Universidad del Bío-Bío
Facultad de Ciencias Empresariales
Departamento de Ciencias de la Computación y Tecnologías de la Información

Tesis de Magíster en Ciencias de la Computación

Framework para la Comparación y Selección de Esquemas para la Autenticación Multi-Factor

Chillán, Chile, Marzo 2017

Estudiante: Ignacio Andrés Velásquez Lagos
Directora de Tesis: María Angélica Caro Gutiérrez
Co-Director de Tesis: Alfonso Rodríguez Ríos

Índice General

Resumen

Autenticación es el proceso de verificar la identidad de un usuario, como prerrequisito para permitir el acceso a los recursos de un sistema. Un factor de autenticación es, entonces, una pieza de información usada para autenticar a dicho usuario. Existen tres grupos de factores de autenticación: aquellos basados en conocimiento (algo que se sabe), aquellos basados en objetos (algo que se posee) y aquellos basados en la identidad (algo que se es). Esquemas de autenticación de distintos factores pueden ser combinados para incrementar la seguridad, en lo que se conoce como métodos de autenticación multi-factor.

Si bien existen múltiples propuestas de uso de autenticación multi-factor en la literatura, se observa la ausencia de un método que permita la comparación y selección de las distintas técnicas de autenticación de una forma adecuada, especialmente tomando en cuenta los requerimientos de seguridad de los clientes. Por medio de una revisión sistemática de la literatura, se ha encontrado un número de Framework que permiten el análisis de técnicas de autenticación, sin embargo, no proveen todas las herramientas necesarias para realizar una comparación y selección adecuada de éstas, sobre todo considerando los métodos de autenticación multi-factor.

Es por lo anterior que esta investigación se centra en la creación de un Framework de recomendación que guíe en la comparación y selección tanto de esquemas de autenticación de un factor como de métodos de autenticación multi-factor. Esto considerando los requerimientos del cliente, representados como criterios de comparación y selección, y el contexto para el que va dirigida la aplicación a desarrollar, todo esto basándose no solo en el conocimiento que se pueda obtener desde la literatura, si no que complementándolo además con la experiencia que se pueda obtener de parte de expertos en la industria.

Consecuentemente, se ha realizado una revisión sistemática de la literatura, con el objetivo de obtener el conocimiento existente en la academia acerca de esquemas y métodos de autenticación, junto con criterios para su comparación y selección. Y además, se realizan encuestas y entrevistas para recopilar la experiencia de expertos en la industria sobre este mismo tema. En base a lo anterior, se genera una propuesta inicial de un Framework, el cual es validado por medio de un panel de expertos y de casos de estudio. Como resultado, se obtiene un Framework de decisión debidamente validado, que ayuda en la comparación y selección tanto de esquemas de autenticación de un factor como de métodos de autenticación multi-factor, junto con un prototipo de herramienta, que permite un fácil uso del Framework dentro de empresas de desarrollo de Software, cubriendo así la brecha detectada en la literatura.

Abstract

Authentication is the process of verifying the identity of a user, as a prerequisite for allowing access to a system's resources. An authentication factor is, then, a piece of information used to authenticate said user. There are three authentication factor groups: those based on knowledge (something that is known), those based in objects (something that is possessed) and those based on identity (something that one is). Authentication schemes of distinct factors can be combined to increase security, in what is known as multi-factor authentication methods.

Although there are multiple proposals on the use of multi-factor authentication in literature, the absence of a method that allows the comparison and selection of the different authentication techniques in an adequate manner, especially considering the security requirements of clients, is observed. Through a systematic literature review, a number Frameworks that allow the analysis of authentication techniques have been found, but they do not provide all of the tools that are needed to do a correct comparison and selection of these techniques, especially considering multi-factor authentication methods.

Due to the above, this research is centered in the creation of a recommendation Framework that guides the comparison and selection both of single-factor authentication schemes and multi-factor authentication methods. This considering both the clients' requirements, represented as comparison and selection criteria, and the context for which the application to develop is directed, all of this based not only in the knowledge that could be obtained from literature, but also complementing it with the experience that could be obtained from experts in the industry.

Consequently, a systematic literature review is performed, with the objective of obtaining the existing knowledge in academy about authentication schemes and methods, together with criteria for their comparison and selection. Moreover, surveys and interviews are performed to gather the experience of industry experts about this same topic. Based on the above, an initial Framework proposal is generated, which is validated through the realization of an expert panel and study cases. As a result, an adequately validated decision Framework, that helps in the comparison and selection of both single-factor authentication schemes and multi-factor authentication methods, together with a tool prototype, which allows an easy use of the Framework on Software development companies, are obtained, thus covering the detected breach in literature.

Capítulo 1
Introducción

1.1 Planteamiento y Justificación del Trabajo

La Autenticación es el proceso de verificar positivamente la identidad de un usuario, dispositivo u otra entidad en un sistema computacional, generalmente como un prerrequisito para permitir el acceso a los recursos de un sistema (O'Gorman, 2003). Un factor de autenticación es, entonces, una pieza de información usada para autenticar o verificar la identidad de un usuario (Rathgeb y Uhl, 2010). Estos factores pueden ser categorizados en tres grupos: aquellos basados en conocimiento (algo que el cliente sabe, como contraseñas o códigos PIN), aquellos basados en objetos (algo que el cliente posee, dependientes de una posesión física) y aquellos basados en la identidad (algo que el cliente es, biométricas) (Al-Assam *et al.*, 2010; Huang *et al.*, 2011). Esquemas de autenticación (soluciones de autenticación concretas) pertenecientes a distintos factores pueden ser combinados para incrementar la seguridad, lo cual se conoce como autenticación multi-factor (O'Gorman, 2003).

Para diferenciar entre propuestas de un factor y aquellas multi-factor, desde este punto se referirá a las primeras como *Esquemas* de Autenticación, mientras que a las segundas se les llamará *Métodos* de Autenticación Multi-Factor.

Aunque existen múltiples propuestas de uso de autenticación multi-factor en la literatura, tales como (Huang *et al.*, 2011), (Pointcheval y Zimmer, 2008) y (Stebila *et al.*, 2009), es posible observar la ausencia de un método que ayude a decidir cuándo usar uno u otro esquema de autenticación y como combinarlos de la manera más adecuada en una modalidad multi-factor, especialmente tomando en cuenta los requerimientos entregados por los clientes en aplicaciones Software. Si bien existen algunos Framework en la literatura que proveen un análisis de múltiples características de esquemas de autenticación (Bonneau *et al.*, 2012; Forget *et al.*, 2015), éstos se encuentran centrados en los esquemas por separado y no a modo de ser usados como multi-factor, sin poner un énfasis en los requerimientos de los clientes y no entregando una respuesta concreta para cada situación.

Debido a lo anterior, esta propuesta se centra en la creación de un Framework que guíe la selección de esquemas de autenticación y su combinación dentro de un método multi-factor, considerando diferentes contextos de aplicación, definidos según los requerimientos entregados por los clientes, para lo cual se aplican criterios de comparación y selección, basándose tanto en la literatura como en la experiencia de expertos de la industria, complementando los dos puntos de vista.

Se busca comprobar la hipótesis de que *"el uso de un Framework que guíe a desarrolladores de aplicaciones Software en la selección de esquemas de autenticación para su uso combinado, sistematiza y facilita el uso de los métodos de autenticación multi-factor más apropiados al contexto de uso"*.

1.2 Objetivos

1.2.1 Objetivo Principal

Desarrollar un estudio de los esquemas de autenticación y métodos multi-factor propuestos en la literatura, describir sus características e identificar criterios de selección propuestos tanto en la academia como en la industria, tales como usabilidad, factibilidad de implementación, contexto de la aplicación, etc. En base a este material, proponer un Framework que permita hacer la selección de los métodos de autenticación multi-factor más apropiados para un determinado contexto de desarrollo y operación de una aplicación Software.

1.2.2 **Objetivos Específicos**

Los objetivos específicos a realizar para cumplir con el objetivo principal propuesto son los siguientes:

- Realizar una revisión de la literatura con el propósito de conocer los principales esquemas de autenticación y métodos multi-factor utilizados en soluciones de aplicaciones Software.
- Recopilar criterios de selección y diferenciación de los métodos de autenticación multi-factor, tanto aquellos presentes en la literatura, como aquellos utilizados en la industria.
- Crear un Framework que provea una guía para la comparación y selección de esquemas y métodos de autenticación multi-factor, basándose en las experiencias reportadas en la literatura y la industria.
- Construir un prototipo de herramienta que permita la utilización del Framework en diferentes contextos de desarrollo y operación de una aplicación Software.
- Demostrar la validez de la propuesta, junto con la utilidad del prototipo de herramienta, por medio de casos de estudio.

1.3 **Alcance de la Investigación**

Se creará un prototipo de herramienta que facilite la toma de decisiones al momento de seleccionar qué métodos de autenticación multi-factor utilizar en una aplicación Software específica, entregando propuestas según las características de la aplicación y los requerimientos del cliente. Este prototipo será utilizado en los casos de estudio a realizar, para los cuales se contempla la comparación de los esquemas seleccionados por el Framework versus los utilizados en determinada aplicación, o versus los que recomendaría un grupo de expertos.

El Framework a desarrollar se basará en los resultados de la revisión de la literatura y entrevistas a desarrolladores expertos de la industria, pertenecientes a la empresa multinacional Nisum Technologies, la cual posee sedes en Chile, India y Estados Unidos.

La propuesta considera de base los tres factores de autenticación ampliamente conocidos (“algo que se sabe”, “algo que se posee” y “algo que se es”), pudiendo incorporar otros que puedan estar propuestos en la literatura, como aquel de “alguien que conoces” (Brainard *et al.*, 2006).

1.4 **Organización de la Tesis**

El presente capítulo entrega una introducción del tema a desarrollar durante esta investigación, presentando el planteamiento y la justificación del trabajo en la Sección 1.1, el objetivo principal de la investigación, junto con los objetivos específicos para cumplir con éste en la Sección 1.2, el alcance de la investigación en la sección 1.3 y la sección actual que cubre la organización de los capítulos de esta tesis.

El Capítulo 2 cubre la descripción de las metodologías de trabajo utilizadas durante la investigación. En la Sección 2.1 se habla sobre las revisiones sistemáticas de la literatura, mientras que en la Sección 2.2 se toca el desarrollo de encuestas y en la Sección 2.3 se describe la realización de casos de estudio. En la Sección 2.4 se toca la metodología de trabajo que abarca a toda la investigación, la cual es la investigación-acción.

En el Capítulo 3 se presenta el estado del arte obtenido por medio de la realización de la revisión sistemática de la literatura, entregando, en la Sección 3.1, los resultados generales de ésta, para luego presentar los resultados específicos de cada tema considerado en las preguntas de investigación en las

Secciones 3.2, a 3.5. En la Sección 3.6 se discuten los resultados obtenidos, mientras que en la Sección 3.7 se entregan las conclusiones pertinentes.

Se dedica el Capítulo 4 a todo el proceso que se llevó a cabo para la generación del Framework. En la Sección 4.1 se resumen los hallazgos importantes para la investigación obtenidos en la revisión de la literatura, para luego proceder a documentar la realización de encuesta y entrevistas a expertos de la industria en la Sección 4.2, lo cual complementa a lo obtenido en la revisión sistemática de la literatura. En la Sección 4.3 se presenta la propuesta inicial de Framework, la cual es validada posteriormente por un panel de expertos, documentado en la Sección 4.4, y por medio de una encuesta adicional presentada en la Sección 4.5. La propuesta final del Framework es detallada en la Sección 4.6.

En el Capítulo 5 se documenta el prototipo de herramienta que ha sido desarrollado para facilitar el uso del Framework. Las características generales de éste son presentadas en la Sección 5.1, mientras que se describe su base de datos en la Sección 5.2. La Sección 5.3 muestra las principales pantallas del prototipo de herramienta.

El Capítulo 6 abarca la validación realizada respecto de las respuestas que entrega el Framework, la cual fue realizada por medio de casos de estudio. Se utilizaron dos tipos de casos de estudio: se tiene aquellos basados en aplicaciones reales, desarrolladas por expertos de la industria pertenecientes a Nisum Technologies, los cuales son documentados en la Sección 6.1; y aquellos generados hipotéticamente, a modo de validar los casos extremos a los que se podría ver enfrentado el Framework, los que se presentan en la Sección 6.2. En la Sección 6.3 se realizan la discusión y conclusiones relacionadas a los casos de estudio.

Finalmente, en el Capítulo 7 se entregan las conclusiones de la investigación, las cuales incluyen el análisis de los objetivos propuestos y cumplidos, en la Sección 7.1, el principal aporte de la investigación, mencionado en la Sección 7.2, los trabajos futuros que se tienen contemplados, presentados en la Sección 7.3, y el contraste de resultados, que se observa en la Sección 7.4

Capítulo 2
Metodología de Trabajo

En este capítulo se presenta la metodología de trabajo utilizada para el desarrollo de esta tesis, en la cual se define una serie de actividades para la realización de la investigación, entre ellas:

- Realización de una revisión sistemática de la literatura con el propósito de obtener el conocimiento sobre los principales esquemas y métodos de autenticación, además de obtener criterios de comparación y selección entre estos esquemas y métodos.
- Desarrollo de encuestas a expertos en la industria para recopilar su experiencia en cuanto a criterios de selección y diferenciación de esquemas y métodos de autenticación.
- Validación de los resultados de la investigación por medio de la realización de casos de estudio.

Adicionalmente, la totalidad del proceso de investigación que se lleva a cabo para esta tesis puede ser englobado dentro del método de investigación conocido como investigación-acción.

El resto de este capítulo se enfoca en describir cada una de las metodologías de trabajo utilizadas durante el desarrollo de esta tesis. De este modo, en la sección 2.1 se describen las revisiones sistemáticas de la literatura, en la sección 2.2 se aborda el desarrollo de encuestas, en la sección 2.3 se habla sobre los casos de estudio y en la sección 2.4 se trata el tema de la investigación-acción.

2.1 **Revisión Sistemática de la Literatura**

Una Revisión Sistemática de la Literatura (RSL) es un medio para identificar, evaluar e interpretar toda la investigación disponible para responder a unas preguntas de investigación específicas (Keele, 2007). Una RSL difiere de revisiones de la literatura tradicionales principalmente porque se planifican formalmente y se ejecutan de manera sistemática y metódica (Genero *et al.*, 2014). Las revisiones sistemáticas de la literatura pueden ser replicables de forma independiente, lo que les da un mayor valor científico, además, al encontrar, evaluar y resumir toda la evidencia disponible sobre un tema específico de investigación, se puede obtener un alto nivel de validez por medio de sus conclusiones (Genero *et al.*, 2014).

Para llevar a cabo una RSL, se sigue un proceso que consta de tres actividades principales, cada una de ellas con varias tareas secuenciales, como se observa en la Tabla 1 (Keele, 2007).

Tabla 1. Proceso para realizar revisiones sistemáticas de la literatura.

Etapas	**Actividades**
Etapa 1	*Planificar la Revisión*
1.1	Identificar la necesidad de la revisión
1.2	Formular las preguntas de investigación
1.3	Definir el protocolo de la revisión
1.4	Validar el protocolo de la revisión
Etapa 2	*Realizar la Revisión*
2.1	Identificar la investigación relevante
2.2	Seleccionar los estudios primarios
2.3	Extraer los datos relevantes
2.4	Sintetizar los datos extraídos
Etapa 3	*Reportar la Revisión*

2.1.1 **Planificación de la Revisión**

El principal objetivo de esta etapa es especificar todos los aspectos que harán que la revisión sea sistemática y rigurosa, evitando posibles sesgos o ambigüedades, y que se detallan en lo que se denomina protocolo de la revisión (Genero *et al.*, 2014). Las tareas realizadas durante esta etapa son las siguientes:

- **Identificación de la necesidad de la revisión:** ésta surge de la necesidad de resumir toda la información relevante sobre un tema de interés.
- **Formulación de las preguntas de investigación:** la especificación de estas preguntas dirigirá todo el proceso de revisión. En el proceso de búsqueda se deben seleccionar los estudios que sirvan para responderlas; en el proceso de extracción se deben extraer los datos necesarios para responderlas; y en el proceso de análisis de datos éstos se deben de sintetizar de tal manera que las preguntas puedan ser respondidas.
- **Definición del protocolo de revisión:** éste es un plan formal y concreto para llevar a cabo la revisión sistemática, que debe definirse para definir la posibilidad de sesgos (Genero *et al.*, 2014). A continuación se describen los principales elementos que debe tener el protocolo de revisión:
    - **Antecedentes y preguntas de investigación:** éstos corresponden a aquello identificado durante las tareas anteriores de esta etapa.
    - **Estrategia de búsqueda:** define la cadena de búsqueda, el periodo de búsqueda y las fuentes de búsqueda (Genero *et al.*, 2014). Durante esta investigación se está utilizando una variante del método propuesto en (Keele, 2007) para la realización de revisiones sistemáticas (Caro *et al.*, 2005), en donde la estrategia de búsqueda se considera como un protocolo adicional al protocolo de revisión, llevando el nombre de protocolo de búsqueda.
    - **Criterios de selección de estudios:** criterios de inclusión y exclusión que deben ser definidos con el objetivo de identificar los estudios que muestren evidencia con respecto a las preguntas de investigación.
    - **Procedimiento para la selección de estudios:** se indica como son aplicados los criterios de inclusión y exclusión, considerando o no, por ejemplo, la lectura de los artículos completos o solo de su resumen.
    - **Estrategia para la extracción de datos y síntesis de los datos extraídos:** para extraer la información relevante es necesario diseñar un formulario de extracción de datos y también puede ser necesario definir un esquema de clasificación. Para la construcción de conocimiento y para llegar a conclusiones sobre algún tema de interés, es necesario comparar y contrastar la evidencia de varios estudios, para lo cual se debe realizar una síntesis de los datos extraídos.
- **Validación del protocolo de revisión:** es conveniente que el protocolo sea evaluado por expertos. En el caso de estudiantes, es posible que éstos presenten el protocolo a sus directores para que lo evalúen.

2.1.2 **Realización de la Revisión**

En esta etapa se pone en práctica todo lo planificado en el protocolo y se obtienen los resultados que responderán a las preguntas de investigación (Genero *et al.*, 2014). Las tareas a realizar durante esta etapa son las siguientes:

- **Identificación de la investigación relevante:** el conjunto de publicaciones relevantes para responder a las preguntas de investigación se encuentran siguiendo la estrategia de búsqueda definida en el protocolo.
- **Selección de los estudios primarios:** se debe localizar los estudios que muestren evidencia relacionada con las preguntas de investigación, siguiendo lo planificado en el protocolo.
- **Extracción de los datos relevantes:** en esta tarea se rellenará el formulario de extracción de datos definido en el protocolo.
- **Sintetizado de los datos extraídos:** se procede a sintetizar los datos extraídos, a modo de dar respuesta a las preguntas formuladas. La síntesis es comúnmente acompañada de tablas y gráficos para ilustrar los resultados.

2.1.3 **Reporte de la Revisión**

Finalmente, se realiza un informe que refleje todo el proceso de revisión (Genero *et al.*, 2014). Mientras más información haya disponible, más transparencia se dará a la revisión sistemática para quienes quieran usar los datos obtenidos. Al igual que con el protocolo, es importante que el informe sea validado por expertos, en este caso por los directores de tesis.

2.1.4 **Aplicación y Resultados de la Revisión Sistemática de la Literatura**

La planificación de la RSL desarrollada durante esta investigación puede ser encontrada en el Anexo A. Por otro lado, los resultados obtenidos por medio de la realización de esta revisión se encuentran a lo largo del Capítulo 3.

2.2 **Desarrollo de Encuestas**

Las encuestas son, probablemente, el método de investigación más utilizado por todo el mundo (Genero *et al.*, 2014). Una encuesta es un método empírico que se utiliza para recopilar información de personas para describir, comparar o explicar su conocimiento, actitudes o comportamiento. Las encuestas están formadas por una serie de actividades bien definidas (Kitchenham y Pfleeger, 2008) que se enumeran a continuación:

- Establecimiento de los objetivos de la encuesta.
- Diseño de la encuesta.
- Desarrollo del cuestionario.
- Evaluación y validación del cuestionario.
- Obtención de los datos de la encuesta.
- Análisis de los datos obtenidos.
- Reporte de los resultados.

2.2.1 **Establecimiento de los Objetivos de la Encuesta**

Establecer los objetivos es siempre el primer paso de una encuesta (Genero *et al.*, 2014). Cada objetivo debería establecerse como una frase relativa a los resultados esperados tras realizar la propia encuesta.

Los objetivos deben ser lo más claros posibles y han de poder medirse. Éstos determinarán la mayoría del resto de actividades del proceso de realización de encuestas, de ahí que deban establecerse cuidadosamente.

2.2.2 **Diseño de la Encuesta**

Existen distintos tipos de diseño de encuestas, entre los cuales se encuentran aquellos en los que se pide información a los participantes en un instante determinado y aquellos que tratan de conocer la evolución a través del tiempo de una determinada población (Kitchenham y Pfleeger, 2008), o aquellos que comparan poblaciones diferentes o que pretenden medir el impacto de un cambio (Shadish *et al.*, 2002).

Un aspecto importante a tener en cuenta a la hora de diseñar una encuesta es como se va a administrar (Genero *et al.*, 2014). Existen diversas opciones (Kitchenham y Pfleeger, 2008):

- Cuestionarios auto-administrados (vía Internet).
- Encuestas telefónicas.
- Entrevistas personales.

Durante el desarrollo de la presente investigación, se utilizó una combinación de entrevistas personales y cuestionarios auto-administrados, siendo el segundo el método principal.

2.2.3 **Desarrollo del Cuestionario**

Una encuesta pretende obtener respuestas sobre una serie de preguntas por una razón determinada (Genero *et al.*, 2014). Por tanto, a la hora de diseñar un cuestionario conviene partir del objetivo de la investigación. A continuación de comentan las distintas tareas a llevar a cabo para desarrollar correctamente un cuestionario:

- **Consulta de la literatura relevante:** hay que centrarse en la posibilidad de conseguir cuestionarios o cualquier método de recolección de datos que se haya realizado con anterioridad en investigaciones relacionadas con el mismo tema.
- **Tipos de preguntas:** se pueden encontrar dos tipos de preguntas: abiertas o cerradas. Una pregunta abierta permite al encuestado expresar la respuesta utilizando sus propias palabras, mientras que una pregunta cerrada proporciona una lista de posibles respuestas a la pregunta.
- **Diseño de las preguntas:** es necesario pensar detenidamente cómo se quieren plantear las preguntas. Éstas han de ser precisas, carentes de ambigüedad y perfectamente comprensibles por parte de las personas que vallan a responderlas.
- **Diseño de las respuestas:** las respuestas a las preguntas de un cuestionario suelen ser alguna de las siguientes: valores numéricos, categorías, respuestas SI/NO o escalas ordinales.
- **Formato de los cuestionarios:** para conseguir que el aspecto de los cuestionarios no introduzca complejidad innecesaria a la encuesta se tienen recomendaciones tales como dejar un espacio para que los participantes dejen sus comentarios sobre el cuestionario, usar espacio entre las distintas preguntas o el enfatizar la información que lo requiera mediante el uso de negritas, subrayado y mayúsculas (Kitchenham y Pfleeger, 2008). También es importante el orden en el que se plantean las preguntas.
- **Motivación:** se debe conseguir motivar a los participantes para que respondan de manera fiel a una encuesta en la que, en la mayoría de los casos, no han pedido participar.

2.2.4 **Evaluación y Validación del Cuestionario**

Una vez se han definido las preguntas del cuestionario, es esencial que se evalúe (Litwin, 1995). En esta actividad se pretenden diversos objetivos (Kitchenham y Pfleeger, 2008):

- Comprobar que las preguntas se entienden correctamente.
- Evaluar el índice probable de respuestas.
- Evaluar la fiabilidad y validez del cuestionario.
- Comprobar que el método de análisis de datos que se utilizará será compatible con las respuestas que se van a obtener.

Para el caso de la encuesta realizada durante esta investigación, además de la validación entregada por los directores de tesis, se realizó un estudio piloto por medio de la realización de la encuesta a un grupo reducido de personas en la modalidad de entrevistas personales.

2.2.5 **Obtención de los Datos**

A la hora de conseguir los datos, normalmente es imposible contar con las respuestas de toda la población implicada en el estudio, de ahí que haya que recurrir a una muestra de la misma (Genero *et al.*, 2014). Además, se debe indicar la tasa de respuesta de la encuesta.

La idea es encontrar un compromiso entre el tamaño de la muestra y la tasa de respuesta de la encuesta.

2.2.6 **Análisis de los Datos**

Una vez llevada a cabo la encuesta es el momento de analizar los datos obtenidos (Genero *et al.*, 2014). Los puntos más importantes a considerar son la validación de los datos obtenidos (que sean completos y consistentes), la posible división de las respuestas en grupos homogéneos (en función de la información demográfica que se ha obtenido de los participantes) y el análisis de los datos propiamente tal, ya sean numéricos, ordinales o nominales.

2.2.7 **Reporte de los Resultados**

En la mayoría de las ocasiones, se tratará de publicar la información generada durante la realización de la encuesta y el análisis de sus resultados en alguna revista o congreso o incluso como un informe técnico asociado a algún proyecto de investigación.

2.2.8 **Aplicación y Resultados de la Encuesta**

La encuesta fue diseñada utilizando un sitio para la creación de encuestas en línea. Capturas de pantalla de las preguntas consideradas en la encuesta pueden ser encontradas en el Anexo B. Por otro lado, el reporte de los resultados de la encuesta puede ser encontrado en la Sección 2 del Capítulo 4.

2.3 **Casos de Estudio**

Un caso de estudio en ingeniería del software es una investigación empírica que hace uso de múltiples fuentes de evidencia para investigar una instancia de un fenómeno contemporáneo relacionado con la ingeniería del software dentro de su contexto real, específicamente cuando las fronteras entre el fenómeno y su contexto no pueden definirse claramente (Runeson *et al.*, 2012).

Los casos de estudio se caracterizan por:

- Ser un método de investigación flexible, ya que han de tratar con las complejas y dinámicas características de los fenómenos del mundo real.
- Sus conclusiones se basan en una clara cadena de evidencias, recogida de múltiples fuentes de una forma planeada y consistente.
- Añaden conocimiento al ya existente, basándose en una teoría previamente establecida.

A la hora de llevar a cabo un caso de estudio, el proceso más comúnmente utilizado se basa en un conjunto de actividades (Runeson *et al.*, 2012), las cuales son descritas a continuación.

2.3.1 **Diseño y Planificación del Caso de Estudio**

A la hora de planificar un caso de estudio es necesario que, al menos, se tengan en cuenta los siguientes elementos (Robson, 1993):

- **Objetivo:** ¿qué se pretende conseguir? Puede ser, por ejemplo, de tipo exploratorio, descriptivo, explicativo o de mejora.
- **El caso y unidad de análisis:** ¿qué se va a estudiar? En ingeniería del software, el caso y/o la unidad pueden ser un proyecto de desarrollo de software, un individuo, un grupo de personas, un proceso, etc.
- **Teoría:** marco de referencia en el que se encuadra el estudio.
- **Preguntas de investigación:** ¿qué hay que saber?
- **Método:** ¿cómo se van a recoger los datos?
- **Estrategia de selección:** ¿dónde hay que buscar los datos?

2.3.2 **Preparación y Recogida de los Datos**

En función del grado de implicación del investigador en la recogida de los datos, se establece la siguiente división de las técnicas de recogida de datos (Lethbridge *et al.*, 2005):

- **Primer grado:** el investigador está en contacto directo con los sujetos y los datos se recogen en tiempo real.
- **Segundo grado:** el investigador recoge los datos directamente pero sin interactuar con los sujetos.
- **Tercer grado:** se utilizan datos previamente disponibles.

Una de las técnicas más utilizadas a la hora de recoger los datos relativos a un caso de estudio son las entrevistas (Genero *et al.*, 2014). Ésta es una de las técnicas que se aplicó durante el desarrollo de los casos de estudio de esta investigación. El investigador realiza una serie de preguntas a un conjunto de sujetos sobre las áreas de interés del caso de estudio. En base del grado de estructuración de las entrevistas, se establece la siguiente clasificación de las mismas (Robson, 1993):

- **No estructuradas:** se observa cómo los individuos experimentan el fenómeno cualitativamente, con un objetivo exploratorio. Solo se tiene un manual de entrevista con las áreas en las que centrarse, sin preguntas predefinidas.
- **Semi-estructuradas:** se observa cómo los individuos experimentan el fenómeno cualitativa y cuantitativamente, con un objetivo descriptivo y exploratorio. Se tiene una mezcla de preguntas abiertas y cerradas.
- **Completamente estructuradas:** se trata de encontrar relaciones entre conceptos, con un objetivo descriptivo y exploratorio, al igual que las entrevistas semi-estructuradas. Aquí las preguntas son cerradas.

La clase de entrevista que se aplicó para esta investigación fue semi-estructurada.

Otra de las técnicas más utilizadas para recoger datos de un caso de estudio son las observaciones. Un ejemplo típico de su uso consiste en investigar cómo los ingenieros de software realizan una determinada tarea (Genero *et al.*, 2014). Al igual que las entrevistas, también se utilizó observaciones para recopilar una parte de los casos de estudio llevados a cabo durante esta investigación. Los tipos de observaciones se dividen según lo que se puede observar en la Tabla 2.

Tabla 2. Tipos de observaciones en casos de estudio.

	Alto conocimiento del sujeto observado	**Bajo conocimiento del sujeto observado**
Alto grado de interacción por parte del investigador	(Categoría 1) Estudios etnográficos o de investigación-acción. El investigador es parte del equipo. Aquí es visto como un "participante observador".	(Categoría 2) Estudios etnográficos o de investigación-acción. El investigador es parte del equipo. Aquí es visto como un "participante normal".
Bajo grado de interacción por parte del investigador	(Categoría 3) Se utilizan técnicas de recogida de datos de primer grado, como el protocolo de "pensar en voz alta", donde se hacen preguntas como "¿qué opinas sobre…?" o "¿cuál es tu estrategia sobre…?".	(Categoría 4) Los sujetos se observan utilizando técnicas de segundo grado, como grabaciones de video.

Las observaciones utilizadas durante esta investigación corresponden a aquellas de la categoría 4.

2.3.3 **Análisis e Interpretación de los Datos Recogidos**

El análisis de los datos se realiza de manera distinta para datos cualitativos y cuantitativos. Para los datos cuantitativos, se suele utilizar un análisis del tipo estadístico descriptivo, análisis de correlaciones, modelos predictivos y contraste de hipótesis, mientras que para los datos cualitativos se llevan a cabo técnicas de generación y confirmación de hipótesis (Genero *et al.*, 2014).

2.3.4 **Informe Sobre los Resultados Obtenidos**

A la hora de publicar un informe sobre un caso de estudio la estructura lineal analítica (problema, trabajo relacionado, método, análisis y conclusión) es la estructura más aceptada.

2.3.5 **Aplicación y Resultados de los Casos de Estudio**

La totalidad de la aplicación de casos de estudio durante esta investigación es documentada a lo largo del Capítulo 5.

2.4 **Investigación-Acción**

Dos de las definiciones más significativas de la investigación-acción son las siguientes:

- Es la forma que tienen los grupos de personas de preparar las condiciones necesarias para aprender de sus propias experiencias, y hacer estas experiencias accesibles a otros (McTaggart, 1991).
- Consiste en la participación de todas las partes involucradas en la investigación, examinando la situación existente (que sienten como problemática), con los objetivos de cambiarla y mejorarla (Wadsworth, 1993).

De lo anterior se puede deducir que la investigación-acción tiene una doble finalidad: generar un beneficio al "cliente" de la investigación y, al mismo tiempo, generar "conocimiento de investigación" relevante (Kock y Lau, 2001). Una premisa fundamental en esta forma de investigar es que los procesos sociales complejos (como lo es el uso de tecnologías de la información en organizaciones) pueden ser estudiados mejor introduciendo cambios en dichos procesos y observando los efectos de dichos cambios (Baskerville, 1999).

La investigación-acción es una forma de investigar de carácter colaborativo que busca unir teoría y práctica entre investigadores y profesionales mediante un proceso de naturaleza cíclica, produciendo nuevos conocimientos útiles en la práctica, que se obtienen mediante el cambio y/o búsqueda de soluciones a situaciones reales que le ocurren a un grupo de profesionales (Avison *et al.*, 1999). Esto de consigue gracias a la intervención de un investigador en la realidad del mencionado grupo. Los resultados de esta experiencia deben ser beneficiosos tanto para el investigador como para los practicantes (Genero *et al.*, 2014).

2.4.1 **Participantes en la Investigación-Acción**

Se identifican los siguientes cuatro tipos de roles en el método de investigación-acción (Wadsworth, 1993):

- El **investigador**, el individuo o grupo que lleva a cabo de forma activa el proceso investigador.
- El **objeto investigado**, es decir, el problema a resolver.
- El **grupo crítico de referencia**, aquel para quien se investiga en el sentido de que tiene un problema que necesita ser resuelto y que también participa en el proceso de investigación.
- El **beneficiario**, aquel para quien se investiga en el sentido de que puede beneficiarse del resultado de la investigación, aunque no participa directamente en el proceso.

2.4.2 **Aplicación de la Investigación-Acción**

Para identificar el uso de investigación-acción en esta investigación, se puede identificar las personas y/o grupos que pertenecen a uno de los roles descritos previamente:

- El rol de investigador corresponde a quien realiza esta investigación y a los respectivos directores de tesis.
- El objeto investigado es el tema de investigación que se tiene, el cual es la comparación y selección de esquemas y métodos de autenticación.
- Los empleados de la empresa de desarrollo de software Nisum Technologies juegan el rol de grupo crítico de referencia.
- En cuanto al beneficiario, éste es la empresa Nisum Technologies, pero también se considera como beneficiarios a los desarrolladores de software en general.

Capítulo 3
Estado del Arte

En este capítulo se presentan los resultados de la revisión sistemática de la literatura especificada en la Sección 2, los cuales entregan el estado del arte, en el cual se basan los resultados generados por medio de la realización de esta tesis.

La Sección 3.1 entrega los resultados generales de la RSL, mientras que las Secciones 3.2, 3.3, 3.4 y 3.5 entregan los resultados específicos según cada uno de los temas ligados a las preguntas de investigación de la revisión (esquemas de autenticación, métodos de autenticación multi-factor, criterios de comparación y selección de esquemas o métodos de autenticación, y Framework de decisión de esquemas o métodos de autenticación). La Sección 3.6 entrega una discusión de los resultados obtenidos y, finalmente, la Sección 3.7 entrega las conclusiones de la RSL.

3.1 **Resultados Generales**

A continuación se muestran los resultados de la RSL, el detalle de la planificación de ésta puede ser observado en el Anexo A. Una búsqueda fue realizada por cada combinación de términos en cada fuente especificada en el protocolo de búsqueda (Anexo A, sección 3), en total 54 búsquedas distintas fueron realizadas. Por cada búsqueda, 200 publicaciones fueron revisadas. Sin embargo, 15 de éstas entregaron menos de 200 resultados y, entre esas, 5 no entregaron resultados. De este modo, un total de 8.513 artículos fueron revisados.

Con el objetivo de mejorar los resultados obtenidos, algunos refinamientos adicionales fueron realizados en algunas de las fuentes: en Scopus, se limitó el área temática a Ciencias de la Computación, mientras que en Springer se refinó el tipo de contenido a artículo y en Google Schoolar se excluyeron las patentes y citaciones.

De los 8.153 artículos, aquellos que estuvieran repetidos fueron eliminados, obteniendo un total de 3.910 artículos distintos. Luego de una revisión superficial, 1.015 de éstos fueron considerados artículos potencialmente útiles. Un análisis detallado fue realizado posteriormente, y se notó que 33 de los artículos potencialmente útiles no eran relevantes para la investigación actual, por lo que fueron descartados, dejando un total de 982 artículos útiles y aceptados, divididos entre los cuatro temas de investigación como se muestra en la Tabla 3.

Tabla 3. Artículos aceptados divididos por cada Tema de Investigación.

Tema de Investigación	Número de Artículos Aceptados
Esquemas de Autenticación	515
Métodos de Autenticación Multi-Factor	442
Criterios de Comparación y Selección	17
Framework de Decisión	8
Total	982

Una lista conteniendo todas las referencias de los artículos aceptados en esta RSL puede ser encontrada en http://colvin.chillan.ubiobio.cl/mcaro/. A continuación se muestra el análisis de los artículos útiles por cada tema ligado a las preguntas de investigación.

3.2 **Esquemas de Autenticación**

Más del 50% de los artículos, 515, pertenecen al primer tema de investigación. La razón de ello es que los esquemas de autenticación son la base para los otros temas de investigación, por lo que han sido revisados más seguido en la literatura. En cuanto a los resultados, 217 de los artículos se centran en la propuesta de esquemas pertenecientes al factor de inherencia, mientras que 169 proponen el uso del factor de posesión y 124 el factor de conocimiento. Los 5 artículos restantes son relacionados a

otros factores de autenticación que han sido propuestos en la literatura. La Tabla 4 presenta las propuestas de esquemas de autenticación encontradas en la literatura, el factor al que pertenecen y el número de artículos que propone a cada uno.

Tabla 4. Esquemas de autenticación encontrados en la literatura.

Factor	Esquema	Número de Artículos
Conocimiento	Contraseñas de Texto	44
	Contraseñas Gráficas	42
	Autenticación Cognitiva	25
	Número de Identificación Personal (PIN)	7
	Preguntas	4
	Otros Esquemas Basados en Conocimiento	2
	Total	124
Posesión	Basado en ID (Tarjetas Inteligentes)	103
	Contraseñas de Uso Único (One Time Password, OTP, o Tokens)	43
	Basado en Móviles	21
	Otros Esquemas Basados en Posesión	2
	Total	169
Inherencia	Biométricas del Rostro	24
	Biométricas de Pulsación de Teclas	24
	Gestos de la Mano	12
	Biométricas de la Palma de la Mano	12
	Biométricas de Pulsación de la Pantalla	11
	Huellas Dactilares	10
	Biométricas del Iris	8
	Ondas Cerebrales	5
	Latidos del Corazón	5
	Biométricas de los Nudillos	5
	Biométricas del Caminar	4
	Biométricas Multi-Modales	19
	Otras Biométricas	17
	Biométricas del Comportamiento (No Definidas)	13
	Biométricas (No Definidas)	48
	Total	217
Otros Factores		5
	Gran Total	515

El esquema de las contraseñas de texto, el cual es el más usado hoy en día (Bonneau *et al.*, 2012), es el esquema de autenticación perteneciente al factor de conocimiento con la mayor cantidad de artículos relacionados (44), seguido por el esquema de las contraseñas gráficas, con 42 artículos. Por otro lado, la gran mayoría de las propuestas relacionadas al factor de posesión son relacionadas al uso de tarjetas inteligentes, con 103 de los 169 artículos, lo cual corresponde al 60,1% de ellos. Hay varios artículos diferentes relacionados al uso de biométricas para el factor de inherencia, aunque 48 de ellos no definen una biométrica específica para su propuesta, y 13 otros solo mencionan el uso de biométricas del comportamiento pero no una en particular.

La mayoría de los artículos encontrados han sido publicados desde el 2000 en adelante (505) y solo 10 fueron publicados antes. Se puede notar un creciente interés sobre el tema de los esquemas de autenticación, puesto que el número de artículos relacionados a ello ha ido creciendo a lo largo de los años, con la excepción del 2012, el cual posee una notoria disminución en la investigación comparado al año anterior. En el año 2015 se tiene la mayor cantidad de publicaciones relacionadas a esquemas de autenticación, con 82 artículos, mientras que el 2001 posee la menor cantidad, con solo uno. El artículo aceptado más antiguo es (Evans *et al.* 1974), y propone el uso de contraseñas de texto. Ningún artículo previo al 2000 discute el uso de esquemas relacionados al factor de posesión. El gráfico en la Fig. 1 muestra el número de artículos aceptados y el factor de autenticación al que pertenecen, divididos por

año. Es importante mencionar que esta revisión fue realizada entre el segundo y tercer trimestres del 2016, por lo que no todos los artículos de éste año están presentes.

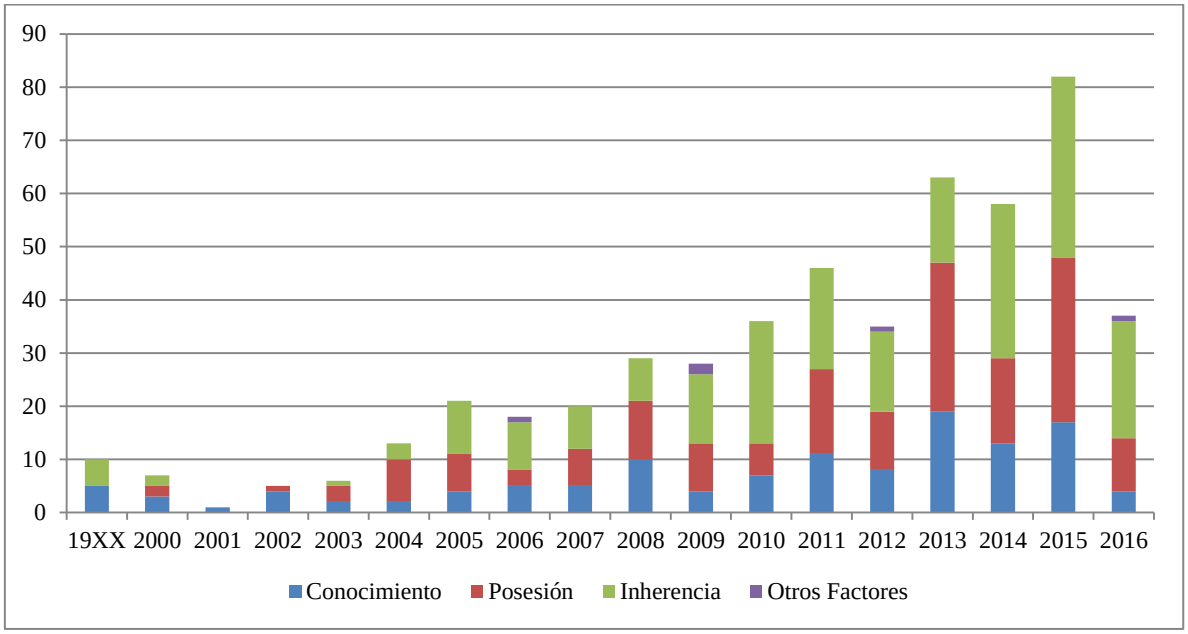


Figura 1. Factores de autenticación según el año de publicación.

Se registró el contexto para el que cada esquema de autenticación fue propuesto. El ambiente móvil fue el contexto más común, seguido por la autenticación remota y el área de la salud. Es importante mencionar que más de la mitad de los artículos, 282, no especificó un contexto en particular para su propuesta. Los diferentes contextos que han sido encontrados pueden ser vistos en la Tabla 5, junto con cuantos esquemas por cada factor de autenticación son propuestos en cada uno de ellos.

Tabla 5. Factores de autenticación y sus contextos.

Factor / Contexto	Conocimiento	Posesión	Inherencia	Otros Factores	Total
Ambiente Móvil y Pantallas Táctiles	24	16	41	0	81
Autenticación Remota	4	33	5	0	42
Área de la Salud	0	13	11	0	24
Ambiente Multi Servidor	2	9	6	0	17
Autenticación Continua	0	0	11	0	11
Redes de Sensores Inalámbricos	2	7	1	0	10
Computación en la Nube	1	6	2	0	9
Banca y Comercio	2	4	2	0	8
Ambiente Inteligente	0	6	1	0	7
Protocolos de Inicio de Sesión	1	2	2	0	5
Aplicaciones Web	2	1	1	1	5
Otros Contextos	4	6	4	0	14
No Especificado	82	66	130	4	282
Total	124	169	217	5	515

3.3 **Métodos de Autenticación Multi-Factor**

Para el segundo tema de investigación se encontraron 442 artículos. La mayoría de los artículos aceptados corresponde a propuestas de métodos que combinan esquemas de los factores de conocimiento y posesión, sumando un total de 270 artículos, lo que corresponde al 60% de los artículos. Hay 44 propuestas que combinan los factores de conocimiento e inherencia y 43 que combinan los factores de posesión e inherencia. Por otro lado, 68 propuestas combinan los tres factores. Se encontraron doce artículos que no proponían una combinación específica de factores, sino que proponían el uso de distintos factores según diferentes situaciones. De forma similar al primer tema de investigación, se encontraron 5 artículos que proponían métodos de autenticación multi-factor cuyas combinaciones de factores incluían un factor propuesto en la literatura distinto a los tres más conocidos. La Tabla 6 presenta las propuestas de métodos de autenticación multi-factor encontradas en la literatura, la combinación de factores a la que pertenecen y el número de artículos que propone a cada una.

Tabla 6. Métodos de autenticación multi-factor encontrados en la literatura.

Combinación	Método	Número de Artículos
Conocimiento Y Posesión	Contraseñas de Texto Y Basado en ID	188
	Contraseñas de Texto Y Basado en Móviles	37
	Contraseñas de Texto Y OTP	34
	Otros Métodos	11
	Total	270
Conocimiento Y Inherencia	Contraseñas de Texto Y Biométricas	36
	Contraseñas Gráficas Y Biométricas	4
	Otros Métodos	4
	Total	44
Posesión Y Inherencia	Basado en ID Y Biométricas	24
	OTP Y Biométricas	9
	Basado en Móviles Y Biométricas	6
	Otros Métodos	4
	Total	43
Conocimiento Y Posesión Y Inherencia	Contraseñas de Texto Y Basado en ID Y Biométricas	47
	Contraseñas de Texto Y OTP Y Biométricas	9
	Contraseñas de Texto Y Basado en Móviles Y Biométricas	7
	Otros Métodos	5
	Total	68
Otras Combinaciones		5
Métodos Dinámicos		12
	Gran Total	442

La combinación de contraseñas de texto y tarjetas inteligentes (Basado en ID) es lejos la que posee más artículos, con un total de 188 artículos (69,4% de los artículos que combinan los factores de conocimiento y posesión). Se observa, también, que las contraseñas de texto y/o las tarjetas inteligentes son los esquemas más utilizados junto con las biométricas para cada otra combinación de factores, destacando la gran cantidad de investigación realizada respecto de los métodos de autenticación basados en estos esquemas.

De forma similar al primer tema de investigación, se puede observar un interés creciente sobre el tema de la autenticación multi-factor, con la diferencia de que no hay bajas significativas en la cantidad de artículos en ningún año en específico. Solo hay 6 artículos previos al año 2000, y todos ellos proponen el uso de una combinación entre los factores de conocimiento y posesión. El 2015 es nuevamente el año con la mayor cantidad de publicaciones, 81. Ninguno de los artículos en la RSL fue publicado durante el 2000, y el artículo más antiguo es (Chang y Wu, 1991). El gráfico en la Fig. 2 presenta el número de artículos aceptados y la combinación de factores de autenticación a la que

pertenecen, divididos por año. Recordar que esta revisión fue realizada entre el segundo y tercer trimestres de 2016, por lo que no todos los artículos de dicho año están presentes.

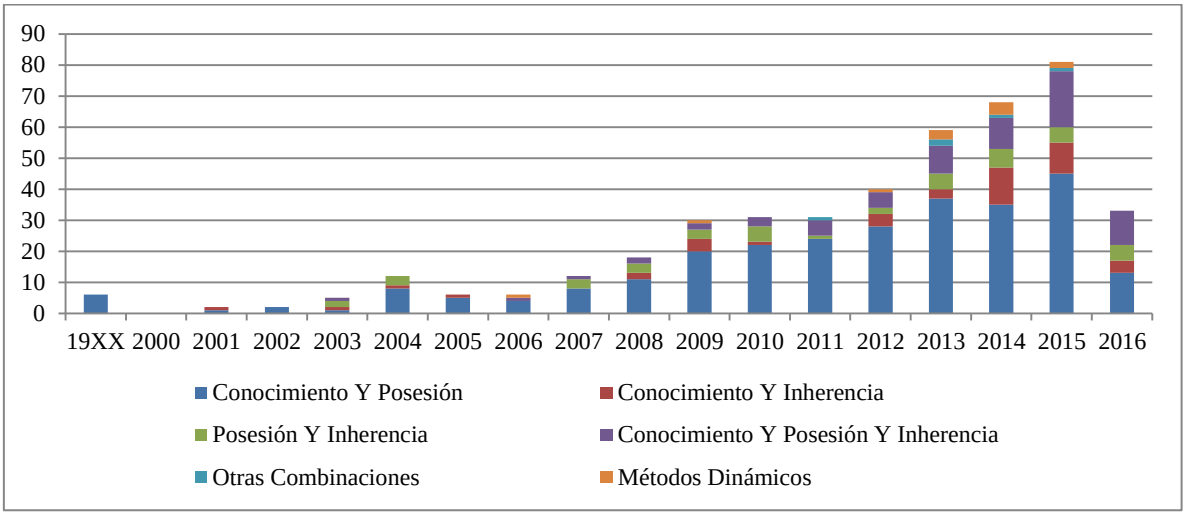


Figura 2. Métodos de autenticación multi-factor de según el año de publicación.

Se registró también el contexto para el que cada método de autenticación multi-factor fue propuesto. En contraste a los esquemas de autenticación, solo un 38,7% de ellos no menciona para qué contexto fue propuesto. La autenticación remota y el área de la salud son los dos contextos más recurrentes pero, a diferencia de los esquemas de autenticación, el ambiente móvil es discutido considerablemente menos. Los diferentes contextos que fueron encontrados pueden ser vistos en la Tabla 7, junto con cuantos métodos por cada combinación de factores de autenticación son propuestos en cada uno de ellos.

Tabla 7. Métodos de autenticación multi-factor y sus contextos.

Contexto	Combinaciones	Conocimiento Y Posesión	Conocimiento Y Inherencia	Posesión Y Inherencia	Conocimiento Y Posesión Y Inherencia	Otras Combinaciones	Dinámicas	Total
Autenticación Remota		45	1	8	10	0	0	64
Área de la Salud		29	3	2	14	0	0	48
Redes de Sensores Inalámbricos		28	0	1	4	0	0	33
Ambiente Multi Servidor		18	1	4	6	0	0	29
Ambiente Móvil y Pantallas Táctiles		11	8	0	2	0	0	21
Computación en la Nube		10	2	1	3	0	1	17
Banca y Comercio		8	1	1	0	0	1	11
Aplicaciones Web		10	1	0	0	0	0	11
Redes Inalámbricas		7	0	0	1	0	0	8
Dispositivos USB		3	0	0	3	0	0	6
Ambiente Inseguro		4	0	1	0	0	0	5
Otros Contextos		10	2	3	2	1	1	19
No Especificado		87	25	22	23	4	9	170
Total		270	44	43	68	5	12	442

3.4 Criterios de Comparación y Selección

Otro de los objetivos de esta revisión era el de identificar diferentes criterios de comparación y selección usados para decidir qué esquema de autenticación o método de autenticación multi-factor usar en una situación dada. Se encontraron 17 artículos relacionados a este tema. Todos éstos consideran uno o más criterios para comparar esquemas o métodos de autenticación, siendo aquellos de usabilidad y seguridad los dos más usados, al ser indicados en 9 artículos cada uno.

Criterios relacionados a los costos del esquema o método son usados 5 veces, y aquellos relacionados al contexto en donde se usará el esquema o método son usados dos veces. Son propuestos, además, otros siete criterios, tales como tendencias futuras del esquema o método o su privacidad, entre distintos artículos, pero cada uno de éstos es propuesto solo una vez.

Cinco de los artículos consideran la autenticación multi-factor. Por otro lado, 13 de ellos consideran un contexto en específico. Los contextos considerados en estos artículos pueden verse en la Fig. 3.

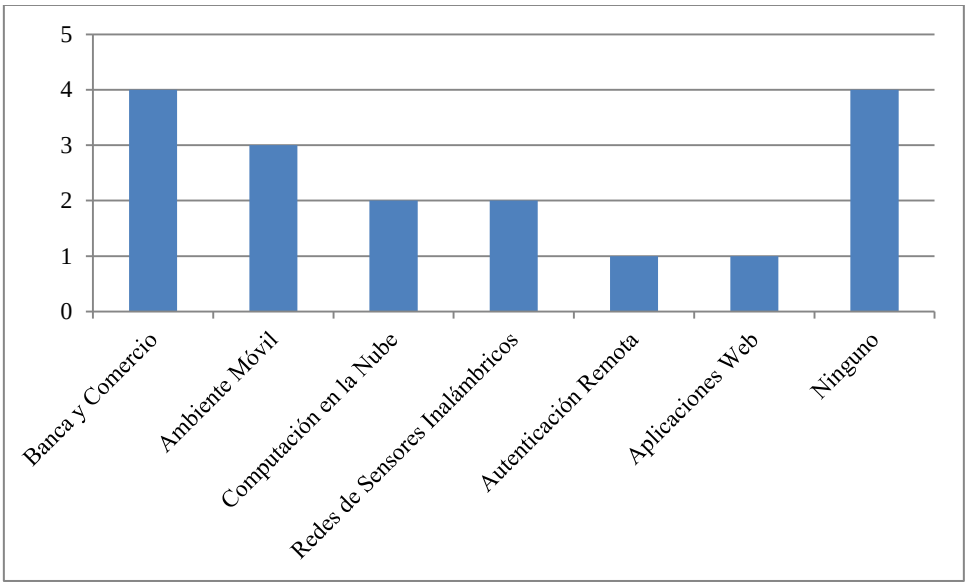


Figura 3. Contextos considerados en los artículos sobre criterios de comparación y selección.

3.5 Framework de Decisión

Se han encontrado ocho Framework de decisión que ayudan en la comparación y selección de esquemas de autenticación y/o métodos de autenticación multi-factor. Una breve descripción de cada uno es entregada en la Tabla 8.

El artículo más antiguo que ha sido encontrado es el de Guel (2002). La mayoría de las propuestas de esquemas y métodos de autenticación encontradas en esta revisión han sido publicadas después de dicho año, por lo que los contenidos del Framework presentado en este artículo podrían estar desactualizados. Por otro lado, el artículo más reciente es (Wang *et al.*, 2016), y la mayoría de las propuestas de esquemas y métodos encontradas son de años previos a dicha publicación, por lo que los contenidos presentados en ésta son probablemente adecuados.

Tabla 8. Framework que ayudan en la decisión de esquemas o métodos de autenticación.

Título del Artículo	Descripción
A criteria-based evaluation framework for authentication schemes in IMS (Eliasson *et al.*, 2009)	Framework de decisión para sistemas multimedia basado en tres criterios principales (seguridad, facilidad de uso y simplicidad) y tres secundarios (conciencia, usabilidad y algoritmos), y además considerando las percepciones de los usuarios.
A Framework for Choosing Your Next Generation Authentication/Authorization System (Guel, 2002)	Realiza una evaluación general de varios esquemas de autenticación en relación a sus ventajas y desventajas. Toca, además, algunos temas relacionados a autorización.
Approach for selecting the most suitable Automated Personal Identification Mechanism (ASMSA) (Palmer, 2010)	Apoya en la selección de la identificación automática más adecuada del factor de conocimiento o del de inherencia, considerando tanto el contexto como los requerimientos de los interesados.
Cost and benefit analysis of authentication systems (Altinkemer y Wang, 2011)	Detallado análisis de esquemas de autenticación y métodos de autenticación multi-factor en relación a criterios relacionados a costos. Pensado para ser usado cuando una compañía cambia de un esquema o método de autenticación a otro.
Efficiency of Paid Authentication Methods for Mobile Devices (Kim, 2016)	Encuesta a administradores de sistemas acerca de sus preferencias en cuanto a esquemas de autenticación pagados para el ambiente móvil. Se consideran la seguridad, la conveniencia y los costos de operación.
The quest to replace passwords: A framework for comparative evaluation of web authentication schemes (Bonneau *et al.*, 2012)	Detallado análisis de múltiples esquemas de autenticación en términos de seguridad, usabilidad y costos. Provee una tabla comparativa que facilita el proceso de toma de decisiones. Menciona la autenticación multi-factor pero muy por encima.
The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes (Wang *et al.*, 2016)	Compara las múltiples propuestas de métodos de autenticación de dos factores que usan contraseñas de texto y tarjetas inteligentes, en relación a sus atributos deseables, requerimientos de usabilidad y eficiencia.
User-centred authentication feature framework (Forget *et al.*, 2015)	Framework orientado a investigadores que evalúa esquemas basados en conocimiento en cuanto a características relacionadas con persuasión, memoria, entrada y salida y ofuscación.

3.6 **Discusión**

Los principales hallazgos y limitaciones de esta revisión son discutidos aquí. Esta revisión nos permite no solo conocer el estado del arte sobre esquemas de autenticación y métodos de autenticación multi-factor, sino que además sirve como una vía para identificar los principales contextos en los que han sido propuestos y usados, junto con entregar una percepción sobre los criterios utilizados cuando se enfrenta la necesidad de decidir qué esquema o método utilizar en diferentes contextos y los Framework existentes que realizan esta tarea.

Entre los esquemas de autenticación, de los tres factores de autenticación bien conocidos, el factor de inherencia es el que ha sido más investigado, mientras que el factor de conocimiento es el que menos, tal vez debido al paradigma actual de que el esquema más representativo de este factor (las contraseñas de texto) no es muy seguro (Bonneau *et al.*, 2012). De todos modos, el esquema más revisado es la autenticación basada en tarjetas inteligentes, el cual pertenece al factor de posesión. Si bien se esperaba que existiera una gran cantidad de investigación, en cuanto a la autenticación, para

algunos contextos, como es el caso del ambiente móvil, la investigación sobre otros contextos no fue identificada tan a menudo como se esperaba, como lo es en la banca y comercio.

La combinación de los factores de conocimiento y posesión es muy predominante entre los métodos de autenticación multi-factor, especialmente el uso de contraseñas de texto y tarjetas inteligentes. La autenticación de tres factores, si bien parece ser que es la menos aplicada (O'Gorman, 2003), es la segunda combinación de factores más investigada. Tanto las contraseñas de texto como las tarjetas inteligentes son usadas en 259 artículos, como uno de los esquemas considerados en la combinación para autenticación multi-factor. La existencia de métodos de autenticación multi-factor dinámicos (Nag *et al.*, 2014; Nag y Dasgupta, 2014; Miranda, 2009) es interesante, puesto que se adaptan a distintos ambientes. Se encontró un método de autenticación multi-factor que usa cuatro diferentes factores (siendo el cuarto factor aquel relacionado a la ubicación del usuario) (Kathrine y Kirubakaran, 2011).

No se encontraron muchos artículos relacionados a criterios de comparación y selección o Framework de decisión para esquemas o métodos de autenticación. Entre los existentes, se notó el uso común de criterios relacionados a usabilidad, seguridad y costos. El contexto de uso también se puede ver como un elemento importante, pues los artículos o lo consideran como uno de los criterios de decisión (O'Gorman, 2003) o la propuesta misma del artículo va dirigida a un contexto en específico (Bruun *et al.*, 2014; Anwar e Imran, 2015).

En cuanto a los Framework de decisión, se puede ver que la autenticación multi-factor no es considerada frecuentemente, mientras que las propuestas que la consideran se enfocan solo en algunos aspectos de autenticación, dejando a otros de lado. No se logró encontrar un Framework que considerara tanto la autenticación de un factor y la multi-factor, junto con suficientes criterios de decisión para realizar una comparación y selección detallada de los esquemas o métodos de autenticación existentes para ser usados.

La aceptación de los artículos para los primeros dos temas de investigación se limitó a aquellos que directamente proponían un nuevo esquema de autenticación o una mejora a uno existente. Además, debido a limitantes de tiempo y a la cantidad de artículos potencialmente útiles en estos temas de investigación, solo se extrajo de ellos la información relevante para esta revisión.

3.7 **Conclusiones de la Revisión Sistemática de la Literatura**

El desarrollo de esta RSL se enfocó en investigar los Framework de decisión existentes y criterios de comparación y selección relacionados a esquemas de autenticación y métodos de autenticación multi-factor, junto con la investigación existente sobre estos esquemas y métodos. Por medio de esta revisión, se encontró un total de 982 artículos que o bien discutían esquemas de autenticación, o métodos de autenticación multi-factor, o Framework y criterios que ayudan en la comparación y selección de éstos en diferentes ambientes. Los principales descubrimientos de esta revisión, en relación a las preguntas de investigación formuladas, son los siguientes:

Q1. *¿Cuáles son los principales esquemas de autenticación existentes en la literatura?*

> Se ha realizado una cantidad considerable de investigación sobre los tres factores de autenticación bien conocidos. Las contraseñas de texto y gráficas son los esquemas más investigados dentro de la autenticación basada en conocimiento, mientras que existen múltiples propuestas de biométricas distintas para el factor de inherencia. El esquema más investigado es el de la autenticación basada en el uso de tarjetas inteligentes, del factor de posesión.

Q2. *¿Qué combinaciones de estos esquemas se pueden encontrar que puedan ser usadas como métodos de autenticación multi-factor?*

Existen muchos métodos de autenticación multi-factor diferentes que combinan los esquemas de autenticación de Q1. Existen tanto propuestas de combinación que consideran dos factores como aquellas que consideran tres, existe incluso una propuesta que considera cuatro factores (el cuarto siendo la autenticación basada en ubicación). Existe una clara prevalencia en el uso de contraseñas de texto y tarjetas inteligentes como uno de los esquemas utilizados para las diferentes combinaciones.

Q3. *¿Qué criterios pueden ser utilizados para comparar y/o seleccionar entre esquemas de autenticación o métodos de autenticación multi-factor?*

La comparación y selección de diferentes esquemas o métodos de autenticación es realizada principalmente por medio de criterios de usabilidad y seguridad, siendo considerados de vez en cuando criterios relacionados a costos. Si bien no es considerado como un criterio en los artículos revisados, el contexto es un aspecto importante a examinar, pues la mayoría de los estudios es presentada para contextos específicos.

Q4. *¿Existen Framework que ayuden a comparar y/o seleccionar esquemas de autenticación o métodos de autenticación multi-factor? ¿Cuáles son sus características?*

Se encontraron ocho Framework que ayudan en la decisión de esquemas o métodos de autenticación. Cada Framework tiene sus propias características, algunos consideran un contexto en específico, otros se enfocan en esquema o métodos específicos y otros son más generales. No se logró encontrar ningún Framework que realizara un análisis detallado tanto de esquemas de autenticación como de métodos de autenticación multi-factor.

La intención principal de esta RSL fue de indagar sobre los Framework de decisión existentes y criterios de comparación y selección de esquemas o métodos de autenticación. Sin embargo, los resultados también podrían ser útiles para otros investigadores, ya que los puede ayudar a analizar el trabajo existente sobre diferentes esquemas o métodos de autenticación existentes que han sido encontrados durante su realización, de modo que se puedan identificar espacios para realizar investigaciones futuras sobre ellos. Debido a la observación de que existe un vacío en cuanto a formas para comparar y seleccionar esquemas y métodos de autenticación, además de que ninguno de los Framework de decisión encontrados realiza un análisis a cabalidad tanto de esquemas como de métodos de autenticación, es que nace la idea de definir un Framework para la comparación y selección de esquemas y métodos de autenticación más adecuados para una determinada aplicación.

Capítulo 4
Creación de Framework para la Comparación y Selección de Esquemas y Métodos de Autenticación

En este capítulo se presenta el Framework teórico que fue diseñado en base a lo recopilado de la literatura y de experiencias en la industria, las cuales son documentadas a continuación. Basándose en el conocimiento adquirido por medio de la revisión sistemática de la literatura y encuestas a expertos de la industria, se genera una propuesta inicial del Framework, la cual es validada posteriormente por un panel de expertos, para luego entregar una propuesta de Framework final. En la Fig. 4 se resumen los pasos seguidos para la creación del Framework.

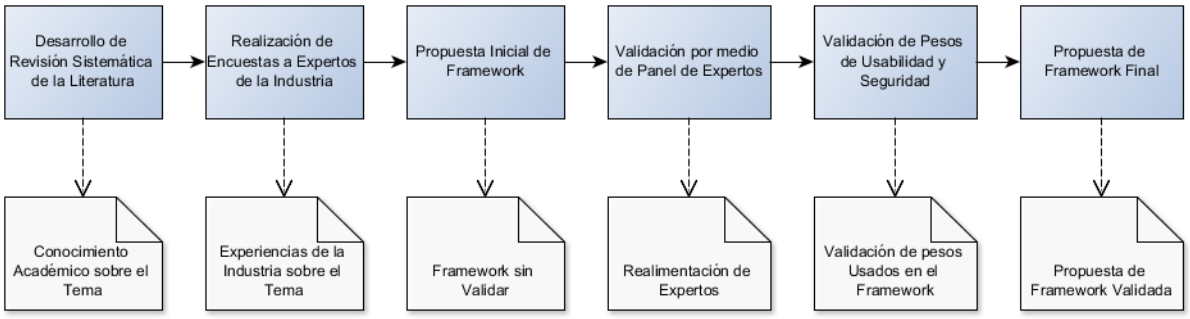


Figura 4. Etapas para la Generación del Framework.

La Sección 4.1 entrega un resumen de los hallazgos importantes del estado del arte para el Framework, obtenidos por medio de la RSL anterior. Posteriormente, en la Sección 4.2, se documentan el desarrollo de encuesta y entrevistas a expertos en la industria, para luego presentar las características de la propuesta inicial de este en la Sección 4.3. Esta propuesta inicial es luego validada por medio de un panel de expertos, como se observa en la Sección 4.4 y por medio de una segunda encuesta, documentada en la Sección 4.5. En la Sección 4.6 se entrega la propuesta de Framework final a la que se llegó por medio de este proceso.

4.1 RSL, Resumen de los Hallazgos

A continuación se describen brevemente los hallazgos más importantes de la revisión sistemática de la literatura, y que tienen directa relación con la generación del Framework para la Comparación y Selección de Esquemas y Métodos de Autenticación Multi-Factor.

Se encontró una gran cantidad de esquemas de autenticación, los cuales son divididos en tres grandes factores de autenticación:

- Factor de Conocimiento: Algo que el usuario sabe. Ejemplos relevantes de este factor son las contraseñas de texto y las contraseñas gráficas.
- Factor de Posesión: Algo que el usuario posee. Aquí se encuentran las tarjetas inteligentes, los OTP o Token y la autenticación basada en dispositivos móviles.
- Factor de Inherencia: Algo que el usuario es. Todo tipo de biométricas pertenece a este factor. Por mencionar algunas de las más estudiadas, están la autenticación por medio de la palma de la mano, de las huellas dactilares, del rostro y del iris. Además, están las biométricas de comportamiento que permiten al usuario autenticarse por medio de su comportamiento.

Se encontraron, además, variados métodos de autenticación multi-factor, que combinaban uno o más de los factores anteriores para obtener una mayor seguridad. Un ejemplo de autenticación de tres factores sería el uso de contraseñas de texto, tarjetas inteligentes y huellas dactilares para una misma aplicación.

Tanto para los esquemas de autenticación como para los métodos de autenticación multi-factor se identificaron contextos comunes donde eran más propuestos dentro de la literatura. Ejemplos de contextos con mayores cantidades de propuestas de esquemas o métodos son el ambiente móvil, la autenticación remota, el ambiente multi-servidor, la computación en la nube, el área de la salud y las redes de sensores inalámbricos.

Por otro lado, se identificaron criterios utilizados para comparar y seleccionar los distintos esquemas y métodos de autenticación. Entre estos criterios destacan aquellos relacionados a la Usabilidad y la Seguridad, los cuales son reportados en 9 artículos cada uno, y aquellos relacionados a los Costos, que son reportados en 5.

Finalmente, se logró identificar ocho Framework de Decisión para esquemas y/o métodos de autenticación. Sin embargo, ninguno de éstos abarcaba a cabalidad tanto esquemas como métodos de autenticación, siendo éste uno de los motivos para llevar a cabo la creación del presente Framework.

4.2 Desarrollo de Encuesta y Entrevistas a Expertos en la Industria

En esta sección se presentan los resultados de las entrevistas y la encuesta realizadas a expertos en la industria en cuanto a autenticación, según lo especificado en la Sección 2. El objetivo de éstas es complementar los resultados obtenidos por medio de la revisión sistemática de la literatura, para así tener una visión tanto por parte de la academia como de la industria en cuanto a la comparación y selección de esquemas y métodos de autenticación para su uso en diferentes contextos.

La Sección 4.2.1 muestra las respuestas recibidas por medio de las entrevistas, mientras que la Sección 4.2.2 entrega los resultados obtenidos en la encuesta. Finalmente, en la Sección 4.2.3 se realiza una discusión sobre los resultados de las dos técnicas de investigación anteriores, contrastándolas con los resultados obtenidos en la RSL, además de entregar las conclusiones pertinentes a la realización de las entrevistas y la encuesta.

4.2.1 Resultados de las Entrevistas

Se entrevistó a un total de 12 expertos de la industria pertenecientes a Nisum Technologies, los cuales son principalmente desarrolladores de software con tres o más años de experiencia trabajando en la industria. Las preguntas realizadas durante estas entrevistas buscan obtener la misma información que las preguntas consideradas en la encuesta documentada a continuación, y se utilizaron a modo de piloto para validar que las preguntas consideradas en la encuesta estuvieran adecuadamente formuladas.

Como primer pregunta, se le consultó a los entrevistados sobre qué esquemas de autenticación conocían, siendo los más conocidos las contraseñas de texto, con 10 menciones, la autenticación basada en móviles, con 8, y OTP, con 7. Las contraseñas gráficas y la autenticación por medio de un proxy solo tuvieron una mención cada una. En la Fig. 5 se pueden observar los esquemas de autenticación conocidos por los entrevistados.

A continuación, se le preguntó a éstos sobre qué métodos de autenticación multi-factor conocían. La combinación de contraseñas de texto junto con OTP es la más conocida, seguida por la combinación de contraseñas de texto con autenticación basada en móviles. La combinación de contraseñas de texto y tarjetas inteligentes es conocida solo por dos de los entrevistados y no hubo mención de la combinación de algún esquema basado en conocimiento o posesión junto con algún esquema basado en inherencia en un carácter de dos factores. Un entrevistado indicó conocer sobre un método de autenticación de tres factores que consideraba la combinación de contraseñas de texto, OTP y biométricas. En la Fig. 6 se presentan las respuestas de los entrevistados a esta pregunta.

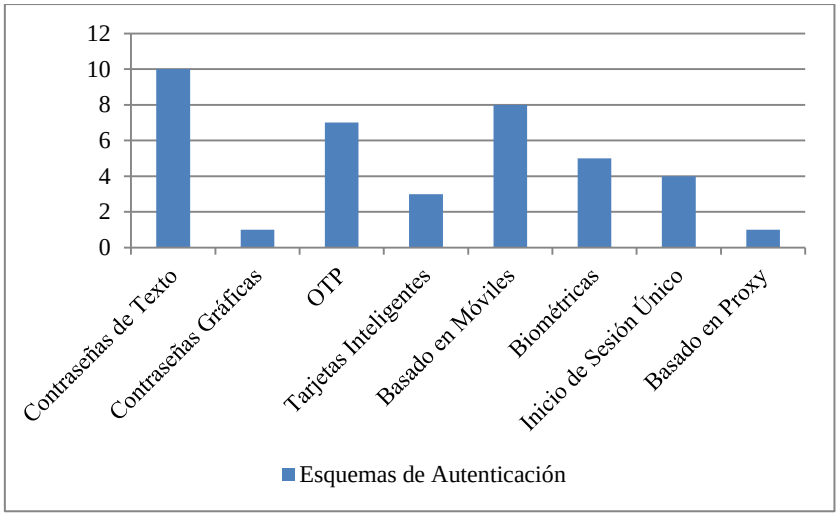


Figura 5. Esquemas de autenticación conocidos por los entrevistados.

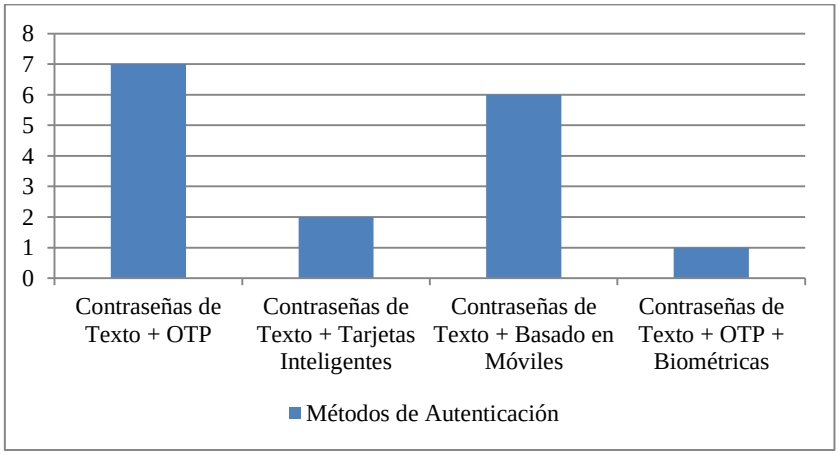


Figura 6. Métodos de autenticación multi-factor conocidos por los entrevistados.

Además de los esquemas y métodos de autenticación que los entrevistados conocían, se les consultó sobre aquellos que habían implementado en aplicaciones que hubieran desarrollado a lo largo del tiempo. En la Fig. 7 se presentan los esquemas y métodos implementados por los entrevistados, mientras que la Fig. 8 muestra los contextos en los cuales implementaron dichos esquemas y métodos. Cabe destacar que cada entrevistado puede haber implementado más de un esquema o método.

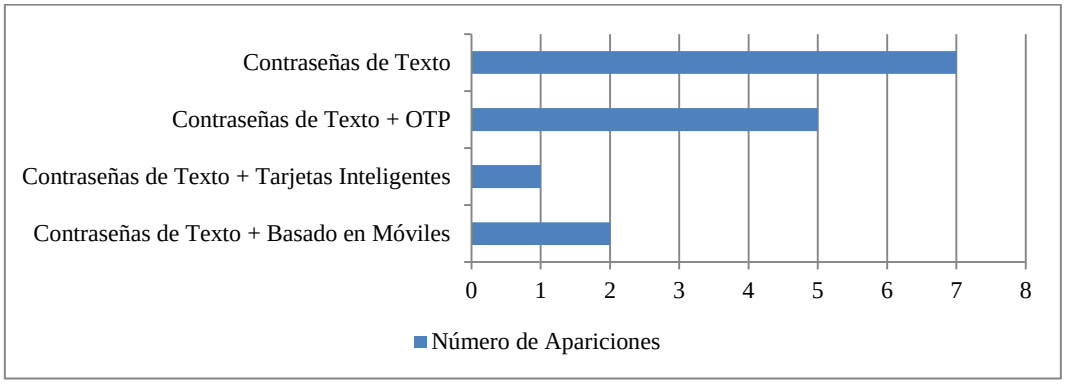


Figura 7. Esquemas y métodos de autenticación implementados por los entrevistados.

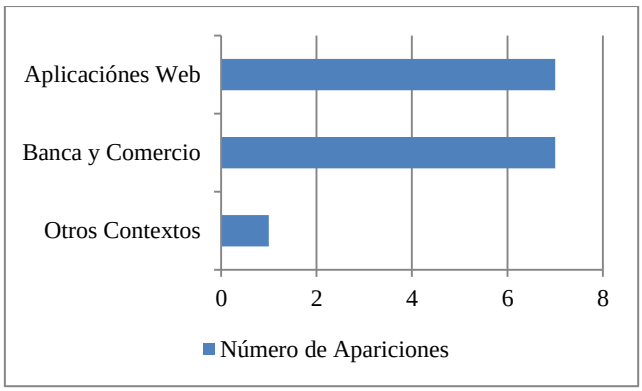


Figura 8. Tipos de aplicaciones en las que los entrevistados han implementado esquemas o métodos de autenticación.

Se puede observar que las contraseñas de texto, junto con la combinación de éstas y OTP, son los esquemas o métodos que han sido más implementados por los entrevistados, habiendo sido implementados 7 y 5 veces, respectivamente. En cuanto a los contextos en los cuales se implementaron estos esquemas y métodos, las aplicaciones Web y la banca y comercio son dominantes, con 7 apariciones cada uno, teniendo solo una aplicación perteneciente a otro contexto.

Finalmente, se le consultó a los entrevistados si consideraban o no cada uno de los siguientes criterios al momento de seleccionar qué esquema o método de autenticación implementar en las aplicaciones que desarrollan:

- Requerimientos del cliente.
- Contexto de la aplicación.
- Criterios relacionados a Usabilidad.
- Criterios relacionados a Costos.
- Criterios relacionados a Seguridad.

Además, se les preguntó si consideraban algún otro criterio que no estuviera englobado en alguno de los anteriores. En la Fig. 9 se observa cuántos entrevistados consideran cada uno de los criterios.

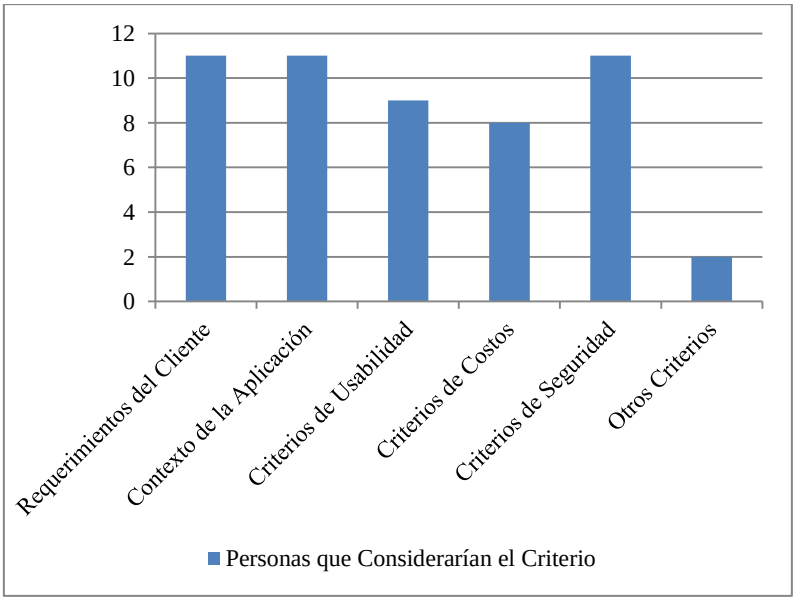


Figura 9. Criterios considerados por los entrevistados al seleccionar qué esquema o método de autenticación implementar.

En general, los requerimientos del cliente, el contexto de la aplicación y criterios relacionados a la seguridad son considerados más importantes que los criterios relacionados a la usabilidad y a los costos, siendo los tres primeros considerados 11 veces cada uno, y los otros 9 y 8 veces respectivamente. Se debe destacar que, de todas maneras, los 5 criterios son considerados por al menos dos tercios de los entrevistados. Otros criterios a considerar mencionados por los entrevistados son las normas y legislación del país en el que se utilizará la aplicación, y la facilidad de implementación del esquema o método para el desarrollador.

4.2.2 **Resultados de la Encuesta**

La formulación de las preguntas de la encuesta puede ser encontrada en el Anexo B. De un total de 83 personas a las que se les envió y solicitó responder la encuesta, todas ellas pertenecientes a la empresa Nisum Technologies, 46 de ellas la respondieron. Sin embargo, uno de los encuestados solo completó la información demográfica, por lo que se recibió un total de 45 respuestas válidas para la encuesta. La distribución de la experiencia de los encuestados (en años trabajando en Nisum y en relación a sus posiciones en la compañía) y el país en el que trabajan pueden ser vistos en la Fig. 10, la Fig. 11 y la Fig. 12.

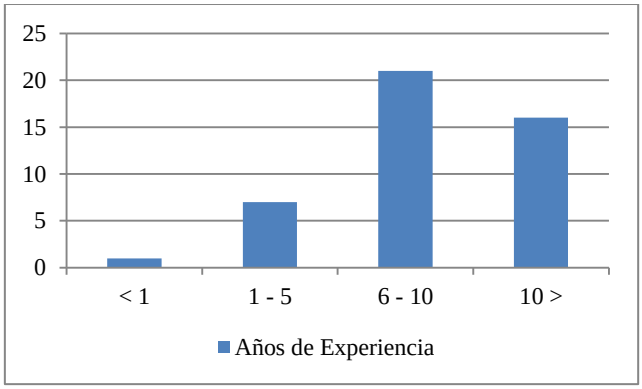


Figura 10. Años de experiencia en Nisum Technologies de los encuestados.

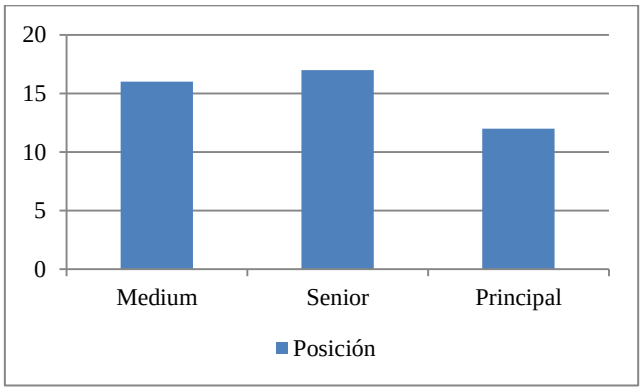


Figura 11. Experiencia de los encuestados en relación a su posición en Nisum Technologies.

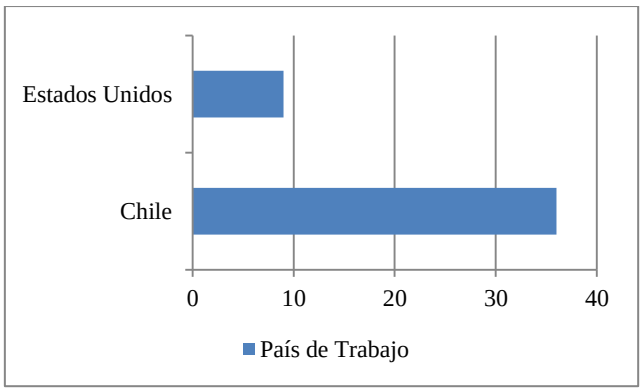


Figura 12. Distribución del país en el que trabajan los encuestados.

Los 45 encuestados tenían conocimiento sobre al menos un esquema de autenticación. Las contraseñas de texto son el esquema más conocido, pues 40 de los encuestados declaró conocer sobre ellas. OTP se queda atrás por poco, siendo reconocido 38 veces. Solo 10 de los encuestados conocían la autenticación cognitiva y 8 la autenticación basada en proxys. En la Fig. 13 se muestran los esquemas de autenticación y el número de encuestados que tenían conocimiento sobre cada uno de ellos.

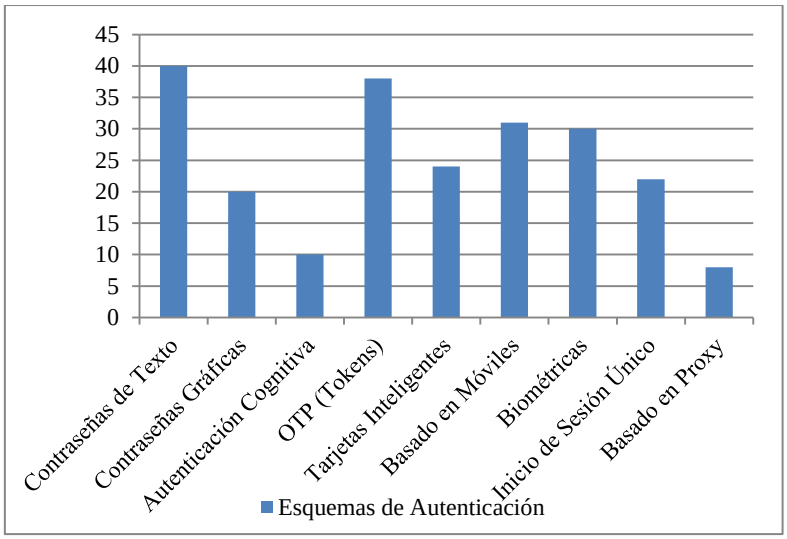


Figura 13. Cantidad de encuestados que tenía conocimiento sobre cada esquema de autenticación.

En cuanto a métodos de autenticación multi-factor, solo 27 de los encuestados tenía conocimiento sobre alguno. Los dos métodos más conocidos fueron la combinación de contraseñas de texto con OTP, y la combinación de contraseñas de texto con biométricas, cada uno con 15 menciones por parte de los encuestados. La combinación de los factores de conocimiento y posesión es la más conocida, con 30 respuestas diferentes entregadas para esta combinación. Por otro lado, solo se recibieron 11 respuestas diferentes para la combinación de los tres factores. La Tabla 9 muestra los métodos de autenticación multi-factor mencionados por los encuestados y el número de veces que fueron mencionados.

Tabla 9. Métodos de autenticación multi-factor mencionados por los encuestados.

Combinación	Método	Cantidad de Menciones
Conocimiento Y Posesión	Contraseñas de Texto Y OTP	15
	Contraseñas de Texto Y Tarjetas Inteligentes	8
	Contraseñas de Texto Y Basado en Móviles	6
	Autenticación Cognitiva Y Basado en Móviles	1
	Total	30
Conocimiento Y Inherencia	Contraseñas de Texto Y Biométricas	15
	Otros Métodos	3
	Total	18
Posesión Y Inherencia	OTP Y Biométricas	6
	Basado en Móviles Y Biométricas	3
	Tarjetas Inteligentes Y Biométricas	3
	Total	12
Conocimiento Y Posesión Y Inherencia	Contraseñas de Texto Y Tarjetas Inteligentes Y Biométricas	7
	Contraseñas de Texto Y OTP Y Biométricas	2
	Otros Métodos	2
	Total	11
	Gran Total	71

Un total de 23 encuestados mencionaron uno o más esquemas o métodos de autenticación que implementaron en alguna aplicación, indicando, además del esquema o método, las características de las aplicaciones y el motivo por el que lo seleccionaron. En la Fig. 14 se presentan los esquemas o métodos mencionados por los encuestados, en la Fig. 15 se muestran los tipos de aplicaciones para los que fueron recomendados y la Fig. 16 indica los motivos que indicaron los encuestados por seleccionar los distintos esquemas o métodos.

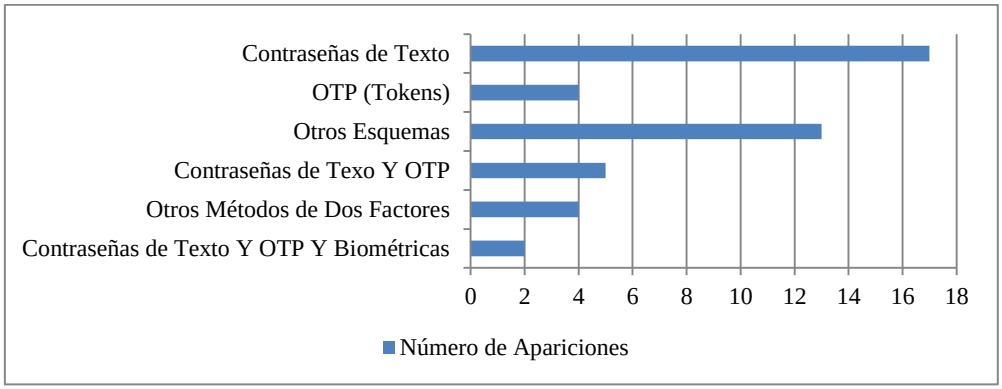


Figura 14. Esquemas y métodos de autenticación implementados por los encuestados.

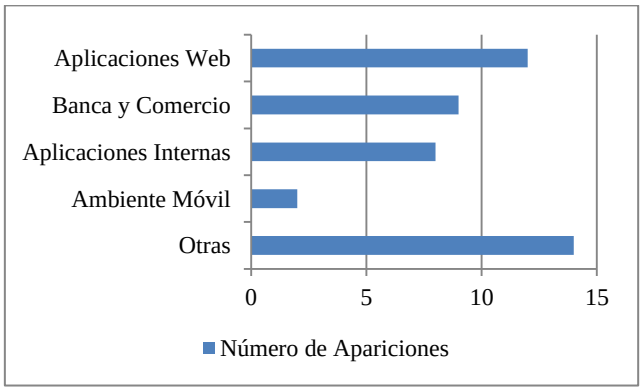


Figura 15. Tipos de aplicaciones en las que los encuestados han implementado esquemas o métodos de autenticación.

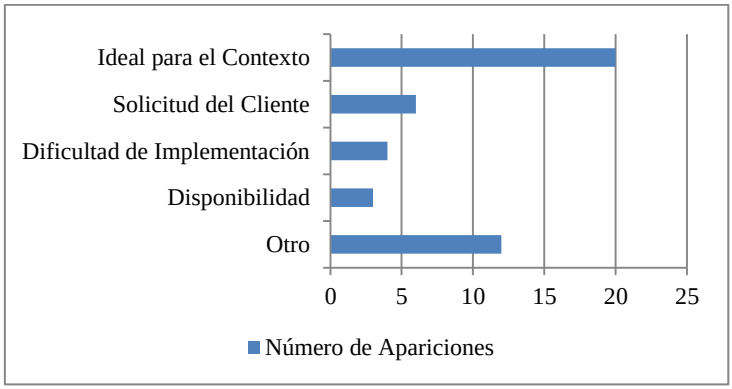


Figura 16. Motivos por los que los encuestados han seleccionado determinado esquema o método de autenticación.

Se puede observar que los dos esquemas más implementados por parte de los encuestados son las contraseñas de texto (17 veces) y OTP (4 veces), además de que la combinación de estos dos esquemas ha sido implementada cinco veces a modo de autenticación de dos factores, y dos veces a modo de autenticación de tres factores, en este caso incluyendo además algún esquema biométrico.

La mayoría de las aplicaciones desarrolladas por los encuestados corresponden a aplicaciones Web comunes (12), aplicaciones bancarias o comerciales (9) y aplicaciones para uso interno por las organizaciones (8). Por otra parte, se puede observar que el motivo más común para la selección de los esquemas o métodos de autenticación es la idealidad de éstos para el contexto al que va dirigida la aplicación.

Finalmente, 29 de los encuestados se sintieron suficientemente experimentados en el tema para evaluar la importancia de distintos criterios propuestos para la comparación y selección de esquemas o métodos de autenticación. Tanto el contexto de la aplicación como su nivel de seguridad requerido son los criterios mejor evaluados, con un valor promedio de 4,41 sobre 5. Otros criterios relevantes son la resistencia del esquema o método a ataques conocidos con un valor de 4,21 y los requerimientos del cliente con 4,17. Por otro lado, los encuestados no evalúan los criterios de usabilidad altamente, pues la facilidad de uso del esquema o método es evaluada en promedio con 3,31, y la facilidad de aprendizaje con 3,28. Además, la necesidad de portar un dispositivo es el criterio evaluado más bajo, con un valor medio de 3,1. La Tabla 10 muestra todos los criterios de comparación y selección y sus valores medios.

Tabla 10. Criterios de comparación y selección evaluados por los encuestados.

Categoría	Criterio	Valor de 1 a 5
Usabilidad	Facilidad de uso del esquema o método	3,31
	Facilidad para el usuario de aprender a utilizar el esquema o método	3,28
	Necesidad de portar un dispositivo, tarjeta u otro objeto	3,10
	Confiabilidad del esquema o método	4,10
Costos	Costos de implementación	4,07
	Costos relacionados a la cantidad de usuarios	4,00
	Compatibilidad con el servidor actual	3,69
	Necesidad de adquirir licencias	3,86
	Tecnologías disponibles	3,93
Seguridad	Nivel de seguridad	4,41
	Resistencia a ataques conocidos de autenticación	4,21
Otros	Requerimientos del cliente	4,17
	Contexto de la aplicación	4,41
	Normas y Legislación	3,90

Además, seis encuestados dieron ideas propias sobre otros criterios de comparación y selección posibles. De éstos, se destacan la facilidad de recuperar la información de autenticación de un usuario y la forma en que el usuario se registra en la aplicación (si lo hace el mismo o lo hace un administrador) por el lado de la usabilidad. Por otro lado, la sensibilidad de la información que está siendo utilizada por la aplicación se destaca en relación a seguridad.

4.2.3 **Discusión y Conclusiones**

Se ha logrado obtener un total de 57 respuestas: 12 por medio de las entrevistas y 45 por medio de la encuesta. Se puede observar que tanto las respuestas entregadas por los entrevistados, como aquellas obtenidas por medio de la encuesta, poseen cierta similitud en cuanto a los resultados que han sido obtenidos entre ambas técnicas de investigación. Lo anterior indica, en cierta forma, que las respuestas obtenidas por medio de estos instrumentos tienen un nivel de validez adecuado.

Las contraseñas de texto son el esquema de autenticación basado en conocimiento más conocido tanto por los entrevistados como por los encuestados. Esto se alinea con los resultados obtenidos durante la RSL, donde el esquema basado en conocimiento más investigado son las contraseñas de texto igualmente. Sin embargo, las contraseñas gráficas, que han sido casi tan investigadas como las contraseñas de texto en la literatura, no son tan conocidas por los expertos de la industria.

En cuanto al factor de posesión, los expertos de la industria tienen amplio conocimiento del uso de OTP y de la autenticación basada en móviles. Si bien también conocen las tarjetas inteligentes, éstas no son reportadas tanto como en la literatura, donde son el esquema de autenticación más investigado.

Un número de expertos indica conocer el inicio de sesión único federado y la autenticación basada en proxys, los cuales, si bien son una forma de realizar autenticación, no son esquemas propiamente tales, pues dependerá de cada implementación de éstos cuál esquema o método de autenticación se utilizará realmente.

Se puede observar que el mayor conocimiento que tienen los entrevistados y encuestados, en cuanto a autenticación multi-factor, es a la combinación de dos factores de contraseñas de texto y algún esquema del factor de posesión. Esto es similar a los resultados obtenidos en la RSL, donde la combinación del factor de conocimiento y el factor de posesión es predominante. Por otro lado, se puede observar que la autenticación de tres factores no es tan ampliamente conocida entre los expertos de la industria.

La gran mayoría de las aplicaciones implementadas tanto por los entrevistados como por los encuestados corresponden a aplicaciones Web o pertenecientes a la banca y al comercio. Esto muestra el hecho de que los tipos de aplicaciones en los que más trabajan los expertos de la industria, versus los contextos de aplicación más investigados en la academia, no son los mismos. A lo anterior se puede atribuir las discrepancias existentes entre el conocimiento de esquemas y métodos de autenticación por parte de los expertos de la industria, en comparación a la cantidad de veces que han sido investigados en la academia, siendo los esquemas que más conocen los expertos aquellos más utilizados dentro de los contextos de aplicación en los que más trabajan.

Los esquemas y métodos de autenticación más implementados por expertos de la industria son las contraseñas de texto, OTP, y la combinación de dos factores de éstos. El mayor motivo, indicado por los encuestados, por el que se seleccionó un esquema o método para cada aplicación es su idoneidad para el contexto en el que se trabajaba.

Se puede observar que ninguno de los criterios de comparación y selección propuestos a los entrevistados fue considerado por menos de dos tercios de éstos a la hora de seleccionar que esquema o método implementar al momento de desarrollar aplicaciones. Lo anterior indica que todos los criterios propuestos son adecuados, hasta cierto punto, para realizar una correcta comparación y selección de

esquemas o métodos de autenticación. Esto puede ser validado por medio de las respuestas entregadas por los encuestados, en una escala de 1 a 5, ninguno de los 14 criterios propuestos recibió un nivel de importancia promedio menor a 3, y siete de estos tuvieron un nivel de importancia 4 o superior.

Si bien existen diferencias entre los resultados obtenidos por medio de la RSL y aquellos obtenidos a través de la encuesta y entrevistas, los cuales, como se mencionó anteriormente, pueden ser atribuidos a la diferencia en los contextos donde se enfocan la academia y la industria, se puede ver que si existe cierta correlación entre el conocimiento entregado por ambas ramas. De todas maneras, el conocimiento obtenido por la RSL, junto con la experiencia reportada por expertos de la industria no son excluyentes, y pueden ser usados en conjunto para complementarse el uno al otro, lo cual permite obtener un valor agregado en cuanto a los resultados que puedan obtenerse basándose tanto en la academia como en la industria.

4.3 **Propuesta Inicial de Framework**

En base a la revisión sistemática de la literatura y a la encuesta y entrevistas a expertos de la industria, se generó una propuesta inicial de Framework, cuyo desarrollo puede ser dividido en tres grandes etapas, las cuales son presentadas en la Fig. 17.

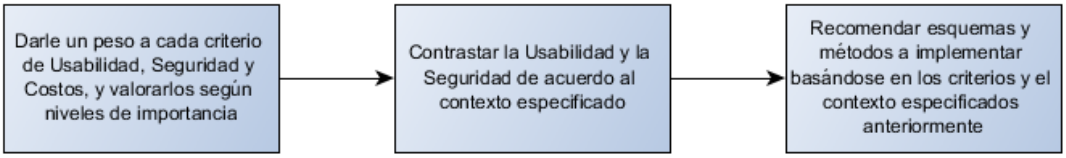


Figura 17. Etapas propuesta inicial de Framework.

La primera etapa consiste en obtener valores medios de cada uno de los grupos de criterios más reportados en la literatura, los cuales son la Usabilidad, la Seguridad y los Costos. De este modo, a cada criterio que considere el Framework se le dará un peso porcentual, donde la suma de los pesos de cada criterio para un grupo de criterios en específico será igual a 100%. Además, a cada criterio se le asignan distintos niveles de importancia, los cuales pueden ser dos o más, siendo uno de estos niveles de importancia equivalente al mínimo valor aceptable, y otro equivalente al máximo valor aceptable. Para obtener un valor promedio para cada grupo de criterios, se realiza una sumatoria del peso de cada criterio por el valor del nivel de importancia de éste, que mejor se adecúe a las características de la aplicación que se esté evaluando.

Una vez finalizada la primera etapa, durante la segunda se debe identificar el contexto para el que va dirigida la aplicación. Basándose en este contexto, se realiza el cálculo de un valor que ha sido denominado como valor de seguridad/usabilidad (SUV). La obtención de éste valor se justifica por medio de la apreciación obtenida durante la RSL, donde se puede notar que no existe un esquema o método de autenticación que sea capaz de brindar una máxima seguridad, una máxima usabilidad y costos mínimos. Asimismo, se observa que, a medida que más se favorezca la usabilidad en una aplicación, menos segura será esta, y, por el otro lado, mientras más se favorezca la seguridad, tendrá menos usabilidad. El SUV indica que, mientras mayor sea su valor, más importancia se le da a la seguridad en la aplicación a desarrollar, y menos se le dará a la usabilidad, y vice-versa. Este valor se calcula como se muestra a continuación:

$$SUV = C_1 Avg_{(S)} + C_2(100 - Avg_{(U)})$$

Donde C_1 y C_2 son constantes dependientes del contexto para el cual va dirigida la aplicación, mientras que $Avg_{(S)}$ y $Avg_{(U)}$ corresponden a los valores promedio de Seguridad y Usabilidad calculados durante la etapa anterior.

La última etapa consiste en la entrega de la recomendación de esquemas o métodos más adecuados para la aplicación evaluada por parte del Framework. Lo anterior se obtiene basándose, en primera instancia, en el SUV y, en segunda, en el valor promedio de costos. Las respuestas entregadas por el Framework variarán también dependiendo del contexto en el que será implementada la aplicación.

En la Sección 4.6 se entrega una descripción más detallada de la propuesta de Framework, ya en un estado final.

4.4 Panel de Expertos

Para asegurar la validez del Framework se trabajó con un panel de expertos pertenecientes a la industria, específicamente de Nisum Technologies, a lo largo de 4 días, oportunidad en la cual se recopiló la información que permitió realizar ajustes en el modelo creado, para que las recomendaciones entregadas por el Framework estuvieran más ajustadas a la realidad. Este panel de expertos contó con la presencia de 5 sujetos. En la Fig. 18 se presenta un diagrama general de las actividades realizadas durante cada una de las sesiones sostenidas con el panel de expertos. Éstas serán profundizadas en el resto de esta sección.

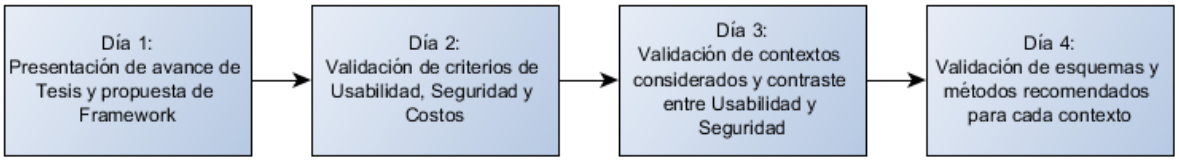


Figura 18. Actividades realizadas durante las sesiones sostenidas con el panel de expertos.

4.4.1 Presentación de Avance de Tesis y Propuesta de Framework

El primer día se realizó una presentación al panel de expertos para explicar el contexto en el que se desarrollaba este trabajo, el cual es de una tesis de magister. Se indicaron los avances obtenidos hasta ese momento, específicamente los descubrimientos obtenidos a través de la revisión de la literatura y los resultados de la encuesta realizada a expertos de la industria. Posteriormente se procedió a presentar las propuestas ideadas para la creación del Framework de recomendación y el posible funcionamiento de éste, utilizando un método deductivo para ello, de modo que los participantes del panel tuvieran una noción general de lo que se busca lograr.

4.4.2 Validación de Criterios de Usabilidad, Seguridad y Costos

Durante el segundo día se discutieron los criterios considerados para la utilización del Framework. Se le consultó al panel de expertos si estos consideraban estos criterios suficientes, si el peso que se le daba a cada uno era apropiado y si los niveles de importancia y valores de cada uno eran adecuados. Como resultado de esta sesión se realizaron cambios especialmente en los criterios relacionados a costos, donde se decidió dar un mayor énfasis a criterios relacionados directamente al presupuesto que se tenga para la implementación del esquema o método, descartando aquellos más indirectos; y el no considerar valores monetarios específicos sino basarse en porcentajes del presupuesto total de la aplicación, pues estos presupuestos pueden variar mucho de proyecto en proyecto, haciendo que ciertos costos parezcan menores para ciertas aplicaciones pero mayores para otras. El panel de expertos consideró que el peso que se le daba a cada criterio y los valores que se le daban a los niveles de importancia eran adecuados.

4.4.3 **Validación de Contextos Considerados y Contraste entre Usabilidad y Seguridad**

El tercer día se centró en la presentación de los contextos a considerar en el Framework, además de explicar el razonamiento de contrastar la Usabilidad y la Seguridad como características inversamente proporcionales. La pregunta de fondo en esta sesión fue el averiguar la opinión del panel de expertos en cuanto al peso que se le da a la Usabilidad y a la Seguridad para cada uno de los contextos considerados. El acto de contrastar la Usabilidad y la Seguridad fue bien recibido por el panel, pero hubo contextos que se consideró debían ser agrupados (autenticación remota, computación en la nube y ambiente multi-servidor) y otro que debía ser descartado (inicio de sesión único federado) debido a éste no siempre es considerado un contexto sino otro método de autenticación en sí por la gente de la industria. En cuanto a los pesos de la usabilidad y seguridad para cada contexto, si bien el panel dio su opinión en general sobre ellos, éstos consideraron que era necesario realizar una mayor validación en cuanto a este punto, a modo de tener una fundamentación más sólida y correcta sobre los pesos a ser considerados. Se decidió realizar una nueva encuesta para recopilar la información requerida de un número de expertos definido.

4.4.4 **Validación de Esquemas y Métodos Recomendados para cada Contexto**

La última sesión se enfocó en analizar los esquemas y métodos que eran recomendados para cada contexto considerado por el Framework. El mayor ajuste fue la fusión de los tres contextos mencionados anteriormente en uno solo que englobara a los tres, además de que se sugirió que algunos contextos fueran descritos con mayor detalle, a modo de evitar lo más posible que ciertas aplicaciones pudieran ser consideradas en más de un contexto. No hubo cambios mayores en cuanto a los esquemas y métodos recomendados para cada contexto.

4.5 **Peso de la Seguridad y la Usabilidad**

Se realizó una encuesta a un grupo en concreto de expertos de la industria, específicamente de Nisum Technologies, sobre sus apreciaciones en cuanto a la importancia de la seguridad y de la usabilidad de esquemas o métodos de autenticación para contextos en específico. En total se encuestó a 9 personas, entre las cuales se tiene a aquellas pertenecientes al grupo que conformó el panel de expertos.

La encuesta tenía una única pregunta, la cual consistía en darle un peso, porcentual, a la seguridad y a la usabilidad de esquemas de autenticación para los diferentes contextos propuestos en la encuesta. Este peso denota la importancia relativa de la usabilidad y de la seguridad en cada contexto. La suma de los pesos de seguridad y de usabilidad debía dar un 100%. En la Tabla 11 se pueden observar los resultados obtenidos.

Tabla 11. Pesos promedio de seguridad y usabilidad según los resultados de la encuesta.

Contexto	Peso Seguridad Promedio	Peso Usabilidad Promedio
Ambiente Móvil	45,56	54,44
Autenticación Remota, Ambiente Multi-Servidor, Computación en la Nube	64,44	35,56
Área de la Salud	57,78	42,22
Redes de Sensores Inalámbricos	63,33	36,67
Banca y Comercio	73,33	26,67
Aplicaciones Web Comunes	28,89	71,11

Se puede ver que en la mayoría de los contextos se le da una mayor importancia a la seguridad por sobre la usabilidad. Además, salvo por el área de la salud, donde la encuesta le da un peso más alto a la seguridad, los resultados obtenidos se aproximan considerablemente a las apreciaciones obtenidas por medio de la realización de la RSL y de la encuesta inicial a expertos de Nisum. Se consideraron las apreciaciones del autor, correspondientes a la percepción entregada por la academia, como una respuesta de mayor valor en la encuesta, teniendo un peso de 30% en ésta. Los pesos promedio obtenidos, aproximados a múltiplos de 5, son los utilizados por el Framework. La Tabla 12 presenta los pesos promedio finales, antes de ser aproximados a múltiplos de 5.

Tabla 12. Pesos promedio de seguridad y usabilidad, considerando las apreciaciones del autor.

Contexto	Peso Seguridad Promedio	Peso Usabilidad Promedio
Ambiente Móvil	45,39	54,61
Autenticación Remota, Ambiente Multi-Servidor, Computación en la Nube	63,11	36,89
Área de la Salud	52,45	47,55
Redes de Sensores Inalámbricos	60,83	39,17
Banca y Comercio	73,83	26,17
Aplicaciones Web Comunes	27,72	72,28

4.6 **Propuesta de Framework Final**

A continuación se presenta la versión final del Framework y la forma en que éste debe ser utilizado.

Inicialmente se ha considerado un número de criterios para la utilización del Framework. Estos criterios, presentados en la Tabla 13, son tomados principalmente de aquellos más predominantes en la literatura y que se consideraron de relevancia para las intenciones del Framework: se seleccionaron criterios de usabilidad basándose en (Bonneau *et al.*, 2012), (Anwar e Imran, 2015), (Kumari *et al.*, 2015), (Alizadeh *et al.*, 2016), (Zviran y Erlich, 2006), (Park *et al.*, 2014) y (Eliasson *et al.*, 2009), criterios de seguridad según (Bonneau *et al.*, 2012), (Kumari *et al.*, 2015), (Alizadeh *et al.*, 2016), (Madhusudhan y Mittal, 2012), (O'Gorman, 2003), (Choksi, 2014), (Eliasson *et al.*, 2009) y (Wang *et al.*, 2016) y criterios de costos por medio de (Bonneau *et al.*, 2012), (Zviran y Erlich, 2006), (O'Gorman, 2003), (Park *et al.*, 2014) y (Altinkemer y Wang, 2011). Cabe mencionar que no se consideraron criterios que apuntaran al uso de tecnologías específicas, tales como "compatibilidad con el servidor" o "tecnologías disponibles", pues el Framework no está pensado para ser utilizado solo dentro del contexto de una tecnología en específico, si no que entrega una propuesta de uso de esquemas o métodos de autenticación independientemente de ese tipo de criterio. Por otro lado, se consideraron otros criterios según los resultados obtenidos por medio de la encuesta realizada a expertos de Nisum, como por ejemplo el criterio de "recuperación de información de autenticación". Los valores y pesos de las afirmaciones fueron definidos según las apreciaciones de importancia percibidas por los expertos de Nisum para cada criterio por medio de la encuesta realizada. A continuación se describen brevemente los criterios utilizados en el Framework:

- Usabilidad
  - Facilidad de Uso: La complejidad que presentan las acciones que deben ser realizadas por el usuario al momento de autenticarse.
  - Facilidad de Aprendizaje: El tiempo promedio que le toma a un usuario acostumbrarse a utilizar el esquema o método de autenticación.
  - Recuperación de Información de Autenticación: Complejidad que presenta para el usuario recuperar la información que debe utilizar para autenticarse, en caso de pérdida u olvido de ésta.
  - Necesidad de Utilización de un Dispositivo: Cuan aceptable es que el usuario tenga que portar un dispositivo, ya sea de posesión (algo único) o biométrico (que le permita demostrar su información de inherencia).
  - Confiabilidad del Esquema o Método para Autenticación: Recurrencia aceptable en la que el esquema o método de autenticación pueda entregar falsos negativos (que no reconozca la información de autenticación del usuario y no le permita el ingreso, aun cuando la información entregada es la correcta, forzándolo a intentarlo de nuevo).
- Seguridad
  - Nivel de Seguridad: Apreciación general de la importancia de la seguridad en la aplicación por parte del equipo de desarrollo, según la información que haya sido especificada ya sea por el cliente o el mismo equipo de desarrollo.
  - Sensibilidad de la Información: Tipo de información con la que trabajará la aplicación y nivel de sensibilidad que ésta posee.
  - Resistencia a Observación de Terceros: Que el esquema o método sea capaz de ser utilizado en lugares donde existan personas que podrían estar observando a los usuarios al momento de autenticarse.
  - Resistencia a Phishing: Que sea difícil para un atacante discernir la información de autenticación de un usuario, aun si éste adquiere conocimiento relacionado a ésta por medio de aplicación de ingeniería social al usuario.
  - Resistencia a Ataques de Repetición: Que el costo de intentar obtener la información de autenticación de un usuario por medio de ataques de fuerza bruta o repetición sea mayor a las ganancias que pueda conseguir el atacante si es que logra obtener dicha información.
- Costos
  - Costos de Implementación: El valor monetario que está dispuesto a invertir el cliente o el equipo de desarrollo para la implementación de los aspectos de seguridad y autenticación en la aplicación a desarrollar.
  - Costos por Usuario: Voluntad del cliente o del equipo de desarrollo para incurrir en gastos adicionales por cada usuario que se registre en la aplicación, ya sea por la necesidad de entregar dispositivos de autenticación u otros motivos.

Tabla 13. Selección de importancia de criterios de usabilidad, seguridad y costos.

	Criterio	Importancia	Valor	Peso
USABILIDAD (U)	Facilidad de uso	El esquema necesariamente debe ser fácil de usar El esquema preferentemente debe ser fácil de usar No es necesario que el esquema sea fácil de usar	100 60 20	25%
	Facilidad de aprendizaje	No se debe tardar más de un día en aprender a usar el esquema No se debe tardar más de una semana en aprender a usar el esquema No importa el tiempo que se deba tardar en aprender a usar el esquema	100 60 20	25%
	Recuperación de información de autenticación	El proceso de recuperar la información de autenticación debe ser simple El proceso de recuperar la información de autenticación debe ser complejo	100 20	10%
	Necesidad de utilización de un dispositivo	El esquema no debe necesitar utilizar un dispositivo El esquema puede necesitar utilizar un dispositivo de posesión o uno biométrico El esquema puede necesitar utilizar un dispositivo de posesión y uno biométrico	100 60 20	10%
	Confiabilidad del esquema o método para autenticación	El esquema no debe fallar nunca o casi nunca al autenticarse El esquema no debe fallar ocasionalmente al autenticarse El esquema puede fallar ocasionalmente al autenticarse No importa cuán seguido falle el esquema al autenticarse	100 75 45 20	30%
SEGURIDAD (S)	Nivel de seguridad	La seguridad es un aspecto crucial de la aplicación La seguridad es un aspecto importante de la aplicación La seguridad es un aspecto secundario de la aplicación	100 60 20	45%
	Sensibilidad de la información	La aplicación trabaja con información sensible de la empresa y de los usuarios La aplicación trabaja con información sensible de la empresa La aplicación trabaja con información sensible de los usuarios La aplicación no trabaja con información sensible	100 75 45 20	25%
	Resistencia a observación de terceros	El esquema es resistente El esquema no es resistente	100 20	10%
	Resistencia a phishing	El esquema es resistente El esquema no es resistente	100 20	10%
	Resistencia a ataques de repetición	El esquema es resistente El esquema no es resistente	100 20	10%
COSTOS (C)	Costos de implementación	El esquema debe presentar costos menores al 10% del presupuesto El esquema debe presentar costos menores al 30% del presupuesto El esquema puede presentar costos de implementación de cualquier monto	100 60 20	65%
	Costos por usuario	El esquema no debe presentar costos adicionales por cada usuario registrado El esquema puede presentar costos adicionales por cada usuario registrado	100 20	35%

Se optó por tener un valor mínimo de Usabilidad, Seguridad y Costos que no fuera 0, pues en la realidad no sería adecuado tener una aplicación en la que no se le dé un valor, aunque sea mínimo, a alguno de estos criterios.

Una vez definidas estas afirmaciones, es posible calcular valores medios de Usabilidad (U), Seguridad (S) y Costos (C) según las siguientes fórmulas:

$$U = \sum_{por\ cada\ criterio\ de\ U} ValorAfirmación * PesoCriterio$$

$$S = \sum_{por\ cada\ criterio\ de\ S} ValorAfirmación * PesoCriterio$$

$$C = \sum_{por\ cada\ criterio\ de\ C} ValorAfirmación * PesoCriterio$$

Se seleccionaron, además, los Contextos (Ct) estudiados más frecuentemente en la literatura como contextos comunes para ser utilizados como un criterio de selección dentro del Framework. Si bien la banca y comercio, junto con las aplicaciones Web comunes no han sido estudiados tan ampliamente como contextos para la autenticación por investigadores, éstos son contextos utilizados frecuentemente en la industria según los resultados obtenidos en la encuesta realizada a los expertos de Nisum, por lo que se han incluido considerando tanto el conocimiento obtenido de la RSL como aquel entregado por los expertos de Nisum para cada contexto. Además, basándose en el Ct que se seleccione, se calcula el Valor de Seguridad/Usabilidad (SUV), según lo indicado por la fórmula correspondiente en la Tabla 14, según el Ct que va dirigida la aplicación. Los pesos de los valores de usabilidad y seguridad para cada contexto son obtenidos de la apreciación del autor, según el conocimiento adquirido durante la realización de la RSL, más la de expertos de Nisum, por medio de una breve encuesta realizada con posterioridad, la cual es detallada más adelante. El valor de U se invierte ($100 - U$) debido a que el valor de SUV ha de indicar que mientras mayor sea éste, más importante será la seguridad para la aplicación, lo cual indirectamente significa que ésta tendrá que sacrificar cierto nivel de usabilidad para satisfacer el nivel de seguridad deseado. Inversamente, si la seguridad no es tan importante para la aplicación, más valor se le dará a la usabilidad de ésta. En otras palabras, un SUV alto implicará que se requiere utilizar esquemas o métodos de autenticación más seguros, y un SUV bajo implicará que se requiere utilizar esquemas o métodos de autenticación con una mayor usabilidad. El aspecto de los costos, debido a que no es reportado tan seguido en la RSL como la seguridad y la usabilidad, es considerado como un criterio secundario, el cual dividirá los esquemas o métodos de autenticación a sugerir por el Framework solo una vez que ya se haya identificado el nivel de seguridad y usabilidad que se desea tener. Todo lo anterior debido a que no existe un esquema o método de autenticación que sea capaz de entregar tanto seguridad como usabilidad máximos y costos mínimos, como se puede apreciar, por ejemplo, en (Bonneau *et al.*, 2012), donde se presenta una tabla indicando posibles características de esquemas de autenticación, en la cual ninguno de los esquemas analizados poseía todas estas características.

Tabla 14. Cálculo de Valor de Seguridad/Usabilidad (***SUV***) para cada contexto.

ID	Contexto	Valor de Seguridad/Usabilidad (SUV)
Ct1	Ambiente Móvil	$SUV = 0{,}45S + 0{,}55(100 - U)$
Ct2	Autenticación Remota, Ambiente Multi-Servidor, Computación en la Nube	$SUV = 0{,}65S + 0{,}35(100 - U)$
Ct3	Área de la Salud	$SUV = 0{,}5S + 0{,}5(100 - U)$
Ct4	Redes de Sensores Inalámbricos	$SUV = 0{,}6S + 0{,}4(100 - U)$
Ct5	Banca y Comercio	$SUV = 0{,}75S + 0{,}25(100 - U)$
Ct6	Aplicaciones Web Comunes	$SUV = 0{,}3S + 0{,}7(100 - U)$
	Otros Contextos	$SUV = 0{,}5S + 0{,}5(100 - U)$

A continuación se entrega una breve descripción de los contextos considerados por el Framework:

- Ambiente Móvil: Aplicaciones cuyo usuario final haga uso de ellas por medio de un dispositivo móvil, ya sea un teléfono inteligente, una Tablet u otro dispositivo de similares características, y cuyo énfasis no sea la realización de transacciones de dinero.
- Autenticación Remota, Ambiente Multi-Servidor y Computación en la Nube: Aplicaciones en las que los usuarios se autenticarán a una red de forma remota, cuya información se encuentre almacenada dentro de más de un servidor y/o basadas en el uso de internet para proveer servicios o almacenamiento.
- Área de la Salud: Aplicaciones dirigidas a ambientes médicos o de la salud, especialmente para el cuidado de pacientes o de personas de la tercera edad.
- Redes de Sensores Inalámbricos: Aplicaciones encargadas de monitorear condiciones físicas o ambientales y de recopilar dicha información para su uso posterior.
- Banca y Comercio: Aplicaciones bancarias o comerciales, independiente de la plataforma para la que están enfocados, donde el énfasis está en las transacciones de dinero.
- Aplicaciones Web Comunes: Aplicaciones simples dentro del internet, tales como blogs o páginas de noticias.

Con la información anterior se puede obtener la recomendación del Framework, la cual se ve reflejada en las Tablas 15-21. El o los esquemas o métodos de autenticación indicados en cada fila de cada tabla serán el o los esquemas o métodos que el Framework recomendará según los criterios y contexto definidos en cada uso de éste. Para la selección de qué esquemas o métodos de autenticación recomendar para cada fila, inicialmente se calcularon valores aproximados de usabilidad, seguridad y costos para cada esquema de autenticación, basándose en las características que posee cada uno reportadas en (Bonneau *et al.*, 2012). En este artículo se presenta un Framework de análisis de variados esquemas de autenticación según características de usabilidad, seguridad y costos, indicando si poseen, casi poseen o no poseen las características consideradas. Posteriormente, se identificaron los esquemas y métodos más investigados y usados para cada contexto, según lo reportado por la RSL y (para los contextos más usados en la industria mencionados en el punto anterior) la encuesta realizada a expertos de la industria. Los esquemas se organizaron en tres niveles, principalmente según la cantidad de factores que consideraban, implicando el hecho de que mientras más factores se utilicen, más seguro será el esquema o método de autenticación, pero más baja será su usabilidad, y viceversa.

Posteriormente cada nivel se dividió nuevamente entre aquellos esquemas o métodos de mayor y menor costo, culminando con seis posibles niveles por contexto.

Al lado de cada esquema o método de autenticación presentado en las Tablas 15-21 se tiene un número utilizado para ordenarlos de mayor a menor recomendado para cada caso. Este número indica la cantidad de veces que cada combinación de esquemas para cada esquema o método ha sido propuesta en la literatura o por expertos de la industria para el contexto en el que se está considerando, dividido, en el caso de los métodos de autenticación, por la cantidad de esquemas que considera el método.

Por ejemplo, si tenemos un método de autenticación que combina tres esquemas de autenticación, se debe sumar la cantidad de veces que el uso de cada esquema por separado ha sido propuesto para el contexto, la cantidad de veces que el uso de todas las posibles combinaciones de dos factores de los esquemas han sido propuestas para el contexto y la cantidad de veces que el uso de la combinación de tres factores de los esquemas ha sido propuesta para el contexto. Finalmente, debido a que es un método de autenticación de tres factores, la suma anterior se divide por tres. Ahora bien, si se considera un esquema de autenticación de un factor como otro ejemplo, solo se debe contar la cantidad de veces que el uso de dicho esquema ha sido propuesto para el contexto, dividiendo por uno, debido a que se considera un solo esquema.

Tabla 15. Esquemas o métodos recomendados por el Framework para Ambiente Móvil.

		Ct1 – Ambiente Móvil
Nivel 1	$\boldsymbol{SUV \geq 65}$ $\boldsymbol{C < 60}$	Contraseñas Gráficas + Tarjetas Inteligentes + Biométricas de Comportamiento **15,3** Contraseñas de Texto + OTP + Biométricas de Comportamiento **13,6** Contraseñas Gráficas + OTP + Biométricas de Comportamiento **12,6** Contraseñas Gráficas + OTP + Biométricas del Rostro **5,6**
	$\boldsymbol{SUV \geq 65}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto + Tarjetas Inteligentes + Biométricas de Comportamiento **19,3** Contraseñas de Texto + Tarjetas Inteligentes + Biométricas del Rostro **12,3**
Nivel 2	$\boldsymbol{35 < SUV < 65}$ $\boldsymbol{C < 60}$	Contraseñas Gráficas + Biométricas de Comportamiento **17** OTP + Biométricas de Comportamiento **14** Contraseñas de Texto + Palma de la Mano o Huellas Dactilares **7,5** Contraseñas Gráficas + OTP **6**
	$\boldsymbol{35 < SUV < 65}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto + Biométricas de Comportamiento **17,5** Contraseñas de Texto + Tarjetas Inteligentes **14,5**
Nivel 3	$\boldsymbol{SUV \leq 35}$ $\boldsymbol{C < 60}$	Biométricas de Comportamiento **24** Contraseñas Gráficas **8** Biométricas del Rostro **3** Palma de la Mano o Huellas Dactilares **2**
	$\boldsymbol{SUV \leq 35}$ $\boldsymbol{C \geq 60}$	Biométricas de Comportamiento **24** Contraseñas de Texto **9** Contraseñas Gráficas **8**

Tabla 16. Esquemas o métodos recomendados por el Framework para Autenticación Remota, Ambiente Multi-Servidor y Computación en la Nube.

		Ct2 – Autenticación Remota, Ambiente Multi-Servidor y Computación en la Nube
Nivel 1	$\boldsymbol{SUV \geq 65}$ $\boldsymbol{C < 60}$	Contraseñas Gráficas + Tarjetas Inteligentes + P. de la Mano o Huellas Dactilares **33,3** Contraseñas Gráficas + Tarjetas Inteligentes + Biométricas de Comportamiento **31** Contraseñas de Texto + OTP + Biométricas de Comportamiento **7,3** Contraseñas Gráficas + OTP + Palma de la Mano o Huellas Dactilares **5**
	$\boldsymbol{SUV \geq 65}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto + Tarjetas Inteligentes + Biométricas de Comportamiento **48** Contraseñas de Texto + Basado en Móviles + P. de la Mano o Huellas Dactilares **8,3** Contraseñas de Texto + Basado en Móviles + Biométricas de Comportamiento **7**
Nivel 2	$\boldsymbol{35 < SUV < 65}$ $\boldsymbol{C < 60}$	Tarjetas Inteligentes + Palma de la Mano o Huellas Dactilares **32,5** Tarjetas Inteligentes + Biométricas de Comportamiento **30,5** Contraseñas Gráficas + Tarjetas Inteligentes **23** Contraseñas de Texto + OTP **7** OTP + Biométricas de Comportamiento **5** Contraseñas de Texto + Basado en Móviles **5**
	$\boldsymbol{35 < SUV < 65}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto + Tarjetas Inteligentes **55,5** Tarjetas Inteligentes + Biométricas de Comportamiento **30,5** Contraseñas Gráficas + Tarjetas Inteligentes **23** Contraseñas de Texto + Basado en Móviles **5**
Nivel 3	$\boldsymbol{SUV \leq 35}$ $\boldsymbol{C < 60}$	Tarjetas Inteligentes **44** Palma de la Mano o Huellas Dactilares **10** Biométricas del Rostro **6** Biométricas de Comportamiento **6** Iris **6**
	$\boldsymbol{SUV \leq 35}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto **6** Biométricas de Comportamiento **6**

Tabla 17. Esquemas o métodos recomendados por el Framework para Área de la Salud.

		Ct3 – Área de la Salud
Nivel 1	$\boldsymbol{SUV \geq 65}$ $\boldsymbol{C < 60}$	Contraseñas de Texto + Tarjetas Inteligentes + Biométricas de Comportamiento **20,6** Contraseñas de Texto + OTP + Biométricas de Comportamiento **3,6** Contraseñas de Texto + OTP + Palma de la Mano o Huellas Dactilares **3,6** Contraseñas de Texto + OTP + Biométricas del Rostro **3,6** Contraseñas de Texto + OTP + Iris **3,6**
	$\boldsymbol{SUV \geq 65}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto + Tarjetas Inteligentes + Biométricas de Comportamiento **20,6** Contraseñas de Texto + Basado en Móviles + Biométricas de Comportamiento **4,3** Contraseñas de Texto + Basado en Móviles + P. de la Mano o Huellas Dactilares **4,3**
Nivel 2	$\boldsymbol{35 < SUV < 65}$ $\boldsymbol{C < 60}$	Tarjetas Inteligentes + Biométricas de Comportamiento **10,5** OTP + Biométricas de Comportamiento **5,5** OTP + Palma de la Mano o Huellas Dactilares **5,5** OTP + Biométricas del Rostro **5,5** OTP + Iris **5,5** Basado en Móviles + Biométricas de Comportamiento **4,5** Basado en Móviles + Palma de la Mano o Huellas Dactilares **4,5**
	$\boldsymbol{35 < SUV < 65}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto + Tarjetas Inteligentes **18**
Nivel 3	$\boldsymbol{SUV \leq 35}$ $\boldsymbol{C < 60}$	Biométricas del Rostro **9** Biométricas de Comportamiento **9** Palma de la Mano o Huellas Dactilares **9** Iris **9**
	$\boldsymbol{SUV \leq 35}$ $\boldsymbol{C \geq 60}$	Biométricas de Comportamiento **9**

Tabla 18. Esquemas o métodos recomendados por el Framework para Redes de Sensores Inalámbricos.

		Ct4 – Redes de Sensores Inalámbricos
Nivel 1	$\boldsymbol{SUV \geq 65}$ $\boldsymbol{C < 60}$	Contraseñas de Texto + Tarjetas Inteligentes + Biométricas de Comportamiento **14,3**
	$\boldsymbol{SUV \geq 65}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto + Tarjetas Inteligentes + Biométricas de Comportamiento **14,3**
Nivel 2	$\boldsymbol{35 < SUV < 65}$ $\boldsymbol{C < 60}$	Tarjetas Inteligentes + Biométricas de Comportamiento **4,5** Tarjetas Inteligentes + Palma de la Mano o Huellas Dactilares **4,5**
	$\boldsymbol{35 < SUV < 65}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto + Tarjetas Inteligentes **18,5** Tarjetas Inteligentes + Biométricas de Comportamiento **4,5**
Nivel 3	$\boldsymbol{SUV \leq 35}$ $\boldsymbol{C < 60}$	Biométricas del Rostro **1** Biométricas de Comportamiento **1** Palma de la Mano o Huellas Dactilares **1** Iris **1**
	$\boldsymbol{SUV \leq 35}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto **2** Biométricas de Comportamiento **1**

Tabla 19. Esquemas o métodos recomendados por el Framework para Banca y Comercio.

		Ct5 – Banca y Comercio
Nivel 1	$\boldsymbol{SUV \geq 65}$ $\boldsymbol{C < 60}$	Contraseñas de Texto + OTP + Biométricas de Comportamiento **4,3** Contraseñas Gráficas + Tarjetas Inteligentes + Biométricas de Comportamiento **1,6** Contraseñas Gráficas + OTP + Biométricas de Comportamiento **1,3**
	$\boldsymbol{SUV \geq 65}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto + Basado en Móviles + Biométricas de Comportamiento **3,3** Contraseñas de Texto + Tarjetas Inteligentes + Biométricas de Comportamiento **3**
Nivel 2	$\boldsymbol{35 < SUV < 65}$ $\boldsymbol{C < 60}$	Contraseñas de Texto + OTP **4** Basado en Móviles + Biométricas de Comportamiento **2,5** OTP + Biométricas de Comportamiento **1,5**
	$\boldsymbol{35 < SUV < 65}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto + Basado en Móviles **4,5** Contraseñas de Texto + Tarjetas Inteligentes **2**
Nivel 3	$\boldsymbol{SUV \leq 35}$ $\boldsymbol{C < 60}$	Biométricas de Comportamiento **2** Biométricas del Rostro **1** Palma de la Mano o Huellas Dactilares **1** Iris **1**
	$\boldsymbol{SUV \leq 35}$ $\boldsymbol{C \geq 60}$	Contraseñas de Texto **2** Biométricas de Comportamiento **2**

Tabla 20. Esquemas o métodos recomendados por el Framework para Aplicaciones Web Comunes.

		Ct6 – Aplicaciones Web Comunes
Nivel 1	$SUV \geq 65$ $C < 60$	Contraseñas de Texto + OTP + Biométricas de Comportamiento **5,6** Contraseñas de Texto + OTP + Palma de la Mano o Huellas Dactilares **5,6** Contraseñas de Texto + OTP + Biométricas del Rostro **5,6** Contraseñas de Texto + OTP + Iris **5,6**
	$SUV \geq 65$ $C \geq 60$	Contraseñas de Texto + Tarjetas Inteligentes + Biométricas de Comportamiento **4,6** Contraseñas de Texto + Basado en Móviles + Biométricas de Comportamiento **4,6**
Nivel 2	$35 < SUV < 65$ $C < 60$	Contraseñas de Texto + OTP **7,5** Basado en Móviles + Biométricas de Comportamiento **1**
	$35 < SUV < 65$ $C \geq 60$	Contraseñas de Texto + Tarjetas Inteligentes **6** Contraseñas de Texto + Basado en Móviles **5,5**
Nivel 3	$SUV \leq 35$ $C < 60$	Biométricas del Rostro **1** Biométricas de Comportamiento **1** Palma de la Mano o Huellas Dactilares **1** Iris **1**
	$SUV \leq 35$ $C \geq 60$	Contraseñas de Texto **10** Biométricas de Comportamiento **1**

Tabla 21. Esquemas o métodos recomendados por el Framework para Otros Contextos.

		Otros Contextos
Nivel 1	$SUV \geq 65$ $C < 60$	Contraseñas de Texto + OTP + Biométricas de Comportamiento **81,3** Contraseñas Gráficas + Tarjetas Inteligentes + Biométricas de Comportamiento **81,3** Contraseñas Gráficas + OTP + Biométricas de Comportamiento **56,6** Contraseñas Gráficas + Basado en Móviles + Biométricas de Comportamiento **47,6** Contraseñas Gráficas + OTP + Palma de la Mano o Huellas Dactilares **43**
	$SUV \geq 65$ $C \geq 60$	Contraseñas de Texto + Tarjetas Inteligentes + Biométricas de Comportamiento **154,6** Contraseñas de Texto + Basado en Móviles + Biométricas de Comportamiento **73,3**
Nivel 2	$35 < SUV < 65$ $C < 60$	Contraseñas de Texto + OTP **60,5** OTP + Biométricas de Comportamiento **60,5** Basado en Móviles + Biométricas de Comportamiento **48** Contraseñas Gráficas + OTP **43,5** Contraseñas Gráficas + Basado en Móviles **32**
	$35 < SUV < 65$ $C \geq 60$	Contraseñas de Texto + Tarjetas Inteligentes **162,5** Contraseñas Gráficas + Biométricas de Comportamiento **57,5** Contraseñas de Texto + Basado en Móviles **51**
Nivel 3	$SUV \leq 35$ $C < 60$	Biométricas de Comportamiento **69** Contraseñas Gráficas **42** Palma de la Mano o Huellas Dactilares **28** Biométricas del Rostro **24**
	$SUV \leq 35$ $C \geq 60$	Biométricas de Comportamiento **69** Contraseñas de Texto **44** Contraseñas Gráficas **42**

A continuación se presenta una breve descripción de cada uno de los esquemas de autenticación que podría llegar a recomendar el Framework:

- Esquemas Basados en el Factor de Conocimiento:
  - Contraseñas de Texto: Un usuario ingresa un nombre de usuario conocido (por ejemplo, su correo electrónico o un número de identificación), junto con una contraseña (una cadena de caracteres que solo él conoce) para demostrar su identidad.
  - Contraseñas Gráficas: Similar a las contraseñas de texto, pero en vez de recordar una cadena de caracteres, el usuario debe recordar un patrón basado en imágenes.
- Esquemas Basados en el Factor de Posesión:
  - Tarjetas Inteligentes: Una tarjeta inteligente es una tarjeta no más grande que un bolsillo que posee circuitos integrados. Para autenticarse con este esquema de autenticación, un usuario debe demostrar que éste posee su tarjeta inteligente.
  - Contraseñas de Uso Único (OTP): También conocidas como Tokens. Éstas vienen en diferentes formas, como por ejemplo: Token de Hardware, que consisten en un dispositivo que genera un número aleatorio; Token de Software, que generan un número aleatorio por medio de una aplicación; y Token de papel o de cuadrícula, que consisten en coordenadas que poseen números aleatorios. Se le solicita al usuario ingresar el número correspondiente entregado por el Token para autenticarse.
  - Autenticación Basada en Móviles: El usuario debe utilizar su teléfono celular para autenticar su identidad. Esto se realiza por medio de mensajes de texto (SMS) o a través de una aplicación instalada en el dispositivo, por ejemplo.
- Esquemas Basados en el Factor de Inherencia:
  - Biométricas del Rostro: La autenticación es realizada por medio del reconocimiento de los rasgos faciales del usuario.
  - Biométricas de Comportamiento: A diferencia de otras biométricas, que se preocupan de características físicas, en este caso el usuario es autenticado por medio de su propio comportamiento. Por ejemplo, la forma en la que presiona las teclas del teclado o cómo presiona la pantalla del dispositivo.
  - Palma de la Mano y Huellas Dactilares: Para las biométricas de la palma de la mano, un usuario es autenticado por medio del reconocimiento de la palma de su mano. Para las huellas dactilares, el proceso es similar, pero una o más de las huellas dactilares del usuario son usadas en vez de la palma de su mano.
  - Iris: El usuario es autenticado por medio del reconocimiento del iris en su ojo.

Una vez identificadas las recomendaciones del Framework, resta decidir cuál de las recomendaciones implementar en la aplicación a desarrollar y proceder a ello. En la Fig. 19 se resumen los principales pasos para el uso del Framework que fueron explicados anteriormente. Luego se detalla brevemente cada paso.

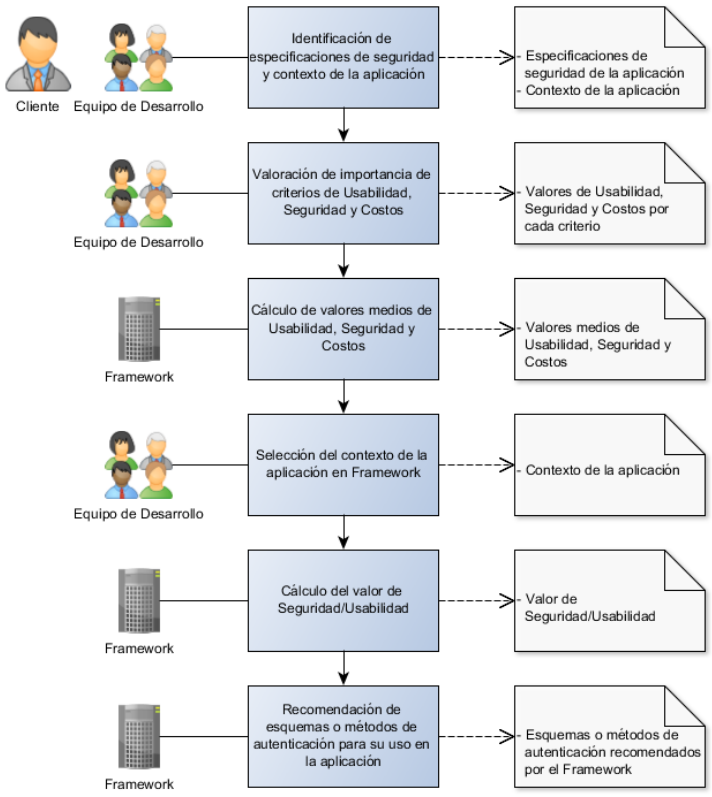


Figura 19. Etapas para el uso del Framework, participantes y entregables obtenidos en cada etapa.

Antes de comenzar a utilizar el Framework, se debe identificar la información relevante de la aplicación a desarrollar. Esto es realizado principalmente por medio de conversaciones entre el equipo de desarrollo y su cliente, durante la licitación de requerimientos o procesos similares. Al hacer esto, tanto las especificaciones de la aplicación y el contexto para el que va dirigida pueden ser identificados.

El próximo paso involucra valorar la importancia de cada criterio considerado por el Framework para la aplicación, basándose en la información recopilada durante el paso anterior. Esto se realiza para cada criterio definido en la Tabla 13. Es en este paso que el Framework en sí comienza a ser utilizado. Los valores de cada criterio para este uso del Framework son obtenidos en este paso.

Ya con los valores de cada criterio, es posible calcular los valores promedios para cada categoría de criterios usando las fórmulas del Framework. De este modo, los valores medios de Usabilidad (U), Seguridad (S) y Costos (C) son obtenidos.

Una vez calculados los valores U, S y C, el desarrollador debe identificar el Contexto (Ct) considerado por el Framework que mejor refleje aquel de la aplicación que se está desarrollando. Los contextos considerados por el Framework pueden ser observados en la Tabla 14.

Habiendo seleccionado el Ct y calculado los valores U, S y C, se calcula el Valor de Seguridad/Usabilidad (SUV), según lo indicado por la fórmula correspondiente en la Tabla 14, según el Ct que va dirigida la aplicación.

Una vez calculado el valor de SUV, se debe ubicar en la tabla correspondiente al Ct de la aplicación que ha sido identificado (Tablas 15-21), la fila para la que correspondan los valores de C y SUV calculados. El o los esquemas o métodos de autenticación indicados en esa fila serán el o los esquemas o métodos que el Framework le recomendará al desarrollador implementar en una aplicación para el contexto y los criterios de usabilidad, seguridad y costos que éste haya especificado.

Capítulo 5
Construcción de Prototipo de Herramienta

En el capítulo anterior se presentó la definición del Framework para la Comparación y Selección de Esquemas y Métodos de Autenticación, mostrando el proceso que se llevó a cabo para su generación, desde la obtención del conocimiento necesario para generar una propuesta inicial, hasta la creación de una propuesta final validada por un panel de expertos. Se puede observar que el uso del Framework requiere seguir una serie de pasos, en los cuales se deben realizar operaciones matemáticas que podrían dificultar que sea usado de forma fácil y rápida. Para solventar lo anterior, se construyó un prototipo de una herramienta que permitiera utilizar el Framework de forma más cómoda. Éste prototipo de herramienta es una aplicación Web que ha sido pensada para ser usada dentro de empresas de desarrollo de software para seleccionar de forma rápida y sencilla las recomendaciones que entregaría el Framework para las aplicaciones que éstas se vean enfrentadas a desarrollar.

El prototipo de herramienta puede ser descargado desde http://colvin.chillan.ubiobio.cl/mcaro/. Para poder ser utilizado dentro de empresas de desarrollo de software, luego de seguir los pasos presentes en el archivo README.txt que incluye, se debe montar la aplicación dentro de un servidor, para luego poder ser utilizada por medio de la Web.

La Sección 5.1 habla sobre las características generales del prototipo de herramienta, mientras que la Sección 5.2 presenta la base de datos de la aplicación, y la Sección 5.3 entrega las pantallas principales de ésta, para ilustrar su funcionamiento.

5.1 Características Generales del Prototipo de Herramienta

Para la construcción del prototipo de herramienta se trabajó bajo el patrón de diseño Modelo Vista Controlador, apoyado por el Framework Spring, el cual es usado dentro del lenguaje de programación orientado a objetos Java. Además, se utiliza el gestor de base de datos PostgreSQL para almacenar la información necesaria de la aplicación.

El prototipo de herramienta considera dos tipos de usuarios: el licitador de requerimientos o encargado del equipo de desarrollo, el cual es quien hace uso del Framework propiamente tal, seleccionando los esquemas y/o métodos de autenticación para las aplicaciones que se vayan a implementar; y el administrador del Framework, que se encarga de gestionar a otros usuarios y las configuraciones propias del prototipo de herramienta.

Para hacer uso del Framework, el licitador de requerimientos o encargado del equipo de desarrollo debe, como primer paso, especificar las características de la aplicación a desarrollar, seleccionando los niveles de importancia adecuados para cada criterio de Usabilidad, Seguridad y Costos que le presente el prototipo de herramienta. Posteriormente, se le presenta al usuario una lista de contextos de aplicación, donde éste debe seleccionar el que más se acomode a la aplicación a desarrollar. Luego de una pantalla de confirmación, el prototipo de herramienta mostrará a continuación las recomendaciones que entregaría el Framework para las características y el contexto seleccionados. Con el objetivo de fomentar un buen uso del proceso anterior, el prototipo de herramienta le facilita al usuario descripciones de cada criterio y contexto considerados por el Framework.

Como se mencionó anteriormente, la aplicación está pensada para ser usada dentro de empresas de desarrollo de Software, por lo que es deseable que se trabaje en toda la empresa bajo una misma configuración, la cual es definida por el administrador de la aplicación. Si bien el prototipo de herramienta trabaja inicialmente con las configuraciones entregadas por el Framework, podría llegar a ser deseable para la empresa modificar el peso que se le da a los distintos criterios o contextos, ya sea para adaptar la aplicación a las necesidades propias de la empresa, para ajustar las respuestas del Framework ante cambios debido al paso del tiempo, o cualquier otro motivo. El administrador es capaz de modificar estos pesos de modo que sean efectivos para todos los usuarios de la empresa.

El administrador, además, está a cargo de la gestión de usuarios, incluida la creación de usuarios nuevos. El prototipo de herramienta guarda registros de uso del Framework y de modificaciones de pesos, los cuales pueden ser vistos por los usuarios correspondientes.

La Fig. 20 muestra el diagrama de casos de uso de la aplicación, el cual ilustra las funcionalidades que puede realizar cada uno de los usuarios como se describe anteriormente.

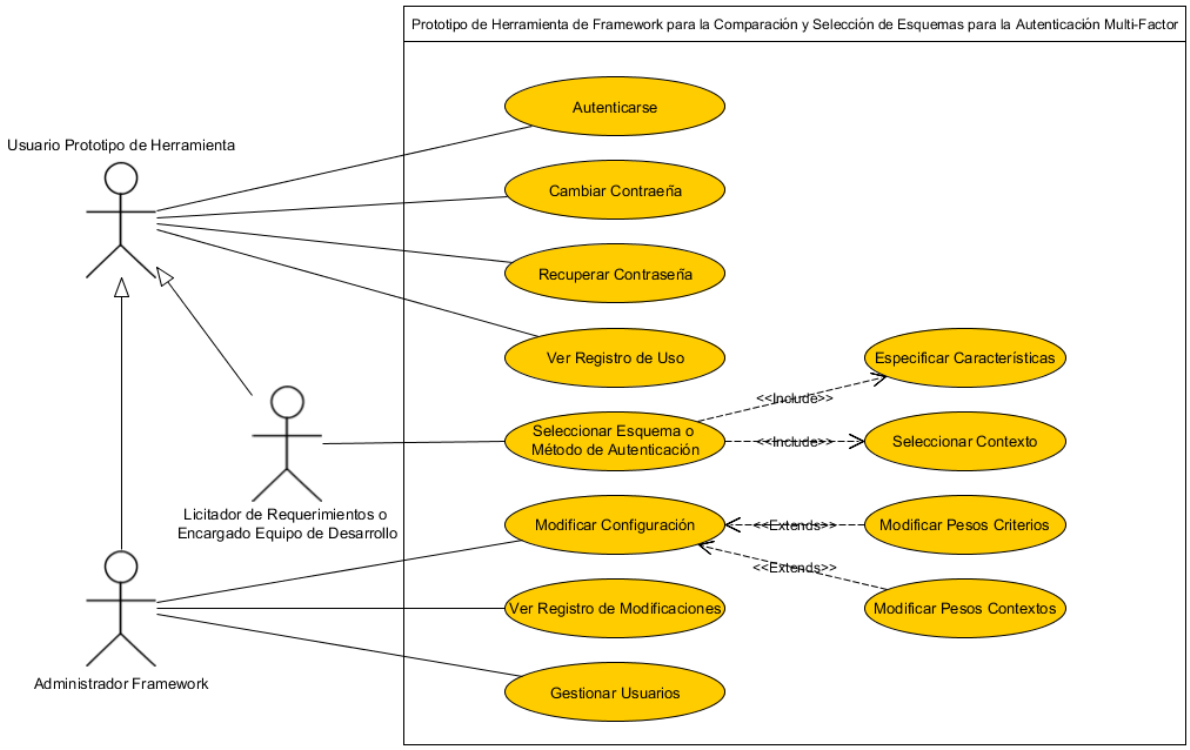


Figura 20. Diagrama de casos de uso del prototipo de herramienta.

5.2 **Base de Datos del Prototipo de Herramienta**

La base de datos del prototipo de herramienta almacena datos relacionados a las configuraciones que se le han dado a la aplicación y a cada uso que se le ha dado para seleccionar algún esquema o método de autenticación para alguna aplicación. Además, se guarda información respecto a los usuarios de la aplicación y a los métodos de autenticación que pueden llegar a ser recomendados. En la Fig. 21 se puede observar el esquema de la base de datos del prototipo de herramienta.

A continuación se describen las entidades más relevantes del prototipo de herramienta:

- **weights_instance (Instancia de Pesos):** Almacena los pesos de cada criterio y contexto con los que trabaja el prototipo de herramienta. Solo puede existir una instancia de pesos activa, lo cual es moderado por una de sus columnas. Se almacena, además, la fecha y el email del usuario que realizó los cambios, junto con una descripción o comentario de éstos, a modo de tener un mayor registro de las modificaciones realizadas.
- **selected_values (Valores Seleccionados):** Almacena los valores que han sido seleccionados para cada uso del Framework por medio del prototipo de herramienta. De igual forma, se almacenan la fecha y el email del usuario que utilizó la aplicación para mantener un registro de uso. Esta entidad referencia a weights_instance para recordar la instancia que estaba activa durante cada uso.

- **app_user (Usuario de la Aplicación):** Almacena la información de los usuarios registrados en el prototipo de herramienta. Los roles de estos usuarios son almacenados separadamente, en la entidad user_role (Rol de Usuario). La información almacenada por cada usuario se limita a su email, su nombre, el estado (activo o inactivo) y su contraseña, la cual se encuentra debidamente encriptada.
- **method (Método):** Almacena la información de cada esquema y método de autenticación recomendado por el Framework para cada caso en particular, registrando toda la información necesaria de estos, como lo son el contexto para el que es recomendado, si es costoso o no, el nivel de seguridad/usabilidad al que pertenece y la cantidad de veces que ha sido recomendado en la academia o en la industria.

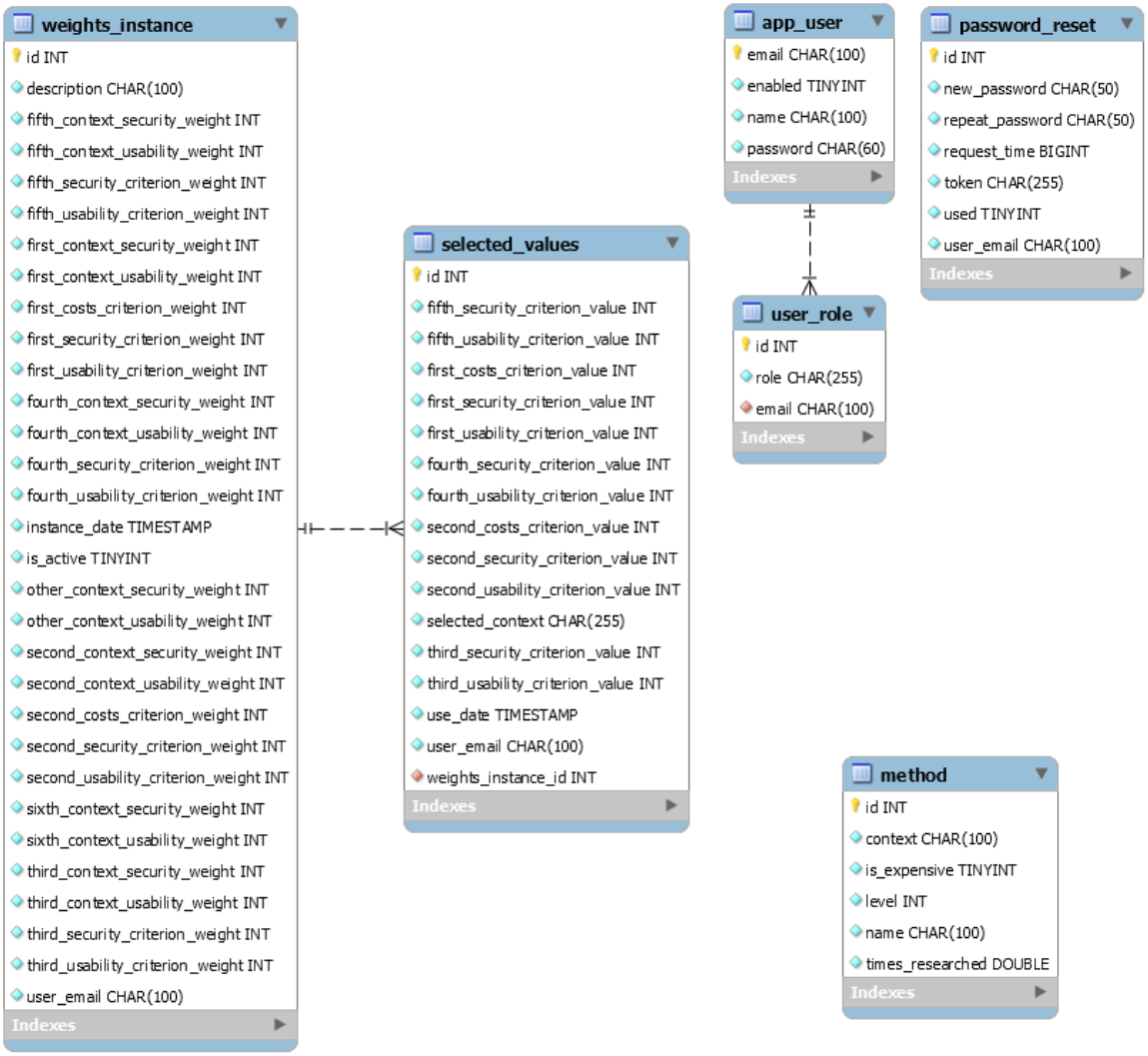


Figura 21. Esquema de la base de datos del prototipo de herramienta.

5.3 **Pantallas Principales del Prototipo de Herramienta**

Se presentan las principales pantallas del prototipo de herramienta, junto a una breve descripción de cada una de las funciones presentadas en éstas.

La Fig. 22 muestra la primera pantalla a la que se accede al momento de seleccionar un esquema o método de autenticación. Como se puede observar, el usuario debe ir marcando los niveles de importancia correspondientes a cada criterio, en base al conocimiento que tenga de los requerimientos de la aplicación a desarrollar. Para una mayor facilidad de uso, los criterios se dividen entre aquellos relacionados a la Usabilidad, aquellos relacionados a la Seguridad y aquellos relacionados a los Costos. El usuario puede seleccionar qué criterios ver en cada momento al presionar los mensajes que aparecen entre el título de la página y la tabla.

Además, si el usuario desliza el puntero sobre los símbolos de pregunta que aparecen al lado de cada criterio, se le proveerá una breve descripción del criterio en cuestión, como se puede observar en la Fig. 23. Esta funcionalidad está presente no solo en la página para definir los criterios, si no que en todas las páginas donde se enlistan criterios y también para los contextos.

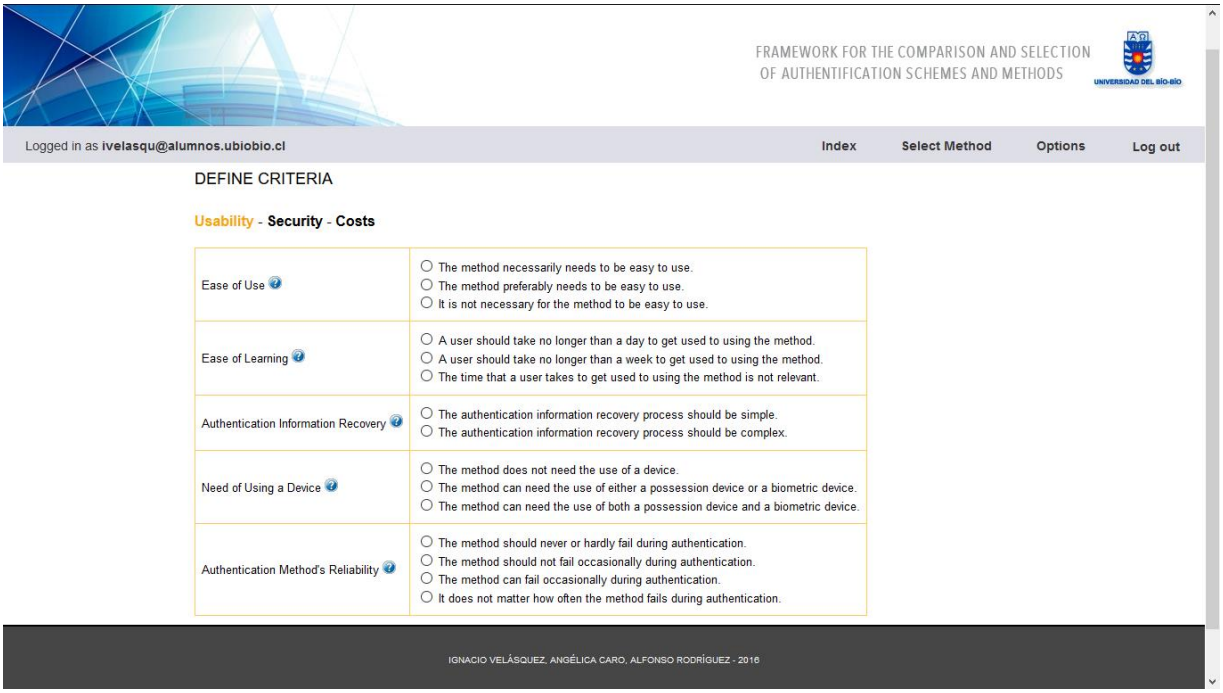


Figura 22. Pantalla de definición de criterios.

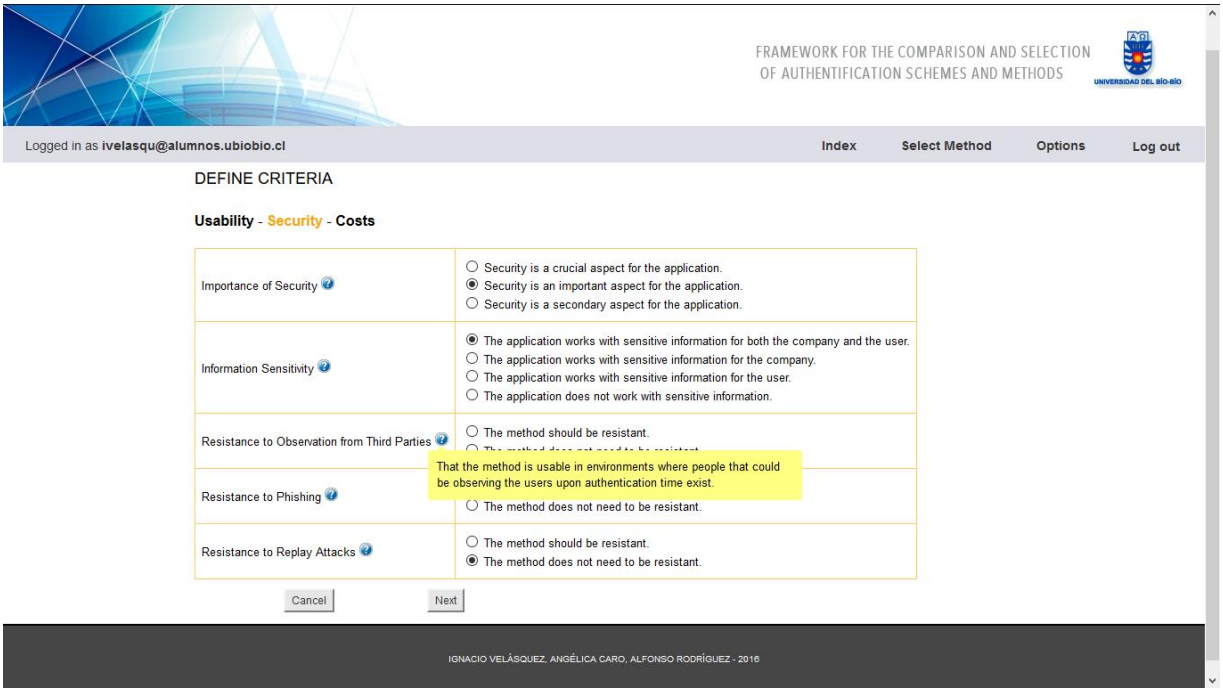


Figura 23. Pantalla con descripción de criterio por el que se deslizó el puntero.

Una vez definidos los criterios de Usabilidad, Seguridad y Costos, el usuario procede a la pantalla de selección de contexto, donde se listan los contextos que considera el Framework, como se aprecia en la Fig. 24. Antes de entregar las recomendaciones para los criterios y contexto seleccionados, el usuario debe pasar por una pantalla de confirmación, como se muestra en la Fig. 25, para luego pasar a la pantalla donde se le recomiendan los esquemas y/o métodos de autenticación a implementar en su aplicación, como se puede observar en la Fig. 26.

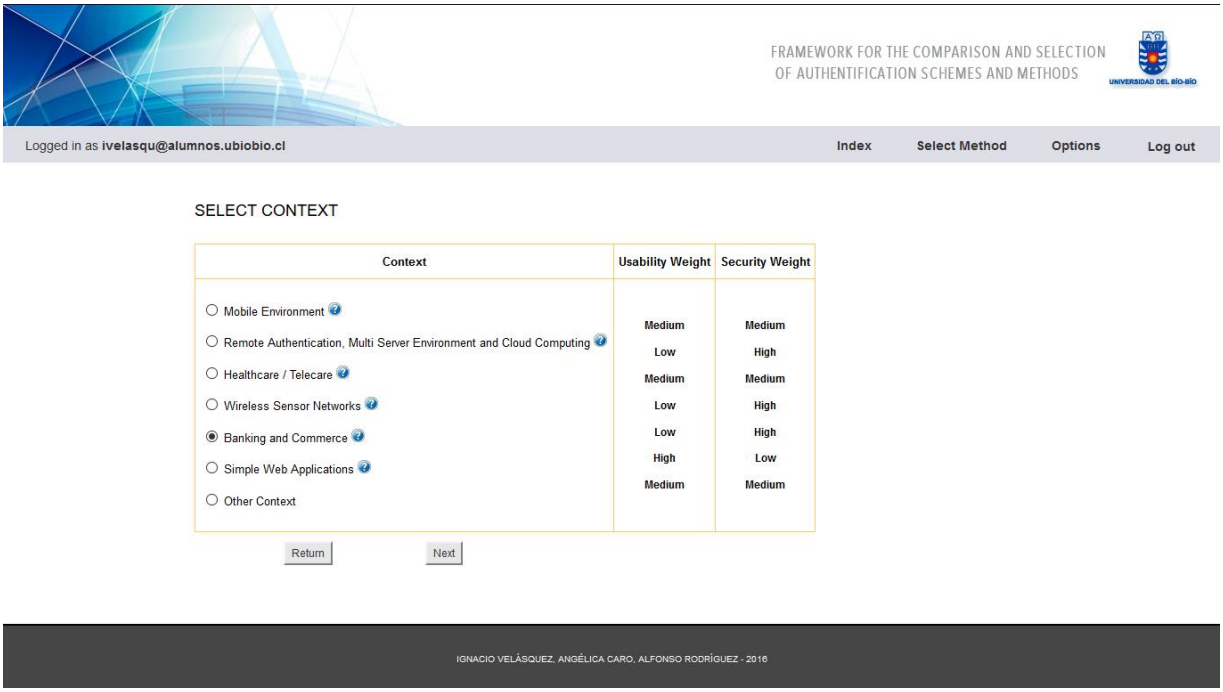


Figura 24. Pantalla de selección de contexto.

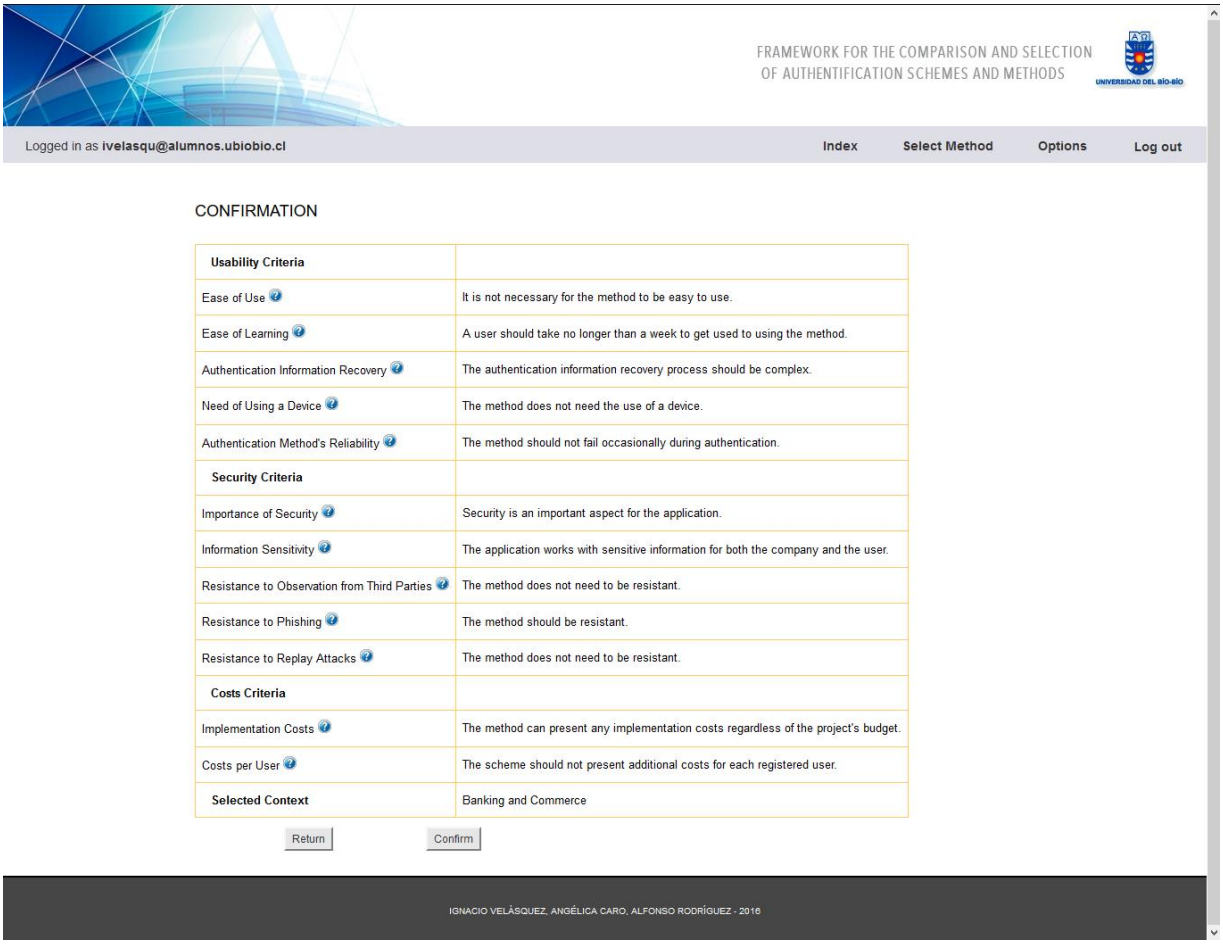


Figura 25. Pantalla de confirmación.

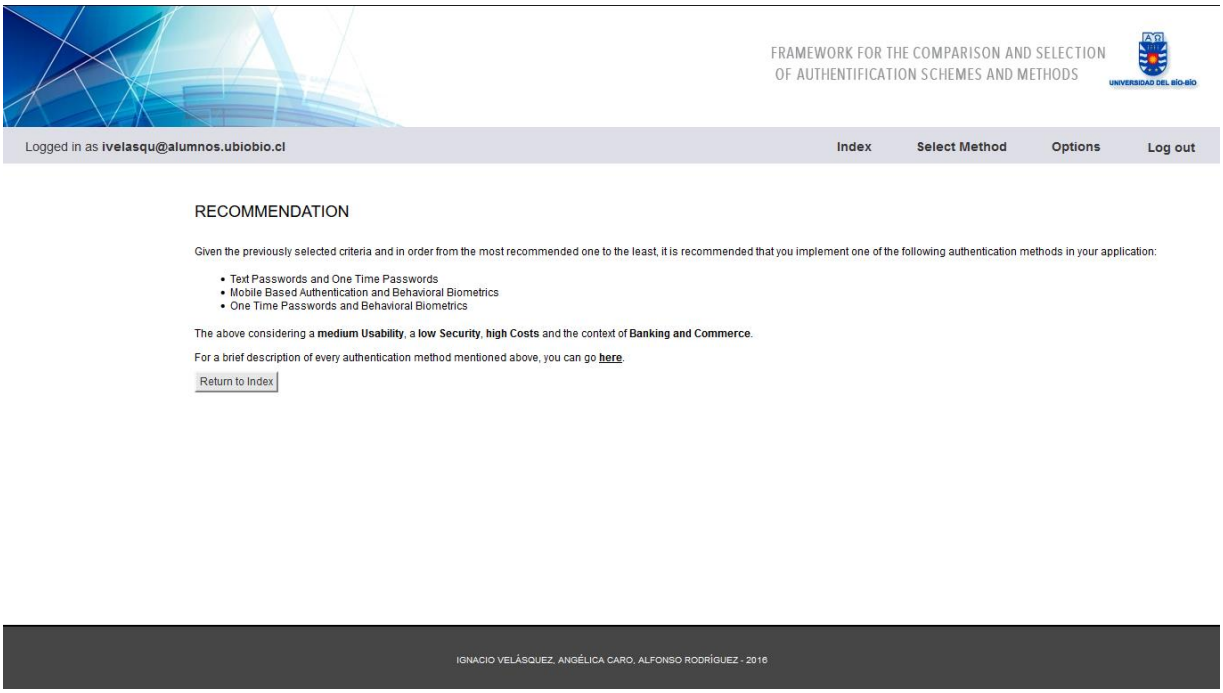


Figura 26. Pantalla de recomendación de esquemas y/o métodos de autenticación.

Por otro lado, en la Fig. 27 se puede observar la pantalla para la modificación de los pesos de los distintos criterios de Usabilidad, Seguridad y Costos y, en la Fig. 28, la pantalla para la modificación de los pesos de Usabilidad y Seguridad de cada contexto. Éstas son opciones disponibles únicamente para el administrador de la aplicación.

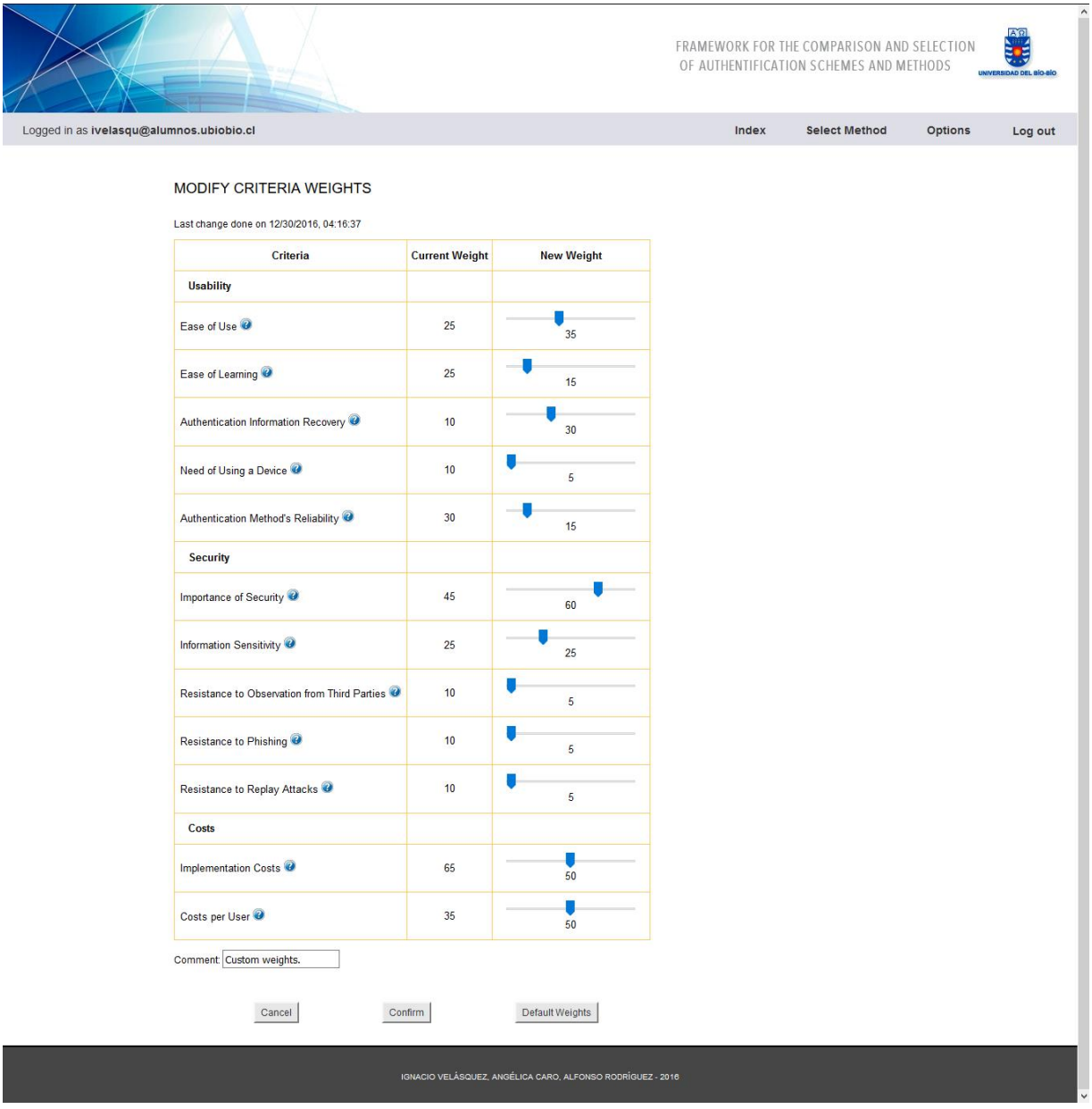


Figura 27. Pantalla para la modificación de los pesos de los distintos criterios.

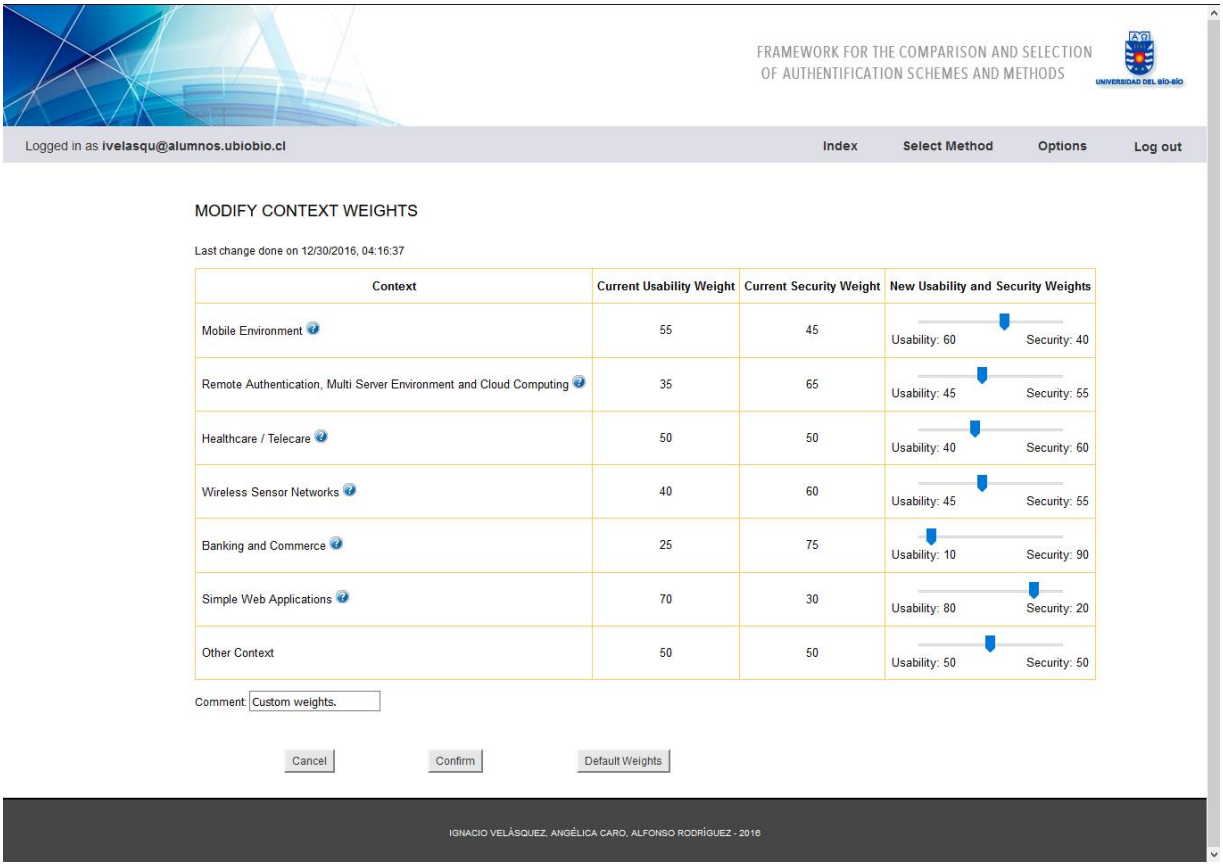


Figura 28. Pantalla para la modificación de los pesos de Usabilidad y Seguridad de cada contexto.

Se debe tener en consideración que las pantallas anteriores podrían no reflejar la apariencia final del prototipo de la herramienta debido a posibles cambios realizados de forma posterior a la captura de éstas. Del mismo modo, solo se presentan las pantallas más importantes, por lo que existen otras funcionalidades generales que no han sido mostradas, como por ejemplo la gestión de usuarios y el inicio y cierre de sesión.

Capítulo 6
Validación por Medio de Casos de Estudio

Una vez definido el Framework para la Comparación y Selección de Esquemas y Métodos de Autenticación y construido el prototipo de la herramienta que permite una fácil utilización de éste, se requiere, a continuación, validar que las recomendaciones que entregará el Framework fueran acordes a la realidad de las aplicaciones. En el presente capítulo se aborda la validación de las respuestas entregadas por el Framework, para lo cual se utilizó una batería de casos de estudio para comparar las respuestas que entrega el Framework, versus las respuestas a las que ya se haya llegado en aplicaciones desarrolladas previamente por expertos de la industria, o las respuestas que entregaría un experto para conjuntos de características predefinidos.

Para la realización de los casos de estudio, se contó con el apoyo de Nisum Technologies, empresa que facilitó la información de proyectos tanto internos de la compañía, como de proyectos para sus clientes externos, desarrollados por expertos de la industria. Se utilizó la técnica para recoger datos de casos de estudio conocida como observaciones para obtener la información relevante para la investigación de cada una de las aplicaciones provistas. Se debe destacar que, en el caso de los proyectos para clientes externos, se contó con el debido resguardo de la privacidad de la información de los clientes de la compañía.

Por otro lado, se generaron cuatro casos de estudio hipotéticos, los cuales fueron aplicados a expertos de Nisum en forma de entrevistas semi-estructuradas, donde se entregaban a los expertos de la industria las características que poseían los casos hipotéticos y, basándose en esas características, se les consultaba qué esquema o método de autenticación implementarían para dicha aplicación. Se entrevistó a diez expertos de la industria, pertenecientes a Nisum Technologies, aplicando cada uno de los cuatro casos de estudio hipotéticos a cada entrevistado, obteniendo un total de 40 respuestas, 10 por cada caso. Cabe destacar que parte de los casos de estudio hipotéticos fueron diseñados basándose en los casos de estudio basados en aplicaciones existentes, y que consideran los casos extremos a los que puede verse enfrentado el Framework.

La Sección 6.1 muestra el detalle de los casos de estudio basados en aplicaciones existentes, mientras que la Sección 6.2 muestra el detalle de aquellos que son hipotéticos. Finalmente, en la Sección 6.3 se realiza una discusión y se entregan las conclusiones respecto a la realización de los casos de estudio.

6.1 **Casos de Estudio Basados en Aplicaciones Existentes**

Como se mencionó anteriormente, para realizar el análisis de aplicaciones existentes implementadas por expertos de la industria, se contó con el apoyo de Nisum Technologies. En total se pudo acceder a la información de cinco aplicaciones implementadas o en proceso de implementación por parte de la compañía. Las Tablas 22-26 presentan la información de cada uno de los casos de estudio basados en aplicaciones reales, donde se indican las características de la aplicación, el contexto para el que fue desarrollada, el esquema o método de autenticación implementado, el o los esquemas o métodos de autenticación recomendados por el Framework para el caso, y las observaciones y análisis de los resultados obtenidos en cada caso de estudio. Se indica, además, si se trata de un proyecto interno de la compañía, o para algún cliente externo.

Tabla 22. Caso de estudio N°1.

Caso de Estudio N°1 (Proyecto Interno)	
Características	La aplicación es para uso interno entre empleados de Nisum y no considera información sensible, pues es usado mayormente para eventos no formales de la compañía. Por ende, la importancia de la **seguridad es baja**, mientras que la **usabilidad tiene un alto valor** y se enfocaron en tener **bajos costos**.
Contexto de la Aplicación	Aplicación Web Común
Esquema o Método Implementado	Inicio de Sesión Único Federado por medio del uso de contraseñas de texto y OTP usando email en un carácter de dos factores.
Esquemas o Métodos Propuestos por el Framework para éste Caso de Estudio, del más al menos Recomendado.	- Contraseñas de Texto - Biométricas de Comportamiento
Análisis de los Resultados	Se entiende que, al ser un proyecto interno y de baja importancia, éste es en parte utilizado por los empleados para practicar y probar tecnologías que sean nuevas para ellos, lo cual puede ser el motivo por el que el método de autenticación implementado no coincide con las recomendaciones del Framework. Además, observando que la seguridad no es importante para esta aplicación, pero que si lo es la usabilidad, el Framework considera que un método de autenticación de dos factores es demasiado complejo para ésta.

Tabla 23. Caso de estudio N°2.

Caso de Estudio N°2 (Proyecto Externo)	
Características	El sistema es usado para mantener información sensible protegida de intrusos no deseados (físicamente). Por ende, la **usabilidad no es tan importante**, pero la **seguridad es relativamente importante**. **No existía mucha preocupación por los costos**.
Contexto de la Aplicación	Otro Contexto
Esquema o Método Implementado	Autenticación de dos factores por medio de contraseñas de texto y tarjetas inteligentes.
Esquemas o Métodos Propuestos por el Framework para éste Caso de Estudio, del más al menos Recomendado.	- Contraseñas de Texto, OTP y Biométricas de Comportamiento - Contraseñas Gráficas, Tarjetas Inteligentes y Biométricas de Comportamiento - Contraseñas Gráficas, OTP y Biométricas de Comportamiento - Contraseñas Gráficas, Basado en Móviles y Biométricas de Comportamiento - Contraseñas Gráficas, OTP y Palma de la Mano o Huellas Dactilares
Análisis de los Resultados	Si bien ninguna de las recomendaciones entregadas por el Framework para este caso calza con el método de autenticación implementado, se están entregando respuestas que contemplan una seguridad aún mayor. Lo anterior, sumado a que la usabilidad no es lo importante dentro de este sistema, indica que las recomendaciones entregadas por el Framework deberían ser las adecuadas para el sistema de todas maneras.

Tabla 24. Caso de estudio N°3.

Caso de Estudio N°3 (Proyecto Interno)	
Características	La aplicación es usada para generar reportes para la compañía, estos reportes contienen información sensible. Al mismo tiempo, esta aplicación será usada por gente que no son expertos en computación, por lo que existe la necesidad de que sea tan usable como sea posible. Por ende, tanto la **usabilidad como la seguridad son importantes** para esta aplicación. Además, el presupuesto para este proyecto es muy reducido, por lo que los **costos deben ser tan bajos** como sea posible.
Contexto de la Aplicación	Otro Contexto
Esquema o Método Implementado	Inicio de Sesión Único Federado usando contraseñas de texto (No se encuentra implementado aun y no es una decisión final).
Esquemas o Métodos Propuestos por el Framework para éste Caso de Estudio, del más al menos Recomendado.	- Contraseñas de Texto y Tarjetas Inteligentes - Contraseñas Gráficas y Biométricas de Comportamiento - Contraseñas de Texto y Basado en Móviles
Análisis de los Resultados	Se entiende que últimamente se estaban barajando las opciones disponibles para implementar la autenticación en la aplicación, sin embargo, se le solicitó al equipo de desarrollo tener otras funcionalidades listas para una fecha pronta, por lo que dejaron el tema de la autenticación de lado para enfocarse en las funcionalidades que se les solicitaban. Debido a ello, el esquema a implementar fácilmente podría ser reconsiderado por el equipo de desarrollo de aquí al momento de su implementación, por lo que, para este caso, no se tiene un esquema o método para comparar las recomendaciones del Framework adecuadamente.

Tabla 25. Caso de estudio N°4.

Caso de Estudio N°4 (Proyecto Externo)	
Características	La aplicación funciona como un punto de venta y trabaja con información comercial sensible, por lo que su **seguridad debe ser alta**. Por otro lado, la aplicación debe poder ser usada rápidamente por los vendedores cuando interactúan con los clientes, por lo que la **usabilidad es de la mayor importancia** también. Pese a que existe un alto presupuesto para el desarrollo de la aplicación, no mucho de éste es para ser usado para temas de autenticación, por lo que los **costos deben mantenerse bajos**.
Contexto de la Aplicación	Banca y Comercio
Esquema o Método Implementado	Autenticación de dos factores basada en la posesión de un dispositivo móvil y contraseñas de texto.
Esquemas o Métodos Propuestos por el Framework para éste Caso de Estudio, del más al menos Recomendado.	- Contraseñas de Texto y Basado en Móviles - Contraseñas de Texto y Tarjetas Inteligentes
Análisis de los Resultados	En este caso, el método de autenticación implementado en la aplicación coincide con aquel que es más recomendado por el Framework para los criterios y el contexto identificados.

Tabla 26. Caso de estudio N°5.

Caso de Estudio N°5 (Proyecto Externo)	
Características	La aplicación permite a los usuarios mantener registros de información relacionada a ellos. La información es privada, pero no sensible, por lo que la **seguridad no es tan importante**. La **usabilidad debería ser importante**, pero el cliente no está dispuesto a invertir en cosas que podrían cambiar sus políticas, por lo que los **costos deben ser muy bajos**.
Contexto de la Aplicación	Otro Contexto
Esquema o Método Implementado	Posesión de un OTP que no cambia a lo largo del tiempo.
Esquemas o Métodos Propuestos por el Framework para éste Caso de Estudio, del más al menos Recomendado.	- Biométricas de Comportamiento - Contraseñas de Texto - Contraseñas Gráficas
Análisis de los Resultados	Se entiende que el OTP utilizado es un identificador enviado al correo de los usuarios, el cual es usado para muchas actividades dentro de la compañía del cliente, por lo que no es posible cambiarlo fácilmente. Debido a lo anterior, el equipo de desarrollo no tuvo poder de decisión respecto al esquema o método de autenticación a implementar, por lo que no es posible comparar adecuadamente la recomendación entregada por el Framework con el esquema que se encuentra implementado.

6.2 Casos de Estudio Hipotéticos

En esta ocasión, se trabajó con diez expertos de Nisum Technologies, la totalidad de ellos teniendo el rol de Desarrollador, con distintos niveles de experiencia, los cuales pueden ser vistos en la Fig. 29. Por otro lado, la mayoría de éstos desarrolladores tiene entre 6 y 10 años de experiencia, como se puede observar en la Fig. 30.

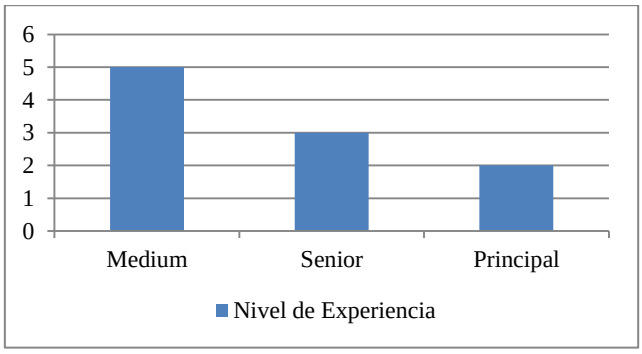


Figura 29. Experiencia de los encuestados en relación a su posición en Nisum Technologies.

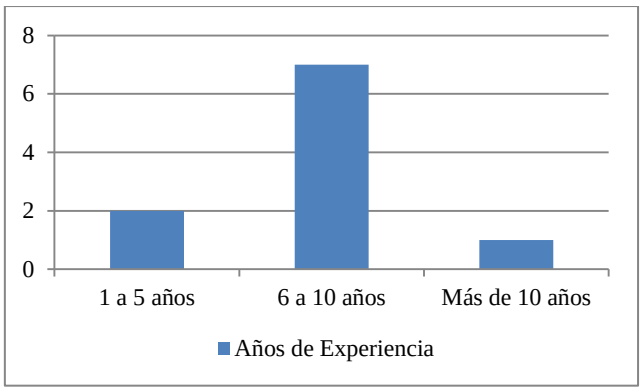


Figura 30. Años de experiencia en Nisum Technologies de los encuestados.

6.2.1 **Caso de Estudio 1: Alta Usabilidad, Baja Seguridad y Presupuesto Limitado**

Para el primer caso de estudio, se consideró un caso hipotético en el cual la usabilidad fuera un aspecto crucial de la aplicación. Por otro lado, la seguridad se consideró un aspecto menos importante, indicando que la información con la que trabajaría la aplicación no sería sensible. Además, como caso base se consideró un presupuesto limitado para implementar la aplicación, y que ésta pertenecería al contexto de aplicaciones Web comunes. Bajo estas circunstancias iniciales, se le consultó a los entrevistados sobre qué esquema o método de autenticación implementarían para este caso. La totalidad de los entrevistados respondió, al menos como una de sus opciones, que implementarían contraseñas de texto, el cual es uno de los esquemas considerados por el Framework bajo estas características.

Como primer variante de este problema, se modificó únicamente la variable de costos, considerando ahora que no se tenía un límite de presupuesto, y se volvió a consultar a los entrevistados sobre qué esquema o método de autenticación implementarían. Nuevamente, la mayoría de los entrevistados contestó que implementarían contraseñas de texto, a excepción de uno, que contestó que al no tener límites de costos implementaría algún tipo de biométricas, lo cual se alinea a la respuesta que entregaría el Framework.

Posteriormente, se le consultó a los entrevistados sobre qué implementarían en una aplicación con las mismas características anteriores, pero esta vez considerando que el contexto es un ambiente móvil. Si bien nuevamente la mayoría de las respuestas fue que utilizarían contraseñas de texto, algunos indicaron que implementarían otros esquemas de autenticación, tales como contraseñas gráficas, autenticación basada en móviles o algún tipo de biométricas.

Luego, se le indicó a los entrevistados que la recomendación entregada por el Framework para el caso original (vale decir, alta usabilidad, baja seguridad y costos limitados para una aplicación Web común) era el utilizar contraseñas de texto como primera opción, que es la respuesta que todos entregaron, y biométricas de comportamiento como una segunda opción. Ante esta segunda opción, el 60% de los entrevistados indicó que no estaba de acuerdo con ello, sin embargo, durante la realización de las entrevistas se pudo notar que una gran cantidad de los entrevistados, aun con la explicación inicial que se les dio de cada esquema de autenticación considerado por el Framework, no tenía suficientemente claro de que trataban las biométricas de comportamiento, por lo que a la segunda mitad de entrevistados se les realizó un mayor entrenamiento en cuanto a qué trataban éstas, pudiéndose notar una considerable alza en cuanto a la recepción de estas como un posible esquema para el problema en cuestión. La Fig. 31 ilustra esta situación.

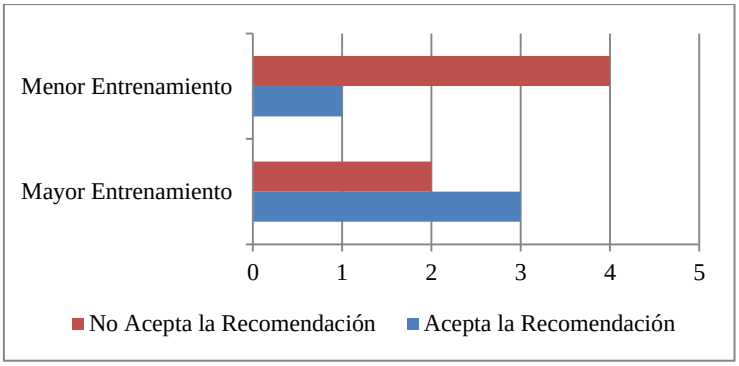


Figura 31. Comparación de respuestas entre entrevistados ante distintos niveles de conocimiento entregado.

Este caso hipotético posee considerables similitudes con el primer caso de estudio basado en aplicaciones existentes (ver Tabla 22), por lo que, a modo de cierre, se le consultó a los entrevistados si considerarían implementar el método de autenticación de dos factores implementado para ese caso, el cual consiste en el uso de contraseñas de texto y una contraseña de uso único por medio del correo electrónico, sin que estos tuvieran conocimiento de que éste se encontraba implementado en una aplicación real. El 80% de los entrevistados indicó que no consideraría implementar dicho método, pues afectaría negativamente a la usabilidad de la aplicación, que es lo que mayor importancia tiene en este caso. La respuesta general de los entrevistados se alinea con la recomendación que entregaría el Framework, pues éste tampoco considera adecuado el uso de un método de dos factores en una aplicación con las características entregadas.

6.2.2 Caso de Estudio 2: Baja Usabilidad, Alta Seguridad y Presupuesto Ilimitado

En el segundo caso de estudio, se invirtieron los criterios a considerar. Aquí, la seguridad pasa a tener un rol principal, pues se considera que se está trabajando con información sensible dentro de una aplicación bancaria. De este modo, la usabilidad pasa a tener una importancia secundaria. Por otro lado, se considera inicialmente que no existen límites de presupuesto. Ante estas características, un 50% de los entrevistados indicó que implementaría un método de autenticación de dos factores, mientras que el otro 50% dijo que implementaría uno de tres factores. El segundo grupo coincide con la respuesta del Framework, el cual considera la implementación de un método de tres factores para este caso.

Al plantear el mismo caso, pero considerando que se tiene un presupuesto limitado, el 80% de los entrevistados indicó que solo implementaría un método de autenticación de dos factores. Además, un entrevistado dijo que no tomaría el proyecto, pues se estaría corriendo un riesgo al implementar una aplicación que requiriera tanta seguridad teniendo un presupuesto limitado. El décimo entrevistado mantuvo su respuesta de implementar un método de autenticación de tres factores, comentando que para este tipo de aplicación el presupuesto no es transable para el tema de la autenticación, y que debería ser limitado en otros aspectos de la aplicación.

Se consultó a los entrevistados sobre qué implementarían para una aplicación de similares características, pero orientada para el área de la salud. La mayoría consideró que la información sensible dentro de un contexto bancario era más importante que aquella dentro de un contexto médico, por lo que, en lo general, entregaron respuestas más flexibles que aquellas entregadas para la aplicación bancaria. Lo anterior puede ser denotado de cierta forma en los pesos que le da el Framework a la usabilidad y a la seguridad, donde el contexto banca y comercio tienen el peso más alto para la seguridad.

Finalmente, se le indicó a los entrevistados que las recomendaciones que entregaría el Framework para una aplicación bancaria con las características entregadas originalmente (baja usabilidad, alta

seguridad y sin límites de presupuesto) consistirían en métodos de autenticación de tres factores, que utilizarían contraseñas de texto o gráficas para el factor de conocimiento, OTP o tarjetas inteligentes para el factor de posesión, y biométricas de comportamiento para el factor de inherencia. La totalidad de los entrevistados indicó que las recomendaciones entregadas por el Framework son correctas, algunos incluso mencionando que la respuesta de éste era mejor que la de ellos, pues consideraba aún más seguridad.

6.2.3 **Caso de Estudio 3: Alta Usabilidad, Alta Seguridad y Presupuesto Limitado**

Este caso hipotético está basado en el tercer caso de estudio basado en aplicaciones existentes (ver Tabla 24), donde se considera el caso extremo de que el cliente quiera tanto una alta seguridad como una alta usabilidad y a un bajo costo, para una aplicación encargada de la generación de reportes. Si bien un 40% de los entrevistados indicó que con el uso de contraseñas de texto o gráficas era suficiente, el otro 60% entregó como respuesta el uso de métodos de autenticación de dos factores, lo cual se alinea con la respuesta que entregaría el Framework.

Para el mismo problema, pero considerando que no existen limitantes de presupuesto, el 80% de los entrevistados mencionó que implementaría un método de autenticación de dos factores, mientras que uno de los entrevistados restantes dijo que igualmente implementaría un esquema de autenticación y el otro que implementaría un método de autenticación de tres factores.

El 90% de los encuestados mencionó estar de acuerdo o parcialmente de acuerdo con las recomendaciones de dos factores entregadas por el Framework para el problema, considerando que sí existen limitantes de presupuesto. Las recomendaciones entregadas por el Framework son, en concreto, la combinación de contraseñas de texto y tarjetas inteligentes, la combinación de contraseñas gráficas y biométricas de comportamiento, y la combinación de contraseñas de texto y autenticación basada en móviles. Para la mayoría de aquellos que no estaban completamente de acuerdo, nuevamente se puede atribuir esto a la falta de conocimiento o de experiencia que tenían respecto al uso de biométricas de comportamiento, las cuales son consideradas como parte de una de las combinaciones de factores entregadas como respuesta por el Framework para este caso.

Finalizando con este caso, se le consultó a los entrevistados si considerarían implementar el esquema de autenticación que se está considerando implementar en el problema original del caso de estudio basado en aplicaciones, nuevamente sin darles a conocer sobre la existencia de tal aplicación. Solo el 40% de los entrevistados consideraría implementar solo contraseñas de texto para este problema, mientras que el 60% restante considera esta solución como insuficiente en cuanto a seguridad.

6.2.4 **Caso de Estudio 4: Baja Usabilidad y Baja Seguridad**

Para el último caso hipotético se decidió considerar un caso extremo que podría llegar o no a darse en la realidad, el cual consiste en que el cliente no le de importancia ni a la seguridad, ni a la usabilidad, ni a los costos. Dando como única información adicional, en este caso, que la aplicación está pensada para ser implementada en un ambiente de la nube. Ante tan vagas características, el 90% de los entrevistados indicó que tan solo implementarían contraseñas de texto, debido a que no se ve que al cliente le importe la seguridad, por lo que ellos optarían por valorar la usabilidad. El décimo entrevistado comentó que simplemente no implementaría un esquema o método de autenticación, pues lo consideraría innecesario.

Al consultarles si considerarían implementar un método de autenticación de dos factores, el 50% de los entrevistados dijo que no lo considerarían, mientras que solo un 20% indicó que sí. El 30% restante

mencionó que tal vez lo considerarían, pero tendrían que tener un mayor conocimiento de la aplicación a desarrollar.

Pese a lo anterior, al comentarle a los entrevistados que la recomendación que entregaría el Framework sería una que no considerara tan importante la seguridad ni la usabilidad, sino más bien una que estuviera en el medio, vale decir, de dos factores (y sin entrar en detalle en cuanto a las recomendaciones concretas que entregaría), el 60% de éstos indicó que encontraba la respuesta del Framework acorde al problema, el 20% dijo que estaba parcialmente de acuerdo, nuevamente argumentando que se requería mayor información, y solo un 20% se mantuvo en total desacuerdo respecto a la respuesta que entregaría el Framework.

6.3 **Discusión y Conclusiones**

A modo de sintetizar la información anterior, la relación entre los casos de estudio basados en aplicaciones reales y los casos de estudio hipotéticos basados en éstos puede ser observada en las Tablas 27, 28 y 29. En la tabla 27 se presentan los casos de estudios basados en aplicaciones existentes, mostrando, para cada uno, el esquema o método implementado en la aplicación existente y el esquema o método más recomendado por el Framework. En la tabla 28 se presentan los casos de estudio hipotéticos, mostrando, para cada uno, el esquema o método más recomendado por expertos de la industria, el esquema o método más recomendado por el Framework y el porcentaje de aceptación de la recomendación del Framework por parte de los expertos de la industria. La Tabla 29 vuelve a presentar los casos de estudio basados en aplicaciones existentes y los casos de estudio hipotéticos que poseen una relación entre ellos, mostrando, para cada pareja de caso de estudio basado en aplicación existente y caso de estudio hipotético, cada una de las columnas descritas para las tablas 27 y 28.

Tabla 27. Casos de estudio basados en aplicaciones existentes.

Casos de Estudio Involucrados	Esquema o Método Implementado	Esquema o Método más Recomendado por el Framework
Caso de Estudio Basado en Aplicación Existente 1	Autenticación de dos factores (Contraseñas de Texto + OTP)	Contraseñas de Texto
Caso de Estudio Basado en Aplicación Existente 2	Autenticación de dos factores (Contraseñas de Texto + Tarjetas Inteligentes)	Autenticación de tres factores (Contraseñas de Texto + OTP + Biométricas de Comportamiento)
Caso de Estudio Basado en Aplicación Existente 3	Contraseñas de Texto	Autenticación de dos factores (Contraseñas de Texto + Tarjetas Inteligentes)
Caso de Estudio Basado en Aplicación Existente 4	Autenticación de dos factores (Contraseñas de Texto + Basado en Móviles)	Autenticación de dos factores (Contraseñas de Texto + Basado en Móviles)
Caso de Estudio Basado en Aplicación Existente 5	OTP (Impuesto por el cliente)	Biométricas de Comportamiento

Tabla 28. Casos de estudio hipotéticos.

Casos de Estudio Involucrados	Esquema o Método más Recomendado por Expertos	Esquema o Método más Recomendado por el Framework	Porcentaje de Aceptación de la Recomendación del Framework
Caso de Estudio Hipotético 1	Contraseñas de Texto	Contraseñas de Texto	100%
Caso de Estudio Hipotético 2	Autenticación de dos o tres factores	Autenticación de tres factores	100%
Caso de Estudio Hipotético 3	Autenticación de dos factores	Autenticación de dos factores (Contraseñas de Texto + Tarjetas Inteligentes)	90%
Caso de Estudio Hipotético 4	Contraseñas de Texto	Autenticación de dos factores	80%

Tabla 29. Casos de estudio basados en aplicaciones existentes con una contraparte hipotética.

Casos de Estudio Involucrados	Esquema o Método Implementado	Esquema o Método más Recomendado por Expertos	Esquema o Método más Recomendado por el Framework	Porcentaje de Aceptación de la Recomendación del Framework
Caso de Estudio Basado en Aplicación Existente 1 **Caso de Estudio Hipotético 1**	Autenticación de dos factores (Contraseñas de Texto + OTP)	Contraseñas de Texto	Contraseñas de Texto	100%
Caso de Estudio Basado en Aplicación Existente 3 **Caso de Estudio Hipotético 3**	Contraseñas de Texto	Autenticación de dos factores	Autenticación de dos factores (Contraseñas de Texto + Tarjetas Inteligentes)	90%

Se puede observar que las recomendaciones entregadas por el Framework son, en lo general, acordes a las recomendaciones que haría un experto de la industria para similares problemas. Del mismo modo, si bien el Framework entregó una respuesta distinta para un 80% de los casos de estudio basados en aplicaciones existentes, se puede notar que para estos casos, o la recomendación entregada por el Framework se acercaba suficientemente al método de autenticación implementado y/u ofrecía un mayor nivel de seguridad, o existía un motivo que podría explicar la incongruencia en cuanto a las respuestas, como lo es, por ejemplo, la existencia de alguna política interna de la compañía para la que es desarrollada la aplicación.

Para los casos de estudio hipotéticos, se puede notar que las mayores discrepancias están en el primer y cuarto casos hipotéticos. Para el primero, muchos de los entrevistados consideran que las biométricas de comportamiento no son adecuadas para el problema que se está considerando. Lo anterior se puede atribuir, en parte, a que por medio de la realización de las entrevistas, se pudo notar que la mayoría de los entrevistados no tiene un alto conocimiento o experiencia respecto a este tipo de biométricas y, como se menciona anteriormente, al explicarles con un mayor detalle de que tratan éstas, las respuestas de varios de éstos cambiaron favorablemente a considerar las biométricas de comportamiento como una solución viable para el problema.

En relación al cuarto caso hipotético, si bien ninguno de los entrevistados consideró usar autenticación de dos factores para el problema planteado, la mayor parte de éstos terminó considerando adecuada la recomendación que entregó el Framework. Esto es en parte debido a que, a diferencia de los desarrolladores encargados de implementar el esquema o método de autenticación, quienes pueden

ser capaces de adquirir mayor información respecto al problema que se está tratando, el Framework debe entregar una respuesta exacta basándose solamente en el conocimiento que se le entrega inicialmente como información de entrada.

Al consultarle a los entrevistados si implementarían los esquemas o métodos de autenticación implementados o considerados para implementación dentro de las aplicaciones existentes, éstos contestaron principalmente que no, lo cual se alinea con las recomendaciones que haría el Framework para esos casos, pues no considera recomendable el esquema o método de autenticación implementado o considerado para implementación.

Finalmente, se puede notar, a través de las respuestas tanto de los casos de estudio basados en aplicaciones como de aquellos basados en conocimiento de expertos, que las contraseñas de texto son el esquema de autenticación más recomendado por expertos de la industria por un alto margen. Esto hace sentido al ver que dicho esquema de autenticación es el más implementado dentro de la industria. Aquí se puede notar una de las mayores utilidades que puede entregar el Framework, pues un desarrollador normalmente opta por utilizar el esquema de autenticación que mejor conoce, sin realizar un proceso de comparación y selección para elegir el método de autenticación que realmente sería el más adecuado para su aplicación. Este proceso es el que este Framework busca apoyar, para así facilitar la toma de decisiones de los desarrolladores que se vean enfrentados a la necesidad de implementar un esquema o método de autenticación en su aplicación.

Capítulo 7
Conclusiones

7.1 **Análisis de los Objetivos Propuestos/Cumplidos**

Por medio de la presente investigación se buscó cubrir una brecha existente en la literatura, la cual es la falta de un método adecuado para la comparación y selección de esquemas de autenticación y métodos de autenticación multi-factor.

Producto de la investigación, se presenta el Framework para la Comparación y Selección de Esquemas y Métodos de Autenticación, el cual cubre las falencias existentes en los Framework de decisión existentes para el ámbito de la autenticación, con énfasis en la autenticación multi-factor.

El objetivo principal de la investigación fue el de "desarrollar un estudio de los esquemas de autenticación y métodos multi-factor propuestos en la literatura, describir sus características e identificar criterios de selección propuestos tanto en la academia como en la industria, tales como usabilidad, factibilidad de implementación, contexto de la aplicación, etc. En base a este material, proponer un Framework que permita hacer la selección de los métodos de autenticación multi-factor más apropiados para un determinado contexto de desarrollo y operación de una aplicación Software". Para el cumplimiento de lo anterior, se buscó cumplir con un conjunto de objetivos específicos. A continuación se presenta un análisis del cumplimiento de cada uno de estos.

Objetivo 1, 2. *Realizar una revisión de la literatura con el propósito de conocer los principales esquemas de autenticación y métodos multi-factor utilizados en soluciones de aplicaciones Software. Recopilar criterios de selección y diferenciación de los métodos de autenticación multi-factor, tanto aquellos presentes en la literatura, como aquellos utilizados en la industria.*

Se realizó una revisión sistemática de la literatura para conocer los principales esquemas y métodos de autenticación, la cual permitió encontrar 982 artículos, de los cuales 515 daban a conocer distintos esquemas de autenticación y 442 daban a conocer métodos de autenticación multi-factor. Además, 17 artículos encontrados permitieron discernir los criterios de comparación y selección de esquemas y métodos de autenticación más usados en la literatura. Finalmente, se encontraron 8 artículos que reportaban la existencia de Framework de decisión para esquemas y métodos de autenticación, cuyo análisis demostró la falta de un Framework que fuera capaz de cubrir tanto la autenticación de un factor como la autenticación multi-factor considerando un número adecuado de criterios que permitieran realizar una adecuada toma de decisiones.

En cuanto a la experiencia de la industria, ésta fue adquirida por medio de la realización de encuestas y entrevistas, con el apoyo de los expertos de Nisum Technologies. En total se entrevistó a 12 y se encuestó a 45 expertos pertenecientes a dicha empresa, los cuales compartieron su conocimiento y experiencias en cuanto a esquemas y métodos de autenticación, junto con los criterios que consideraban al momento de comparar y seleccionar esquemas y métodos de autenticación para las aplicaciones que debían desarrollar.

De este modo, se logró identificar los múltiples esquemas y métodos de autenticación existentes, junto con los criterios comúnmente utilizados para su comparación y selección, tanto por medio del conocimiento de la academia como de la experiencia de expertos de la industria.

Objetivo 3. *Crear un Framework que provea una guía para la comparación y selección de esquemas y métodos de autenticación multi-factor, basándose en las experiencias reportadas en la literatura y la industria.*

Basándose en el conocimiento adquirido por medio de la revisión sistemática de la literatura, junto con las experiencias obtenidas de expertos de la industria, se formuló una propuesta inicial de un Framework de decisión de esquemas y métodos de autenticación. Posteriormente, esta propuesta se validó por medio de la realización de un panel de expertos junto a expertos de Nisum Technologies. De acuerdo a la realimentación obtenida, se generó una propuesta de Framework más robusta, la cual, para

guiar en la comparación y selección de qué esquema o método de autenticación utilizar en cada aplicación, basa sus recomendaciones en los criterios más usados encontrados en la literatura, los cuales son la Usabilidad, la Seguridad y los Costos, además del contexto para el que va dirigida la aplicación.

Objetivo 4. *Construir un prototipo de herramienta que permita la utilización del Framework en diferentes contextos de desarrollo y operación de una aplicación Software.*

Para hacer un mejor uso del Framework, se construyó un prototipo de herramienta que facilitara la utilización de éste. El prototipo de herramienta permite una fácil valoración de los criterios considerados por el Framework y del contexto para el que va dirigida la aplicación para la cual se está seleccionando un esquema o método, para luego entregar las recomendaciones que daría el Framework dada la información entregada.

El prototipo de herramienta se construyó pensando su uso dentro de empresas de desarrollo de Software, permitiendo que este sea configurado para satisfacer de mejor manera las necesidades de cada empresa.

Objetivo 5. *Demostrar la validez de la propuesta, junto con la utilidad del prototipo de herramienta, por medio de casos de estudio.*

Se demostró la validez del Framework creado a través de la realización de casos de estudio, los cuales fueron realizados con el apoyo de Nisum Technologies. La empresa facilitó la información de aplicaciones desarrolladas, o en proceso de desarrollo, para comparar los esquemas o métodos implementados en dichas aplicaciones y aquellos que el Framework hubiera recomendado para la misma aplicación. Del mismo modo, se generaron casos de estudio hipotéticos que fueron aplicados a expertos de la industria pertenecientes a Nisum Technologies, donde se les consultó sobre qué esquema o método de autenticación implementarían para cada caso, comparando sus respuestas nuevamente con aquellas que entregaba el Framework.

7.2 Principal Aporte

El principal aporte de esta investigación es la creación de un Framework de recomendación que permite a los desarrolladores de Software realizar una adecuada comparación y selección, tanto de esquemas de autenticación como de métodos de autenticación multi-factor, a la hora de seleccionar qué esquema o método implementar al momento de desarrollar aplicaciones. Este Framework ha sido creado basándose tanto en el conocimiento adquirido por parte de la academia, como en la experiencia reportada por expertos de la industria, los cuales ayudaron, además, a una adecuada validación del Framework, tanto en cuanto a su forma, como a las respuestas que éste entrega.

Esta experiencia de expertos en la industria ha sido obtenida gracias a la colaboración recibida por la empresa de desarrollo de Software Nisum Technologies, con la cual se trabajó en conjunto durante la realización de esta investigación. Producto de esta colaboración, además, se generó un White Paper para compartir los resultados de esta investigación con la gente de la industria.

Finalmente, se destaca la importancia de la revisión sistemática de la literatura desarrollada, la cual permitió obtener una visión de cómo ha sido abordada anteriormente la temática tratada durante esta investigación.

7.3 Trabajos Futuros

Existe una cantidad de tareas que podrían ser realizadas a modo de trabajo futuro, con el objetivo de complementar los resultados obtenidos por medio de la realización de esta investigación, las cuales son listadas a continuación:

- Se puede observar que el funcionamiento del Framework presenta una gran similitud a un sistema de recomendación. Al mismo tiempo, es deseable que las respuestas que entrega el Framework pudieran ir actualizándose según los cambios que puedan ir surgiendo en cuanto a tendencias o descubrimientos sobre autenticación del futuro. Debido a lo anterior, se podría adaptar el Framework para que funcione de forma similar a un sistema de recomendación, los cuales normalmente tienen la cualidad de que las respuestas que entregan se van adaptando según el uso que les dan los usuarios a lo largo del tiempo, para ir entregando respuestas cada vez más precisas.
- Desde un punto de vista orientado a la industria, sería útil que el Framework propusiera, además del esquema o método a implementar, implementaciones propiamente tales de cada esquema o método de autenticación que recomienda, en distintos lenguajes de programación, a modo de facilitar aún más el trabajo de los desarrolladores de Software.
- Se podría tratar de expandir, además, el tema que abarca el Framework, que es la autenticación, incorporando aspectos relacionados a autorización u otras temáticas relacionadas a la seguridad de las aplicaciones.
- Es posible profundizar en cuanto a la validación del Framework, trabajando con otras empresas que se enfoquen en contextos diferentes a los que se orienta Nisum Technologies. Esto permitiría realizar nuevos casos de estudio e incluso expandir, quizás, los contextos que actualmente cubre el Framework.
- Refinar el prototipo de herramienta, para obtener un producto de Software final del Framework.

7.4 Contraste de Resultados

Se participó en el V Encuentro de Investigaciones de Estudiantes de Postgrado, realizado por la Universidad del Bío-Bío durante el año 2016, donde se presentaron los resultados obtenidos por medio de la revisión sistemática de la literatura y se dieron las primeras nociones que se tenían respecto al Framework a desarrollar. Lo anterior por medio de una exposición en modalidad oral.

Se redactó un artículo detallando la realización de la RSL y los hallazgos obtenidos por medio de esta. Dicho artículo fue enviado y se encuentra en proceso de revisión en la revista Information and Software Technology de Elsevier.

Se redactó un artículo detallando el proceso de creación del Framework, incluyendo un breve resumen del estado del arte, la colaboración con Nisum Technologies para la obtención de la experiencia de la industria, junto con la validación del Framework tanto en cuanto a su forma y a las respuestas entregadas por medio de los casos de estudio, el prototipo de herramienta y el Framework propiamente tal. Dicho artículo fue enviado para su revisión a la revista Information and Software Technology de Elsevier, y actualmente se está a la espera de una respuesta por parte de ella.

Se redactó, en colaboración con Nisum Technologies, un White Paper orientado a la industria, en el cual se plantea la importancia de tener un adecuado nivel de autenticación en aplicaciones, junto con la necesidad de un método que apoye a desarrolladores durante la selección de qué método de autenticación implementar en dichas aplicaciones, presentando posteriormente posibles soluciones a esta problemática, siendo una de ellas el Framework generado por medio de esta investigación.

Referencias

La lista con las referencias de los 982 artículos aceptados durante la revisión sistemática de la literatura puede ser encontrada en http://colvin.chillan.ubiobio.cl/mcaro/. A continuación se presenta la bibliografía referenciada directamente en este informe, la cual puede o no estar también presente en el enlace anterior:

Al-Assam, H., Sellahewa, H., Jassim, S.: On security of multi-factor biometric authentication. In: Internet Technology and Secured Transactions (ICITST), 2010 International Conference for, pp. 1-6. IEEE, (2010)

Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S., Sakurai, K.: Authentication in mobile cloud computing: A survey. Journal of Network and Computer Applications 61, 59-80 (2016)

Altinkemer, K., Wang, T.: Cost and benefit analysis of authentication systems. Decision Support Systems 51, 394-404 (2011)

Anwar, M., Imran, A.: A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication. In: MAICS, pp. 13-18. (2015)

Avison, D.E., Lau, F., Myers, M.D., Nielsen, P.A.: Action research. Communications of the ACM 42, 94-97 (1999)

Baskerville, R.L.: Investigating information systems with action research. Communications of the AIS 2, 4 (1999)

Bonneau, J., Herley, C., Van Oorschot, P.C., Stajano, F.: The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: 2012 IEEE Symposium on Security and Privacy, pp. 553-567. IEEE, (2012)

Brainard, J., Juels, A., Rivest, R.L., Szydlo, M., Yung, M.: Fourth-factor authentication: somebody you know. In: Proceedings of the 13th ACM conference on Computer and communications security, pp. 168-178. ACM, (2006)

Bruun, A., Jensen, K., Kristensen, D.: Usability of Single-and Multi-factor Authentication Methods on Tabletops: A Comparative Study. In: International Conference on Human-Centred Software Engineering, pp. 299-306. Springer, (2014)

Caro, Angélica, Rodríguez, Alfonso, Calero, C., Fernández-Medina, E., Piattini, M.: Análisis y revisión de la literatura en el contexto de proyectos de fin de carrera: Una propuesta. Revista Sociedad Chilena de Ciencia de la Computación 6, (2005)

Chang, C.-C., Wu, T.-C.: Remote password authentication with smart cards. IEE Proceedings E-Computers and Digital Techniques 138, 165-168 (1991)

Choksi, S.: Comparative Study on Authentication Schemes for Cloud Computing. In: International Journal of Engineering Development and Research. IJEDR, (2014)

Eliasson, C., Fiedler, M., Jørstad, I.: A criteria-based evaluation framework for authentication schemes in IMS. In: Availability, Reliability and Security, 2009. ARES'09. International Conference on, pp. 865-869. IEEE, (2009)

Evans Jr, A., Kantrowitz, W., Weiss, E.: A user authentication scheme not requiring secrecy in the computer. Communications of the ACM 17, 437-442 (1974)

Forget, A., Chiasson, S., Biddle, R.: User-centred authentication feature framework. Information & Computer Security 23, 497-515 (2015)

Genero, M., Cruz-Lemus, J., Piattini, M.: Métodos de investigación en ingeniería del software. RA-MA Editorial (2014)

Guel, M.D.: A Framework for Choosing Your Next Generation Authentication/Authorization System. Information Security Technical Report 7, 63-78 (2002)

Huang, X., Xiang, Y., Chonka, A., Zhou, J., Deng, R.H.: A generic framework for three-factor authentication: preserving security and privacy in distributed systems. IEEE Transactions on Parallel and Distributed Systems 22, 1390-1397 (2011)

Kathrine, G.J.W., Kirubakaran, E.: Four-factor based privacy preserving biometric authentication and authorization scheme for enhancing grid security. Int J Comput Appl 30, 13-20 (2011)

Keele, S.: Guidelines for performing systematic literature reviews in software engineering. Technical report, Ver. 2.3 EBSE Technical Report. EBSE, (2007)

Kim, J.Y.: Efficiency of Paid Authentication Methods for Mobile Devices. Wireless Personal Communications 1-9

Kitchenham, B.A., Pfleeger, S.L.: Personal opinion surveys. Guide to Advanced Empirical Software Engineering, pp. 63-92. Springer (2008)

Kock, N., Lau, F.: Information systems action research: Serving two demanding masters. vol. 14(1), pp. 6-11, Information Technology and People (Special issue on Action Research in Information Systems) (2001)

Kumari, S., Khan, M.K., Atiquzzaman, M.: User authentication schemes for wireless sensor networks: A review. Ad Hoc Networks 27, 159-194 (2015)

Lethbridge, T.C., Sim, S.E., Singer, J.: Studying software engineers: Data collection techniques for software field studies. Empirical software engineering 10, 311-341 (2005)

Litwin, M.S.: How to measure survey reliability and validity. Sage Publications (1995)

Madhusudhan, R., Mittal, R.: Dynamic ID-based remote user password authentication schemes using smart cards: A review. Journal of Network and Computer Applications 35, 1235-1248 (2012)

McTaggart, R.: Principles for participatory action research. Adult Education Quarterly 41, 168-187 (1991)

Miranda, L.H.F.M.: Context-aware multi-factor authentication. Faculdade de Ciências e Tecnologia (2009)

Nag, A.K., Dasgupta, D.: An adaptive approach for continuous multi-factor authentication in an identity eco-system. In: Proceedings of the 9th Annual Cyber and Information Security Research Conference, pp. 65-68. ACM, (2014)

Nag, A.K., Dasgupta, D., Deb, K.: An adaptive approach for active multi-factor authentication. In: 9th Annual Symposium on Information Assurance (ASIA'14), pp. 39. (2014)

O'Gorman, L.: Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE 91, 2021-2040 (2003)

Palmer, A.J.: Approach for selecting the most suitable Automated Personal Identification Mechanism (ASMSA). computers & security 29, 785-806 (2010)

Park, K.C., Shin, J.W., Lee, B.G.: Analysis of Authentication Methods for Smartphone Banking Service using ANP. TIIS 8, 2087-2103 (2014)

Pointcheval, D., Zimmer, S.: Multi-factor authenticated key exchange. In: International Conference on Applied Cryptography and Network Security, pp. 277-295. Springer, (2008)

Rathgeb, C., Uhl, A.: Two-factor authentication or how to potentially counterfeit experimental results in biometric systems. In: International Conference Image Analysis and Recognition, pp. 296-305. Springer, (2010)

Robson, C.: Real world research: A resource for social scientists and practitioners-researchers. Massachusetts: Blackwell Pushers (1993)

Runeson, P., Host, M., Rainer, A., Regnell, B.: Case study research in software engineering: Guidelines and examples. John Wiley & Sons (2012)

Shadish, W.R., Cook, T.D., Campbell, D.T.: Experimental and quasi-experimental designs for generalized causal inference. Houghton, Mifflin and Company (2002)

Stebila, D., Udupi, P., Chang, S.: Multi-factor password-authenticated key exchange. In: Proceedings of the Eighth Australasian Conference on Information Security-Volume 105, pp. 56-66. Australian Computer Society, Inc., (2010)

Wadsworth, Y.: What is participatory action research? Action Research Issues Association (1993)

Wang, D., Gu, Q., Cheng, H., Wang, P.: The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, pp. 475-486. ACM, (2016)

Zviran, M., Erlich, Z.: Identification and authentication: technology and implementation issues. Communications of the Association for Information Systems 17, 4 (2006)

Anexos

Anexo A. Planificación de la Revisión Sistemática de la Literatura

Se presenta la planificación previa a la realización de la revisión sistemática de la literatura. El proceso exacto aplicado durante esta investigación puede ser observado en la Fig. 32.

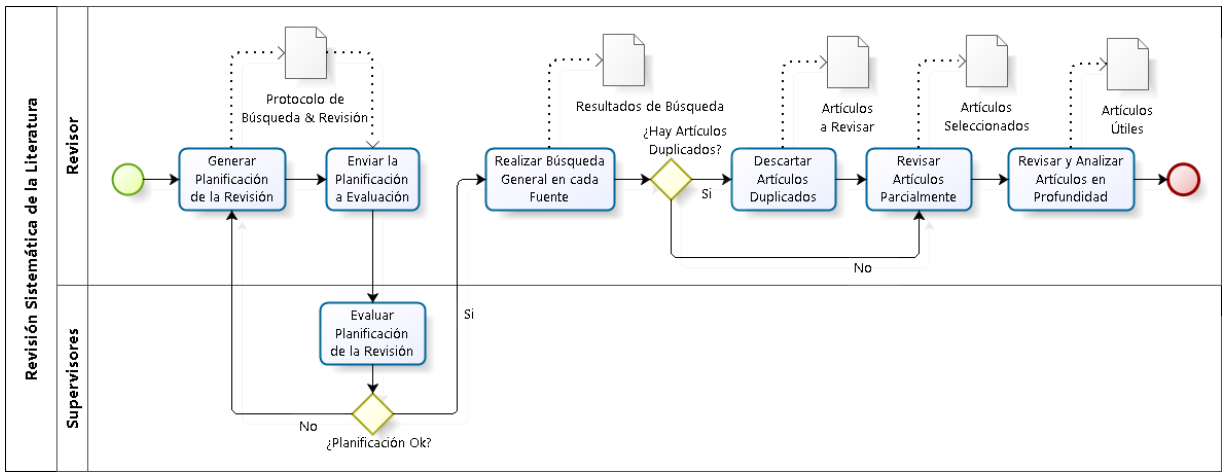


Figura 32. Proceso de revisión sistemática de la literatura aplicado durante esta investigación.

Primero, se realizó la planificación de la revisión, de la cual, junto con la identificación de la necesidad de investigación, se obtuvieron los protocolos de búsqueda y revisión. Dos supervisores analizaron esta planificación y evaluaron su adecuación. Posteriormente, se realizó una búsqueda general en las diferentes fuentes especificadas durante la planificación de la revisión. De los resultados de la búsqueda, los artículos duplicados fueron descartados, y una revisión parcial fue realizada en los artículos restantes, obteniendo una lista de artículos seleccionados que eran potencialmente útiles. Se analizó en profundidad los artículos seleccionados y se obtuvo la lista de artículos útiles para esta investigación. Los detalles de la planificación de la revisión se especifican a continuación, mientras que los resultados de la realización del proceso de búsqueda y revisión se encuentran documentados en el capítulo 3.

A.1 Identificación de la Necesidad de Revisión

El objetivo de la revisión fue el de identificar esquemas de autenticación propuestos en la literatura y posibles combinaciones de ellos para su uso como métodos de autenticación multi-factor, detectando, además, criterios usados para su comparación y selección y la existencia de Framework que se encarguen de dicha tarea. Basándose en este objetivo, las siguientes Preguntas (Q) fueron formuladas para definir más detalladamente la necesidad de investigación:

Q1. ¿Cuáles son los principales esquemas de autenticación existentes en la literatura?

Q2. ¿Qué combinaciones de estos esquemas se pueden encontrar que puedan ser usadas como métodos de autenticación multi-factor?

Q3. ¿Qué criterios pueden ser utilizados para comparar y/o seleccionar entre esquemas de autenticación o métodos de autenticación multi-factor?

Q4. ¿Existen Framework que ayuden a comparar y/o seleccionar esquemas de autenticación o métodos de autenticación multi-factor? ¿Cuáles son sus características?

A.2 **Recursos para la Realización de la Revisión Sistemática de la Literatura**

Para poder realizar la RSL, se utilizaron fuentes que se relacionan al tema a tratar, específicamente, Scopus (https://www.scopus.com/), Springer (http://link.springer.com/), Science Direct (http://www.sciencedirect.com/), IEEE (http://ieeexplore.ieee.org/Xplore/home.jsp), y ACM (http://dl.acm.org/).

Adicionalmente, se utilizó Google Scholar (https://scholar.google.com/) para profundizar en la investigación para aquellas publicaciones potencialmente útiles que no estuvieran indexadas en las fuentes mencionadas anteriormente.

A.3 **Protocolo de Búsqueda**

Se define el protocolo que fue utilizado para realizar la búsqueda en las fuentes definidas anteriormente. Se definen los Términos (T) usados para la revisión, junto con sus Combinaciones (C) (ver Tabla 30).

Tabla 30. Términos y combinaciones usados para realizar la revisión sistemática de la literatura.

Términos	T1: authentication T2: scheme T3: method	T4: multi-factor T5: two-factor T6: three-factor	T7: comparison T8: selection T9: criteria	T10: decision T11: framework
Combinaciones	C1: T1 and (T2 or T3) C2: (T4 or T5 or T6) and T1 C3: (T4 or T5 or T6) and T1 and (T2 or T3) C4: T1 and (T2 or T3) and (T7 or T8 or T9 or T10) C5: (T4 or T5 or T6) and T1 and (T7 or T8 or T9 or T10) C6: (T4 or T5 or T6) and T1 and (T2 or T3) and (T7 or T8 or T9 or T10) C7: T1 and (T2 or T3) and (T7 or T8 or T9 or T10) and T11 C8: (T4 or T5 or T6) and T1 and (T7 or T8 or T9 or T10) and T11 C9: (T4 or T5 or T6) and T1 and (T2 or T3) and (T7 or T8 or T9 or T10) and T11			

Se definieron algunas guías generales para la realización de la búsqueda en concordancia con cada una de las fuentes, entre las cuales:

- En algunos casos, los términos de búsqueda pueden ser ingresados de forma escalada, restringiendo los resultados de una búsqueda anterior.
- Por cada búsqueda realizada, los primeros 200 resultados deben ser revisados.
- Si los resultados de búsqueda tienen acceso restringido, el documento debe ser buscado por medios alternativos (por ejemplo, en los sitios personales de los autores).
- Se debe tener en consideración la posibilidad de la aparición de nuevos términos o conceptos que puedan ayudar a encontrar nuevos trabajos de interés.

Un gestor de referencias en línea fue utilizado para facilitar el registro de los resultados de búsqueda y sus fuentes. Adicionalmente, los resultados de cada búsqueda fueron registrados en una tabla conteniendo, por cada búsqueda, la fuente, la combinación de términos, el número de artículos encontrados y la fecha de búsqueda. Por cada entrada en la tabla descrita anteriormente, se utilizó otra tabla para registrar la referencia de cada artículo revisado, su aceptación o rechazo, una breve descripción explicando los motivos de la aceptación o rechazo y el tema de aceptación al que pertenece.

A.4 **Protocolo de Revisión**

Se realizó una revisión parcial con el motive de obtener los artículos potencialmente útiles para la investigación. Para revisar cada artículo en este paso, se leyó el resumen de cada uno. De ser necesario, también se leyeron la introducción y las conclusiones, mientras que en algunos casos específicos se también se leyó parte del cuerpo del artículo. Una vez realizada cada búsqueda, se tomó la decisión de incluir o no el artículo como uno potencialmente útil, de acuerdo a los criterios de este protocolo. Se mantuvo un control de los artículos aceptados y rechazados usando las tablas descritas anteriormente.

Se incluyó todo artículo que estuviera relacionado a alguno de los siguientes temas de aceptación (AT), los cuales se encuentran relacionados a cada una de las preguntas de investigación formuladas anteriormente:

AT1. Esquemas de autenticación.

AT2. Métodos de autenticación multi-factor.

AT3. Criterios de comparación y selección para esquemas de autenticación o métodos de autenticación multi-factor.

AT4. Framework que apoyan a la decisión de esquemas de autenticación o métodos de autenticación multi-factor.

Por otro lado, se excluyó cualquier artículo que contuviera los términos de búsqueda o combinaciones de ellos, pero que no contuviera información relevante para alguno de los temas de aceptación.

Posteriormente se realizó un análisis en profundidad sobre estos artículos potencialmente útiles, de acuerdo al tema de aceptación de cada artículo. Para aquellos en AT1 y AT2, se identificaron el esquema o método de autenticación, junto con el o los factores de autenticación al que pertenecen y (si se menciona) el contexto para el que el esquema o método fue propuesto. Se realizó un complete análisis de los artículos en AT3 y AT4, a modo de comprender adecuadamente las propuestas e identificar sus ventajas y desventajas, enfatizando los criterios usados en cada uno.

Se extrajo la información de los artículos aceptados, siendo sintetizada y almacenada en una tabla según su tema de aceptación. Para los esquemas de autenticación, se almacenaron la referencia, el esquema propuesto, el factor al que pertenecen y una breve descripción. Para los métodos de autenticación multi-factor, se almacenaron la referencia, los factores combinados, los esquemas en combinados en específico y una breve descripción. Para los criterios de comparación y selección, se almacenaron la referencia, los criterios utilizados y una breve descripción. Finalmente, para los Framework de decisión se almacenaron la referencia, una breve descripción y las fortalezas y debilidades observadas.

Anexo B. Diseño de las Preguntas de la Encuesta y Entrevistas

Las preguntas incluidas en la encuesta son similares a las realizadas durante las entrevistas, pues éstas fueron desarrolladas a modo de validar que la encuesta estuviera correctamente formulada. La encuesta fue diseñada y enviada para ser contestada utilizando un sitio para la creación de encuestas en línea, el cual facilita la obtención y en análisis de los datos. A continuación se presentan las preguntas de la encuesta según cómo son presentadas por el sitio en cuestión (Fig. 33-39).

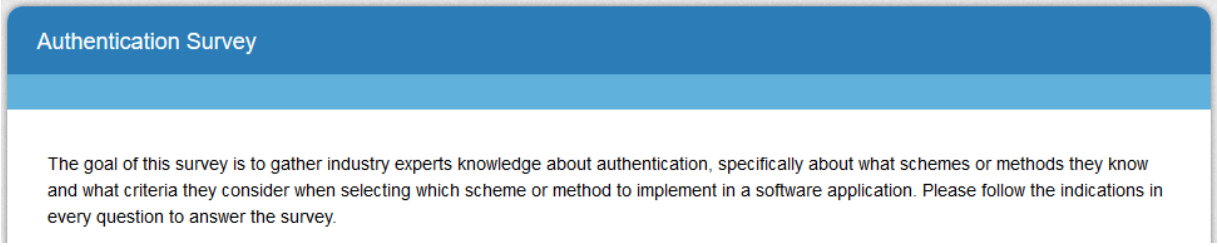


Figura 33. Presentación del motivo y los objetivos de la encuesta.

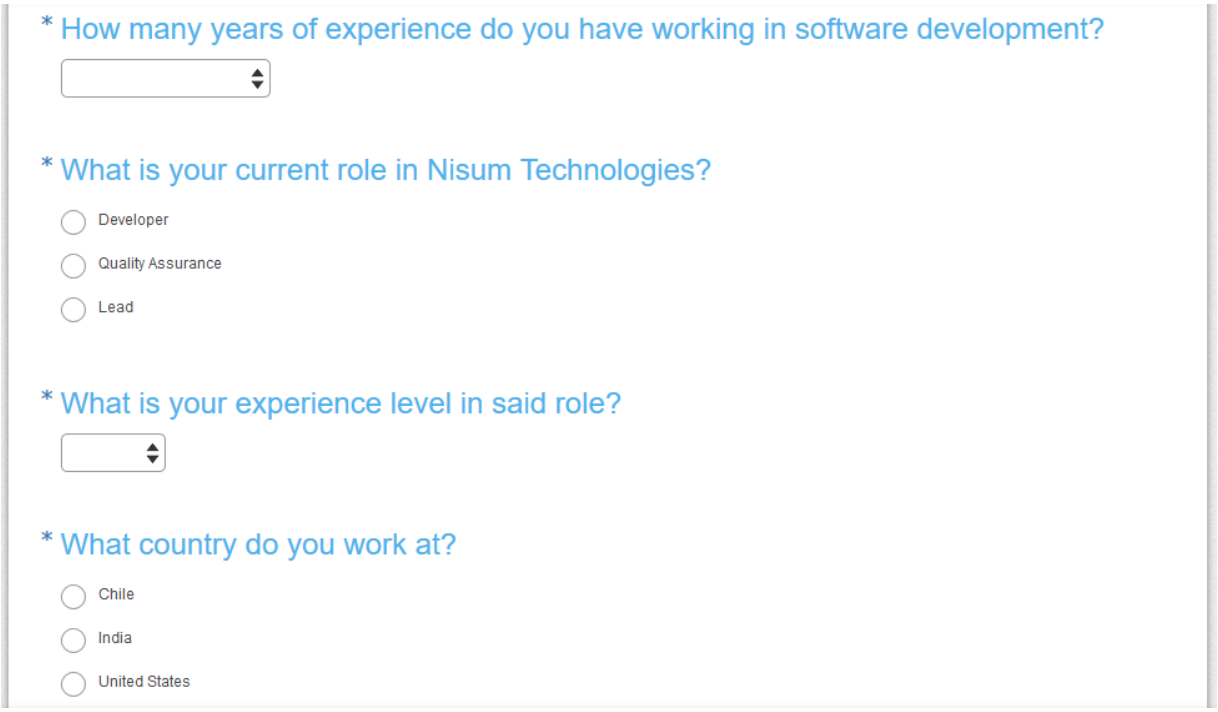


Figura 34. Datos demográficos consultados por la encuesta.

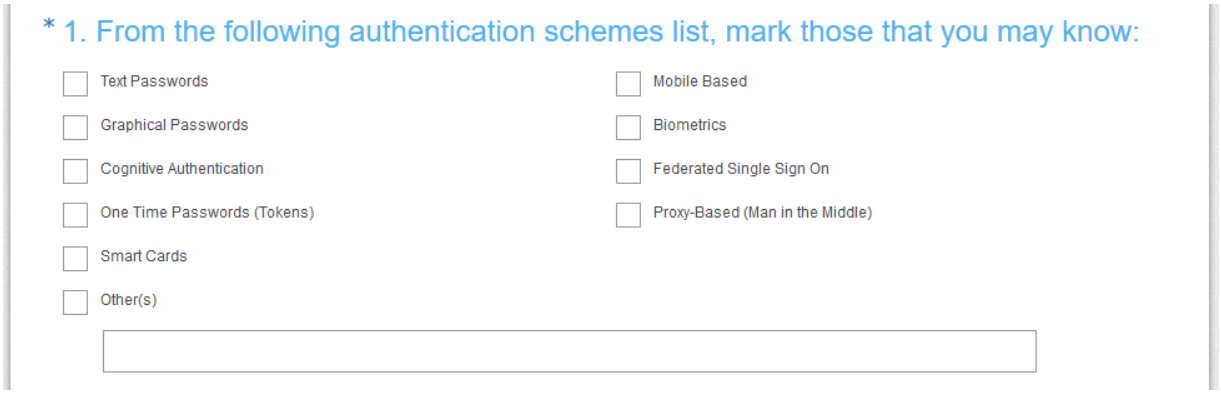


Figura 35. Primer pregunta de la encuesta: esquemas de autenticación conocidos por los encuestados.

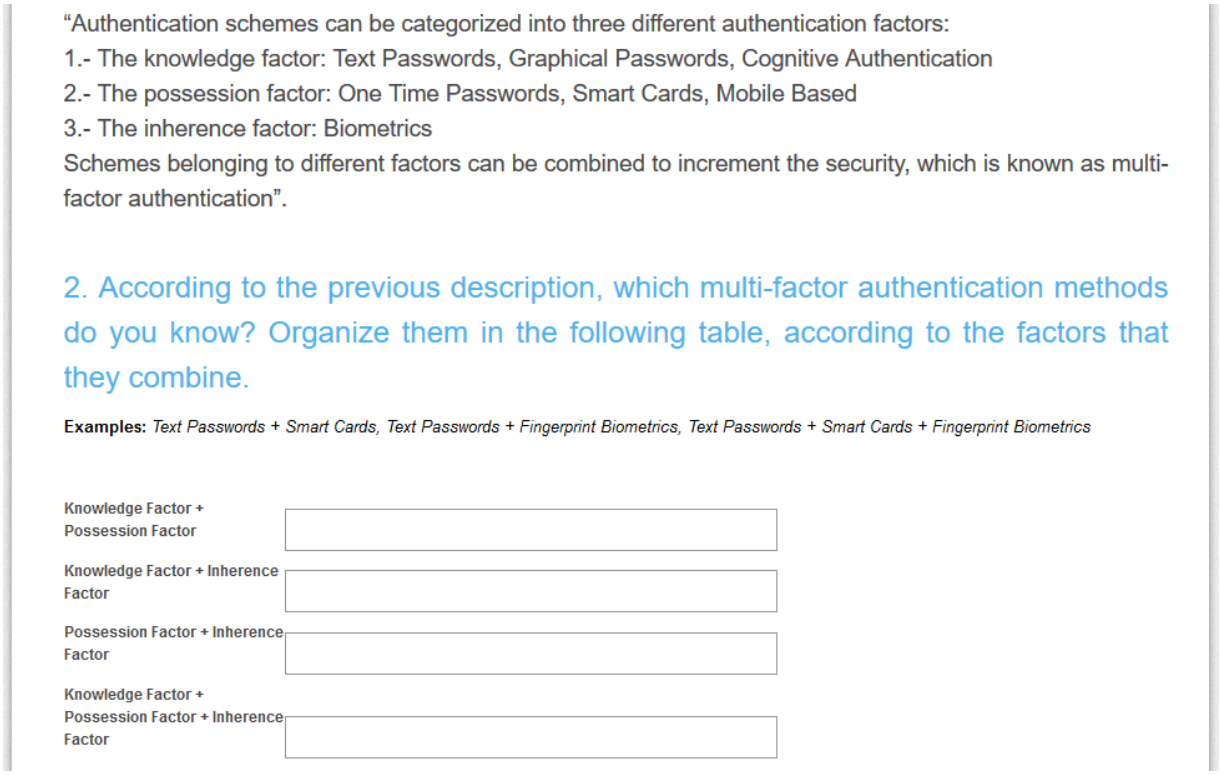


Figura 36. Segunda pregunta de la encuesta: métodos de autenticación multi-factor conocidos por los encuestados.

3. According to the previous questions, what authentication schemes and/or multi-factor authentication methods have you implemented or certified in applications that you have developed, what are their characteristics and what is the reason for your selection? Enumerate them below.

Example:

Scheme or Method	Text Passwords
Application's Characteristics	A simple blog page with an administrator account
Selection Reason	There was not a real need for a strong authentication so a simple scheme was selected

Scheme or Method 1:

Scheme or Method	
Application's Characteristics	
Selection Reason	

Scheme or Method 2:

Scheme or Method	
Application's Characteristics	
Selection Reason	

Scheme or Method 3:

Scheme or Method	
Application's Characteristics	
Selection Reason	

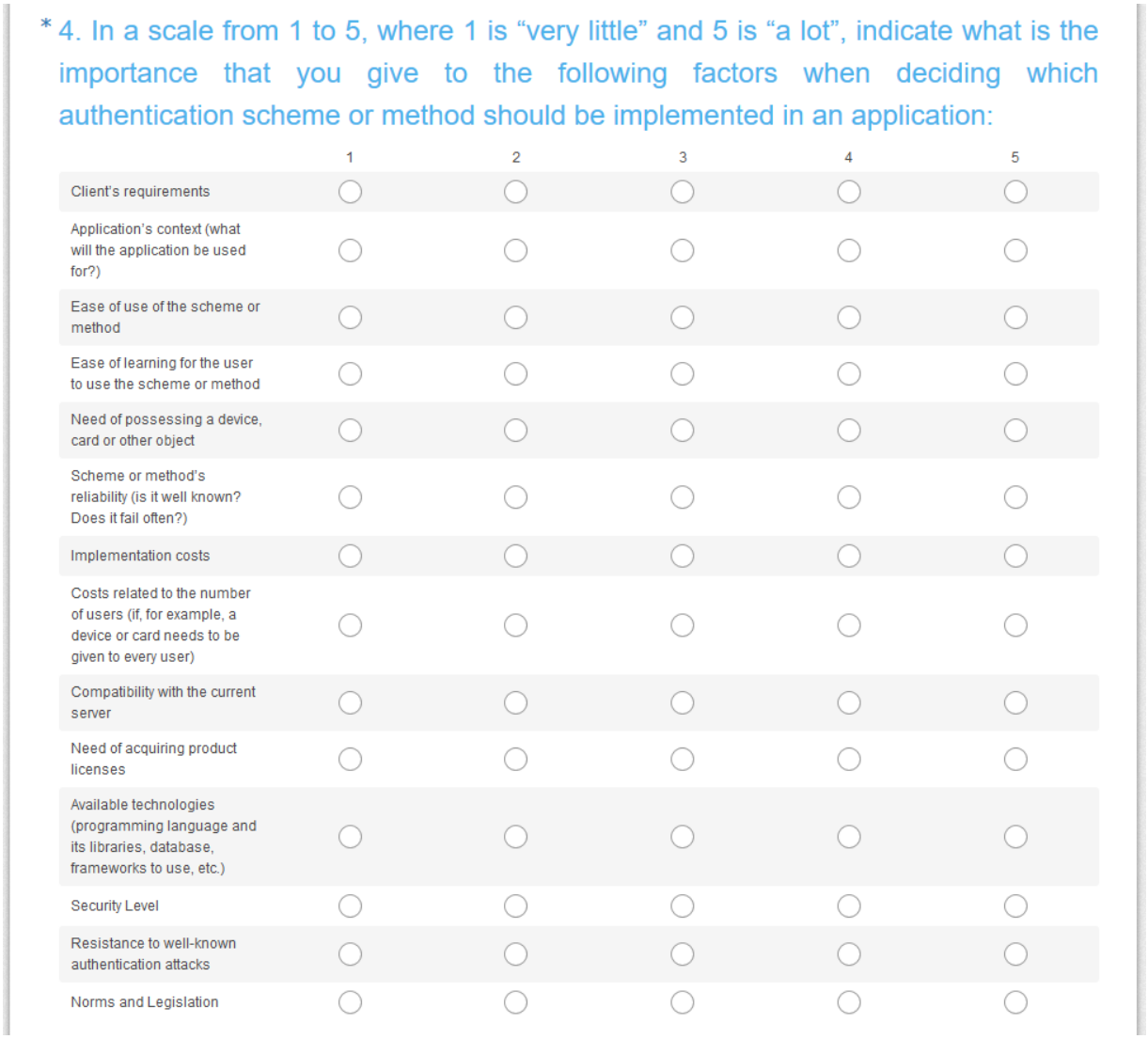
Scheme or Method 4:

Scheme or Method	
Application's Characteristics	
Selection Reason	

Scheme or Method 5:

Scheme or Method	
Application's Characteristics	
Selection Reason	

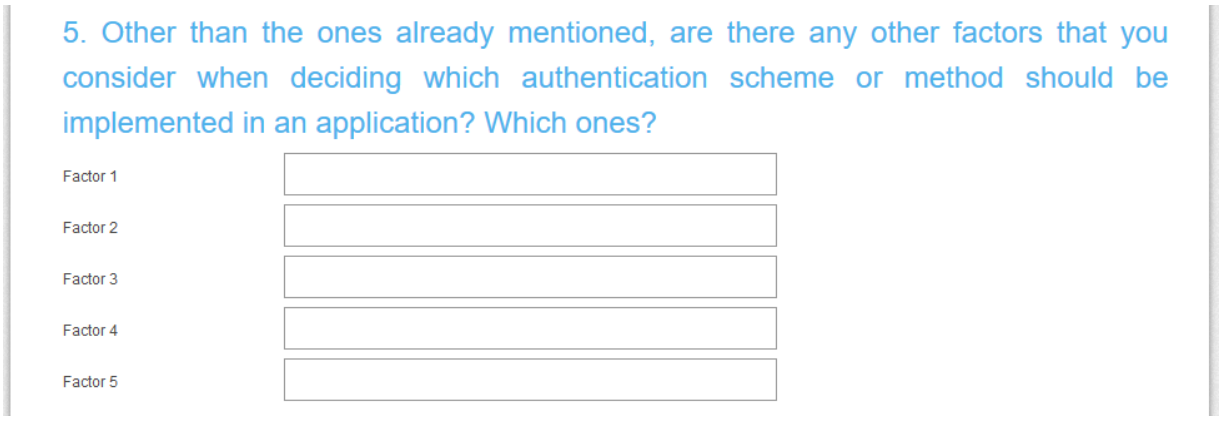
Figura 37. Tercer pregunta de la encuesta: esquemas y métodos de autenticación implementados por los encuestados.



* 4. In a scale from 1 to 5, where 1 is “very little” and 5 is “a lot”, indicate what is the importance that you give to the following factors when deciding which authentication scheme or method should be implemented in an application:

	1	2	3	4	5
Client's requirements	○	○	○	○	○
Application's context (what will the application be used for?)	○	○	○	○	○
Ease of use of the scheme or method	○	○	○	○	○
Ease of learning for the user to use the scheme or method	○	○	○	○	○
Need of possessing a device, card or other object	○	○	○	○	○
Scheme or method's reliability (is it well known? Does it fail often?)	○	○	○	○	○
Implementation costs	○	○	○	○	○
Costs related to the number of users (if, for example, a device or card needs to be given to every user)	○	○	○	○	○
Compatibility with the current server	○	○	○	○	○
Need of acquiring product licenses	○	○	○	○	○
Available technologies (programming language and its libraries, database, frameworks to use, etc.)	○	○	○	○	○
Security Level	○	○	○	○	○
Resistance to well-known authentication attacks	○	○	○	○	○
Norms and Legislation	○	○	○	○	○

Figura 38. Cuarta pregunta de la encuesta: valoración de criterios para la comparación y selección de esquemas o métodos.



5. Other than the ones already mentioned, are there any other factors that you consider when deciding which authentication scheme or method should be implemented in an application? Which ones?

Factor 1

Factor 2

Factor 3

Factor 4

Factor 5

Figura 39. Quinta pregunta de la encuesta: criterios de comparación y selección considerados por los encuestados.