de Software - IDIS**, sobre el carácter confidencial y adecuado manejo de la información que reciben.
f) No usar la información de modo que pueda ser de alguna manera, directa o indirectamente, perjudicial para los intereses y/o seguridad de **EL FONDUC**.
g) Mantener bajo reserva cualquier información adicional elaborada por sus empleados, asesores, consultores, y/o socios con base en la información entregada por **EL FONDUC**.
h) Cumplida la finalidad para la cual fue entregada la información y los documentos en que esté contenida, destruir los documentos o devolverlos a **EL FONDUC**, de acuerdo con las instrucciones que ésta última imparta en ese sentido.

CUARTA.- RESPONSABILIDAD: **Investigación y Desarrollo en Ingeniería de Software - IDIS** será responsable por cualquier uso inadecuado de la información confidencial.

QUINTA.- APLICABILIDAD: El presente Acuerdo de confidencialidad no se aplicará en los siguientes casos:

a) Cuando **Investigación y Desarrollo en Ingeniería de Software - IDIS** se vea obligado a revelar la información por mandato legal judicial, administrativo u otro de similar naturaleza, debiendo informar previamente a **EL FONDUC**, indicándole el nombre de la autoridad correspondiente y la razón legal por la cual **Investigación y Desarrollo en Ingeniería de Software - IDIS** debe entregar dicha información.
b) Cuando la información sea o se convierta en accesible al público en general por razones distintas al incumplimiento de este Acuerdo.
c) Cuando se le proporcione a **Investigación y Desarrollo en Ingeniería de Software - IDIS** de una manera no confidencial por otra fuente que no sea **EL FONDUC** entendiendo que esta fuente no está actuando bajo un acuerdo de confidencialidad.
d) Cuando se trate de información que sea o haya sido desarrollada independientemente por **Investigación y Desarrollo en Ingeniería de Software - IDIS**.

SEXTA.- PROPIEDAD: Investigación y Desarrollo en Ingeniería de Software - IDIS reconoce que la información que proporcione **EL FONDUC**, es de propiedad de éste último y permanecerá siéndolo, mientras no medie Acuerdo en contrario entre **EL FONDUC** y **Investigación y Desarrollo en Ingeniería de Software - IDIS**. No se permite ningún uso distinto al previsto en el presente Acuerdo, ni éste implica la cesión efectiva de ningún derecho.

SEPTIMA.- CESION: Este Acuerdo no puede ser cedido por **Investigación y Desarrollo en Ingeniería de Software - IDIS**.

OCTAVA.- TERMINO: Se conviene que durante el desarrollo y ejecución de la investigación que **Investigación y Desarrollo en Ingeniería de Software - IDIS** le preste a **EL FONDUC** y aun después de finalizado el contrato, **Investigación y Desarrollo en Ingeniería de Software - IDIS** no revelará o divulgará la información recibida a ninguna persona natural o jurídica.

NOVENA.- PENA:- El incumplimiento por parte de **Investigación y Desarrollo en Ingeniería de Software - IDIS** le hará incurrir automáticamente en una pena a favor de **FONDUC** por una suma equivalente a Veinte (20) SALARIOS MÍNIMOS LEGALES MENSUALES VIGENTES, sin perjuicio que **FONDUC** pueda adelantar las acciones legales que tiendan al resarcimiento total de los perjuicios causados. El pago de la suma estipulada como pena, no releva al **Investigación y Desarrollo en Ingeniería de Software - IDIS** del cumplimiento de la obligación de confidencialidad contraída mediante este Documento; en consecuencia, deberá pagar a **FONDUC** cada vez que la incumpla.

SOLUCIÓN DE CONTROVERSIAS: Cualquier diferencia o discrepancia que surja del presente acuerdo deberá ser resuelta por los medios alternativos de solución de

conflictos previstos en la ley, tales como la conciliación, amigable composición o transacción.

PARÁGRAFO: Sin perjuicio de lo anterior las partes convienen que si dentro de los diez (10) días siguientes a la notificación de la diferencia no se ha llegado a un acuerdo sobre el mecanismo de solución seleccionado y/o cualquier otro punto relacionado con el mismo, el asunto en conflicto será resuelto por un árbitro, designado por el Centro de Conciliación y Arbitraje de la Cámara de Comercio de Popayán. El árbitro fallará en derecho, de acuerdo con lo alegado y probado en el respectivo proceso arbitral.

Para constancia se firma en la ciudad de Popayán el 1 de Septiembre de dos mil dieciséis (2016).

JUAN FELIPE VALLEJO MATUS
Representante Legal FONDC
NIT. 891.502.063-1

CÉSAR ALBERTO COLLAZOS ORDÓÑEZ
Representante - Investigación y Desarrollo en Ingeniería de Software - IDIS

ANEXO H: Encuesta de Satisfacción – Usuarios

Documento guía para los usuarios

Estimado(a) colaborador(a):

Usted participará en una prueba para evaluar el grado de usabilidad de la plataforma virtual del **FONDUC** www.fonduc.com.co, el cual es un sistema de banca electrónica exclusivo para docentes y administrativos de planta de la universidad del Cauca. La prueba tiene por objetivo detectar la existencia de problemas en el uso de dicho sitio web, en el marco de un estudio de usabilidad, a fin de mejorar la experiencia del usuario.

SE ESTÁ EVALUANDO EL SITIO WEB, NO EL DESEMPEÑO DE USTED COMO USUARIO, POR LO TANTO, ¡NO SE PREOCUPE SI COMETE ALGÚN ERROR!

Toda la información que usted nos proporciona es absolutamente confidencial y muy relevante para nuestro estudio, por lo cual le agradecemos su cooperación.

La prueba tiene 3 etapas:

(1) En la primera etapa usted deberá complementar un breve cuestionario con preguntas relativas a su experiencia en el uso de sistemas de banca electrónica.
(2) En la segunda etapa se le proporcionará un conjunto de tareas que se deben realizar a través del sitio web www.fonduc.com.co.
(3) En la tercera etapa usted deberá completar un breve cuestionario que tiene por objetivo obtener la percepción general sobre su experiencia en el uso del sitio web.

AL MANEJAR INFORMACIÓN CONFIDENCIAL, LAS DUDAS NO PUEDEN SER ACLARADAS DE MANERA INMEDIATA. SI TIENE ALGUNA DUDA, Y NO PUEDE SOLUCIONARLA, SUSPENDA LA PRUEBA Y CONTACTE CON EL EVALUADOR.

(1) Cuestionario pre-test

Conteste el siguiente cuestionario.

i. Datos personales

1. Sexo ( ) Femenino ( ) Masculino

2. Edad _____

3. Nivel más alto de educación completado o en proceso

Universitario	( ) Completa	( ) En proceso
Especialización	( ) Completa	( ) En proceso
Maestría	( ) Completa	( ) En proceso
Doctorado	( ) Completa	( ) En proceso

Otro ¿Cuál? _____

4. ¿Cuál es su ocupación? _____

ii. Información sobre experiencia en el uso de sistemas de banca electrónica

5. ¿Con qué frecuencia utiliza la oficina virtual del FONDUC?

( ) Nunca
( ) Casi nunca
( ) Ocasionalmente
( ) Frecuentemente

6. ¿Ha realizado .. (bono)?

7. ¿Tiene experiencia previa con el uso de sistemas de banca electrónica?
( ) Si
( ) No

(2) Lista de tareas

Tarea N 1: Acceder al aplicativo virtual

1. Ingresar al sitio web www.fonduc.com.co.
2. Busque el enlace denominado “Oficina Virtual” y haga clic.
3. Ingrese sus datos e inicie la sesión.

Tarea N 2: Verifique si el sistema cuenta con logos de seguridad

1. Generalmente, las aplicaciones de banca electrónica presentan en su interfaz logos referentes a la seguridad del sistema.

Tarea N 3: Verifique si hay recomendaciones de seguridad

1. Generalmente, las aplicaciones de banca electrónica presentan recomendaciones de seguridad.

Tarea N 4: Verifique si tiene alguna sanción

1. Haga clic en la pestaña “Mis productos y servicios”.
2. Haga clic en la pestaña “Sanciones y Novedades”.
3. Verifique el estado.

Tarea N 5: Descargue el documento de estado de la cuenta

1. Haga clic en la pestaña “Certificaciones y descargas”.
2. Haga clic en la pestaña “Descargas”.
3. En estado de la cuenta seleccione el correspondiente al mes de enero de 2016 “ENE-2016”.
4. Haga clic en “Descargar”.

Tarea N 6: Agregar y eliminar un contacto

1. Haga clic en la pestaña “Actualización de datos”.
2. Haga clic en la pestaña “Información socioeconómica”.
3. Haga clic en la pestaña “Contactos”.
4. Haga clic en “Agregar”.
5. Considere las siguientes especificaciones:
   Tipo de Contacto: Personales
   Nombre: PRUEBA
   Dirección: Unicauca
   Teléfono: 1234
   Ciudad: POPAYÁN – CAUCA
6. Verifique que se ha creado el anterior registro con los datos especificados.
7. En la última columna del registro (“Eliminar”), haga clic en el icono de confirmación.

(3) Cuestionario post-test

Encierre en un círculo la nota más apropiada para cada una de las siguientes preguntas.

1. ¿Pudo completar las tareas?

1	2	3	4	5
Muy difícilmente	Difícilmente	Neutral	Fácilmente	Muy fácilmente

2. ¿Considera que la información requerida en la prueba ha sido fácil de entender?

1	2	3	4	5
Muy difícilmente	Difícilmente	Neutral	Fácilmente	Muy fácilmente

3. La disposición de la información en el aplicativo virtual es:

1	2	3	4	5
Muy difusa	Difusa	Neutral	Clara	Muy clara

4. ¿Es fácil la navegación a través del sitio web?

1	2	3	4	5
Muy difícil	Difícil	Neutral	Fácil	Muy fácil

5. ¿Considera que la información requerida en la prueba ha sido fácil de entender?

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

6. ¿Se ha sentido bien informado u orientado dentro del sitio web?

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

7. ¿El aplicativo virtual le inspira confianza para realizar los movimientos?

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

8. Usted califica su grado de satisfacción en el uso del aplicativo virtual como:

1	2	3	4	5
Insatisfactorio	Poco satisfactorio	Neutral	Satisfactorio	Muy satisfactorio

9. Si ha usado otros sistemas de banca electrónica, la experiencia con este le ha parecido:

1	2	3	4	5
Mucho peor	Peor	Neutral	Mejor	Muy satisfactorio

10. ¿Cómo evalúa su experiencia como colaborador de la prueba?

1	2	3	4	5
Muy desagradable	Desagradable	Neutral	Agradable	Muy agradable

ANEXO I: Comentarios – Encuesta de Satisfacción – Usuarios

USUARIO 1:

No presenta comentarios.

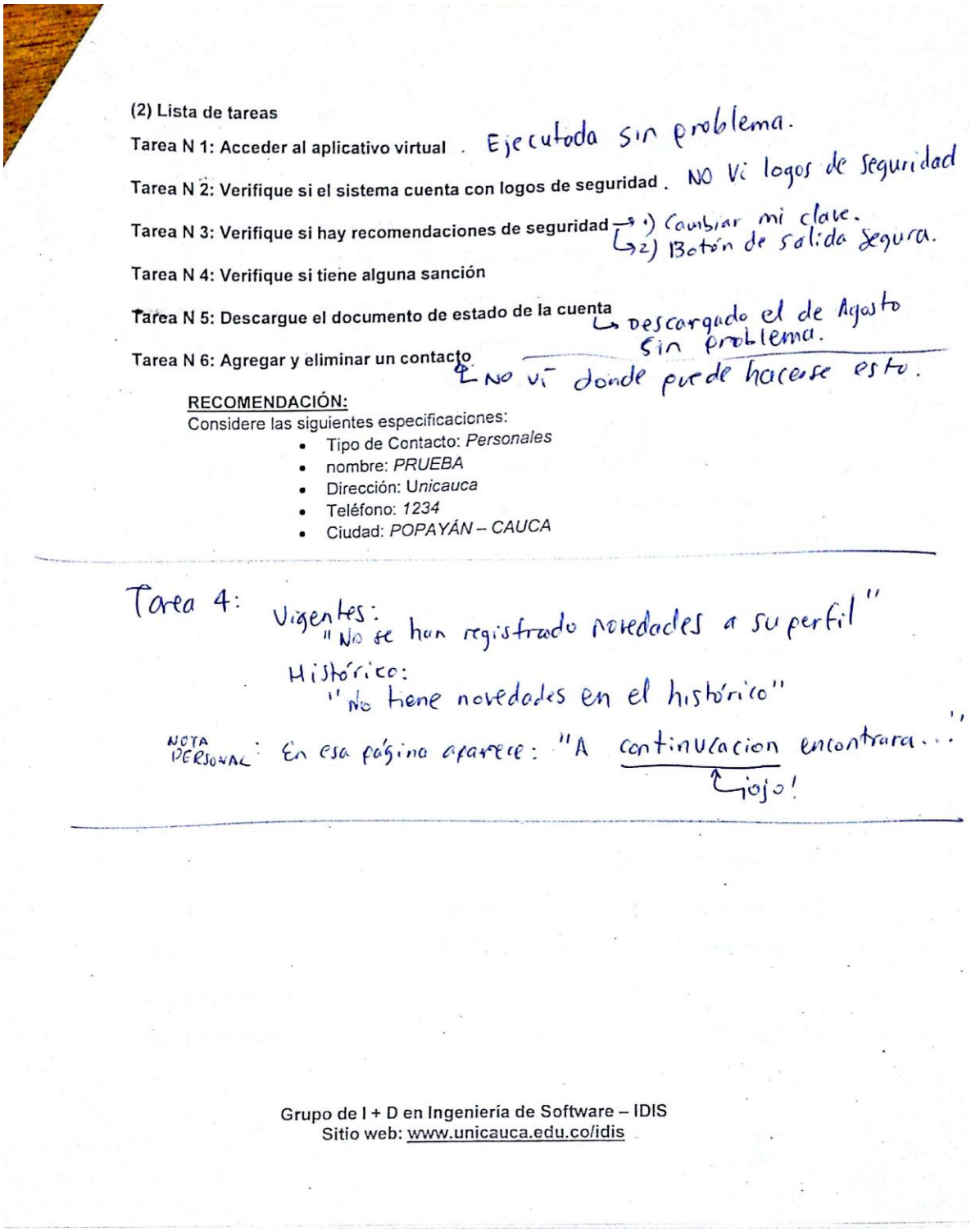
USUARIO 2:

No presenta comentarios.

USUARIO 3:

No presenta comentarios.

USUARIO 4:



(2) Lista de tareas

Tarea N 1: Acceder al aplicativo virtual . Ejecutada sin problema.

Tarea N 2: Verifique si el sistema cuenta con logos de seguridad . NO Vi logos de seguridad

Tarea N 3: Verifique si hay recomendaciones de seguridad → 1) Cambiar mi clave.
↳ 2) Botón de salida segura.

Tarea N 4: Verifique si tiene alguna sanción

Tarea N 5: Descargue el documento de estado de la cuenta → descargado el de Agosto sin problema.

Tarea N 6: Agregar y eliminar un contacto
↳ No vi donde puede hacerse esto.

RECOMENDACIÓN:
Considere las siguientes especificaciones:

- Tipo de Contacto: *Personales*
- nombre: *PRUEBA*
- Dirección: *Unicauca*
- Teléfono: *1234*
- Ciudad: *POPAYÁN – CAUCA*

Tarea 4: Vigentes:
"No se han registrado novedades a su perfil"
Histórico:
"No tiene novedades en el histórico"

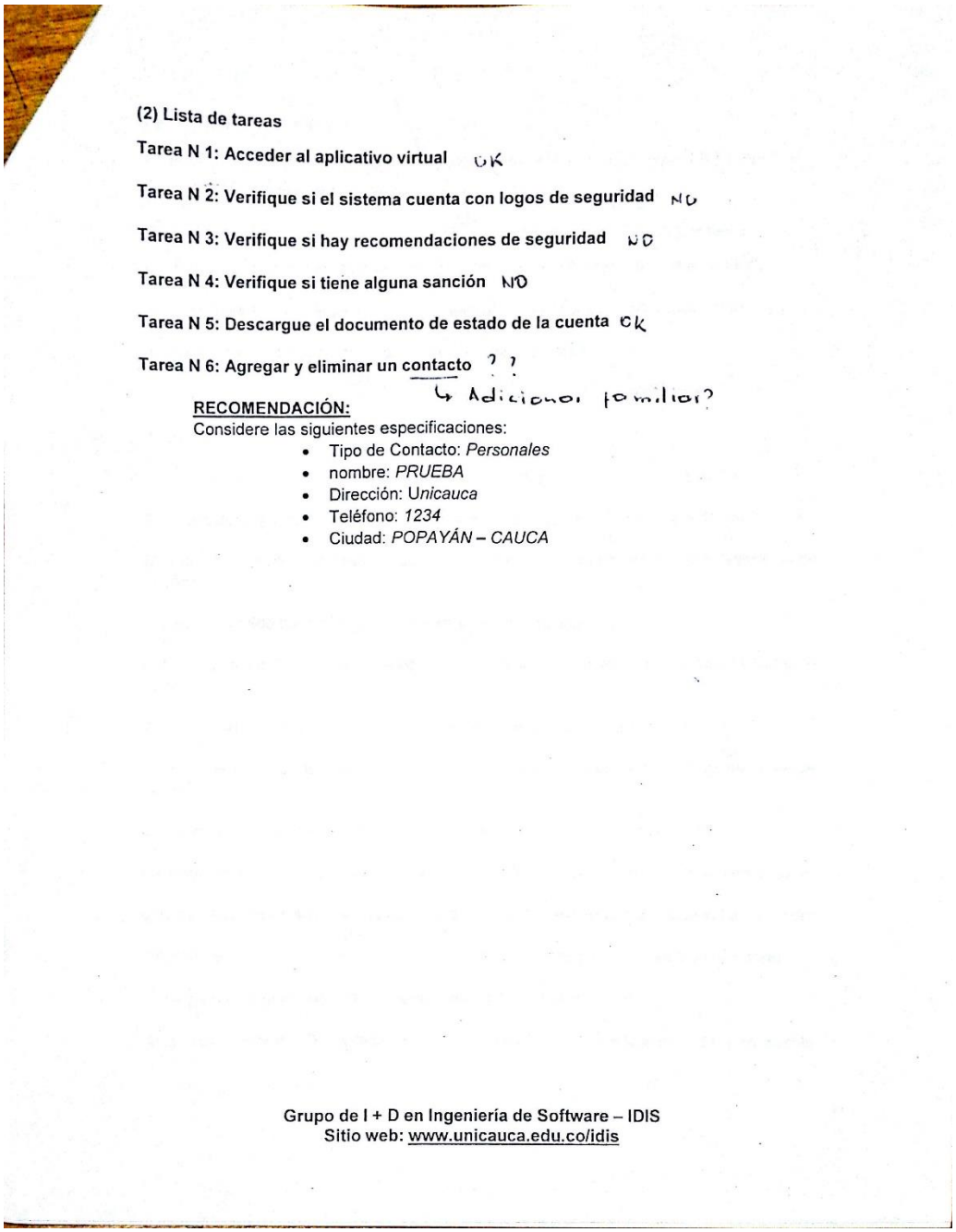
NOTA PERSONAL: En esa página aparece: "A continuacion encontrara..."
↑ ojo!

Grupo de I + D en Ingeniería de Software – IDIS
Sitio web: www.unicauca.edu.co/idis

USUARIO 5:

No presenta comentarios.

USUARIO 6:



(2) Lista de tareas

Tarea N 1: Acceder al aplicativo virtual OK

Tarea N 2: Verifique si el sistema cuenta con logos de seguridad NO

Tarea N 3: Verifique si hay recomendaciones de seguridad NO

Tarea N 4: Verifique si tiene alguna sanción NO

Tarea N 5: Descargue el documento de estado de la cuenta OK

Tarea N 6: Agregar y eliminar un contacto ? ?

↳ Adicionar familiar?

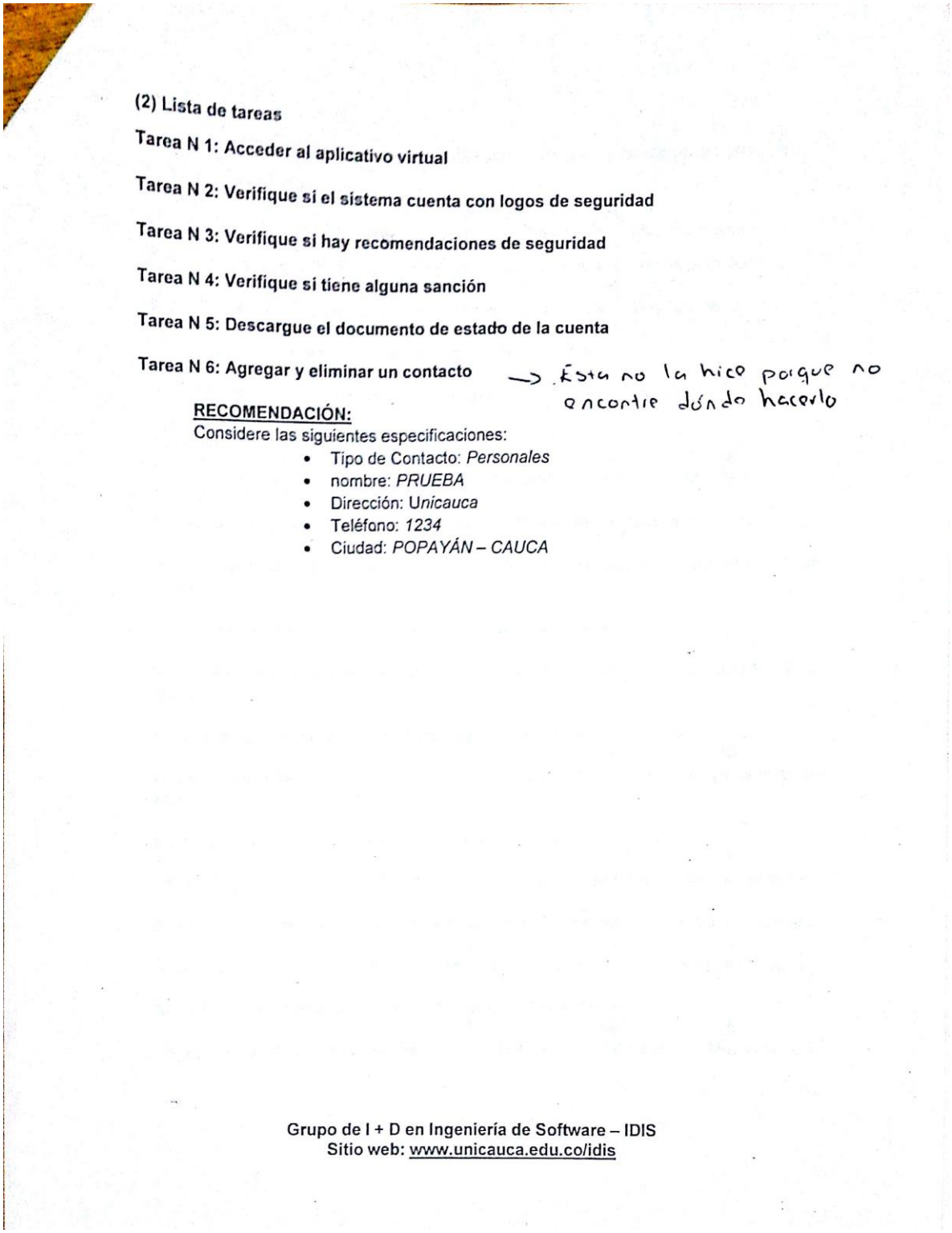
RECOMENDACIÓN:

Considere las siguientes especificaciones:

- Tipo de Contacto: *Personales*
- nombre: *PRUEBA*
- Dirección: *Unicauca*
- Teléfono: *1234*
- Ciudad: *POPAYÁN – CAUCA*

Grupo de I + D en Ingeniería de Software – IDIS
Sitio web: www.unicauca.edu.co/idis

USUARIO 7:



(2) Lista de tareas

Tarea N 1: Acceder al aplicativo virtual

Tarea N 2: Verifique si el sistema cuenta con logos de seguridad

Tarea N 3: Verifique si hay recomendaciones de seguridad

Tarea N 4: Verifique si tiene alguna sanción

Tarea N 5: Descargue el documento de estado de la cuenta

Tarea N 6: Agregar y eliminar un contacto → Esta no la hice porque no encontre dónde hacerlo

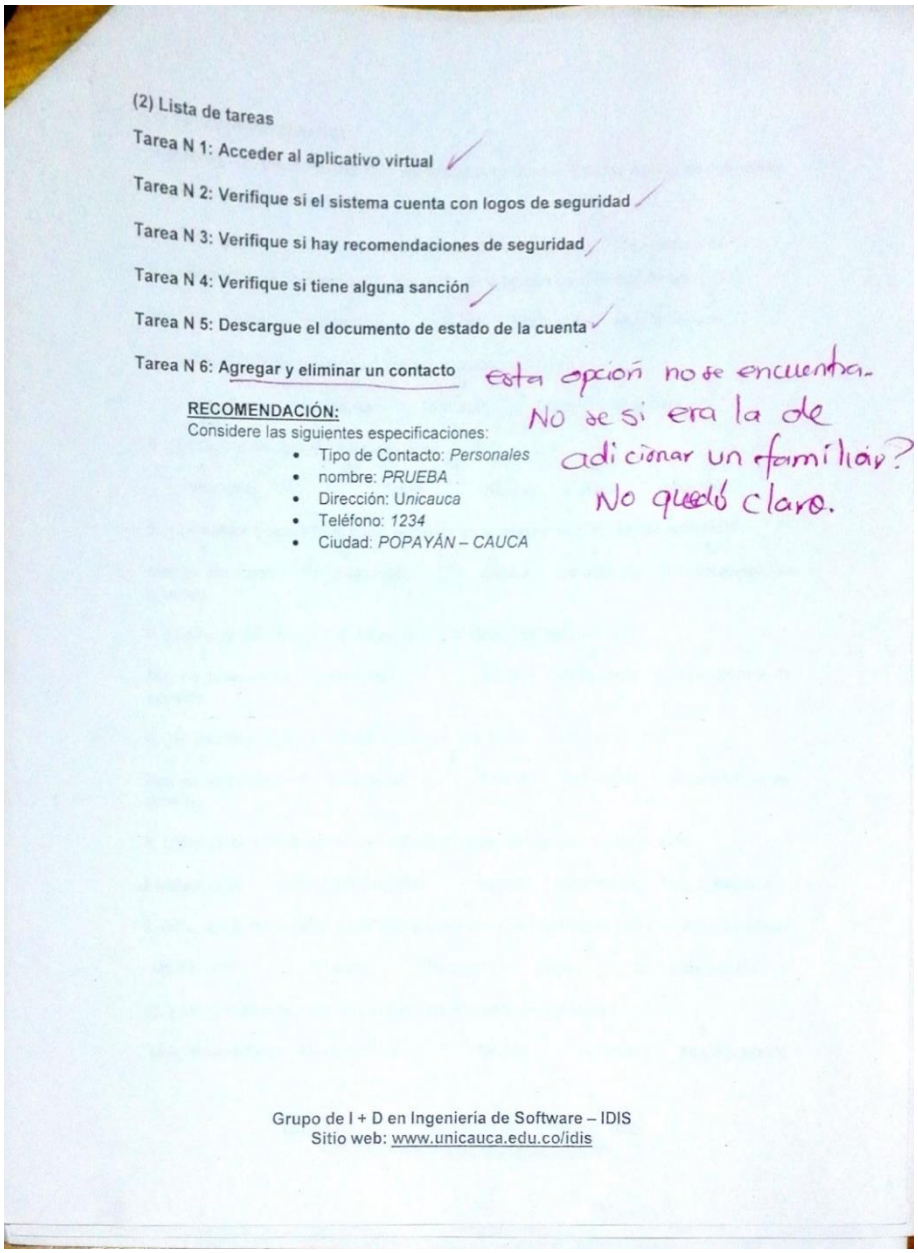
RECOMENDACIÓN:

Considere las siguientes especificaciones:

- Tipo de Contacto: *Personales*
- nombre: *PRUEBA*
- Dirección: *Unicauca*
- Teléfono: *1234*
- Ciudad: *POPAYÁN – CAUCA*

Grupo de I + D en Ingeniería de Software – IDIS
Sitio web: www.unicauca.edu.co/idis

USUARIO 8:



(2) Lista de tareas

Tarea N 1: Acceder al aplicativo virtual ✓

Tarea N 2: Verifique si el sistema cuenta con logos de seguridad ✓

Tarea N 3: Verifique si hay recomendaciones de seguridad ✓

Tarea N 4: Verifique si tiene alguna sanción ✓

Tarea N 5: Descargue el documento de estado de la cuenta ✓

Tarea N 6: Agregar y eliminar un contacto esta opción no se encuentra. No se si era la de adicionar un familiar? No quedó claro.

RECOMENDACIÓN:
Considere las siguientes especificaciones:

- Tipo de Contacto: *Personales*
- nombre: *PRUEBA*
- Dirección: *Unicauca*
- Teléfono: *1234*
- Ciudad: *POPAYÁN – CAUCA*

Grupo de I + D en Ingeniería de Software – IDIS
Sitio web: www.unicauca.edu.co/idis

USUARIO 9:

No presenta comentarios.

USUARIO 10:

No presenta comentarios.

ANEXO J: Información para el Auditor y Formulario de Consentimiento Informado - Auditores

Información para el evaluador y formulario de consentimiento informado

Título del estudio: "Evaluación Heurística de Seguridad Usable Aplicada en Sistemas e-Banking**"**.
Estudiantes: Andrés Felipe Gómez Daza, Andrés Felipe Orozco Orozco.
Director: Ph.D(c). Paulo César Realpe Muñoz
Codirector: Ph.D. César Alberto Collazos Ordóñez
Entidad: Universidad del Cauca – Popayán – Facultad Ingeniería Electrónica y Telecomunicaciones FIET.

Propósito
Evaluar un conjunto de sub-heurísticas de Seguridad Usable que permita contribuir en el diseño de los sistemas e-Banking con respecto a su Seguridad sin que se vean afectados los aspectos de Usabilidad en la plataforma virtual del FONDUC (Fondo de Profesores de la Universidad del Cauca).

Procedimiento
Si usted acepta participar se le solicitará:

1. Ingresar a la plataforma virtual del FONDUC.
2. Llenar el formulario de evaluación bajo las condiciones de experto.

Bajo ningún motivo los implicados en el desarrollo del estudio podrán monitorear, grabar o interrumpir su sesión.
La información diligenciada será única y exclusivamente utilizada para el desarrollo de esta investigación y no compromete información personal o financiera de su cuenta FONDUC.

Beneficios de su participación en el estudio
Participar en el estudio no genera un beneficio directo para usted como evaluador, sin embargo, los resultados obtenidos del estudio podrán generar valor agregado para otras personas interesadas en el campo de la Seguridad Usable.

Voluntariedad
Su participación es voluntaria. Si usted decide no participar o retirarse del estudio en cualquier momento, aun cuando haya iniciado su participación del estudio puede hacerlo sin que esto ocasione una sanción o castigo para usted.

Confidencialidad
Si usted decide participar, garantizamos que toda la información suministrada será manejada con absoluta confidencialidad, sus datos personales no serán publicados ni revelados, los implicados en el desarrollo del estudio se hacen responsables de la custodia y privacidad de los mismos.

Compartir los resultados
Los resultados de la investigación se compartirán en tiempos adecuados en publicaciones, revistas, conferencias, etc., pero la información personal permanecerá confidencial.

Contactos
Si tiene dudas puede comunicarse con los estudiantes **Andrés Felipe Gómez Daza** al correo **gomezdaza@unicauca.edu.co** ó **Andrés Felipe Orozco Orozco** al correo electrónico **andfelorozco@unicauca.edu.co**. Datos del grupo de investigación que avala el proyecto: César Alberto Collazos Ordóñez Líder. Grupo de Investigación y Desarrollo en Ingeniería de Software - IDIS. Universidad del Cauca FIET-Sector Tulcan. Tel 57-28209800 ext. 2133. Página web del Grupo de Investigación: www.unicauca.edu.co/idis

He entendido la información que se expone en este consentimiento y me han respondido las dudas e inquietudes surgidas.

Autorización
Estoy de acuerdo o acepto participar en el presente estudio.
Para constancia, firmo a los ___ días del mes de _____ del año _____.

_____

Firma y Cédula del Participante

Declaración de los estudiantes
Nosotros certificamos que le hemos explicado a esta persona la naturaleza y el objetivo de la investigación, y que esta persona entiende en qué consiste su participación.

Todas las preguntas que esta persona ha hecho le han sido contestadas en forma adecuada. Así mismo, hemos leído y explicado adecuadamente las partes del consentimiento informado. Hacemos constar con nuestras firmas.

_____ _____

Firma y Cédula del Responsable #1 Firma y Cédula del Responsable #2

ANEXO K: Comentarios – Formulario de Evaluación - Auditores

AUDITOR 14:

		Comentarios
REQ_ID	**Sub-Heurística asociada**	**Descripción**
1	S11- El sistema soporta y hace uso por defecto del protocolo HTTPS?	
	O1- ¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?	
2	S3- ¿El proceso de autenticación hace cumplir un límite de intentos de acceso no válidos consecutivos por un usuario?	Incrementa la seguridad pero afecta la usabilidad de manera negativa
3	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	
4	U2- ¿La información de seguridad presentada en pantalla es relevante?	No encontré la sección ayuda
	U11- ¿La información relacionada con la seguridad es presentada de una manera coherente y estandarizada?	No encontré la sección ayuda
	U19- ¿La información necesaria para tomar una buena decisión de seguridad, es adecuada y está disponible antes de que se adopte la medida?	No encontré la sección ayuda
	U22- ¿La información proporcionada por la ayuda es relevante?	No encontré la sección ayuda
5	U9- ¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?	

6	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?	
	S8- ¿El sistema hace cumplir el nivel de complejidad de la contraseña, con los requisitos mínimos exigidos?	
	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?	
	A3- En un proceso de autenticación, ¿el sistema evita esfuerzo adicional?	No entiendo "evita esfuerzo adicional"
7	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?	
	S9- ¿El sistema posee políticas de privacidad para comercio o contenido del usuario?	
8	A2-¿El sistema evita el uso de claves aleatorias para la etapa de registro o autenticación?	
9	U7-¿Las sentencias de alerta son simples, cortas y comprensibles?	
	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?	
	O2- En un proceso de autenticación, ¿este tiene palabras adecuadas para desarrollar una acción en particular?	
	F3- Si el proceso de inicio de sesión falla, ¿el sistema evita indicarle al usuario qué parte del proceso es incorrecto?	
10	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?	
11	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?	
	S2- Si el sistema utiliza "cookies informáticos", ¿la información sobre la privacidad del sistema describe con precisión el uso de estas cookies?	
	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?	
	S7- ¿El sistema describe cada opción de privacidad en detalle?	
	F2- ¿Está claramente establecido el propósito de utilizar la información personal del usuario?	
12	S5- ¿La información de privacidad del sistema garantiza al usuario el derecho a optar por compartir información no crítica con terceros?	
13	U24- ¿El sistema notifica a los usuarios si está interactuando con fuentes no confiables e interpone algún tipo de bloqueo que evita males mayores?	

	S6- ¿El sistema notifica y da posibles soluciones al usuario sobre vulnerabilidades asociados a incidentes de seguridad detectados?	
14	U12- En un proceso de autenticación por conocimiento, ¿el sistema permite minimizar la carga de memoria para los usuarios?	
	A1- ¿El sistema permite usar passwords gráficos para usuarios con dificultades de lectura?	
	A3- En un proceso de autenticación, ¿el sistema evita esfuerzo adicional?	No entiendo "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?	
15	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	
	F1- ¿La interfaz ayuda al usuario a tener una experiencia segura y satisfactoria con el sistema?	
16	U25- ¿El sistema muestra logos de seguridad?	
	U26- ¿El sistema tiene certificados de seguridad otorgados por entidades externas reconocidas?	
	O1- ¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?	
17	U21- ¿Hay una función de ayuda de seguridad visible?	

18	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?	
19	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?	
20	U3- ¿Los íconos de seguridad son identificables y diferenciables?	
	U4- ¿Las etiquetas de seguridad son sencillas, fáciles de entender y representativas?	
	U6- ¿El sistema está diseñado de manera que los botones con nombres similares, no desarrollen acciones de seguridad opuesto?	
	U20- ¿Los iconos de seguridad poseen etiqueta?	
21	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	
22	U23- ¿El sistema provee soporte técnico en línea para solucionar problemas de seguridad?	Solo línea telefónica no es suficiente
23	U1- Después de que el usuario complete una acción de seguridad, ¿la realimentación indica que el siguiente grupo de acciones puede ser iniciado?	

No presenta comentarios generales.

AUDITOR 2:

		Comentarios
REQ_ID	**Sub-Heurística asociada**	**Descripción**
1	S14- El sistema soporta y hace uso por defecto del protocolo HTTPS?	Hace uso del protocolo y el usuario no siente a qué hora usa el protocolo. Sin embargo sólo funciona bien en Internet Explorer y no en otros browsers. Lo que amenza también la accesibilidad.
	O1- ¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?	No soy muy experto en las normas, pero por mi experiencia, la autenticación en temas bancarios debiera ser más segura. Una clave que se envía al correo y no contar con una segunda clave es muy peligroso. Aquí a la usabilidad le va muy bien, parece haber sido priorizada sobre la seguridad.
2	S4- ¿El proceso de autenticación hace cumplir un límite de intentos de acceso no válidos consecutivos por un usuario?	Si y en términos de seguridad cumple. Pero en términos de usabilidad es muy pobre, no avisa sobre el número de intentos y saber que pasó y recuperar a clave muchas veces no es sencillo.
3	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	No lo hace
4	U2- ¿La información de seguridad presentada en pantalla es relevante?	Sólo el tema del cambio de contraseña y usuario autenticado.

		Es malo para los dos atributos.
	U11- ¿La información relacionada con la seguridad es presentada de una manera coherente y estandarizada?	Consecuente con la anterior pregunta.
	U19- ¿La información necesaria para tomar una buena decisión de seguridad, es adecuada y está disponible antes de que se adopte la medida?	Te va mostrando el workflow con posibilidad de devolverte, pero en términos de seguridad no hay impedimentos.
	U22- ¿La información proporcionada por la ayuda es relevante?	No vi ayudas para ninguno de los dos atributos de calidad.
5	U9- ¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?	No hay vocabulario en términos de seguridad más allá de la contraseña. Esto favorece la usabilidad porquen o deterioró ningún aspecto.
6	U8- ¿Las preguntas de seguridad son expresadas en un lenguaje claro y sencillo?	No las hay
	U9- ¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?	Debiera ser "excesivo" en la pregunta porque qyedó igual que la U9
	S10- ¿El sistema hace cumplir el nivel de complejidad de la contraseña, con los requisitos mínimos exigidos?	No lo hace. Esto hace que la Usabilidad se beneficie, pero es un peligro para el usaurio.
	S13- Si es necesario realizar autenticación por multi-factor, ¿el uso de PIN es implementada, dándole libertad al usuario para decidir el número de dígitos?	Se le dá libertad, se le informa y no afecta la usabilidad
	A3- En un proceso de autenticación, ¿el sistema evita esfuerzo adicional?	Para entrar no hay problema. Para ejecutar procesos es que se descubre que sólo funciona bien con iternet Explorer. Allí

		está el esfuerzo adicional.
7	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?	No hay mucha información sobre las prácticas de privacidad.
	S12- ¿El sistema posee políticas de privacidad para comercio o contenido del usuario?	No se perciben las políticas más allá de los mismos servicios
8	A2-¿El sistema evita el uso de claves aleatorias para la etapa de registro o autenticación?	No lo evita esto me parece riesgoso. Además es poco usable el proceso. De 10 cambios en 6 ocasiones he tenido que ir a soporte técnico.
9	U7-¿Las sentencias de alerta son simples, cortas y comprensibles?	Pocas sentencias de alerta que afectan ambos atributos, pero es más crítico con la seguridad.
	U15- ¿Los mensajes de error relacionados con la seguridad son significativos y sensibles al problema?	No veo tales mensajes. Debe estar afectando la seguridad. La Usabilidad no se ve afectada por este aspecto.
	U16- ¿Los mensajes de error relacionados con la seguridad indican la acción que el usuario debe tomar para corregir el error?	Idem anterior pregunta
	U17- ¿Los mensajes de error relacionados con la seguridad son adecuados al lenguaje del usuario?	Idem anterior pregunta
	U18- ¿Los mensajes de error relacionados con la seguridad indican al usuario dónde obtener ayuda?	Idem anterior pregunta
	O2- En un proceso de autenticación, ¿este tiene palabras adecuadas para desarrollar una acción en particular?	La operatividad es buena en términos de uso, pero es peligrosa en términos de seguridad

	F4- Si el proceso de inicio de sesión falla, ¿el sistema evita indicarle al usuario qué parte del proceso es incorrecto?	No. Al indicarle que la clave es incorrecta le confirma que el usuario existe. Al ponerle un usuario inexistente el sistema informa. Esto es muy bueno en términos de uso, pero pésimo considerando la seguridad.
10	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?	El usuario se puede desplazar fácilmente por todo el sistema, no pide una autenticación adicional. Fácil pero inseguro.
11	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?	No existen. Si existen están muy bien camuflados. En téminos de seguridad me parece muy bueno porque no van indicando las zonas vulnerables. Pero en términos de awarness del usaurio sobre el cuidado es pobre.
	S3- Si el sistema utiliza "cookies informáticos", ¿la información sobre la privacidad del sistema describe con precisión el uso de estas cookies?	No usa cookies
	S6- ¿Se presenta al usuario mensajes de notificación concernientes a la seguridad y privacidad antes de acceder al sistema?	No, por lo tanto generan desconocimiento, pero no entorpecen el modelo mental de uso del sistema.
	S7- ¿La información de privacidad del sistema garantiza al usuario el derecho a optar por compartir información no crítica con terceros?	Esto no lo puedo evaluar, nunca lo ha pedido.
	S9- ¿El sistema describe cada opción de privacidad en detalle?	No lo hace. Así que no genera ruido en téminos de usabilidad. Pero en términos de

		seguridad genera desconocimiento.
	F2- ¿Está claramente establecido el propósito de utilizar la información personal del usuario?	No
12	S7- ¿La información de privacidad del sistema garantiza al usuario el derecho a optar por compartir información no crítica con terceros?	No
13	U24- ¿El sistema notifica a los usuarios si está interactuando con fuentes no confiables e interpone algún tipo de bloqueo que evita males mayores?	Lo hace para la contraseña, pero no notifica. En términos de seguridad es bueno, pero en términos de usabilidad es pésimo el no saber que está pasando.
	S8- ¿El sistema notifica y da posibles soluciones al usuario sobre vulnerabilidades asociados a incidentes de seguridad detectados?	No lo hace. Pésimo para la seguridad, no interfiere la usabilidad.
14	U12- En un proceso de autenticación por conocimiento, ¿el sistema permite minimizar la carga de memoria para los usuarios?	No pregunta es nada. Usable pero poco segura.
	A1- ¿El sistema permite usar passwords gráficos para usuarios con dificultades de lectura?	Malo para ambos atributos.
	A3- En un proceso de autenticación, ¿el sistema evita esfuerzo adicional?	Si pero afecta la seguridad.
	A4- ¿El sistema provee a los usuarios otras alternativas para autenticarse?	No, pero es bueno en términos de seguridad. Un agujero menos que tapar.
	A5- ¿El método de autenticación sirve a usuarios nuevos y experimentados?	Si es simple. Pero un muy experimentado puede acceder pidiendo de nuevo la contraseña, accediendo a su correo, cambiando la cuenta de depósito y

		haciendo un avance de prima(el cual ya cuenta con el pagaré en el Foduc)
15	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	No
	F1- ¿La interfaz ayuda al usuario a tener una experiencia segura y satisfactoria con el sistema?	Más o menos, pero no es cierta
16	U25- ¿El sistema muestra logos de seguridad?	No. Esto lo hace usable pero no seguro.
	U26- ¿El sistema tiene certificados de seguridad otorgados por entidades externas reconocidas?	No. Esto lo hace usable pero no seguro.
	O1- ¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?	Segurisimo que no. Pero entonces el proceso de uso es muy fácil.
17	U21- ¿Hay una función de ayuda de seguridad visible?	No. Esto es muy malo para cubrir los dos atributos.
18	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?	No lo hace. Esto lo hace simple de usar, pero no es nada seguro.
19	U13- ¿Los mensajes de error relacionados con la seguridad informan al usuario de la gravedad del error?	No hay información. Eso es muy bueno en términos de seguridad, un intruso explorando y ganando información sería peligrosísimo.
	U14- ¿El sistema facilita la posibilidad al usuario de solucionar problemas a posibles errores?	No hay información. Eso es muy bueno en términos de seguridad, un intruso explorando y ganando información sería peligrosísimo.
	U15- ¿Los mensajes de error relacionados con la seguridad son significativos y sensibles al problema?	No hay información. Eso es muy bueno en términos de seguridad,

		un intruso explorando y ganando información sería peligrosísimo.
	U16- ¿Los mensajes de error relacionados con la seguridad indican la acción que el usuario debe tomar para corregir el error?	No hay información. Eso es muy bueno en términos de seguridad, un intruso explorando y ganando información sería peligrosísimo.
20	U3- ¿Los íconos de seguridad son identificables y diferenciables?	No y esto es bueno en términos de uso. Sólo está la llavecita.
	U4- ¿Las etiquetas de seguridad son sencillas, fáciles de entender y representativas?	No y esto es bueno en términos de uso. Sólo está la llavecita.
	U6- ¿El sistema está diseñado de manera que los botones con nombres similares, no desarrollen acciones de seguridad opuesto?	Como es poco esto anda bien.
	U20- ¿Los iconos de seguridad poseen etiqueta?	Si, la llavecita.
21	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	Si pero no indica mucho.
22	U23- ¿El sistema provee soporte técnico en línea para solucionar problemas de seguridad?	No, pero es un agujero menos de seguridad por cubrir.
23	U1- Después de que el usuario complete una acción de seguridad, ¿la realimentación indica que el siguiente grupo de acciones puede ser iniciado?	Si esto lo indica directamente, no lo envía encriptado a algún correo. Es muy bueno en términos de feedback, pero es inseguro que le indiquen en el correo información que no es conveniente que intrusos sepan.

COMENTARIOS GENERALES	
1	El sistema no es muy usable en téminos del manejo de las equivocaciones en el uso, hay poco feedback. Sin embargo esto lo hace más críptico y por lo tanto más difícil de violentar.
2	El sistema operacionalmente es muy limpio, no se interfiere en el muchos aspectos de segurar. Esto lo hace más fácil de usar desde la perspectiva operacional, pero es preocupante saber que no hay un nivel seguridad mayor.

AUDITOR 3:

		Comentarios
REQ_ID	**Heurística asociada**	**Descripción**
1	S14- El sistema soporta y hace uso por defecto del protocolo HTTPS?	
	O1- ¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?	No cifra contraseñas. Tuve problemas con la recuperación de contraseña.
2	S4- ¿El proceso de autenticación hace cumplir un límite de intentos de acceso no válidos consecutivos por un usuario?	No lo pude comprobar para no bloquear la cuenta de mi colega Julio
3	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	Evidencia cambiar clave de manera vistoza. No se que otras opciones de seguridad se refieren
4	U2- ¿La información de seguridad presentada en pantalla es relevante?	No se a que se refieren a la “informacion de seguirdad”, es una aplicación bancaria, se maneja dinero
	U11- ¿La información relacionada con la seguridad es presentada de una manera coherente y estandarizada?	
	U19- ¿La información necesaria para tomar una buena decisión de seguridad, es adecuada y está disponible antes de que se adopte la medida?	
	U22- ¿La información proporcionada por la ayuda es relevante?	La aplicación no tiene ayuda

5	U9- ¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?	
6	U8- ¿Las preguntas de seguridad son expresadas en un lenguaje claro y sencillo?	Preguntas de seguridad? Como cuales?
	U9- ¿Se evita el uso de vocabulario técnico o avanzado relacionado con seguridad o privacidad?	
	S10- ¿El sistema hace cumplir el nivel de complejidad de la contraseña, con los requisitos mínimos exigidos?	No valida seguridad en la contraseña
	S13- Si es necesario realizar autenticación por multi-factor, ¿el uso de PIN es implementada, dándole libertad al usuario para decidir el número de dígitos?	No tiene autenticacion multifactor. No ofrece una autenticación segura gracias a una gran variedad de opciones sencillas de verificación, como llamadas telefónicas, mensajes de texto o notificaciones de aplicaciones móviles, lo que permite a los usuarios elegir el mecanismo que prefieran.
	A3- En un proceso de autenticación, ¿el sistema evita esfuerzo adicional?	
7	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?	
	S12- ¿El sistema posee políticas de privacidad para comercio o contenido del usuario?	No evidencié ninguna politica
8	A2-¿El sistema evita el uso de claves aleatorias para la etapa de registro o autenticación?	
9	U7-¿Las sentencias de alerta son simples, cortas y comprensibles?	
	U15- ¿Los mensajes de error relacionados con la seguridad son significativos y sensibles al problema?	No es claro el mensaje: “Intente más tarde”
	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?	
	O2- En un proceso de autenticación, ¿este tiene palabras adecuadas para desarrollar una acción en particular?	
	F4- Si el proceso de inicio de sesión falla, ¿el sistema evita indicarle al usuario qué parte del proceso es incorrecto?	
10	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?	
11	U5- ¿Existen indicadores visuales de privacidad informando a los usuarios sobre las prácticas de privacidad del sistema?	
	S3- Si el sistema utiliza "cookies informáticos", ¿la información sobre la privacidad del sistema describe con precisión el uso de estas cookies?	
	S6- ¿Se presenta al usuario mensajes de notificación concernientes a la seguridad y privacidad antes de acceder al sistema?	
	S7- ¿La información de privacidad del sistema garantiza al usuario el derecho a optar por compartir información no crítica con terceros?	
	S9- ¿El sistema describe cada opción de privacidad en detalle?	
	F2- ¿Está claramente establecido el propósito de utilizar la información personal del usuario?	
12	S7- ¿La información de privacidad del sistema garantiza al usuario el derecho a optar por compartir información no crítica con terceros?	
13	U24- ¿El sistema notifica a los usuarios si está interactuando con fuentes no confiables e interpone algún tipo de bloqueo que evita males mayores?	
	S8- ¿El sistema notifica y da posibles soluciones al usuario sobre vulnerabilidades asociados a incidentes de seguridad detectados?	

14	U12- En un proceso de autenticación por conocimiento, ¿el sistema permite minimizar la carga de memoria para los usuarios?	
	A1- ¿El sistema permite usar passwords gráficos para usuarios con dificultades de lectura?	
	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?	
15	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	No se a que se refieren con “elementos de seguirdad”
	F1- ¿La interfaz ayuda al usuario a tener una experiencia segura y satisfactoria con el sistema?	
16	U25- ¿El sistema muestra logos de seguridad?	
	U26- ¿El sistema tiene certificados de seguridad otorgados por entidades externas reconocidas?	El certificado de seguridad lo da Symantec Corporation
	O1- ¿El método de autenticación empleado sigue normas conocidas (sean estándares o no) donde su seguridad sea adecuada?	Le faltan detalles
17	U21- ¿Hay una función de ayuda de seguridad visible?	
18	S1- ¿El sistema permite acceder a las áreas protegidas o confidenciales con algún método de autenticación?	
19	U13- ¿Los mensajes de error relacionados con la seguridad informan al usuario de la gravedad del error?	No encontre mensajes al respecto
	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?	
20	U3- ¿Los íconos de seguridad son identificables y diferenciables?	Icono de seguridad? El unico es la llave de cambiar contraseña
	U4- ¿Las etiquetas de seguridad son sencillas, fáciles de entender y representativas?	
	U6- ¿El sistema está diseñado de manera que los botones con nombres similares, no desarrollen acciones de seguridad opuesto?	
	U20- ¿Los iconos de seguridad poseen etiqueta?	
21	U10- ¿Los menús en la interfaz de usuario hace evidente cuáles elementos de seguridad pueden ser seleccionados?	Elementos de seguridad? Esto confunde, ya estando en la aplicación todo hace parte de las tareas que el usuario puede hacer, es difcil sabe cuales de esas son clasificadas dentro de elementos de seguridad.
22	U23- ¿El sistema provee soporte técnico en línea para solucionar problemas de seguridad?	
23	U1- Después de que el usuario complete una acción de seguridad, ¿la realimentación indica que el siguiente grupo de acciones puede ser iniciado?	No pude probar esto.

COMENTARIOS GENERALES	
1	Las preguntas no son fáciles de interpretar, sobre todo al referirse con “elementos de seguridad”

ANEXO L: Marco Metodológico ajustado a la metodología Scrum

1.1 CREACIÓN DE LA PILA DEL PRODUCTO.

La pila de producto es el corazón de Scrum. La Pila de Producto es, básicamente, una lista priorizada de requisitos, o historias.

Historias de Usuario – Proyecto Trabajo de Grado **Evaluación Heurística de Seguridad Usable Aplicada en Sistemas e-Banking**					
ID	Historia	Importancia	Tiempo Total (días)	Estado	Fecha de finalización
1	Fase de exploración: Exploración de los núcleos temáticos, Seguridad Usable (USec), heurísticas de evaluación, principios de evaluación, e-Banking, HCISec	100	52	Terminado	01/03/2016
2	Fase de exploración: Entrega Anteproyecto	100	40	Terminado	15/03/2016
3	Fase de ejecución: Consolidar requerimientos e-Banking	70	60	Terminado	20/06/2016
4	Fase de ejecución: Consolidar principios e-Banking	60	30	Terminado	25/07/2016
5	Fase de ejecución: Consolidar estudio de caso a llevar a cabo.	60	120	Terminado	15/08/2016
6	Fase de ejecución: Conceptos Matemáticos para cálculo de USec	80	60	Terminado	30/08/2016
7	Fase de ejecución: Herramienta matemática para cálculo de USec	100	120	Terminado	20/09/2016
8	Fase de ejecución: Escala para la medición de USec	70	20	Terminado	30/09/2016
9	Fase de ejecución: Contactar con Expertos, Auditores y Usuarios	70	60	Terminado	31/10/2016
10	Fase de ejecución: Contactar con Matemático	50	90	Terminado	28/10/2016

11	Fase de ejecución: Encuesta de satisfacción	50	60	Terminado	28/10/2016
12	Fase de ejecución: Herramienta para expertos	80	30	Terminado	20/09/2016
13	Fase de ejecución: Herramienta para auditores	80	30	Terminado	01/10/2016
14	Diligenciar formulario expertos, encuestas de satisfacción y evaluación auditores	100	60	Terminado	4/11/2016
15	Fase de consolidación: Análisis de resultados	100	5	Terminado	09/11/2016
16	Fase de consolidación: Conclusiones, limitaciones y trabajo futuro	70	2	Terminado	09/11/2016
17	Fase de divulgación: Entrega Monografía	100	1	Terminado	09/11/2016
18	Fase de divulgación: Sustentación de trabajo de grado	100	1	En ejecución	14/12/2016

Sprints Realizados.

Primer Sprint

1. REQUISITO: Construcción Capitulo 1
SUBACTIVIDADES
1.1. Definición del problema
1.2. Definición de objetivos
1.3. Contribuciones del trabajo

Segundo Sprint

2. REQUISITO: Construcción Capítulo 2
SUBACTIVIDADES
2.1. Establecer estado del arte
2.2. Revisión de avances director de trabajo de grado

2.3. Correcciones
2.4. Validación

Tercer Sprint

3. REQUISITO: Construcción Capítulo 3
SUBACTIVIDADES
3.3 Recolección de requerimientos
3.4 Recolección de principios
3.5 Construcción de formato de evaluación heurística para sistemas e-Banking

Cuarto Sprint

4. REQUISITO: Construcción Capítulo 4.
SUBACTIVIDADES
4.1 Recolección de conceptos matemáticos para la construcción de modelo matemático
4.2 Consolidar primer prototipo de modelo matemático
4.3 Validar del modelo con matemático
4.4 Ajustar Modelo Matemático

Quinto Sprint

5. REQUISITO: Construcción Capítulo 5.
SUBACTIVIDADES
5.1 Realizar encuesta de satisfacción
5.2 Evaluación Heurística
5.3 Análisis de resultados

Sexto Sprint

6. REQUISITO: Construcción Capítulo 6
SUBACTIVIDADES
5.1 Presentación 11CCC
5.2 Desarrollo de conclusiones, limitaciones y trabajo futuro.

5.3 Entrega de monografía y sustentación de trabajo de grado