

Universidad Politécnica de Madrid  
Escuela Técnica Superior de Ingenieros de Telecomunicación



# **ESTUDIO SISTEMÁTICO DE LITERATURA DE METODOLOGÍAS PARA LA OBTENCIÓN DE REQUISITOS DE PRIVACIDAD**

**TRABAJO FIN DE MÁSTER**

**Gonzalo Pérez-Tomé Estévez**

2015

Universidad Politécnica de Madrid  
Escuela Técnica Superior de Ingenieros de Telecomunicación

**Máster Universitario en  
Ingeniería de Redes y Servicios Telemáticos**

**TRABAJO FIN DE MÁSTER**

**ESTUDIO SISTEMÁTICO DE LITERATURA DE  
METODOLOGÍAS PARA LA OBTENCIÓN DE  
REQUISITOS DE PRIVACIDAD**

Autor

**Gonzalo Pérez-Tomé Estévez**

Director

**José María del Álamo Ramiro**

Departamento de Ingeniería de Sistemas Telemáticos

2015

## RESUMEN

---

Los nuevos sistemas de información y comunicaciones empiezan a ver a la privacidad como un punto clave a tener en cuenta en el desarrollo software; dentro de un marco social, legal, mediático y de negocio que cada vez más la demandan. Disciplinas como la ingeniería de requisitos, el análisis y la gestión de riesgos, la gestión de privacidad, y la misma ingeniería software, tratan de encontrarse para consensuar definiciones y conceptos de privacidad, los cuales a menudo discrepan entre el mundo técnico y el mundo legal.

Para ello la ingeniería de privacidad introduce recientemente a la privacidad por diseño, esto es, tener en cuenta a la privacidad desde el principio del ciclo de vida software; frente a la idea anterior de aplicarla a modo de parche en las etapas finales del mismo.

Fruto de esta idea nacen las metodologías y procesos de ingeniería de privacidad, con el objetivo de garantizar dicho concepto de privacidad por diseño de manera sistemática y reproducible.

Si bien este tipo de metodologías han ido creciendo en número en los últimos diez años, muchas de ellas resultan ser marcos de trabajo para dominios muy concretos, donde se ven mezcladas la privacidad con la seguridad. No obstante, hoy por hoy se observa un creciente interés por el desarrollo y mejora de las mismas, desvinculando en la medida de lo posible a la privacidad de la seguridad.

El presente Trabajo Fin de Máster se cimienta en un enfoque investigador, dejando en segundo plano la naturaleza práctica de trabajos como el estudio de nuevas herramientas y tecnologías, y centrándose más en un análisis del estado del arte en el dominio de la ingeniería de requisitos de privacidad.

Para esto se utilizarán técnicas de investigación como la revisión y el estudio sistemático de la literatura, con el fin de hacer acopio de referencias, analizarlas, sintetizar la información y extraer conclusiones en base a lo obtenido.

Como aspecto inicial importante de este trabajo a destacar está el que resultase autocontenido, por lo que se ha provisto de la información necesaria para que el lector entienda los conceptos, definiéndolos y clarificándolos antes de su uso.

Además de ofrecer información relevante sobre la privacidad, este trabajo seguirá un estudio sistemático que, a modo de resultado, llegará a una tabla comparativa de nueve metodologías de obtención de requisitos de privacidad conocidas hasta la fecha, y aplicables a la ingeniería software. Finalmente se extraerán las conclusiones a la vista de esa tabla, siguiendo los criterios que las destacan o diferencian entre sí.

## ABSTRACT

---

Last information and communication systems start keeping in mind the privacy as an essential issue to consider in software development, in a stricter social, legal, media and business context. Disciplines like requirements engineering, risk management and analysis, privacy management, and software engineering itself, manage to find common privacy definitions and concepts – which often disagree between technical and legal environments.

In order to achieve this, privacy engineering recently introduces privacy-by-design (aka. PbD), which considers privacy from the very first step of software life-cycle, in contrast to the previous idea of applying privacy as a patch at final steps of the development process.

As a consequence, this idea supposes the origin of privacy engineering methodologies and processes, which grant the previously mentioned PbD concept as the main target in a systematical and reproducible way.

Although this kind of methodologies had been growing in number in the last 10 years, most of them are to be frameworks that could apply only to concrete domains, where security and privacy requirements seem to be mixed. Nevertheless, today it is also noticeable a growing interest for developing and improve these methodologies and, at the same time, for decoupling privacy from security whenever possible.

Present end-of-master project relies on a research approach, leaving in the background the practical nature of projects like the study of new tools and/or technologies, and focusing on the state of the art analysis of the privacy requirements engineering's domain.

To do so, research techniques like systematic literature review and survey will be used, in order to collect the references needed, analyze them, synthesize information and extract conclusions of the results.

It is important to highlight as an initial aspect of this project its self-contained sense, so that concrete information is provided to the reader for understanding concepts, defining and clarifying them whenever necessary before its use.

In addition of providing such relevant information about privacy, this project will be a systematic literature survey that, as a result, will end in a comparative table of 9 methodologies for the privacy requirements elicitation in software engineering. Finally, conclusions will be extracted taking in consideration the mentioned table, and following criteria that highlight or differentiate them among each other.

# Contenido

Resumen.....	2
Abstract .....	3
1 Introducción .....	6
1.1 La Ingeniería de privacidad .....	7
1.2 La ingeniería software .....	8
1.3 La ingeniería de requisitos .....	9
1.4 La gestión de riesgos .....	10
2 Motivación y objetivos .....	12
3 Planificación del trabajo.....	14
4 Procedimiento del trabajo .....	15
4.1 La Revisión sistemática de Literatura (SLR).....	15
4.2 El Estudio Sistemático de Literatura (SLS).....	16
4.3 Definición del tema del área de investigación .....	16
4.4 Búsqueda documental .....	17
4.4.1 Términos de búsqueda e Identificación de artículos .....	17
4.4.2 Bibliografía, bases de datos, motores de búsqueda y gestores de referencias..	18
4.4.3 Filtros de inclusión y exclusión.....	19
4.4.4 Sobre los artículos descartados.....	19
4.4.5 Otros trabajos relacionados .....	20
4.4.6 Resumen de la búsqueda documental y resultados .....	20
4.4.7 Selección final y resultado de la búsqueda .....	22
4.5 Evaluación de los artículos seleccionados y síntesis .....	23
5 Metodologías de obtención de requisitos para la privacidad.....	24
5.1 LINDDUN .....	24
5.2 NFR .....	26
5.3 PriS.....	27
5.4 RBAC.....	29
5.5 Framework Tropos y GSRM.....	30
5.6 STRAP .....	31
5.7 PRET.....	32
5.8 Marco de trabajo 'Privacy-Friendly' .....	33
5.9 PRIPARE .....	34
6 Análisis y resultados .....	36
6.1 Publicación .....	37

6.2	Evidencias empíricas .....	37
6.3	Software de apoyo .....	37
6.4	Fuentes de requisitos .....	37
6.5	Enfoque de obtención de requisitos .....	38
6.6	Descripción de los requisitos.....	38
6.7	Complementariedad .....	38
6.8	Actividades de ingeniería de requisitos .....	38
6.9	Actividades de ingeniería software .....	39
7	Conclusiones.....	40
8	Referencias.....	42
9	Anexos.....	49
9.1	Plantilla de análisis .....	49
9.2	Referencias 1ª iteración .....	51
9.3	Referencias 2ª iteración .....	58
9.4	Referencias 3ª iteración .....	63

# 1 INTRODUCCIÓN

---

Durante los últimos años la importancia de la privacidad del usuario ha ido cada vez más en aumento. Pasamos de un ciclo de desarrollo software donde la privacidad apenas se tenía en cuenta, en todo caso como un requisito no funcional de escasa importancia, y se empieza a ver poco a poco a la privacidad como un componente que podría tener valor de negocio propio (como es el caso de las nuevas redes sociales).

La definición de privacidad aún sigue en discusión, pues su mayor problema reside en las múltiples versiones de ésta y la falta de unanimidad.

De un modo generalista, la Declaración Universal de los Derechos Humanos [1] y el Pacto Internacional de Derechos Civiles y Políticos [2] la definen como la capacidad de evitar *“injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia”*, o denegar *“ataques a su honra o a su reputación”*.

La legislación de países europeos, y particularmente la Constitución Española de 1978 [3], introducen de una manera más concreta el *“derecho al honor, a la intimidad personal y familiar y a la propia imagen”*, la *“limitación de la informática”* (para garantizar a los anteriores); y quizás lo más importante, el concepto de *“consentimiento”*. A ésta se le suman las definiciones aplicadas en Estados Unidos, donde cada organismo competente en materia de privacidad la define a su manera.

Por ello se hace necesario en este Trabajo Fin de Máster poder definirla, aunque sea sacando factor común de las anteriores definiciones. Se entiende, por tanto, a la privacidad como la capacidad del usuario de poder controlar el ocultamiento o revelado de información sensible del mismo. Los desarrolladores de aplicaciones poco a poco van teniendo en cuenta a la privacidad a lo largo de todo el proceso de desarrollo software, incluyendo nuevas metodologías y técnicas para poder garantizarla, llegando así a lo que se conoce como *privacidad por diseño*.

La obtención de requisitos de privacidad tiene su origen tanto en el mundo de la ingeniería de requisitos como en el de la seguridad, aunque mayormente en el segundo. Esto hace que los conceptos de seguridad y privacidad muchas veces vayan de la mano, y se utilice en dichos procesos casi siempre la misma jerga de términos (p.ej. roles, amenazas, anonimato, etc.).

Frente al posible revelado de información del usuario, dicha información puede provenir tanto de los datos como de los metadatos (información sobre los datos). Actualmente ambos son utilizados por empresas y organismos regulatorios para diversos fines, si bien el usuario rara vez está totalmente de acuerdo o conoce todos los detalles de qué se hace con sus datos.

Por parte de las empresas, la obtención de datos que permitan conocer mejor a sus clientes constituye a todas luces una ventaja competitiva. Aun no siendo cierto que todas sepan explotar dichos datos de manera eficiente, muchas de ellas los almacenan para un futuro indeterminado en que puedan sacarle provecho.

La postura de los gobiernos frente a la privacidad de datos depende de las leyes del país donde se alojen estos últimos. En EE.UU por ejemplo, cuentan con varios organismos de regulación dependiendo del dominio: sanidad, seguridad ciudadana, etc. En cambio, en la UE existe un único organismo regulador en materia de privacidad.

Desde el punto de vista de los usuarios, por un lado son conscientes de la importancia de garantizar su privacidad. Por el otro en cambio, la actitud que estos adoptan frente al tema resulta contraria a sus preocupaciones.

Los argumentos por los cuales un usuario adopta este tipo de actitudes son de muy diverso tipo: desde conseguir un beneficio inmediato a cambio de información (i.e. dar datos personales a una tienda para comprar un artículo en el momento), pasando por la necesidad de pertenecer a un círculo social (i.e. ceder los datos para no quedar fuera de tu círculo socio-familiar), hasta verse "protegido" dentro de un agregado mayor (i.e. mientras uno no destaque, no será objetivo de un ataque).

En cualquier caso, a día de hoy un ingeniero software se ve en el compromiso de garantizar la privacidad del usuario, teniendo presentes ciertos objetivos de negocio a nivel de organización, así como el entorno de la legislación del país o región en el que se sitúe.

En el campo de la ingeniería de privacidad, existen una serie de metodologías a seguir durante el ciclo de desarrollo de un sistema, las cuales pasarán a ser explicadas en el trabajo. Éstas permiten identificar sistemáticamente los requisitos de privacidad durante las fases de análisis, diseño, etc., pudiendo ser implantadas directamente en el modelo de procesos de un negocio en particular – ya sea pequeña, mediana o gran empresa según proceda.

## **1.1 LA INGENIERÍA DE PRIVACIDAD**

Según el organismo de estandarización americano NIST, la ingeniería de privacidad puede definirse como “una disciplina enfocada a facilitar guías y buenas prácticas para disminuir riesgos de privacidad; permitiendo a las organizaciones tomar decisiones fundamentadas sobre la localización de los recursos, así como una implementación efectiva de los protocolos de control en los sistemas de información”[4].

A esta definición se podría añadir, del concepto mismo de ‘ingeniería’, que dicha disciplina engloba un conjunto de conocimientos (metodologías y técnicas) aplicando a lo anteriormente dicho de una manera sistemática y disciplinada.

La ingeniería de privacidad es una disciplina incipiente en la actualidad, que hasta los últimos años no se le ha dado toda atención que merece. Uno de los motivos de esta falta de atención es la escasa existencia de herramientas y manuales de buenas prácticas. Los desarrolladores tienen que entregar el software rápidamente para minimizar el tiempo de puesta en producción y el esfuerzo; casi siempre reutilizando componentes ya existentes a pesar de las brechas de privacidad que ello puede ocasionar. Desafortunadamente hoy en día hay pocos heurísticos para aplicaciones y servicios respetuosos con la privacidad [5].

Hasta ahora se ha ido teniendo en cuenta a la privacidad como un proceso retrospectivo derivado del mundo legal. Esto quiere decir que hasta que el sistema no ha sido desarrollado, no es cuando se aplican medidas para garantizar la privacidad a modo de parche; y casi siempre se hace únicamente desde el punto de vista legal (i.e. políticas de privacidad).

Este último hecho está cambiando, y la manera de entender la privacidad se mira desde un nuevo concepto que los artículos denominan ‘privacy-by-design’ [6]. Se entiende privacidad por diseño al hecho de tener en cuenta a la privacidad desde el principio del ciclo de vida del software, siendo necesario integrar nuevas metodologías en los procesos de desarrollo ya conocidos: análisis, diseño, implementación, pruebas y validación, operación y mantenimiento. En contraposición con lo anterior se trataría, por tanto, de un enfoque prospectivo.



A la hora de tener en cuenta a la privacidad en la producción de software, se justifica la necesidad de un proceso sistemático y reproducible que, llevado a una economía de escala, ayude a reducir los costes de las organizaciones de forma significativa. De esta forma, un sistema amigable con la privacidad podría reducir, por ejemplo, los costes del departamento legal, mejorar la experiencia del usuario, e incluso disminuir en conjunto los costes de producción totales (una vez integrada una metodología en el proceso de desarrollo).

## 1.2 LA INGENIERÍA SOFTWARE

Respecto a la ingeniería software, se define desde un punto de vista formal como *el estudio y aplicación de ingeniería al diseño, desarrollo y mantenimiento del software* [7]–[9].

Según los organismos de estandarización ISO, IEC e IEEE, es *“la aplicación sistemática del conocimiento científico y tecnológico, métodos y experiencia en el diseño<sup>1</sup>, implementación, pruebas y documentación del software”*[10].

Es considerada hoy en día una parte de la ingeniería de sistemas; además de tener puntos comunes con la ciencia de computación<sup>2</sup> y ciencia de gestión<sup>3</sup>. La ingeniería software tiene como sub-disciplinas [7]:

- Ingeniería de requisitos: La obtención, análisis, especificación y validación de los requisitos del software.
- Diseño: El proceso de definición de la arquitectura, componentes, interfaces y otras características de un sistema o componente. También se define como el resultado de todo el proceso anterior.
- Implementación o construcción: La creación detallada del software a través de una combinación de varias etapas (programación, verificación, pruebas unitarias, pruebas de integración y depuración).
- Pruebas (aka. *testing*): Una investigación técnica y empírica para facilitar a las partes interesadas información sobre la calidad del producto o servicio bajo prueba.
- Mantenimiento: Todas las actividades requeridas para proveer de soporte al software de manera eficiente en cuanto a costes.
- Gestión de la configuración: Identificación de la configuración de un sistema en distintos puntos temporales con el propósito de controlar los cambios en la configuración de manera sistemática, así como el mantenimiento de la integridad y trazabilidad de la configuración en el ciclo de vida del sistema.
- Gestión de la ingeniería software: Aplicación de las actividades de gestión (planificación, coordinación, medición, monitorización, control y reporte) para asegurar que el desarrollo y mantenimiento del software sigue un proceso sistemático, disciplinado y medible.
- Procesos de ingeniería software: Definición, implementación, aseguramiento, medición, gestión, cambio y mejora del propio proceso o ciclo de desarrollo software.
- Herramientas y métodos de ingeniería software: Las herramientas computacionales que pretenden ayudar a los procesos del ciclo de vida software. También se incluyen los métodos que dotan de estructura a la actividad de la ingeniería software, con el

---

<sup>1</sup> En este contexto, el término anglosajón ‘design’ incluye tanto la actividad de análisis de requisitos como la actividad de diseño propiamente dicho.

<sup>2</sup> Del inglés: ‘Computer science’.

<sup>3</sup> Del inglés: ‘Management science’.

objetivo de realizar las actividades de manera sistemática y, en definitiva, garantizar en la medida de lo posible su éxito.

- Gestión de la calidad del software: Grado del cumplimiento de los requisitos por partes de las características del software.

### 1.3 LA INGENIERÍA DE REQUISITOS

La ingeniería de requisitos (abreviada RE<sup>4</sup>) queda definida actualmente como la disciplina que atiende a los procesos de *definición, documentación y mantenimiento de requisitos* dentro de la ingeniería de sistemas en general, y la ingeniería del software en particular [11]–[13].

Como se ha podido observar en el apartado de ingeniería software, la ingeniería de requisitos constituye a todas luces uno de los pilares más importantes de la primera. Sin embargo, se hace necesario recalcar que esta disciplina de la ingeniería de sistemas abarca muchos más aspectos no relacionados directamente con la ingeniería software. Sólo una parte de una, resulta ser un dominio particular de la otra.

Las etapas de la ingeniería de requisitos se resumen a continuación [14]:

1. Concepción, revelado o captura de requisitos: Metodologías o procesos para la obtención desde cero de los requisitos de un sistema.
2. Identificación de requisitos: Definición y relaciones con otros requisitos.
3. Análisis y negociación de requisitos: Comprobación y resolución de conflictos con las partes interesadas del sistema.
4. Especificación de requisitos: Documentación formal tanto a nivel de negocio como a nivel técnico (este último recogido en el SRS<sup>5</sup>).
5. Modelado del sistema: Modelos derivados del sistema, casi siempre utilizando notaciones como el Lenguaje de Modelado Unificado (UML<sup>6</sup>).
6. Validación de requisitos: Comprobación de la consistencia entre los requisitos documentados y las necesidades de las partes interesadas.
7. Gestión de requisitos: Gestión de cambios de los requisitos a medida que el sistema se va desarrollando y poniendo en producción.

Teniendo en cuenta los muchos tipos de requisitos que hay, todos ellos se suelen separar en dos grandes conjuntos que son:

1. Requisitos funcionales: definen la aplicación de un sistema a nivel de negocio.
2. Requisitos no funcionales: definen las características técnicas de un sistema, tales como la fiabilidad, calidad de servicio, etc.

Tanto la seguridad como la privacidad no son requisitos que aporten un valor de negocio de por sí, por lo que se los considera dentro de los requisitos no funcionales. Existe una diferencia importante que separa los requisitos de seguridad de los de privacidad. Los primeros tienen en cuenta únicamente a la organización responsable del desarrollo y operación del sistema (la posible víctima de un ataque), mientras que los requisitos de privacidad han de tener en cuenta también a los propietarios de datos o terceras partes interesadas: ellos también pueden convertirse en víctimas de un ataque a la privacidad y, en consecuencia, impactaría negativamente en la empresa desarrolladora.

---

<sup>4</sup> Del inglés: 'Requirements Engineering'.

<sup>5</sup> Del inglés: 'Software Requirements Specification'.

<sup>6</sup> Del inglés: 'Unified Modeling Language'.

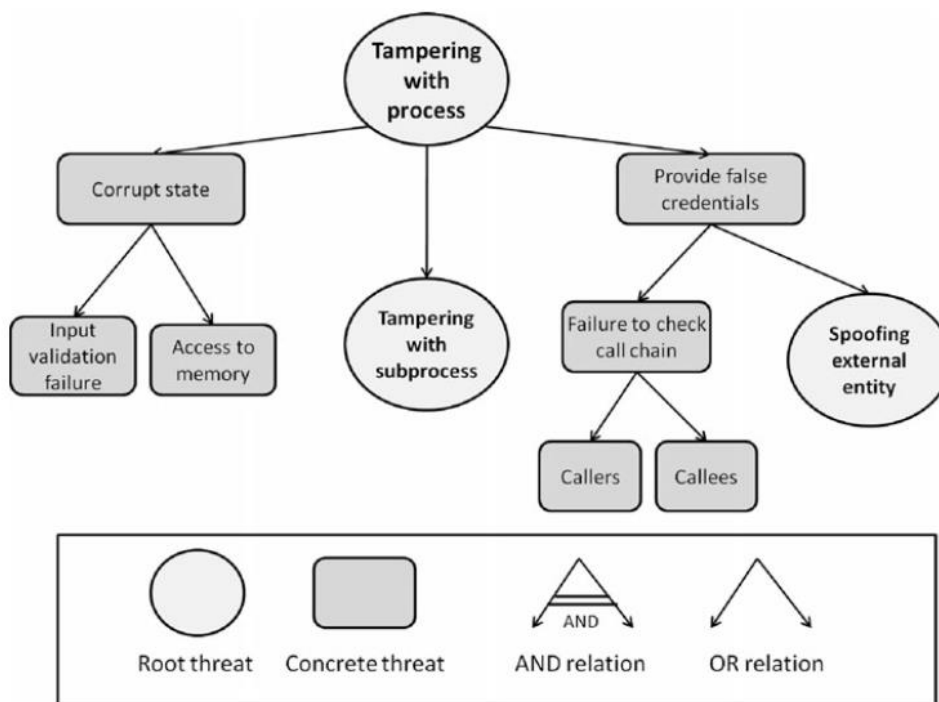


Ilustración 1: Patrón de árbol de amenazas de [15]

## 1.4 LA GESTIÓN DE RIESGOS

ISO 31000 [16] hace referencia al concepto de riesgo como el efecto de la indeterminación en los objetivos. Asimismo, se define la gestión de riesgos como la identificación, valoración y priorización de éstos seguido de una aplicación de recursos coordinada y económica para minimizar, monitorizar y controlar la probabilidad y/o impacto de eventos desafortunados, o maximizar la creación de oportunidades. Su objetivo principal es asegurar que aquello que resulte indeterminado no ponga en jaque los objetivos de negocio [17], [18].

A raíz de la disciplina de gestión de riesgos, y orientándose al mundo de las metodologías de privacidad, surge la ‘valoración del impacto en la privacidad’, más conocida como PIA<sup>7</sup>.

Existen diversas metodologías basadas en valoración de riesgos según [19], aunque no son aplicables de forma sencilla debido a su estructura no del todo acertada, imprecisión o complejidad.

La idea de ir aplicando catálogos y repositorios de riesgos y amenazas ya conocidos se conoce como enfoque heurístico. La mejora y perfeccionamiento de estos resultan a día de hoy una fuerte corriente de investigación debido a ventajas tan claras como son la rapidez de la elaboración de requisitos, o incluso prescindir de parte de los servicios de consultoría experta.

Los árboles de amenazas constituyen un ejemplo de heurístico en el mundo de la gestión de riesgos. Dentro de las metodologías de privacidad que veremos, a continuación se describen las metodologías obtenidas de modo general. Un lector curioso puede encontrar información más detallada dentro de cada referencia a la metodología en cuestión. Así pues, las metodologías explicadas son LINDDUN [15], NFR [79]–[81], PriS [32], RBAC [83], Tropos y GSRM

<sup>7</sup> Del inglés: ‘Privacy Impact Assessment’.

[84] (marco de trabajo mixto), STRAP [30], PRET [89], marco de trabajo 'Privacy-Friendly' [6] y PRIPARE [90].

LINDDUN utiliza este tipo de herramienta para obtener requisitos de privacidad a modo de plantilla o patrón prediseñado (i.e. 'Cheatsheet'). En la Ilustración 1: Patrón de árbol de amenazas puede verse un ejemplo de este tipo de heurístico aplicado directamente a la problemática de manipulación de procesos, desde el punto de vista de la privacidad.

## 2 MOTIVACIÓN Y OBJETIVOS

---

Teniendo en cuenta las tres disciplinas anteriores, surge la necesidad de investigación en un dominio común, esto es, la aplicación directa de la ingeniería de requisitos de privacidad en el ciclo de vida software. Puede verse de modo simplificado su origen en la Figura 1: Origen de la ingeniería de requisitos de privacidad.

Los marcos de trabajo existentes en la actualidad parten desde uno de los tres puntos de vista. Profesionales del mundo de la privacidad (p.ej. abogados), o del mundo de la seguridad y de los requisitos (p. ej. ingenieros de sistemas); poco a poco van definiendo y perfeccionando metodologías de obtención y especificación de requisitos, que garantizan la privacidad de las partes interesadas del sistema.

Aunque a día de hoy no hay en absoluto el mismo avance en materia de requisitos de privacidad como en requisitos la seguridad, se está viendo un importante crecimiento en el interés por el primero. Esto puede verse en los grupos de trabajo sobre privacidad que están apareciendo últimamente como los que se describen a continuación, que dan pie a la motivación de la importancia de este Trabajo Fin de Máster.

Por un lado se encuentra el proyecto PRIPARE [20], cuyo objetivo principal puede encontrarse en su sitio web: *“facilitar la aplicación de una metodología de privacidad y seguridad por diseño que contribuirá al advenimiento de un uso libre de Internet frente a interrupciones, censuras y vigilancia, soportará su entrenamiento mediante la comunidad de investigación ICT para la preparación de la práctica industrial; promover la cultura de gestión de riesgos a través de material educativo enfocado a una diversidad de partes interesadas”*.

Otra entidad investigadora que trabaja en un tema similar de metodologías de privacidad es MITRE [21]. Se trata de una corporación estadounidense sin ánimo de lucro que trabaja en múltiples centros de investigación y desarrollo financiados por el gobierno federal (‘FFRDC’). Los dominios sobre los que aplican sus investigaciones son igualmente diversos: defensa e inteligencia, aviación, sistemas civiles, seguridad, sistemas judiciales, cuidados sanitarios y ciberseguridad.

Por el otro lado encontramos comunidades dedicadas a la formación y preparación de conferencias, las cuales reúnen periódicamente a los expertos en la materia, con el objetivo de ir actualizando el estado del arte, incluyendo la presentación de nuevos artículos. Entre estas comunidades destacan ‘Computing Community Consortium – Privacy by Design’ [22], con cuatro conferencias; ‘Internet Privacy Engineering Network’ (aka. IPEN) [5], con dos conferencias; y ‘IEEE Symposium on Security and Privacy’ [23], [24], con hasta treinta y seis workshops que se han ido llevando a cabo desde 1980.

Los dos primeros (CCC e IPEN) son organizaciones impulsadas por entidades públicas que buscan el crear una comunidad multidisciplinar que avance en la práctica, mediante la conexión de la industria con el mundo académico y de expertos legales con técnicos, una en Estados Unidos y la otra en la Unión Europea respectivamente. En cambio, el IEEE celebra conferencias científicas, donde se presentan sólo los últimos avances tecnológicos y/o descubrimientos científicos.

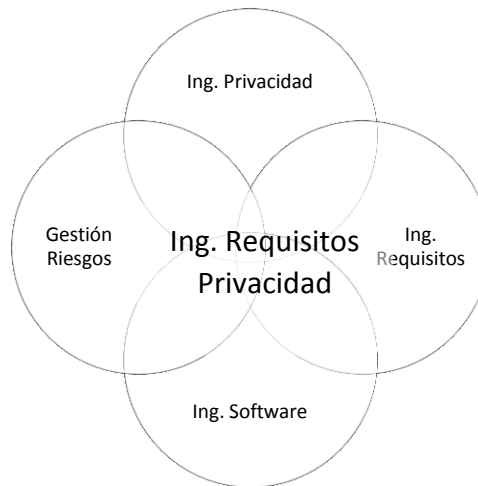


Figura 1: Origen de la ingeniería de requisitos de privacidad

Con todo esto puede verse fácilmente que aún se está trabajando activamente en la aplicación de metodologías de ingeniería de privacidad. El presente Trabajo Fin de Máster parte de lo anterior como motivación y busca recopilar y analizar las distintas metodologías y marcos de trabajo conocidos hasta la fecha, centrados en la ingeniería de requisitos de privacidad. A continuación se detallan los objetivos propuestos:

1. Adquirir el conocimiento base en el campo de la ingeniería de requisitos de privacidad, el cual ofrezca una panorámica general acerca de su estado del arte y futura investigación.
2. Especificar un procedimiento que permita realizar de manera sistemática una consulta de la literatura<sup>8</sup> orientada a la ingeniería de requisitos de privacidad.
3. Conocer las distintas metodologías de obtención de requisitos de privacidad, dentro del mundo de la ingeniería software actual.
4. Sintetizar las metodologías mediante una comparativa en base a unos criterios definidos.
5. Conocer y aplicar metodologías científicas para la exploración sistemática de un campo del conocimiento. En particular, la revisión y el estudio sistemático de la literatura.
6. Conocer y hacer uso de técnicas y herramientas de soporte a la investigación; aplicables por ejemplo a la gestión de referencias (*Mendeley*), a las bases de datos y a motores de búsqueda de artículos (*Google Scholar, ACM, Springer, Emerald Group,...*).

---

<sup>8</sup> Del inglés: 'Systematic literature query'.

### 3 PLANIFICACIÓN DEL TRABAJO

---

El actual Trabajo Fin de Máster ha sido planificado para un margen de tiempo de 6 meses. A continuación se describen las etapas por las que el autor ha ido pasando, siguiendo un orden secuencial.

Durante los dos primeros meses ha tenido lugar una etapa formativa, que ha servido tanto de introducción como para una primera toma de contacto. Durante este tiempo el autor ha ido adquiriendo una base de conocimiento acerca de aspectos sobre la privacidad, la ingeniería software y la ingeniería de requisitos.

Ello ha sido posible gracias a artículos de carácter general e informativo. Éstos van recopilando el estado del arte en materia de privacidad, a la vez que explican conceptos y definiciones comunes para un lector no especializado. Tal es el caso de [25], artículo publicado en diciembre del 2014 por la agencia europea ‘ENISA<sup>9</sup>’, que ofrece una perspectiva amplia del estado de la seguridad y privacidad hasta día de hoy.

Tras la formación y obtención de dicha base de conocimiento se ha continuado con la etapa de búsqueda documental. Dicha etapa ha ocupado un tiempo de uno a dos meses, durante los cuales el autor ha ido aprovisionándose y seleccionando las referencias más relevantes para el trabajo de acuerdo a unos criterios. Dicha etapa se describe con mayor detalle en el capítulo ‘Búsqueda documental’.

En la etapa de análisis, se ha dedicado un mes a la lectura y comparación de referencias mediante una plantilla de análisis. Dicha plantilla es una hoja con los aspectos tanto comunes como específicos que caracterizan a cada metodología. Cada uno de estos aspectos es puesto más adelante en una tabla comparativa de resultados, según apliquen. Tanto dicha plantilla como los resultados del trabajo se describen en detalle en la sección ‘Análisis y resultados’.

Finalmente se ha seguido con la etapa de documentación, validación y maquetación del trabajo, la cual ha abarcado aproximadamente un mes.

Teniendo en cuenta un ritmo de trabajo de 12 horas semanales en media, el esfuerzo por cada actividad del TFM se distribuye como se muestra en la Tabla 1: Planificación del TFM.

<b>Actividad</b>	<b>Horas</b>
<b>Búsqueda documental</b>	75
<b>Análisis</b>	100
<b>Resultados</b>	50
<b>Documentación</b>	50
<b>TOTAL</b>	<b>275</b>

Tabla 1: Planificación del TFM

---

<sup>9</sup> ‘European Union Agency for Network and Information Security’.

## 4 PROCEDIMIENTO DEL TRABAJO

---

A continuación se describirá el procedimiento de la realización del trabajo. Se comenzará explicando la revisión sistemática de literatura (SLR) y el de estudio sistemático de literatura (SLS). Con estos dos conceptos en mente, el lector entenderá que el Trabajo Fin de Máster sea afín al segundo, ya que la temática escogida aún carece del nivel suficiente de madurez como para facilitar los resultados que requiere una SLR.

Seguidamente se definirá el tema del área de investigación y pasará a explicarse en detalle la búsqueda documental, en donde se detallará el porqué de las fuentes escogidas frente a las descartadas. Además, se provee al final de una sección acerca de trabajos relacionados, donde se aporta el valor diferencial de éste, frente a otros artículos de análisis y estado del arte de metodologías.

Finalmente se hablará de la evaluación de los artículos seleccionados, es decir, el análisis de los mismos; y cómo se ha llevado a cabo el proceso de síntesis.

### 4.1 LA REVISIÓN SISTEMÁTICA DE LITERATURA (SLR)

Una revisión de la literatura es una descripción del estado actual del arte en un área determinada de conocimiento. Ésta debe evaluar de forma crítica las distintas fuentes teóricas y estudios de investigación más relevantes en la materia. En el caso de un artículo, deberá ir un paso más allá incluyendo una contribución al conocimiento por parte de su autor [26].

En cuanto al término *sistemática*, hace referencia a la recolección y revisión de dicha literatura usando explícitamente métodos que puedan ser verificados de manera independiente [27]. Por lo tanto, en una revisión de la literatura estarán documentados todos los procedimientos que se lleven a cabo, facilitando la completa reproducibilidad del estudio.

Cuando se sigue una lista de una base de datos de referencias (i.e. Google Scholar, IEEE Xplore,...) o se salta directamente a citas de un determinado artículo, se necesita un sistema para guardar estos datos bibliográficos: autor, fecha, título del artículo o capítulo, publicación, volumen, ISSN/ISBN, edición, etc. Adicionalmente se debería anotar ciertos comentarios sobre el contenido, que en su mayoría indicarán un futuro análisis más profundo.

En una revisión sistemática de la literatura (en adelante SLR<sup>10</sup>) se encuentran dos propósitos principales:

1. Mostrar el *interés* en el estado del arte de un campo particular. Esto no sólo compete a quién ha escrito qué, sino a toda la investigación empírica que hay hasta la fecha, posiciones teóricas, controversias y avances, así como enlaces a otras áreas de conocimiento relacionadas.
2. Ofrecer una *base de conocimiento* al autor de una investigación. En el proceso de revisión de la literatura, de acuerdo con [28] se debería incluir un motivo de la elección de dicho problema de investigación, así como la metodología de trabajo escogida. Debería ayudar al investigador a definir las hipótesis o preguntas de investigación, mostrándole que, dando respuesta a esas preguntas, contribuiría en efecto al avance

---

<sup>10</sup> Del inglés: 'Systematic Literature Review'.



en el conocimiento de la materia. Por otro lado puede servirle además para dar una visión particular, apoyar los argumentos o encontrar nuevas carencias.

Según se indica en [26], a la hora de realizar una SLR se distinguen cuatro pasos comunes (con independencia del campo de conocimiento al que aplique ésta):

1. Definir el tema del área de investigación.
2. Localizar la literatura clave al respecto (búsqueda documental).
3. Analizar la literatura.
4. Estructurar y escribir la revisión de la literatura.

En cuanto al primero, el tema de investigación podría ser en sus inicios más o menos amplio, ya que es en la propia revisión de literatura donde se va a redefinir la temática, ajustándose adecuadamente a una determinada extensión, y enmarcándose en una o más preguntas particulares.

En cuanto al segundo, empieza usando palabras clave y buscando términos en las principales bases de datos más relevantes, pudiendo también buscar en alguna particular (fruto de fuentes recomendadas o ya conocidas).

El resultado de este paso es una serie de resúmenes o *abstracts* que, de nuevo, tendrán que ser filtrados para terminar con una selección más objetiva y científica. A todo este proceso de aprovisionamiento de referencias se le conoce también como búsqueda documental.

Ya en el tercer paso los artículos seleccionados son leídos y resumidos, poniendo especial interés en aquéllas notas que se han ido añadiendo durante su lectura.

Finalmente en el cuarto y último paso se estructura y escribe el trabajo de acuerdo a lo que se ha ido averiguando a lo largo del proceso entero.

## **4.2 EL ESTUDIO SISTEMÁTICO DE LITERATURA (SLS)**

En esta sección se describirá el procedimiento que se llevó a cabo en el presente trabajo, a raíz de particularizar lo anteriormente dicho al campo de la ingeniería de la privacidad.

Puesto que la ingeniería de requisitos aplicada al campo de la privacidad es, precisamente, un tema en vías de investigación, no es posible encontrar una metodología de obtención de este tipo de requisitos con la suficiente madurez. Ello implica que no puedan presentarse resultados requeridos en una SLR, y se tenga que optar por un enfoque ligeramente distinto para este trabajo.

En esencia, un estudio sistemático de la literatura (en adelante SLS<sup>11</sup>) consiste en la realización de una SLR, donde las referencias empleadas carecen de resultados o evidencias medibles, y aportan únicamente conocimiento de estudios teóricos. Este tipo de estudio es el que finalmente se llevará a cabo en el presente Trabajo Fin de Máster.

## **4.3 DEFINICIÓN DEL TEMA DEL ÁREA DE INVESTIGACIÓN**

El área de investigación escogida es la ingeniería de la privacidad. Como es de esperar, inicialmente esta área es muy amplia y toca a su vez multitud de temáticas. Sin embargo, a lo largo del proceso de búsqueda documental se habrá ido afinando más en los procesos de

---

<sup>11</sup> Del inglés: 'Systematic Literature Survey'.

desarrollo de sistemas, y particularmente en el proceso de adquisición de requisitos de privacidad.

La elección del tema en concreto a tratar fue posible gracias a una búsqueda documental preliminar de la literatura sobre ingeniería de la privacidad. Esta primera fase pretendió empaparse del conocimiento necesario para posteriormente detectar vacíos, donde posteriormente pudo haber una revisión más profunda de dicho tema de investigación.

A partir de este punto se encuentran referencias como [29]–[33], las cuales se centran en establecer metodologías o marcos de trabajo para la obtención sistemática de requisitos de privacidad. En otros casos como en [34], [35], se realiza un resumen de algunas de ellas, que finalmente se exponen en una tabla de acuerdo a unos criterios comparativos.

Este trabajo de investigación se centra en la misma idea, esto es, a la hora de obtener requisitos de privacidad durante el desarrollo de un sistema, qué metodologías o marcos de trabajo encontramos hoy en día, y de acuerdo a ciertos criterios<sup>12</sup>, cuál o cuáles serían óptimas para distintas circunstancias (i.e. empresas o particulares, mucha o poca madurez, etc.).

## 4.4 BÚSQUEDA DOCUMENTAL

Una vez decidido el tema de investigación: metodologías y marcos de trabajo sobre la obtención de requisitos de privacidad durante el proceso de desarrollo de un sistema, se procede al segundo avance, cuyo objetivo principal es localizar la literatura clave que hay al respecto.

En adelante se identifican y describen las etapas que conforman este proceso particularizado a nuestro tema de investigación.

### 4.4.1 Términos de búsqueda e Identificación de artículos

1. Se enuncia el tema a revisar:

“Métodos de obtención de requisitos de privacidad en el proceso de desarrollo de un sistema.”

2. Se identifican las palabras clave:

*‘métodos’, ‘obtención’, ‘requisitos’, ‘privacidad’, ‘proceso’, ‘desarrollo’ y ‘sistema’.*

3. Se ordenan por importancia o generalidad:

*‘privacidad’, ‘requisitos’, ‘obtención’, ‘método’, ‘sistema’, ‘proceso’, ‘desarrollo’.*

4. LA DOCUMENTACIÓN SE ENCUENTRA EN INGLÉS. LAS PALABRAS CLAVE QUEDARÍAN:

*‘privacy’, ‘requirement’, ‘elicitation’, ‘method’, ‘system’, ‘process’, ‘design’<sup>13</sup>.*

---

<sup>12</sup> Se espera definir dichos criterios más tarde, de acuerdo a la información obtenida del análisis de las referencias que se escojan fruto de la búsqueda documental.

<sup>13</sup> Aunque la palabra ‘desarrollo’ en inglés se traduzca como ‘development’, de cara a la ingeniería de requisitos su uso hace referencia a sistemas explícitamente software. Por este motivo se ha decidido cambiarla por la palabra ‘design’ (diseño) que, en la jerga anglosajona, engloba todo el proceso de desarrollo de un sistema general – no sólo software.

A continuación se añaden manualmente las posibles palabras clave que vemos que pueden añadir referencias relevantes. Este es el caso del anglicismo *'framework'*<sup>14</sup>, que complementa a la palabra *'method'*. La lista de palabras clave queda entonces como sigue:

***'privacy', 'requirement', 'elicitation', 'method', 'framework', 'system', 'process', 'design'.***

Teniendo la lista de palabras clave final, pasamos a elaborar la lista de los términos de búsqueda. Una buena manera de hacerlo se propone en [27], que consiste relacionar o combinar las palabras clave mediante operaciones booleanas como sigue:

***privacy AND requirement AND (elicitation AND/OR method AND/OR framework AND/OR system AND/OR process AND/OR design).***

Saliendo términos de búsqueda como:

- 'Privacy requirement'.
- 'Privacy requirement elicitation method'.
- 'Privacy requirement elicitation framework'.
- ...

Adicionalmente se añaden los términos de búsqueda manualmente, aquéllos que se ha visto anteriormente que aportan buenas referencias:

- Privacy engineering.

Los términos de búsqueda fijados se muestran a continuación:

1. 'Privacy requirement framework'
2. 'Privacy requirement method'
3. 'Privacy requirement elicitation'
4. 'Privacy requirement design'

#### **4.4.2 Bibliografía, bases de datos, motores de búsqueda y gestores de referencias**

Un punto a tener en cuenta es que la investigación sobre la ingeniería de la privacidad se encuentra todavía en auge. En cuanto a los libros que hay a día de hoy destacan [36] y [37]. Éstos tratan sobre la privacidad a muy alto nivel, o bien se centran en ontologías y marcos de trabajo para definir términos; en ningún caso se facilita metodología alguna para aplicarla en un ciclo de vida software.

Por el momento en los libros referentes de las diversas temáticas relacionadas, como la ingeniería del software, se aprecian apenas breves menciones a la privacidad. Por ejemplo en [38] éstas se encuentran dentro de los requisitos no funcionales que tienen que ver con la seguridad. Incluso dentro de los organismos de estandarización como es el IETF, la privacidad se ha considerado como un tema transversal que, según ellos, merece una RFC aparte [39].

Por esta razón el trabajo se centra en la búsqueda de artículos científicos publicados en revistas y consorcios, usando como principales motores de búsqueda Google Scholar e IEEE eXplore, como gestor de referencias Mendeley y, como selector de revistas, la plataforma *'Web Of Knowledge'*.

---

<sup>14</sup> En español, marco de trabajo.

#### **4.4.3 Filtros de inclusión y exclusión**

Siguiendo los pasos anteriores se espera encontrar más de cien referencias, sobre las cuales se hará una selección para ser evaluadas y sintetizadas posteriormente. De las referencias seleccionadas se estima que serán alrededor de cincuenta o setenta de ellas.

Para incluir un artículo a la lista de referencias seleccionadas, deberá cumplir los siguientes criterios:

1. Aplicar a aspectos de privacidad.
2. Tener en cuenta como mínimo la actividad de obtención de requisitos.
3. Estar probada empíricamente (casos prácticos).
4. Aplicar a un dominio general.

#### **4.4.4 Sobre los artículos descartados**

La búsqueda documental ha dado como resultado una serie de artículos relevantes, aunque no todos ellos aplican directamente al objetivo del Trabajo Fin de Máster. Recordemos que este último trata de hacer un análisis comparativo de las metodologías de obtención de requisitos de privacidad, de carácter general; es decir, que pueden aplicarse a cualquier dominio y, como mínimo, indican los pasos a seguir para obtener requisitos.

Dicho lo anterior, muchas referencias tienen como objetivo ofrecer información del estado del arte [40]–[49]. Estas últimas han sido descartadas tras haber escogido como más relevantes [6], [25], [34], [35], [47], [48] (incluyen ya toda la información provista por las descartadas).

Por otro lado se encuentran aquellas descartadas porque aplican a un dominio muy concreto como son aplicaciones de comercio electrónico, páginas web, ‘data mining’, sistemas sanitarios, etc. [50]–[59].

También se han descartado aquellas metodologías que no obtienen requisitos de privacidad, aunque sí pueden aplicar a otras actividades como especificación y gestión de los mismos. Este es el caso de artículos como [60]–[63], la mayoría de los cuales se centran en requisitos de seguridad, y dejan a los requisitos de privacidad en un segundo plano. Esto hace que no se pueda garantizar una cobertura razonable, pues los requisitos de privacidad no son más que un objetivo derivado del principal.

Otros artículos como [31], [50], [62], [64] hablan de la privacidad en exclusiva, centrándose en técnicas de mejora de la misma (PETs) y buenas prácticas, pero no de cómo obtener los requisitos que finalmente lleven a implantar dichas técnicas. Cabe destacar que referencias como [63], [65], [66] sí que hablan de los requisitos de privacidad aunque, como se ha dicho, no de su obtención sino de su análisis o gestión.

Finalmente se hace mención de la referencia [67], la cual aun siendo descartada por no ser una metodología de obtención de requisitos, sí es importante por ser la única aportada al respecto por un organismo de estandarización como es OASIS.

Con respecto a los organismos de estandarización, se ha buscado en el mencionado OASIS, ISO, W3C, ITU-T, IETF, IEEE, ETSI, CEN/CENELEC, ECMA y NISTA. No se han encontrado resultados de metodologías de privacidad dentro de los mismos, aunque sí información relevante para este Trabajo Fin de Máster: ISO [68], [69]; NIST [70]; e IETF [39].

#### 4.4.5 Otros trabajos relacionados

De entre las referencias encontradas se puede distinguir dos tipos. Por un lado las referencias primarias, que son aquéllas que hablan acerca de una metodología o marco de trabajo en particular, constituyendo una fuente de información directa del autor sobre la misma. Por el otro lado se encuentran las referencias secundarias que, a diferencia de las primeras, pueden ser artículos cuyos autores hablen de una metodología o marco de trabajo de otros (citando convenientemente la fuente primaria). Proveen información (a menudo resumida), no siendo la fuente directa.

Respecto de estos últimos, es fácil encontrarse con artículos sobre el estado del arte en una materia, revisiones o estudios sistemáticos. Un ejemplo de ello es [34], cuyo trabajo es similar en objetivos a este Trabajo Fin de Máster.

A diferencia de [34], en donde se hace únicamente una comparativa entre LINDDUN [15], PriS [32] y el marco de trabajo 'Privacy-friendly' [6], este documento resulta ser una búsqueda actualizada y más sucinta de metodologías de privacidad, dejando de lado aquéllas que son exclusivas de la seguridad. Por un lado no se especifica el motivo por el que el autor no añade más metodologías a su lista (aparte de las tres mencionadas); y por otro lado, se provee de unos criterios de comparación distintos, que pueden verse en la sección de 'Análisis y resultados'.

El artículo que más parecido tiene respecto a este trabajo es [35]. En efecto, los autores hacen un análisis comparativo de las metodologías de privacidad conocidas hasta el 2009; si bien las escogidas siguen un criterio no tan estricto, ya que se incluyen entre ellas metodologías exclusivas de la seguridad como 'M-N' e 'i\*'. Ambas se dicen de poder ser utilizadas en el dominio de la privacidad, pero no se ha encontrado ningún artículo que haga tal uso de ellas, con las correspondientes evidencias prácticas que suelen tener al final este tipo de trabajos. Además, verá el lector que aquí se ofrece un marco comparativo bastante más amplio en la sección 'Análisis y resultados'.

De esta manera, las metodologías descartadas quedarían como se indica en la siguiente tabla:

METODOLOGÍA	MOTIVO DE DESCARTE
I* [71]	Falta de evidencias de uso. Exclusiva de seguridad.
KAOS [72]	Falta de evidencias de uso. Exclusiva de seguridad.
M-N [73]	Falta de evidencias de uso. Exclusiva de seguridad.
GBRAM [74]	Falta de evidencias de uso. Dominio concreto.
B-S [75]	Dominio concreto. Ya forma parte de STRAP.

Tabla 2: Metodologías descartadas

#### 4.4.6 Resumen de la búsqueda documental y resultados

Todo este proceso de búsqueda da como resultado una serie de *abstracts* ya seleccionados, que de nuevo pueden volver a ser filtrados para una selección más objetiva y científica.

Puesto que se dispone de un marco temporal limitado para la realización del trabajo, es necesario establecer cuándo y dónde parar. Según [26], lo ideal es continuar buscando hasta el punto en que no se encuentre nueva información al respecto. Esto es, que mientras se sigan encontrando puntos de vista distintos (nuevas metodologías o marcos de trabajo en nuestro caso), el proceso de búsqueda debe continuar.

#### **4.4.6.1 Primera iteración**

En esta primera iteración se comprueba que, en efecto, una gran muestra de artículos incluyen a la privacidad dentro de la seguridad. De cara a evitar excluir accidentalmente una referencia que trate sobre la obtención de requisitos de privacidad, aun siendo un requisito de seguridad para el autor, se han incluido algunos métodos de obtención de requisitos de seguridad.

Por otro lado, se encuentran artículos que se centran en la obtención de requisitos de privacidad en exclusiva, creando un framework o conjunto de técnicas para una circunstancia concreta: aplicaciones que utilicen redes WiFi, acceso anonimizado a bases de datos, sistemas o software sanitario, sistemas que cumplan con la legislación, etc.

Juntando estos tres tipos de resultados, los criterios de selección para esta primera iteración son:

- *Resultados genéricos sobre el estado del arte de ingeniería de requisitos de privacidad.*
- *Resultados de metodologías acerca de ingeniería de requisitos aplicada a la seguridad y/o privacidad.*
- *Resultados de frameworks acerca de ingeniería de requisitos aplicada a la seguridad y/o privacidad en aplicaciones concretas.*

Finalmente se añaden aquéllas referencias ya conocidas previamente y las encontradas en los organismos de estandarización.

Número total de referencias encontradas<sup>15</sup>: 90.

#### **4.4.6.2 Segunda iteración**

Puesto que el objetivo es quedarse con las referencias más relevantes, se hace necesario seleccionar nuevamente un subconjunto específico de las anteriores, acotando más todavía los criterios de selección.

En la primera iteración se obtuvieron 30 resultados de carácter generalista con el término 'Privacy requirement engineering', por lo que en esta iteración se restringe únicamente a 3 artículos (los más relevantes).

Ahora, para esta segunda iteración los criterios de selección de artículos quedan<sup>16</sup>:

- *Resultados genéricos sobre el estado del arte de ingeniería de requisitos de privacidad – no más de 3.*
- *Resultados de metodologías de obtención de requisitos de seguridad y privacidad.*
- *Frameworks de obtención de requisitos de privacidad para aplicaciones concretas.*

En la segunda iteración se pone más cuidado en que se informe sobre mecanismos de obtención de requisitos de privacidad, no de soluciones a su implementación. Además, nos fijamos sólo en los marcos de trabajo que tienen que ver única y exclusivamente con la privacidad, excluyendo a la seguridad. Adicionalmente, se decide incluir también las referencias encontradas en los organismos de estandarización, ya que únicamente se ha encontrado una y puede ser digna de mención futura.

---

<sup>15</sup> Agregación de los resultados obtenidos por Google Scholar (68), los organismos de estandarización (1) y anteriores (21).

<sup>16</sup> Nótese que los resultados sobre el estado del arte han sido excluidos.

Número total de referencias seleccionadas en la segunda iteración<sup>17</sup>: 60.

#### 4.4.6.3 Tercera iteración

En la anterior iteración se ha conseguido reducir significativamente el número de referencias especificando más los criterios de selección. Dado que se tienen 60 referencias y aún puede particularizarse más dichos criterios, se realiza una tercera iteración con el fin de llegar a resultados más específicos y detallados para el trabajo.

Los criterios de inclusión de esta tercera iteración quedan como sigue:

- *Resultados genéricos sobre el estado del arte de ingeniería de requisitos de privacidad (los 3 más relevantes).*
- *Resultados de metodologías de obtención de requisitos de privacidad.*
- *Frameworks de obtención de requisitos de privacidad para aplicaciones concretas.*

Cabe destacar que se ha tenido en cuenta las metodologías que explícitamente están enfocadas a la obtención de requisitos de privacidad, excluyendo aquellas más afines al mundo de la seguridad. Se incluyen, como se indicó en previas iteraciones, las referencias anteriores y las encontradas en los organismos de estandarización.

Número total de referencias seleccionadas en la tercera iteración<sup>18</sup>: 49.

#### 4.4.7 Selección final y resultado de la búsqueda

Dentro de las 49 referencias anteriores se han podido encontrar 14 referencias sobre metodologías de obtención de requisitos de privacidad, y todas ellas no se cierran a un dominio en concreto. Siguiendo el esquema de los apartados anteriores, serían referencias que siguen el siguiente criterio en exclusiva:

- *Resultados de metodologías de obtención de requisitos de privacidad (dominio genéricos).*

A continuación en la tabla de abajo se muestran, a modo de resumen, el número de referencias que se han tenido en cuenta durante todo el proceso de búsqueda documental (de acuerdo a los criterios establecidos en dicha sección). Todas estas referencias se facilitan en los anexos de este trabajo.

La diferencia entre 'selección final' y 'total metodologías' radica en que algunas de las referencias aluden a la misma metodología o mezcla de otras, siendo el 'total metodologías' las que realmente aportan conocimiento y han sido comparadas en los resultados de este Trabajo Fin de Máster.

Iteración 1	Iteración 2	Iteración 3	Selección final	Total metodologías
90	60	49	14	9

Tabla 3: Número de referencias por etapas

<sup>17</sup> Agregación de los resultados obtenidos en la segunda iteración (38), los organismos de estandarización (1) y anteriores referencias (21).

<sup>18</sup> Agregación de los resultados obtenidos en la tercera iteración (27), los organismos de estandarización (1) y anteriores referencias (21).

## 4.5 EVALUACIÓN DE LOS ARTÍCULOS SELECCIONADOS Y SÍNTESIS

Como se ha dicho en el punto anterior, en esta fase del trabajo se ha de tener ya una larga lista de referencias ya seleccionadas con sus *abstracts*. El propósito principal es el de leerlas y evaluarlas de una manera metódica.

Sobre la lectura y evaluación, se procederá a ir añadiendo notas en las partes de especial interés, teniendo en cuenta que es en ese momento cuando se han de encontrar criterios con que pueden compararse las distintas metodologías, de cara a la siguiente fase de síntesis de las referencias.

Además, se utilizará una plantilla a modo de resumen de cada metodología. Dicha plantilla servirá para una posterior comparativa entre ellas que se pondrá como resultados del trabajo. La plantilla puede verse en el anexo 'Plantilla de análisis'.

En la fase de síntesis se espera tener los resultados de nuestro trabajo. Dichos resultados estarán orientados a una comparativa entre metodologías, atendiendo a los criterios que se elijan durante la fase de lectura.

Como se explica en [27] y en [76], hay tres tipos de síntesis que pueden llevarse a cabo:

- Estadística o numérica<sup>19</sup>: Se ofrecen los resultados de la investigación numéricamente, fruto de pruebas estadísticas.
- Narrativa: Los resultados son resumidos verbalmente y organizados de acuerdo a unos criterios.
- Conceptual: Se propone un nuevo concepto en base a otros citados en el artículo.

El objetivo del trabajo es afín a la síntesis del tipo *narrativa*, ya que se espera comparar las distintas metodologías y marcos de trabajo encontrados, en consonancia con a los criterios elegidos en la fase de evaluación de los artículos. Finalmente se llegará a hacer una tabla comparativa de los resultados obtenidos.

---

<sup>19</sup> También conocida como meta-análisis, ya que en ellas se analiza también cómo se ha llevado a cabo el análisis estadístico publicado.



## 5 METODOLOGÍAS DE OBTENCIÓN DE REQUISITOS PARA LA PRIVACIDAD

---

A continuación se describen las metodologías obtenidas de modo general. Un lector curioso puede encontrar información más detallada dentro de cada referencia a la metodología en cuestión. Así pues, las metodologías explicadas son LINDDUN [15], NFR [79]–[81], PriS [32], RBAC [83], Tropos y GSRM [84] (marco de trabajo mixto), STRAP [30], PRET [89], marco de trabajo ‘Privacy-Friendly [6] y PRIPARE [90].

### 5.1 LINDDUN

En una publicación de la revista ‘Requirements Engineering’ del año 2011, Mina Deng et al. [15] proponen esta metodología como un marco de trabajo orientado a la obtención de requisitos de privacidad. Por su parte, Kristian Beckers la describe en su artículo *“Comparing privacy requirements engineering approaches”* [34] junto con otras tres que él mismo consideró más relevantes ([6], [32], [77]).

La metodología puede considerarse una aplicación en el mundo de la privacidad de lo que ya se conocía como su referente en el mundo de la seguridad: STRIDE. Su nombre, LINDDUN, es el acrónimo de *“Linkability”, “Identifiability”, “Non-repudiation”, “Detectability”, “information Disclosure”, “content Unawareness”* y *“policy/consent Non-compliance”*. Éstas son propiedades deseables que ha de tener un sistema a la hora de poder garantizar la privacidad, aunque en pocas situaciones aplican todas ellas.

El dominio de aplicación no está definido para uno en particular, sino que propone una solución general a cualquier sistema dentro del entorno de ingeniería software. En [15] encontramos como ejemplo un caso práctico de la aplicación de la metodología en una red social ficticia que los autores llaman ‘Social Network 2.0’. Más que aportar una evidencia de uso como tal, trata de clarificar los conceptos teóricos del artículo de una forma menos conceptual y más pragmática, intercalando el ejemplo a medida que va avanzando en cada sección.

No obstante, en el año 2014 tres de los autores de esta metodología aportan ya evidencias empíricas reales mediante tres estudios experimentales descritos en [78]. Los dos primeros estaban orientados a probar dicha metodología en distintas etapas del desarrollo software, a nivel de requisitos y a nivel de arquitectura (diseño) respectivamente. Fueron desarrollados por alumnos de máster de Ingeniería Computacional y Telecomunicaciones (Universidad de Trento), y alumnos de máster de Ciencia Computacional (KU Leuven en Bélgica), con ambos resultados satisfactorios.

En cambio, el último buscaba señalar la robustez de la misma, evaluando si LINDDUN podría dejar olvidada alguna amenaza en su proceso, la cual podría haber sido descubierta de otra manera por expertos en privacidad. La conclusión de este último afirma que la metodología tiene una fiabilidad del 63%, por lo que no se podría considerar aún como una metodología del todo fiable.

En el artículo se ofrece un trasfondo detallado acerca de los aspectos de la privacidad y la frontera que comparte con el mundo de la seguridad, apelando a la necesidad de formalizar un proceso sistemático de obtención de requisitos de privacidad.

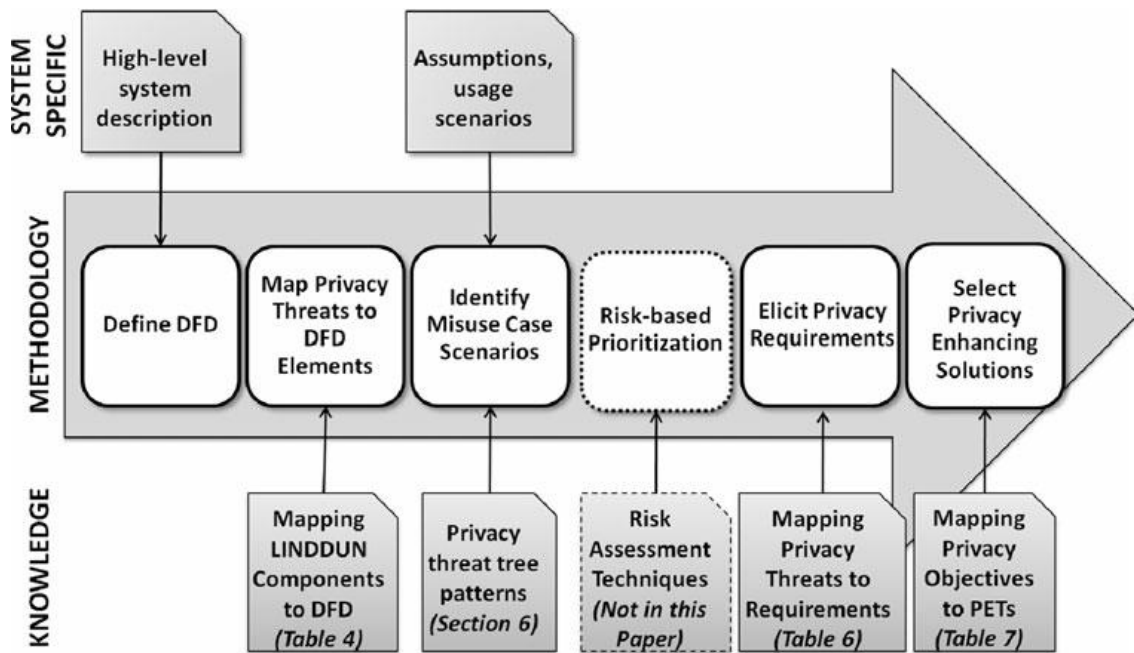


Ilustración 2: Esquema de LINDDUN de [15]

Se parte inicialmente de uno o varios grafos denominados diagramas de flujo de datos. En ellos se describen los contenedores y canales por los que fluye información sensible, a fin de identificar posible amenazas respecto de los mismos. Estas últimas se visualizan y relacionan entre sí con ayuda de otro grafo conocido como árbol de amenazas.

Los árboles de amenazas siguen a menudo la misma estructura, por lo que los autores los agrupan en patrones de amenazas. Por esta misma razón, y desde el punto de vista de ingeniería de requisitos, se puede afirmar que la metodología adopta tanto un enfoque basado en riesgos o amenazas, como uno heurístico basado en patrones ya conocidos de éstas.

Como ejemplos de patrones de árboles de amenazas está el de ‘manipulación con procesamiento’, ‘spoofing con entidad externa’ o ‘relación de entidad’<sup>20</sup>.

Desde un punto de vista de la ingeniería de requisitos, LINDDUN adquiere protagonismo en las actividades de obtención, identificación, modelado y gestión de requisitos.

Frente a la ingeniería software, se trata de una metodología que aplica al análisis de requisitos, el diseño y la implementación. Respecto a la evaluación de impacto no se provee de un método concreto, aunque se cita su gran utilidad de cara al desarrollador que quiera integrar este proceso.

<sup>20</sup> Linkability of entity.

## 5.2 NFR

Este método surgió en el año 2000 también del mundo de la seguridad (obtención de requisitos). Su nombre NFR [79]–[81] es debido a que los requisitos de privacidad son considerados no funcionales, ya que no aportarían a priori ningún valor adicional para el cliente, aunque sí es necesaria por cualquier otra razón (por ejemplo, la legislación del país).

Así pues, tratándose de un método orientado a objetivos, puede ser tenido en cuenta en cualquier parte del proceso de desarrollo, aunque la mayoría de veces se hace en las etapas más tempranas.

Al ser requisitos no funcionales, estos objetivos ('goals'), pasarán a llamarse objetivos blandos ('softgoals'), en un modelo que se conoce como Grafo de interdependencias entre requisitos (SIG) del sistema completo.

Dicho modelo ordena cada requisito por niveles, y los relaciona entre sí con enlaces. Cada enlace representa una interdependencia, y da pie a un refinamiento hacia un requisito más específico (nivel más bajo). Puede haber interdependencias entre requisitos de distintos niveles. Al final, se evalúan en conjunto tanto 'softgoals' como interdependencias para obtener los deseados requisitos de privacidad.

Se pueden usar grafos tipo, según la naturaleza de los requisitos que quieran obtenerse. Además utiliza UML como lenguaje de especificación junto con extensiones de éste. Existen ya catálogos de grafos específicos para la obtención requisitos de seguridad y privacidad, lo que reafirma el enfoque heurístico que sigue esta metodología.

En cuanto a si adoptar este método o no en el mundo empresarial, éste resulta ser un proceso de obtención de requisitos de privacidad y seguridad muy conocido y experimentado, por lo que su uso es bastante recomendable. Tanto el usuario como el organismo regulador, deberán ser modelados como un nodo cada uno del grafo, si se quieren tener en cuenta.

En el ámbito de la ingeniería de requisitos, esta metodología aplica en la obtención, identificación, análisis y especificación; sin llegar a meterse en el modelado del sistema.

Desde el punto de vista del ingeniero software, NFR constituye una metodología que aplica al análisis de requisitos y al diseño; aunque este último sólo en parte (diagramas conceptuales de dominio y diagramas de clases).

Finalmente y como era de esperar, esta metodología que ya parte de la experiencia del mundo de seguridad aporta hasta tres casos de estudio para corroborar su robustez. No obstante cabe destacar que gran parte de los requisitos que se obtienen siguen siendo de seguridad, dejado aún a los de privacidad en segundo plano.

### 5.3 PRIS

Los autores Christos Kolloniatis y Evangelia Kavakli publicaron en el año 2008 una forma de abordar la privacidad durante la fase del diseño de un sistema, en la revista Requirements Engineering. Este método conocido como PriS [32] resulta el acrónimo de ‘privacy safeguard’, y nace de un entorno de seguridad siguiendo un enfoque orientado a objetivos (aka. ‘goal-oriented’).

El fin último de esta metodología consiste en descubrir requisitos relevantes de privacidad que puedan tener repercusiones a nivel de negocio en un sistema. Los pasos que se llevan a cabo se resumen a continuación.

Primeramente se centra en la realización de un modelo conceptual del negocio con 7 elementos críticos bien definidos: clientes, procesos, objetivos, objetivos internos, objetivos de privacidad de usuario, requisitos de privacidad y patrones de procesos.

A continuación, se pasa al análisis del impacto de estos elementos u objetivos. Esto es, analizar el riesgo de cada uno de ellos, valorando qué impacto tendría cada caso, qué probabilidad tienen de ocurrencia, y cómo debería abordarse según qué escenarios.

Finalmente se termina por construir un grafo de objetivos que tapen las posibles brechas de privacidad más relevantes del negocio, así como las relaciones que tienen entre sí.

Este método tiene bastante en cuenta al usuario final del sistema, el cual se describe como una de las posibles partes interesadas (en efecto, es uno de los 7 puntos críticos que se enunciaron anteriormente). Los organismos de regulación son también tenidos en cuenta. Éstos, según el país o región, van añadiendo e imponiendo nuevos requisitos a tener en cuenta de cara a la privacidad.

Tanto desde este último punto de vista del organismo regulador, como del de una corporación, PriS valora desde un principio si merece la pena o no garantizar ciertos requisitos de privacidad, pudiendo resultar aceptable para la empresa el riesgo derivado de su

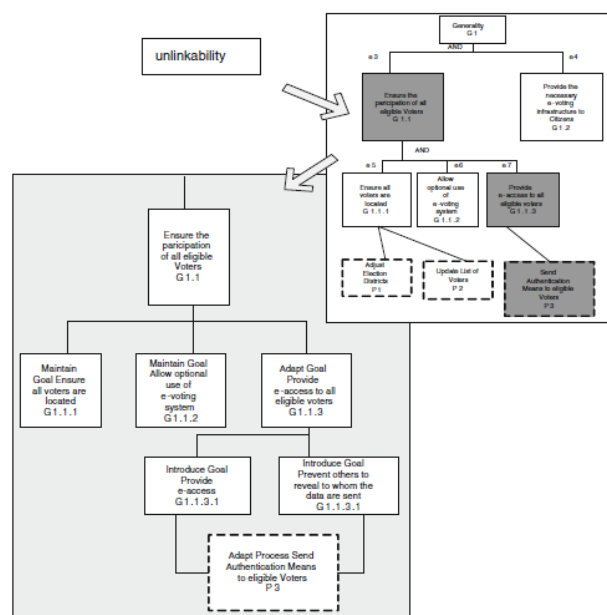


Ilustración 3: Análisis de impacto del objetivo 'Unlinkability' de [32]

incumplimiento. Por ello es necesario el conocimiento pleno de la situación interna de dicha empresa y de su entorno, siendo recomendable su uso sólo para aquéllas con expertos en análisis de riesgos, abogados, etc., así como cierta experiencia previa en el mercado.

Las actividades de ingeniería de requisitos que son llevadas a cabo en esta metodología van desde la fase más temprana de obtención de requisitos hasta el modelado del sistema (se incluyen la identificación, análisis y especificación de los mismos). Quizá sea esta última actividad de modelado del sistema lo que la hace ser tan especial, ya que provee técnicas para la implementación de ciertos requisitos.

En cuanto a las actividades que engloba dentro de la ingeniería software, éstas son el análisis de requisitos, el diseño, la implementación y, como valor añadido, la evaluación de impacto.

Finalmente, se añade como caso práctico un ejemplo de aplicación de voto electrónico. Cabe destacar que los mismos autores han ido trabajando en futuros artículos como [82] (2007), para aportar más evidencias empíricas (aunque en este caso resulte en el mismo ejemplo de aplicación de voto electrónico anterior).

## 5.4 RBAC

En el año 2003, Dongwang Shin et al. siguieron con la idea de utilizar procesos ya conocidos del mundo de la seguridad para la obtención de requisitos de privacidad. Uno de los resultados es el método RBAC [83], abreviatura de 'Role-Based Access Control' (control de acceso basado en roles).

Se trata de un método orientado a 'role-agent', por el que los agentes del sistema son identificados con sus roles y permisos junto con tres elementos relacionados directamente con la privacidad: el propósito de acceso a los datos, las condiciones para acceder y las obligaciones del que accede.

Propone un proceso de obtención de dichos elementos de privacidad dividido en dos fases:

'Role Permission Analysis' (RPA). Análisis del nivel de permiso del rol.

'Role Permission Refinement' (RPR). Refinamiento del nivel de permiso del rol.

Ambos se centran en lo mismo: qué roles tienen qué permisos, aunque con diferentes niveles de abstracción (siendo RPA más general que RPR).

Se trata de una metodología enfocada a roles y objetivos, que obtiene y define los requisitos de forma textual. Esto lo hace con la ayuda de un álgebra, usando tuplas como <usuario, rol, permiso> ó <propósito, condición, obligación>.

Utiliza además políticas de privacidad y tiene una gran complementariedad con ciertos requisitos provenientes del mundo legal. De hecho, el caso práctico que propone no es más que un ejemplo de sistema de salud, un sector de la industria y servicios donde ha de ponerse especial cuidado en los requisitos que imponga la regulación competente.

Respecto a la ingeniería de requisitos, las actividades involucradas en esta metodología son la obtención, identificación, análisis y especificación de los requisitos; y no se mete en la parte de modelado como sí lo hacen otras metodologías (LINDDUN, Pris,...).

La ingeniería software contempla a esta metodología únicamente como un proceso de análisis de requisitos, puesto que no ofrece unas guías para el diseño, y mucho menos técnicas para implementar alguno de los requisitos obtenidos.

Por último se añade a modo de comentario de sus autores que el dominio de esta metodología puede ser genérico, aunque inicialmente fue desarrollada para aplicaciones del sector sanitario (donde se ha validado hasta ahora con casos prácticos en [83]).

## 5.5 FRAMEWORK TROPOS Y GSRM

En el año 2010, Shareeful Islam et al. publicaron un artículo en la revista 'Requirements Engineering' sobre un marco de trabajo [84] que obtiene tanto requisitos de seguridad como de privacidad, pero teniendo como fuente los mismos a la legislación.

Los autores no le pusieron un nombre concreto a este marco de trabajo que hace uso de las ya conocidas metodologías i\* [71] (de donde tiene su origen), GSRM [85] y Tropos [86]; todas ellas procedentes del mundo de la seguridad.

La principal ventaja que ofrece es que puede llevarse a cabo en todas las fases de desarrollo, permitiendo así un análisis homogéneo del sistema, y haciéndolo ideal para procesos iterativos en el ciclo de vida software.

En definitiva, parte de un entorno legal que define como ambiguo (no se representa de manera formal) y cambiante o evolutivo, para terminar con una especificación de requisitos que tienen en cuenta tanto a los usuarios finales del sistema como a los procesos y objetivos de la organización que implementa la metodología. Este marco de trabajo a su vez permite cierta complementariedad con requisitos funcionales, a parte de los ya mencionados de seguridad y legislativos.

Por ello, en relación con la ingeniería de requisitos, las actividades que engloba son la obtención, identificación, análisis, especificación y gestión de los mismos. De cara a la especificación de requisitos, posee un lenguaje de modelado basado en dos actores principales: la parte interesada y el sistema en sí (dicho lenguaje extiende de UML y se conoce como AUML).

Desde el punto de vista del ingeniero software, el marco de trabajo resulta ser un método de análisis de requisitos, sin llegar a entrar en el diseño siquiera; pues no se facilitan guías para éste ni técnicas para ser implementadas que satisfagan los requisitos de privacidad obtenidos (similar a RBAC [83]).

Finalmente se propone como evidencia práctica un sistema de tarjetas inteligentes de un banco alemán, donde se hace ver la robustez de esta metodología incluso es sectores críticos como el bancario.

## 5.6 STRAP

En el año 2005, Carlos Jensen et al. (Instituto de Tecnología de Georgia) propusieron este nuevo método STRAP [30] de obtención de requisitos de privacidad orientado a objetivos.

A diferencia de otros métodos, la obtención de estos requisitos se lleva a cabo exclusivamente durante la fase de diseño del sistema, dentro de la cual sigue un proceso iterativo.

Se trata de un enfoque basado en la realización de un modelo de objetivos, con sus obstáculos y vulnerabilidades; que toma su origen en un proyecto colaborativo anterior al artículo llamado PRIAM ('Privacy Issues in Ambient Intelligence') [87]. Además, respalda y hace uso de las metodologías de seguridad B-S [75], Hong (evolución de la anterior) [88], y KAOS [72].

De cara al proceso en sí, como se ha dicho, es uno de tipo iterativo por el que se elaboran a posteriori los requisitos de privacidad, siguiendo los siguientes cuatro pasos: análisis, refinamiento, evaluación e iteración.

En el primer paso de análisis se elabora un listado de preguntas por cada objetivo, lo que lleva a una lista de vulnerabilidades. A su vez, esto último deriva en un análisis de dichas vulnerabilidades para evitar duplicidades (objetivos distintos pueden resultar en vulnerabilidades similares).

El refinamiento es la fase del proceso en la que se van eliminando de la lista las vulnerabilidades a medida que se proponen las soluciones más fáciles de implementar, lo que lleva a una lista algo más compacta. Puede haber varias soluciones similares en cuanto a dificultad de implementación. En cualquier caso, se tienen en cuenta una o más listas (ya compactadas) para el siguiente paso en que se evalúa la más indicada.

Para terminar, en la evaluación se elige el mejor escenario de diseño, que corresponderá con el que tenga menos vulnerabilidades. Para ello STRAP propone criterios de evaluación a tener en cuenta. Si tras estos pasos se requiere de mayor refinamiento, el equipo de desarrollo puede optar por iterar y continuar de nuevo con el primer paso de análisis, añadiendo o modificando nuevas preguntas que acaben en una nueva lista de vulnerabilidades, etc.

Con respecto a la ingeniería de requisitos, aborda las actividades de obtención, identificación, análisis, especificación y modelado de los mismos; dando una gran completitud a la metodología.

En el marco de ingeniería software aplica a las actividades de análisis de requisitos, diseño, implementación y evaluación de impacto. Sobre esta última actividad hace un análisis del tiempo de desarrollo consumido por el desarrollador software sin necesidad de un conocimiento técnico (problemas que, según los autores, tenían B-S [75] y Hong [88]).

Finalmente esta metodología basada en objetivos ofrece como caso de estudio un calendario web predictivo y compartido que bautiza como Augur; recalcando los beneficios del uso de esta metodología sobre todo en el mundo del software.



## 5.7 PRET

En el año 2008 salió a la luz un nuevo método de obtención de requisitos de privacidad en la conferencia ‘Proceedings of the 3rd IEEE Asia-Pacific Services Computing Conference’: la metodología PRET [89].

Esta metodología comparte con muchas otras sus orígenes en entornos de seguridad, aunque a diferencia de la mayoría, es considerada del tipo ‘orientada a riesgos’ (frente a objetivos).

Dicho entorno de seguridad era anteriormente conocido como SQUARE (‘Security Quality Requirements Engineering’), y consistía en la realización de nueve pasos de manera secuencial, tras los cuales se obtienen requisitos de seguridad (i.e. riesgos para la organización o el sistema).

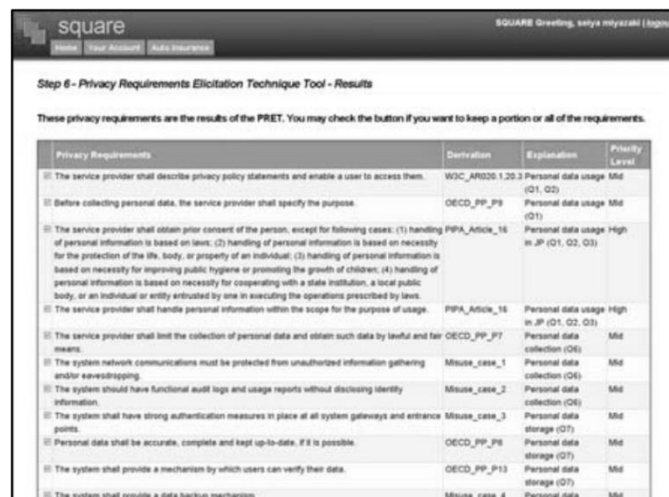
Posteriormente, y a partir de esos requisitos de seguridad, se definen diez preguntas a responder y se elabora una lista de requisitos de privacidad en función de combinaciones de las respuestas. (i.e. respondiendo a Q1 y Q5 se obtiene el requisito R2).

Como valor añadido, PRET ofrece una herramienta software que automatiza la obtención de los requisitos de privacidad en un equipo de desarrollo. Parte de una base de datos con requisitos de privacidad que se van mostrando de acuerdo a cómo se respondieron esas diez preguntas. El software que utilizan los autores no es público ni tiene ningún tipo de licencia abierta o comercial.

Desde la perspectiva de la ingeniería de requisitos, las actividades que tienen relación con esta metodología son la obtención, identificación, análisis, especificación y modelado de requisitos; ofreciendo una gran ventaja en cuanto a la agilidad que ofrecen los enfoques heurísticos como éste.

La ingeniería software se involucra en esta metodología desde el proceso de análisis de requisitos, hasta la evaluación de impacto; pasando por el diseño e implementación.

Finalmente se destaca a esta metodología entre aquéllas que utilizan heurísticos para obtener requisitos de privacidad basados eminentemente en la regulación; pero que, además, ofrece un valor añadido de agilidad en el proceso gracias al uso de la herramienta software.



Privacy Requirements	Derivation	Explanation	Priority Level
<input type="checkbox"/> The service provider shall describe privacy policy statements and enable a user to access them.	W3C_AR020.1.20.3	Personal data usage (D1, Q2)	Mid
<input type="checkbox"/> Before collecting personal data, the service provider shall specify the purpose.	OECD_PP_P9	Personal data usage (D1)	Mid
<input type="checkbox"/> The service provider shall obtain prior consent of the person, except for following cases: (1) handling of personal information is based on laws; (2) handling of personal information is based on necessity for the protection of the life, body, or property of an individual; (3) handling of personal information is based on necessity for improving public hygiene or promoting the growth of children; (4) handling of personal information is based on necessity for cooperating with a state institution, a local public body, or an individual or entity entrusted by one in executing the operations prescribed by laws.	PIPA_Artick_16	Personal data usage High in JP (D1, Q2, Q3)	High
<input type="checkbox"/> The service provider shall handle personal information within the scope for the purpose of usage.	PIPA_Artick_16	Personal data usage High in JP (D1, Q2, Q3)	High
<input type="checkbox"/> The service provider shall limit the collection of personal data and obtain such data by lawful and fair means.	OECD_PP_P7	Personal data collection (OE)	Mid
<input type="checkbox"/> The system network communications must be protected from unauthorized information gathering and/or eavesdropping.	Misuse_case_1	Personal data collection (OE)	Mid
<input type="checkbox"/> The system should have functional audit logs and usage reports without disclosing identity information.	Misuse_case_3	Personal data collection (OE)	Mid
<input type="checkbox"/> The system shall have strong authentication measures in place at all system gateways and entrance points.	Misuse_case_3	Personal data storage (D7)	Mid
<input type="checkbox"/> Personal data shall be accurate, complete and kept up-to-date, if it is possible.	OECD_PP_P8	Personal data storage (D7)	Mid
<input type="checkbox"/> The system shall provide a mechanism by which users can verify their data.	OECD_PP_P13	Personal data storage (D7)	Mid
<input type="checkbox"/> The system shall provide a data backup mechanism.	Misuse_case_4	Personal data	Mid

Ilustración 4: Software utilizado para la obtención de requisitos de [89]

## 5.8 MARCO DE TRABAJO 'PRIVACY-FRIENDLY'

En el año 2009 fue publicado en la revista IEEE 'Transactions on Software Engineering' un artículo de la autora Sarah Spiekermann [6] por el que se analizaba distintos métodos de tener en cuenta a la privacidad en el desarrollo software. El éxito de dicho artículo se debió a la recopilación del estado del arte en materia de privacidad, para después llegar a identificar una nueva forma de obtener requisitos de privacidad más flexible, a la que otros autores denominaron método de elaboración de sistemas 'privacy-friendly'; esto es, respetuosos con la privacidad del usuario.

Para proteger la información del usuario frente a posibles ataques a su privacidad, esta metodología distingue tres 'esferas de dominio' donde puede encontrarse la información:

- Esfera del usuario. Es el dominio sobre el cual el usuario tiene el control de su propia información. Por ejemplo, las cookies de un navegador guardadas en el dispositivo del usuario.
- Esfera conjunta: Es el dominio sobre el cual la empresa tiene el control de la información del usuario. Por ejemplo, los servidores y bases de datos del proveedor de servicios web.
- Esfera recipiente: Es el dominio sobre el cual terceras empresas involucradas tienen el control total o parcial de la información del usuario. Por ejemplo, la red de un proveedor de acceso a internet.

Tras el análisis de estos tres dominios, surgen requisitos de privacidad que deben ser abordados por la empresa.

Las actividades de ingeniería software que se ven implicadas en el artículo son el análisis de requisitos y la fase de diseño.

La flexibilidad de este método reside en la capacidad que tiene el ingeniero software de poder elegir, bien entre una aproximación más favorable al usuario final (privacidad por arquitectura: minimización de datos recogidos), o bien entre otra más favorable a la actividad negocio de la empresa (privacidad por política: maximización de datos recogidos).

Desde el punto de vista de la ingeniería de requisitos, este marco de trabajo aplica sólo a las actividades de obtención e identificación de los mismos, sin entrar en más detalle.

Finalmente este enfoque no presenta caso práctico alguno, dado que inicialmente la autora no tenía como objetivo la explicar en detalle una metodología de requisitos de privacidad; No obstante sí ha sido incluido el artículo en este Trabajo Fin de Máster debido a su innegable reputación y citas en otros artículos relevantes [6], [19], [34].

## 5.9 PRIPARE

Recientemente en este año 2015, el proyecto PRIPARE anteriormente mencionado (sección 'Motivación y Objetivos') ha propuesto en un artículo una metodología que reúne las mejores prácticas de privacidad conocidas hasta ahora [90]. Dicho artículo cobra gran importancia en este Trabajo Fin de Máster dada su afinidad con su objetivo de elaborar una metodología de obtención de requisitos de privacidad; su actualidad en el estado del arte, y la participación de diversos centros de investigación (entre los que se encuentra la Universidad Politécnica de Madrid) en un proyecto europeo de gran envergadura como lo es el mismo PRIPARE.

Sin ir más lejos, esta metodología resulta en una combinación de enfoques; uno orientado a riesgos y otro a objetivos. La principal motivación de esto reside en que, entre un enfoque basado en riesgos y otro en objetivos, la diferencia podría ser a priori un mero tema de expresión en positivo o negativo; y pese a todo, cada uno de ellos están pensado para identificar tipos distintos de requisitos. Por ello, PRIPARE combina ambos enfoques explícitamente, empezando por un enfoque orientado a objetivos y terminando por el orientado a riesgos.

El primero de ellos tiene su sentido en una primera fase de desarrollo, para dar lo antes posible la mayor cobertura de objetivos de privacidad. Esto es posible gracias a catálogos ya conocidos y aceptados por la comunidad que aún se encuentran en desarrollo. En este sentido, la metodología sigue una disciplina heurística, llevando consigo ventajas como la agilidad de su proceso, o el no requerir de un fuerte nivel de conocimiento de la materia; pues los heurísticos en sí ya están pensados por expertos y, de esta forma, el que los utilice sólo tiene que fijarse en si aplican o no a su sistema.

El proceso seguido por el enfoque de objetivos podría resumirse en dos puntos: identificar las fuentes de requisitos (heurísticos, partes interesadas, etc.); y el proceso de gestión de la operativa, que se define como los pasos a seguir para transformar los requisitos de privacidad de alto nivel en requisitos operacionales de forma sistemática, reproducible y fácil de adoptar por ingenieros aún no tan experimentados en implantar la privacidad en sus sistemas.

El segundo enfoque que se aplica es el de un análisis de privacidad basado en riesgos. Éste tiene lugar tras el enfoque basado en objetivos, con el fin de cubrir el resto de requisitos que no se obtengan del anteriormente mencionado. Hacen uso de las ya definidas validaciones de impacto en la privacidad (PIAs) proponiendo los siguientes pasos:

Cumplir con un marco legal. Con ello se espera que los elementos principales cumplan con la legislación, típicamente mediante un cuestionario. Los que han analizado hasta ahora están contruidos por profesionales del mundo legal, y no disminuyen siquiera la necesidad de validar el riesgo de un sistema.

Medir del impacto. Facilita el marco de trabajo [91], el cual se centra principalmente en el propietario de datos (aka. 'data subject'). Sin embargo, PRIPARE recomienda más adelante el uso de una perspectiva dual [92], donde también se tenga en cuenta a las organizaciones.

Medir el riesgo. Se facilitan soluciones como la escala del 1-4 de [91], o bajo-medio-alto de [92], indicando que no debería haber ningún tipo de diferencia entre una u otra; dependiendo incluso del dominio en que apliquen.

Abordar los problemas de privacidad. Tras haber identificado los riesgos de privacidad del sistema, se identifican los requisitos que han de tratar con ellos. Esto lo hace dividiendo entre

1) requisitos que modifican el riesgo, 2) requisitos que lo modifican o reducen y 3) requisitos que lo comparten o transfieren.

Tras estos dos procesos, los autores indican que podría finalmente quedar todavía requisitos residuales, los cuales deberían ser identificados y documentados junto con los anteriores (aunque ahí ya no se especifique cómo). Además, propone tres posibilidades distintas de lidiar con la privacidad de cara a un diseño del sistema: enfoque de arriba hacia abajo, de abajo hacia arriba y horizontal (ver sección 5 de [90]).

Así, por un lado y desde el punto de vista de la ingeniería de requisitos, esta nueva metodología los obtiene, identifica, analiza, especifica y da recomendaciones de modelado.

Por otro lado, en cuanto a la ingeniería software, como mínimo aplica a la actividad de análisis de requisitos, diseño y evaluación del impacto. La implementación, en cambio, dependerá del marco de trabajo escogido<sup>21</sup>.

Finalmente, se pretende adjuntar una evidencia empírica donde se aplica la metodología. Se trata del sistema empotrado en coche eléctrico para su carga inteligente que ya proveyó PMRM como ejemplo [67]. La versión del artículo y la documentación sobre ésta a la que se tiene actualmente acceso sólo hace referencia a dicho caso práctico (no lo describen).

---

<sup>21</sup> Recordemos que, como metodología, PRIPARE propone el qué, dejando la parte del cómo a otros marcos de trabajo ya conocidos.

## 6 ANÁLISIS Y RESULTADOS

Fruto de la lectura de las referencias seleccionadas, a continuación se presenta en la Tabla 4 los resultados de una comparativa entre éstas. Teniendo en cuenta dicha tabla, se elabora seguidamente un análisis de la misma, el cual se facilita en las sub-secciones siguientes.

	LINDDUN	NFR	PriS	RBAC	Tropos y GSRM	STRAP	PRET	privacy-friendly	PRIPARE
Publicación	2010	2004	2006	2003	2010	2005	2008	2008	2015
Evidencias empíricas	X	~	~	~	~	~	~		~
Software de apoyo		X					X		~
<b>Fuentes de requisitos</b>									
- Usuario final	X	X	X	X	X	X	X	X	X
- Empresa desarrolladora	X	X	X	X	X	X	X	X	X
- Marco regulatorio	X		~		X	~	X	X	X
<b>Enfoque de obtención de requisitos</b>									
- Casos de uso indebido	X								
- Objetivos	X	X	X	X	X	X	X	X	X
- Riesgos	~	X					X	X	X
- Heurística	X	X	X			X	X		X
- Regulación				X	X		X		X
<b>Descripción de requisitos</b>									
- Textual	X	X	X	X	X		X	X	~
- Gráfica	X	X	X		X	X			~
- Algebraica				X			X		~
<b>Complementariedad</b>									
- Seguridad	X	X	X	X	X	X	X	X	X
- Requisitos funcionales					X	X			
- Legislación		X		X	X		X		X
- Organismos de estandarización	X	X					X		X
<b>Actividades de Ing. Requisitos</b>									
- Obtención de requisitos	X	X	X	X	X	X	X	X	X
- Identificación de requisitos	X	X	X	X	X	X	X	X	X
- Análisis y negociación		X	X	X	X	X	X		X
- Especificación de requisitos		X	X	X	X	X	X		X
- Modelado del sistema	X		X			X	X		X
- Validación de requisitos									
- Gestión de requisitos	X				X				
<b>Actividades de Ing. Software</b>									
- Análisis de requisitos	X	X	X	X	X	X	X	X	X
- Diseño	X	X	X			X	X	X	X
- Implementación	X		X			X	X		~
- Evaluación de impacto	~		X			X	X		X
- Verificación y pruebas									
- Integración									
- Operación y mantenimiento									

Tabla 4: Comparativa de metodologías de privacidad

Tras haber sido seleccionados los artículos con los criterios expuestos en la sección 'Búsqueda documental', se ha hecho necesario elaborar una plantilla de análisis. El objetivo de esta plantilla es poder establecer una comparativa entre las distintas metodologías que se han ido encontrando. Parte de dicha plantilla puede verse a modo de ejemplo en la sección 'Anexos', en la Tabla 5: Plantilla de análisis.

A partir de la citada plantilla se ha elaborado la Tabla 4: Comparativa de metodologías de privacidad. Ésta última constituye un resumen o síntesis de los resultados de este Trabajo Fin de Máster. A continuación se describen los criterios comparativos escogidos con algunos comentarios acerca de ellos.

## **6.1 PUBLICACIÓN**

El primero de ellos es la fecha de publicación que, aunque de modo individual no aporte mucha información, puede ser una evidencia clara de cuándo empezó a aparecer esta necesidad de defender la privacidad, en torno al año 2003, coincidiendo con la explosión de las redes sociales.

## **6.2 EVIDENCIAS EMPÍRICAS**

El segundo corresponde con las evidencias empíricas. La mayor parte de las metodologías o marcos de trabajo añaden lo que llaman casos de estudio, que corroboran de manera pragmática sus conceptos teóricos. Sin embargo, ninguno de estos ponen de manifiesto su uso en un entorno que no sea académico, lo que hacen que tengan un nivel de madurez aún muy bajo. De este modo, aún se hacen necesarias evidencias experimentales en el mundo empresarial que certifiquen su utilidad.

## **6.3 SOFTWARE DE APOYO**

El tercero nos indica si la metodología o marco de trabajo contempla la posibilidad de uso de un software. En los casos que se han visto, el software incorpora heurísticos sobre dominios concretos que sacan los requisitos derivados de un objetivo de manera automática, eligiendo el usuario aquéllos que apliquen más o menos a su caso (enfoque basado en riesgos y objetivos).

Aun así hay que decir que pocas metodologías hacen uso del software como herramienta de obtención de requisitos de privacidad (NFR y PRET), no siendo así con metodologías del mundo de la seguridad. Lo que hace más atractivo a una metodología de este tipo, es que el software permite agilizar enormemente el proceso. Sin embargo, no siempre se consigue una cobertura o nivel de profundidad suficiente, sobre todo si el dominio de aplicación es desconocido (falta de heurísticos). Por todo ello y de cara a un futuro, la elaboración de este tipo de herramientas puede tener bastante penetración en el mercado del software.

## **6.4 FUENTES DE REQUISITOS**

El siguiente criterio tiene en cuenta cuáles de las partes interesadas son tomadas en cuenta a la hora de hacer un análisis para obtener requisitos. Por lo general, siempre se tiene en cuenta al usuario y a los intereses de la empresa que desarrolla el sistema. En cambio, en algunos de ellos no se piensa directamente en el organismo de regulación competente. Esto quiere decir que no hay todavía una buena integración con el mundo legal, aunque sí que se observa una

evolución favorable; ya que los marcos de trabajo que sí que incorporan estos requisitos procedentes de la regulación, resultan ser los más recientes (2008-2010).

## **6.5 ENFOQUE DE OBTENCIÓN DE REQUISITOS**

Con el siguiente criterio de la tabla, se mira el enfoque o punto de vista desde el cual se mira al sistema. Para obtener los requisitos, según la metodología que sea, se pone atención en casos de uso indebido o amenazas, objetivos de negocio, análisis de riesgos, heurísticos y patrones ya conocidos, o en la regulación y leyes competentes.

Los tres primeros resultan ser enfoques típicos de las metodologías que parten del mundo de la seguridad. Sirva de ejemplo LINDDUN que, aunque no especifique un método concreto de análisis de riesgos, sí que tiene en cuenta dicho paso. Esta metodología es una extrapolación al mundo de la privacidad de lo que es STRIDE, una metodología de obtención de requisitos de seguridad.

Analizando los enfoques de todas las metodologías, puede apreciarse que a la hora de pensar en los requisitos de privacidad, todas ellas ponen especial interés en los objetivos del negocio. Con ello argumentamos que, por parte de una empresa, no debería ser excusa la no adopción de alguna de éstas debido a intereses internos de la misma; estos se valoran en primer lugar.

## **6.6 DESCRIPCIÓN DE LOS REQUISITOS**

Los requisitos pueden ser obtenidos y especificados siguiendo distintos tipos de lenguaje. Entre los más utilizados son el lenguaje textual (como se describen tradicionalmente en el documento SRS), gráfico (mediante diagramas de flujo de datos, objetivos, amenazas, etc.) y algebraico. Este último requiere de un conocimiento técnico mayor, la que quizás sea la razón principal por la que no es ampliamente utilizado. Como ventaja ofrece una manera de evitar dobles interpretaciones, incoherencias o duplicados que generen conflictos entre dos o más requisitos a la hora de ser especificados.

## **6.7 COMPLEMENTARIEDAD**

El criterio de complementariedad indica si la metodología o marco de trabajo permite obtener otros requisitos en el proceso (aparte de los relacionados con la privacidad). Entre ellos pueden estar los relacionados con la seguridad, con la regulación, o incluso con otros requisitos funcionales. El punto clave en el que el lector debería fijarse aquí, es que todas las metodologías de privacidad obtienen, además, requisitos de seguridad derivados. Ello puede servir como evidencia clara la gran dependencia que tiene la privacidad con la seguridad y viceversa, así como el origen de la primera respecto de la segunda.

## **6.8 ACTIVIDADES DE INGENIERÍA DE REQUISITOS**

En relación a la disciplina de ingeniería de requisitos, vemos de qué manera no hay una frontera clara de hasta dónde debe llegar una metodología o marco de trabajo. Algunas se centran únicamente en obtener e identificar requisitos. En cambio otras, no sólo no se paran en especificarlos y analizarlos, sino que proponen soluciones de modelado del sistema en base a una o varias PET<sup>22</sup>. Otras se meten en la gestión de los requisitos sin proponer de forma clara como especificarlos.

---

<sup>22</sup> Del inglés: 'Privacy Enhanced Technique'.

Aquí se puede ver una falta de consenso notable entre ellas; dejando en entredicho hasta qué punto de la ingeniería de requisitos deberían llegar cualquiera de las metodologías o marcos de trabajo futuros.

## **6.9 ACTIVIDADES DE INGENIERÍA SOFTWARE**

Finalmente, hacemos una comparativa desde el punto de vista de la ingeniería software. Teniendo en cuenta las actividades que ésta desarrolla, y como no podría ser de otra manera, todas las metodologías de obtención de requisitos de privacidad cubren la primera actividad: el análisis de requisitos.

Dependiendo de si se tratan de metodologías enfocadas al diseño o a la realización de políticas de seguridad, terminarán metiéndose en la actividad de diseño o no. Algunas ofrecen también técnicas destinadas a mejorar la privacidad (PET) según aparezca un requisito u otro. Éstas pueden exigir ya de una implementación concreta.

Por último destacar que varias de ellas, como NFR o RBAC, facilitan la iteración de manera razonable, haciéndolas muy convenientes para ciclos de vida cortos o de prototipado que se basen en iteraciones rápidas.



## 7 CONCLUSIONES

---

En referencia al mundo de la privacidad, y tras hacer un análisis de las metodologías y marcos de trabajo que hay en la actualidad, uno puede darse cuenta a primera vista de que es difícil encontrar una metodología que guíe a los desarrolladores en todos los pasos de obtención de requisitos de privacidad.

Esto puede verse al comparar los marcos de trabajo del entorno de la privacidad con el de la seguridad. Los primeros se ha visto que surgen de los segundos y, además, los marcos de trabajo orientados a requisitos de seguridad son más numerosos y suelen tener un mayor alcance que los de privacidad.

No obstante también se ha observado que, gracias al estallido de las redes sociales, las metodologías relacionadas con la privacidad han ido apareciendo y evolucionando de manera favorable a partir del año 2003. Los autores han ido creando marcos de trabajo utilizando trabajos anteriores, combinando y haciendo uso de ideas procedentes de varias metodologías distintas. De esta manera, éstos han ido perfeccionándolas para poder llegar en un futuro a definir unas más completas y eficientes; a medida que aumenta la oportunidad de investigación en esta materia.

Respecto a éste último punto sobre la evolución y completitud de las metodologías, se ha indicado cómo han ido apareciendo aspectos que inicialmente no se tenían en cuenta en las nuevas metodologías. Este es el caso, por ejemplo, del marco la legal como fuente de obtención de requisitos. Nuevos métodos relacionados con la regulación se han ido añadiendo a medida que se han publicado los últimos avances en esta materia (las metodologías más recientes ya lo incluyen).

A pesar de todo, aún no hay evidencias de uso en el ámbito empresarial que puedan avalar a cualquiera de las metodologías o marcos de trabajo estudiados. Aquello que se sabe a día de hoy no trasciende del entorno académico, ni tampoco ofrece un valor adicional claro a las empresas frente al no utilizar dichas metodologías. Sin embargo se observan cada vez más intentos de llevar estas metodologías a un entorno más práctico, como puede verse en [15].

Hasta ahora, desde el punto de vista de las empresas la privacidad se ha solventado mediante políticas del 'todo o nada', esto es, o el usuario da consentimiento de todos los puntos donde su privacidad pueda verse comprometida, o no tiene otra opción que renunciar al servicio. La comunidad investigadora quiere trasladar esta idea unilateral a lo que han denominado 'privacidad por diseño', que no es más que tener en cuenta a la privacidad del usuario durante la fase de diseño y desarrollo del sistema. De esta manera, los derechos a la privacidad de éste son garantizados y, de ser necesaria alguna política de consentimiento, se le ofrezcan distintos niveles de servicio según los puntos de acuerdo o desacuerdo del usuario.

Algunas de las metodologías analizadas hacen uso de software de apoyo para la elaboración de requisitos de privacidad. Este tipo de aproximaciones tienen como principal ventaja la rapidez con la que se pueden obtener, no solo los requisitos citados anteriormente, sino también soluciones 'ad-hoc' ya pensadas para determinadas casuísticas (i.e. PETs). Como contrapartida encontramos que este tipo de software suele ser muy especializado en un dominio concreto y que, a menudo, no aportan el nivel de profundidad o cobertura deseado.

Por tanto, podrían ser útiles en una etapa temprana de diseño, o cuando se necesita cierta agilidad en un determinado momento del ciclo de vida; pero no es aplicable para etapas

posteriores o de dominios desconocidos. Por ello que actualmente haya una oportunidad nada despreciable de cara al desarrollo o perfeccionamiento de este tipo de herramientas de software; así como ya las podemos encontrar en el mundo de la seguridad sobre, por ejemplo, requisitos a partir de un análisis de riesgos. No se ha encontrado ningún software específico de privacidad con licencia comercial.

Con respecto a los organismos de estandarización, se ha buscado en OASIS, ISO, W3C, ITU-T, IETF, IEEE, ETSI, CEN/CENELEC, ECMA y NIST. No se han encontrado resultados de metodologías de privacidad dentro de los mismos, aunque sí información relevante para este Trabajo Fin de Máster como conceptos y buenas prácticas: ISO [68], [69], [93], [94]; NIST [4], [70]; IETF [39]; .

El organismo ISO ('International Organization for Standardization') está actualmente trabajando activamente aunque no ha introducido aún ninguna metodología en concreto. El grupo WG 5 de ISO/IEC JTC 1/SC 27 se fija en estándares relacionados con marcos de trabajo a un nivel muy alto: ISO 29100 [93], e ISO 29101 [94]; y también con la gestión de la privacidad: ISO 29134 [68] e ISO 29151 [69].

OASIS por su parte se centra en la mencionada privacidad por diseño. Cuenta con el comité técnico OASIS PMRM TC, el cual busca una metodología para convertir requisitos de privacidad en requisitos operacionales [67]. Por otro lado tiene al comité OASIS PbD-SE TC que se dedica a la documentación de ingeniería software [95]. PRIPARE se encuentra como miembro de la organización OASIS y también participa activamente en estos dos comités técnicos.

En cuanto al organismo CEN/CENELEC ('European Committee for Standardization and European Committee for Electrotechnical Standardization'), según [90], será presentado el proyecto y la metodología PRIPARE para su integración.

W3C hace también un intento de abordar el tema de privacidad como puede verse en [96]; sin embargo, y al igual que el resto de organismos de estandarización (a excepción de OASIS), no establece metodología alguna, limitándose a detectar los riesgos más evidentes, y asentar información de muy alto nivel (sin llegar a entrar en la parte de ingeniería). El grupo de trabajo dedicado a todo ello es el PING ('Privacy Interest Group') [97].

Tanto el organismo norteamericano NIST como IETF son más ejemplo de una aproximación de alto nivel al paradigma de la privacidad actual: NIST [4], [70], e IETF [39],[98].

Todo esto indica un lento avance, aun con un interés creciente, por parte de los organismos de estandarización. Se espera que en los próximos años pasen de asentar conceptos de alto nivel y empiecen a definir metodologías y marcos de trabajo aplicables a la ingeniería de privacidad.

Finalmente, se propone una reflexión del estado actual de la investigación. Ésta necesitaría avanzar en el estudio de nuevas metodologías que contemplen los puntos fuertes de las anteriores (como se ha venido haciendo hasta ahora). Las más recientes se diferencian mucho en su alcance, ya que cubren distintas actividades de la ingeniería de requisitos y software sin haber ningún tipo de consenso, o bien aplican a dominios muy concretos.

De cara a un trabajo posterior, también convendría intentar separar aún más requisitos de seguridad y de privacidad que, en casi todos los casos, terminan obteniéndose indistintamente. Actualmente se están centrando los esfuerzos en mejorar los heurísticos que hay referentes a la privacidad, que constituyen a todas luces una fuente ágil y eficiente de obtención de requisitos para cualquier organización.

## 8 REFERENCIAS

---

- [1] UN, "Declaración Universal de Derechos Humanos," 1948.
- [2] España, "BOE.es - Documento BOE-A-1977-10733." [Online]. Available: [http://www.boe.es/diario\\_boe/txt.php?id=BOE-A-1977-10733](http://www.boe.es/diario_boe/txt.php?id=BOE-A-1977-10733). [Accessed: 05-Jul-2015].
- [3] España, "BOE.es - La Constitución Española," 1978. [Online]. Available: <http://www.boe.es/legislacion/constitucion.php>. [Accessed: 05-Jul-2015].
- [4] NIST, "(DRAFT) Privacy Risk Management for Federal Information Systems - NIST IR 8062," 2015.
- [5] IPEN, "Background and purpose," 2015.
- [6] S. Spiekermann and L. F. Cranor, "Engineering Privacy," 2009.
- [7] A. Abran, P. Bourque, R. Dupuis, and J. W. Moore, *Guide to the software engineering body of knowledge-SWEBOK*. IEEE Press, 2001.
- [8] P. A. Laplante, *What Every Engineer Should Know about Software Engineering*. CRC Press, 2007.
- [9] ACM, "Computing Degrees & Careers » Software Engineering." [Online]. Available: [http://computingcareers.acm.org/?page\\_id=12](http://computingcareers.acm.org/?page_id=12). [Accessed: 16-Jun-2015].
- [10] F. C. D. ISO, "IEC 24765," *Syst. Softw. Eng. Vocab*.
- [11] I. Sommerville and G. Kotonya, *Requirements engineering: processes and techniques*. John Wiley & Sons, Inc., 1998.
- [12] B. Nuseibeh and S. Easterbrook, "Requirements engineering: a roadmap," in *Proceedings of the Conference on the Future of Software Engineering*, 2000, pp. 35–46.
- [13] M. Chemuturi, *Requirements engineering and management for software development projects*. Springer Science & Business Media, 2012.
- [14] I. Sommerville, *Software Engineering*. Pearson, 2011.
- [15] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements," *Requir. Eng.*, vol. 16, pp. 3–32, 2011.
- [16] A. Dali and C. Lajtha, "ISO 31000 Risk Management: 'The Gold Standard,'" *EDPACS*, vol. 45, no. 5, pp. 1–8, May 2012.
- [17] R. Antunes and V. Gonzalez, "A Production Model for Construction: A Theoretical Framework," *Buildings*, vol. 5, no. 1, p. 209, 2015.

- [18] D. W. Hubbard, *The failure of risk management: Why it's broken and how to fix it*. John Wiley & Sons, 2009.
- [19] M. C. Oetzel and S. Spiekermann, "A systematic methodology for privacy impact assessments: a design science approach," *Eur. J. Inf. Syst.*, vol. 23, no. 2, pp. 126–150, 2014.
- [20] PRIPARE, "PRIPARE - PReparing Industry to Privacy-by-design by Supporting its Application in REsearch | PReparing Industry to Privacy-by-design by Supporting its Application in REsearch." [Online]. Available: <http://pripareproject.eu/>. [Accessed: 29-Jun-2015].
- [21] MITRE, "The MITRE Corporation." [Online]. Available: <http://www.mitre.org/>. [Accessed: 29-Jun-2015].
- [22] CCC, "Privacy by Design - Computing Community Consortium." [Online]. Available: <http://www.cra.org/ccc/visioning/visioning-activities/privacy-by-design>. [Accessed: 29-Jun-2015].
- [23] IEEE, "IEEE Symposium on Security and Privacy 2015." [Online]. Available: <http://www.ieee-security.org/TC/SP2015/index.html>. [Accessed: 29-Jun-2015].
- [24] IEEE, "2015 International Workshop on Privacy Engineering - IWPE'15 / International Workshop on Privacy Engineering." [Online]. Available: <http://iee-security.org/TC/SPW2015/IWPE/index.html>. [Accessed: 29-Jun-2015].
- [25] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. Le Metayer, R. Tirtea, and S. Schiffner, "Privacy and Data Protection by Design-from policy to engineering," *arXiv Prepr. arXiv1501.03726*, 2015.
- [26] M. Adolphus, "How to... carry out a literature review for a dissertation or research paper," *Emerald Group Publishing*. [Online]. Available: <http://www.emeraldgrouppublishing.com/research/guides/methods/literature2.htm>. [Accessed: 23-Jan-2015].
- [27] M. Adolphus, "How to conduct a systematic or evidence-based literature review," *Emerald Group Publishing*. [Online]. Available: [http://www.emeraldgrouppublishing.com/authors/guides/write/evidence\\_based.htm](http://www.emeraldgrouppublishing.com/authors/guides/write/evidence_based.htm). [Accessed: 07-Feb-2015].
- [28] P. Steane, "Fundamentals of a literature review," in *Surviving Your Thesis*, 2004, pp. 124–137.
- [29] S. Spiekermann and L. F. Cranor, "Engineering privacy," *IEEE Trans. Softw. Eng.*, vol. 35, pp. 67–82, 2009.
- [30] C. Jensen, J. Tullio, C. Potts, and E. D. Mynatt, "STRAP: A Structured Analysis Framework for Privacy," 2005.
- [31] G. Iachello and G. D. Abowd, "From privacy methods to a privacy toolbox," *ACM Transactions on Computer-Human Interaction*, vol. 15, pp. 1–30, 2008.

- [32] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: The PriS method," *Requir. Eng.*, vol. 13, no. 3, pp. 241–255, 2008.
- [33] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. Le Metayer, R. Tirtea, and S. Schiffner, "Privacy and Data Protection by Design - from policy to engineering," p. 79, Jan. 2015.
- [34] K. Beckers, "Comparing privacy requirements engineering approaches," in *Proceedings - 2012 7th International Conference on Availability, Reliability and Security, ARES 2012*, 2012, pp. 574–581.
- [35] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Methods for designing privacy aware information systems: A review," in *PCI 2009 - 13th Panhellenic Conference on Informatics*, 2009, pp. 185–194.
- [36] M. F. Denedy, J. Fox, and T. Finneran, *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value*. Apress, 2014.
- [37] I. Oliver, *Privacy Engineering: A Dataflow and Ontological Approach*. Createspace Independent Pub, 2014.
- [38] K. A. Saleh, *Software Engineering*. J. Ross Publishing, Inc., 2009, pp. 74–75.
- [39] A. Cooper, H. Tschofenig, B. Aboba, J. Peterson, J. Morris, R. Smith, and M. Hansen, "Privacy Considerations for Internet Protocols," *RFC6973*, p. 36, 2013.
- [40] P. Schaar, "Privacy by design," *Identity Inf. Soc.*, vol. 3, no. 2, pp. 267–274, 2010.
- [41] N. Davies and M. Langheinrich, "Privacy by design," *IEEE Pervasive Computing*, vol. 12, no. 2. Institute of Electrical and Electronics Engineers Inc., pp. 2–4, 2013.
- [42] A. Cavoukian and others, "Privacy by design: The 7 foundational principles," *Inf. Priv. Comm. Ontario, Canada*, 2009.
- [43] M. Langheinrich, "Privacy by design—principles of privacy-aware ubiquitous systems," in *UbiComp 2001: Ubiquitous Computing*, 2001, pp. 273–291.
- [44] J. Hoepman, "Privacy design strategies," *arXiv Prepr. arXiv1210.6621*, p. 12, 2012.
- [45] A. Barth, A. Datta, J. C. Mitchell, and H. Nissenbaum, "Privacy and contextual integrity: Framework and applications," in *Security and Privacy, 2006 IEEE Symposium on*, 2006, p. 15–pp.
- [46] G. Duncan, "Engineering. Privacy by design.," *Science*, vol. 317, no. 5842, pp. 1178–1179, 2007.
- [47] A. Lapouchnian, "Goal-oriented requirements engineering: An overview of the current research," *Univ. Toronto*, 2005.
- [48] A. D. Toro, B. B. Jiménez, A. R. Cortés, and M. T. Bonilla, "A Requirements Elicitation Approach Based in Templates and Patterns.," in *WER*, 1999, pp. 17–29.

- [49] A. I. Anton and J. B. Earp, "A requirements taxonomy for reducing web site privacy vulnerabilities," *Requir. Eng.*, vol. 9, no. 3, pp. 169–185, 2004.
- [50] A. Kung, J. C. Freytag, and F. Kargl, "Privacy-by-design in ITS applications," in *2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2011 - Digital Proceedings*, 2011.
- [51] S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, "Smart meter privacy: A utility-privacy framework," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, 2011, pp. 190–195.
- [52] M. Deng, M. Petkovic, M. Nalin, and I. Baroni, "A Home Healthcare System in the Cloud--Addressing Security and Privacy Challenges," in *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, 2011, pp. 549–556.
- [53] R. Shokri, J. Freudiger, and J.-P. Hubaux, "A unified framework for location privacy," 2010.
- [54] D. Kotz, S. Avancha, and A. Baxi, "A privacy framework for mobile health and home-care systems," ... *Priv. Med. home-care Syst.*, p. 12, 2009.
- [55] S. Pearson, "Taking account of privacy when designing cloud computing services," in *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 2009, pp. 44–52.
- [56] S. Singh and S. Bawa, "A privacy, trust and policy based authorization framework for services in distributed environments," *Int. J. Comput. Sci.*, vol. 2, no. 2, pp. 85–92, 2007.
- [57] S. Agrawal and J. R. Haritsa, "A framework for high-accuracy privacy-preserving mining," in *Data Engineering, 2005. ICDE 2005. Proceedings. 21st International Conference on*, 2005, pp. 193–204.
- [58] S. V. da Rocha, Z. Abdelouahab, and E. Freire, "Requirement Elicitation Based on Goals with Security and Privacy Policies in Electronic Commerce.," in *WER*, 2005, pp. 63–74.
- [59] A. I. Antón, J. B. Earp, and A. Reese, "Analyzing website privacy requirements using a privacy goal taxonomy," in *Requirements Engineering, 2002. Proceedings. IEEE Joint International Conference on*, 2002, pp. 23–31.
- [60] E. Yu, "Designing for privacy and other competing requirements," *2nd Symp. Requir. Eng.*, 2002.
- [61] L. Compagna, P. El Khoury, A. Krausová, F. Massacci, and N. Zannone, "How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns," *Artif. Intell. Law*, vol. 17, no. 1, pp. 1–30, 2009.
- [62] A. I. Antón, J. B. Earp, and R. A. Carter, "Precluding incongruous behavior by aligning software requirements with security and privacy policies," *Inf. Softw. Technol.*, vol. 45, no. 14, pp. 967–977, 2003.

- [63] L. Liu, E. Yu, and J. Mylopoulos, "Security and privacy requirements analysis within a social setting," in *Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International*, 2003, pp. 151–161.
- [64] I. S. Rubinstein, "REGULATING PRIVACY BY DESIGN.," *Berkeley Technol. Law J.*, vol. 26, no. 3, pp. 1409–1456, 2011.
- [65] D. Le Métayer, "A formal privacy management framework," in *Formal Aspects in Security and Trust*, Springer, 2009, pp. 162–176.
- [66] A. I. Antón, J. B. Earp, C. Potts, and T. A. Alspaugh, "The role of policy and stakeholder privacy values in requirements engineering," in *Requirements Engineering, 2001. Proceedings. Fifth IEEE International Symposium on*, 2001, pp. 138–145.
- [67] J. Sabo, M. Willet, and P. F Brown, "Privacy Management Reference Model Version 1.0," 2012.
- [68] ISO/IEC, "ISO/IEC CD 29134 - Privacy impact assessment -- Methodology." [Online]. Available: [http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=62289](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289). [Accessed: 29-Jun-2015].
- [69] ISO/IEC, "ISO/IEC WD 29151 - Code of practice for PII protection." [Online]. Available: [http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=62726](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62726). [Accessed: 29-Jun-2015].
- [70] J. T. FORCE and T. INITIATIVE, "Security and privacy controls for federal information systems and organizations," *NIST Spec. Publ.*, vol. 800, p. 53, 2013.
- [71] E. S. K. Yu, "Modeling organizations for information systems requirements engineering," in *Requirements Engineering, 1993., Proceedings of IEEE International Symposium on*, 1993, pp. 34–41.
- [72] A. Dardenne, A. Van Lamsweerde, and S. Fickas, "Goal-directed requirements acquisition," *Sci. Comput. Program.*, vol. 20, no. 1, pp. 3–50, 1993.
- [73] C. B. Haley, J. D. Moffett, R. Laney, B. Nuseibeh, and W. Hall, "A Framework for Security Requirements Engineering," *Proc. 2006 Int. Work. Softw. Eng. Secur. Syst. SESS 06*, vol. 1, pp. 35–41, 2006.
- [74] A. I. Antón and J. B. Earp, "Strategies for developing policies and requirements for secure electronic commerce systems," in *E-commerce security and privacy*, 2000, vol. 2, pp. 29–46.
- [75] V. Bellotti and A. Sellen, "Design for privacy in ubiquitous computing environments," in *ECSCW*, 1993, pp. 77–92.
- [76] EPPI, "EPPI-Centre Methods form Conducting systematic review," *Evidence for Policy and Practive. Information and co-ordinating centre*, 2007. [Online]. Available: <https://eppi.ioe.ac.uk/cms/LinkClick.aspx?fileticket=hQB8y4uVwI=&tabid=88>.

- [77] B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt, "A comparison of security requirements engineering methods," *Requir. Eng.*, vol. 15, pp. 7–40, 2010.
- [78] K. Wuyts, R. Scandariato, and W. Joosen, "Empirical evaluation of a privacy-focused threat modeling methodology," *Journal of Systems and Software*, 2014.
- [79] L. M. Cysneiros and J. C. do Prado Leite, "Nonfunctional requirements: From elicitation to conceptual models," *Softw. Eng. IEEE Trans.*, vol. 30, no. 5, pp. 328–350, 2004.
- [80] L. M. Cysneiros and E. Yu, "Non-functional requirements elicitation," in *Perspectives on software requirements*, Springer, 2004, pp. 115–138.
- [81] L. Chung and J. C. S. do Prado Leite, "On non-functional requirements in software engineering," in *Conceptual modeling: Foundations and applications*, Springer, 2009, pp. 363–379.
- [82] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Using privacy process patterns for incorporating privacy requirements into the system design process," in *Proceedings - Second International Conference on Availability, Reliability and Security, ARES 2007*, 2007, pp. 1009–1016.
- [83] D. Shin, D. Shin, G.-J. Ahn, G.-J. Ahn, S. Cho, S. Cho, S. Jin, and S. Jin, "On Modeling System-Centric Information for Role Engineering," in *Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies*, 2003, pp. 169–178.
- [84] S. Islam, H. Mouratidis, and S. Wagner, "Towards a framework to elicit and manage security and privacy requirements from laws and regulations," in *Requirements Engineering: Foundation for Software Quality*, Springer, 2010, pp. 255–261.
- [85] S. Islam, "Software development risk management model," in *Proceedings of the doctoral symposium for ESEC/FSE on Doctoral symposium - ESEC/FSE Doctoral Symposium '09*, 2009, pp. 5–8.
- [86] J. Castro, M. Kolp, and J. Mylopoulos, "Towards requirements-driven information systems engineering: the Tropos project," *Inf. Syst.*, vol. 27, no. 6, pp. 365–389, 2002.
- [87] INRIA, "PRIAM: Privacy Issues and AMbient intelligence." [Online]. Available: <http://priam.citi.insa-lyon.fr/>. [Accessed: 30-Jun-2015].
- [88] D. Hong, D. K. W. Chiu, and V. Y. Shen, "Requirements elicitation for the design of context-aware applications in a ubiquitous environment," in *Proceedings of the 7th international conference on Electronic commerce*, 2005, pp. 590–596.
- [89] S. Miyazaki, N. Mead, and J. Zhan, "Computer-aided privacy requirements elicitation technique," in *Proceedings of the 3rd IEEE Asia-Pacific Services Computing Conference, APSCC 2008*, 2008, pp. 367–372.
- [90] Y.-S. Martín, J. M. del Álamo, N. Notario, A. Crespo, D. Le Métayer, T. Antignac, A. Kung, I. Kroener, and D. Wright, "PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology," *PRIPARE*, 2015.



- [91] C. nationale de l'informatique et des libertés (CNIL), "Methodology For Privacy Risk Management." 2012.
- [92] M. C. Oetzel, S. Spiekermann, I. Grüning, H. Kelter, S. Mull, and J. Cantella, "Privacy Impact Assessment Guideline," *Bonn Bundesamt für Sicherheit der Informationstechnik*, 2011.
- [93] ISO/IEC, "ISO/IEC 29100:2011 - Information technology -- Security techniques -- Privacy framework," 2011. [Online]. Available: [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=45123](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123). [Accessed: 05-Jul-2015].
- [94] ISO/IEC, "ISO/IEC 29101:2013 - Information technology -- Security techniques -- Privacy architecture framework," 2013. [Online]. Available: [http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=45124](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45124). [Accessed: 05-Jul-2015].
- [95] A. Cavoukian, F. Carter, D. Jutla, J. Sabo, F. Dawson, J. Fox, T. Finneran, and S. Fieten, "Privacy by Design Documentation for Software Engineers Version 1.0," 2015.
- [96] W3C, "Self-Review Questionnaire: Security and Privacy," 2015. [Online]. Available: <https://w3ctag.github.io/security-questionnaire/>. [Accessed: 05-Jul-2015].
- [97] PING, "W3C Privacy Interest Group," 2013. [Online]. Available: <http://www.w3.org/Privacy/>. [Accessed: 05-Jul-2015].
- [98] IETF, "RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels." [Online]. Available: <https://www.ietf.org/rfc/rfc2119.txt>. [Accessed: 05-Jul-2015].

## 9 ANEXOS

### 9.1 PLANTILLA DE ANÁLISIS

Tabla 5: Plantilla de análisis

Nombre de la metodología:		
<b>Resumen:</b>		
<b>Criterio</b>	<b>Nivel</b>	<b>Valor</b>
<b>Metadatos</b>		
	Autor(es)/Institución/URL/DOI:	
	Índice JCR de la revista en que está publicada:	
	Fecha de publicación:	
	¿Forma parte de un estándar?	<input type="checkbox"/> ¿Cuál?:
	Relación con otra metodología:	
<b>Adopción</b>		
	Número de entidades que la utilizan:	
	Nombre(s) de la(s) entidad(es):	
	Argumentos:	
<b>Respaldo</b>		
	Número de entidades que la recomiendan:	
	Nombre(s) de la(s) entidad(es):	
	Argumentos:	
<b>Nivel de madurez</b>		
	MRL:	
<b>Evidencias empíricas</b>		
	Título del caso práctico:	
	Sector o Industria:	
	Etapa(s) del desarrollo en que aplica:	
<b>Descripción de los requisitos</b>		
	Textual	<input type="checkbox"/>
	Gráfica	<input type="checkbox"/>
	Algebraica	<input type="checkbox"/>
	Otra:	
<b>Herramientas y lenguajes de especificación de requisitos</b>		
	Herramientas o lenguajes de especificación que se utilizan:	
<b>Enfoque de la obtención de los requisitos</b>		
	Casos de uso indebido	<input type="checkbox"/>
	Barreras	<input type="checkbox"/>
	Objetivos	<input type="checkbox"/>
	Riesgos	<input type="checkbox"/>
	Heurística	<input type="checkbox"/>
	Regulación	<input type="checkbox"/>
	Otro:	
<b>Integración de Requisitos</b>		
<b>Fuentes de obtención de requisitos</b>		
	Cliente final	<input type="checkbox"/>
	Empresa desarrolladora	<input type="checkbox"/>
	Marco regulatorio	<input type="checkbox"/>
	Otro:	
<b>Complementariedad con los requisitos</b>		
	Seguridad	<input type="checkbox"/>
	Funcionales	<input type="checkbox"/>
	Legislación	<input type="checkbox"/>
	Heurística	<input type="checkbox"/>
	Estándar	<input type="checkbox"/>
	Otros:	

<b>Relación con actividades de ingeniería de requisitos</b>	
Obtención de requisitos	<input type="checkbox"/>
Identificación de requisitos	<input type="checkbox"/>
Análisis y negociación	<input type="checkbox"/>
Especificación de requisitos	<input type="checkbox"/>
Modelado del sistema	<input type="checkbox"/>
Validación de requisitos	<input type="checkbox"/>
Gestión de requisitos	<input type="checkbox"/>
<b>Relación con actividades de ingeniería del software</b>	
Análisis de requisitos	<input type="checkbox"/>
Diseño	<input type="checkbox"/>
Implementación	<input type="checkbox"/>
Evaluación de impacto	<input type="checkbox"/>
Verificación y pruebas	<input type="checkbox"/>
Integración	<input type="checkbox"/>
Operación y mantenimiento	<input type="checkbox"/>
<b>Integración en procesos de desarrollo o metodologías</b>	
Nombre del proceso o metodología:	
<b>Herramientas de soporte</b>	
¿Admite algún software complementario?:	<input type="checkbox"/> ¿Cuál?:
<b>Métricas</b>	
Otras:	
<b>Dominio de aplicación</b>	
General	
Particular:	<input type="checkbox"/> ¿Cuál?:
<b>Agentes o partes interesadas (a quién se tiene en cuenta)</b>	
Cliente final	<input type="checkbox"/>
Empresa desarrolladora	<input type="checkbox"/>
Organización externa	<input type="checkbox"/>
Organismo de regulación competente	<input type="checkbox"/>
Otro:	

**Notas:**

---

## 9.2 REFERENCIAS 1ª ITERACIÓN

1	Adolphus, M. (n.d.-a). How to conduct a systematic or evidence-based literature review. Retrieved February 07, 2015, from <a href="http://www.emeraldgroupublishing.com/authors/guides/write/evidence_based.htm">http://www.emeraldgroupublishing.com/authors/guides/write/evidence_based.htm</a>
2	Adolphus, M. (n.d.-b). How to... carry out a literature review for a dissertation or research paper. Retrieved January 23, 2015, from <a href="http://www.emeraldgroupublishing.com/research/guides/methods/literature2.htm">http://www.emeraldgroupublishing.com/research/guides/methods/literature2.htm</a>
3	Agarwal, A., & Gupta, D. (2008). Security Requirements Elicitation Using View Points for Online System. In <i>Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on</i> (pp. 1238–1243).
4	Agrawal, S., & Haritsa, J. R. (2005). A framework for high-accuracy privacy-preserving mining. In <i>Data Engineering, 2005. ICDE 2005. Proceedings. 21st International Conference on</i> (pp. 193–204).
5	Anton, A. I., & Earp, J. B. (2004). A requirements taxonomy for reducing web site privacy vulnerabilities. <i>Requirements Engineering</i> , 9(3), 169–185.
6	Antón, A. I., & Earp, J. B. (2000). Strategies for developing policies and requirements for secure electronic commerce systems. In <i>E-commerce security and privacy</i> (Vol. 2, pp. 29–46).
7	Antón, A. I., Earp, J. B., & Carter, R. A. (2003). Precluding incongruous behavior by aligning software requirements with security and privacy policies. <i>Information and Software Technology</i> , 45(14), 967–977.
8	Antón, A. I., Earp, J. B., Potts, C., & Alspaugh, T. A. (2001). The role of policy and stakeholder privacy values in requirements engineering. In <i>Requirements Engineering, 2001. Proceedings. Fifth IEEE International Symposium on</i> (pp. 138–145).
9	Antón, A. I., Earp, J. B., & Reese, A. (2002). Analyzing website privacy requirements using a privacy goal taxonomy. In <i>Requirements Engineering, 2002. Proceedings. IEEE Joint International Conference on</i> (pp. 23–31).
10	Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. In <i>Security and Privacy, 2006 IEEE Symposium on</i> (p. 15–pp).
11	Beckers, K. (2012). Comparing privacy requirements engineering approaches. In <i>Proceedings - 2012 7th International Conference on Availability, Reliability and Security, ARES 2012</i> (pp. 574–581).
12	Breaux, T. D., & Antón, A. I. (2008). Analyzing regulatory rules for privacy and security requirements. <i>Software Engineering, IEEE Transactions on</i> , 34(1), 5–20.
13	Breaux, T. D., Vail, M. W., & Anton, A. I. (2006). Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. In <i>Requirements</i>

	<i>Engineering, 14th IEEE International Conference</i> (pp. 49–58).
14	Castro, J., Kolp, M., & Mylopoulos, J. (2002). Towards requirements-driven information systems engineering: the Tropos project. <i>Information Systems, 27</i> (6), 365–389.
15	Cavoukian, A., & others. (2009). Privacy by design: The 7 foundational principles. <i>Information and Privacy Commissioner of Ontario, Canada</i> .
16	Chiu, D. K. W., & Hung, P. C. K. (2005). Privacy and access control issues in financial enterprise content management. In <i>System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on</i> (p. 95c–95c).
17	Chung, L., & do Prado Leite, J. C. S. (2009). On non-functional requirements in software engineering. In <i>Conceptual modeling: Foundations and applications</i> (pp. 363–379). Springer.
18	Compagna, L., El Khoury, P., Krausová, A., Massacci, F., & Zannone, N. (2009). How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. <i>Artificial Intelligence and Law, 17</i> (1), 1–30.
19	Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Smith, R., & Hansen, M. (2013). Privacy Considerations for Internet Protocols. <i>RFC6973</i> , 36.
20	Crook, R., Ince, D., Lin, L., & Nuseibeh, B. (2002). Security requirements engineering: When anti-requirements hit the fan. In <i>Requirements Engineering, 2002. Proceedings. IEEE Joint International Conference on</i> (pp. 203–205).
21	Cysneiros, L. M., & do Prado Leite, J. C. (2004). Nonfunctional requirements: From elicitation to conceptual models. <i>Software Engineering, IEEE Transactions on, 30</i> (5), 328–350.
22	Cysneiros, L. M., & Yu, E. (2004). Non-functional requirements elicitation. In <i>Perspectives on software requirements</i> (pp. 115–138). Springer.
23	Da Rocha, S. V., Abdelouahab, Z., & Freire, E. (2005). Requirement Elicitation Based on Goals with Security and Privacy Policies in Electronic Commerce. In <i>WER</i> (pp. 63–74).
24	Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. Le, Tirtea, R., & Schiffner, S. (2015). Privacy and Data Protection by Design - from policy to engineering, 79. <i>Cryptography and Security</i> . Retrieved from <a href="http://arxiv.org/abs/1501.03726">http://arxiv.org/abs/1501.03726</a>
25	Dardenne, A., Van Lamsweerde, A., & Fickas, S. (1993). Goal-directed requirements acquisition. <i>Science of Computer Programming, 20</i> (1), 3–50.
26	Davies, N., & Langheinrich, M. (2013). Privacy by design. <i>IEEE Pervasive Computing</i> . Institute of Electrical and Electronics Engineers Inc.
27	Deng, M., Petkovic, M., Nalin, M., & Baroni, I. (2011). A Home Healthcare System in the Cloud--Addressing Security and Privacy Challenges. In <i>Cloud Computing (CLOUD), 2011</i>

	<i>IEEE International Conference on</i> (pp. 549–556).
28	Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. <i>Requirements Engineering</i> , 16, 3–32. doi:10.1007/s00766-010-0115-7
29	Duncan, G. (2007). Engineering. Privacy by design. <i>Science (New York, N.Y.)</i> , 317(5842), 1178–1179.
30	Elahi, G., Yu, E., & Zannone, N. (2010). A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities. <i>Requirements Engineering</i> , 15(1), 41–62.
31	EPPI. (2007). EPPI-Centre Methods form Conducting systematic review. Retrieved from <a href="https://eppi.ioe.ac.uk/cms/LinkClick.aspx?fileticket=hQBu8y4uVwl=&amp;tabid=88">https://eppi.ioe.ac.uk/cms/LinkClick.aspx?fileticket=hQBu8y4uVwl=&amp;tabid=88</a>
32	Fiegen, A. M. (2010). Systematic review of research methods: the case of business instruction. <i>Reference Services Review</i> . doi:10.1108/00907321011070883
33	Firesmith, D. G. (2003). Security use cases. <i>Journal of Object Technology</i> , 2(3).
34	Fung, B. C. M., Wang, K., & Yu, P. S. (2005). Top-down specialization for information and privacy preservation. In <i>Data Engineering, 2005. ICDE 2005. Proceedings. 21st International Conference on</i> (pp. 205–216).
35	Gedik, B., & Liu, L. (2005). Location privacy in mobile systems: A personalized anonymization model. In <i>Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on</i> (pp. 620–629).
36	Giorgini, P., Massacci, F., Mylopoulos, J., & Zannone, N. (2004). Requirements engineering meets trust management. In <i>Trust Management</i> (pp. 176–190). Springer.
37	Giorgini, P., Massacci, F., Mylopoulos, J., & Zannone, N. (2005). Modeling security requirements through ownership, permission and delegation. In <i>Requirements Engineering, 2005. Proceedings. 13th IEEE International Conference on</i> (pp. 167–176).
38	Gritzalis, S., Kavakli, E., Kalloniatis, C., Loucopoulos, P., & Gritzalis, S. (2006). Incorporating privacy requirements into the system design process: The PriS conceptual framework. <i>Internet Research</i> , 16(2), 140–158.
39	Gürses, S., Berendt, B., & Santen, T. (2006). Multilateral security requirements analysis for preserving privacy in ubiquitous environments. In <i>Proceedings of the UKDU Workshop</i> (pp. 51–64).
40	Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering privacy by design. <i>Computers, Privacy &amp; Data Protection</i> , 14.
41	Haley, C. B., Laney, R., Moffett, J. D., & Nuseibeh, B. (2008). Security requirements engineering: A framework for representation and analysis. <i>Software Engineering, IEEE</i>

	<i>Transactions on</i> , 34(1), 133–153.
42	He, Q., Antón, A. I., & others. (2003). A framework for modeling privacy requirements in role engineering. <i>Proc. of REFSQ</i> , 3, 137–146.
43	Herrmann, A., & Paech, B. (2008). MOQARE: misuse-oriented quality requirements engineering. <i>Requirements Engineering</i> , 13(1), 73–86.
44	Hoepman, J. (2012). Privacy design strategies. <i>arXiv Preprint arXiv:1210.6621</i> , 12. Retrieved from <a href="http://arxiv.org/abs/1210.6621">http://arxiv.org/abs/1210.6621</a>
45	Hong, D., Chiu, D. K. W., & Shen, V. Y. (2005). Requirements elicitation for the design of context-aware applications in a ubiquitous environment. In <i>Proceedings of the 7th international conference on Electronic commerce</i> (pp. 590–596).
46	Iachello, G., & Abowd, G. D. (2008). From privacy methods to a privacy toolbox. <i>ACM Transactions on Computer-Human Interaction</i> . doi:10.1145/1375761.1375763
47	Islam, S., Mouratidis, H., & Wagner, S. (2010). Towards a framework to elicit and manage security and privacy requirements from laws and regulations. In <i>Requirements Engineering: Foundation for Software Quality</i> (pp. 255–261). Springer.
48	Jensen, C., Tullio, J., Potts, C., & Mynatt, E. D. (2005). <i>STRAP: A Structured Analysis Framework for Privacy. Technology</i> . Retrieved from <a href="http://smartech.gatech.edu/handle/1853/4450">http://smartech.gatech.edu/handle/1853/4450</a>
49	Juels, A., & Pappu, R. (2003). Squealing Euros: Privacy protection in RFID-enabled banknotes. In <i>Financial cryptography</i> (pp. 103–121).
50	Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2007). Using privacy process patterns for incorporating privacy requirements into the system design process. In <i>Proceedings - Second International Conference on Availability, Reliability and Security, ARES 2007</i> (pp. 1009–1016). doi:10.1109/ARES.2007.156
51	Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2008). Addressing privacy requirements in system design: The PriS method. <i>Requirements Engineering</i> , 13(3), 241–255. doi:10.1007/s00766-008-0067-3
52	Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2009). Methods for designing privacy aware information systems: A review. In <i>PCI 2009 - 13th Panhellenic Conference on Informatics</i> (pp. 185–194). doi:10.1109/PCI.2009.45
53	Kotz, D., Avancha, S., & Baxi, A. (2009). A privacy framework for mobile health and home-care systems. ... <i>Privacy in Medical and Home-Care Systems</i> , 12. doi:978-1-60558-790
54	Kung, A., Freytag, J. C., & Kargl, F. (2011). Privacy-by-design in ITS applications. In <i>2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2011 - Digital Proceedings</i> . doi:10.1109/WoWMoM.2011.5986166

55	Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. In <i>UbiComp 2001: Ubiquitous Computing</i> (pp. 273–291).
56	Lapouchnian, A. (2005). Goal-oriented requirements engineering: An overview of the current research. <i>University of Toronto</i> .
57	Le Métayer, D. (2009). A formal privacy management framework. In <i>Formal Aspects in Security and Trust</i> (pp. 162–176). Springer.
58	Liu, L., Yu, E., & Mylopoulos, J. (2003). Security and privacy requirements analysis within a social setting. In <i>Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International</i> (pp. 151–161).
59	Mayer, N., Rifaut, A., Dubois, E., & others. (2005). Towards a risk-based security requirements engineering framework. In <i>Workshop on Requirements Engineering for Software Quality. In Proc. of REFSQ</i> (Vol. 5).
60	Mellado, D., Blanco, C., Sánchez, L. E., & Fernández-Medina, E. (2010). A systematic review of security requirements engineering. <i>Computer Standards &amp; Interfaces</i> , 32(4), 153–165.
61	Miyazaki, S., Mead, N., & Zhan, J. (2008). Computer-aided privacy requirements elicitation technique. In <i>Proceedings of the 3rd IEEE Asia-Pacific Services Computing Conference, APSCC 2008</i> (pp. 367–372). doi:10.1109/APSCC.2008.263
62	Mokbel, M. F., Chow, C.-Y., & Aref, W. G. (2006). The new Casper: query processing for location services without compromising privacy. In <i>Proceedings of the 32nd international conference on Very large data bases</i> (pp. 763–774).
63	O’flaherty, K. W., Stellwagen Jr, R. G., Walter, T. A., Watts, R. M., Ramsey, D. A., Veldhuisen, A. W., ... Dempster, P. B. (2001). System and method for managing data privacy in a database management system. Google Patents.
64	Otto, P. N., & Antón, A. I. (2007). Addressing legal requirements in requirements engineering. In <i>Requirements Engineering Conference, 2007. RE’07. 15th IEEE International</i> (pp. 5–14).
65	Pearson, S. (2009). Taking account of privacy when designing cloud computing services. In <i>Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing</i> (pp. 44–52).
66	Rajagopalan, S. R., Sankar, L., Mohajer, S., & Poor, H. V. (2011). Smart meter privacy: A utility-privacy framework. In <i>Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on</i> (pp. 190–195).
67	Rodríguez, A., Fernández-Medina, E., & Piattini, M. (2007). M-BPsec: a method for security requirement elicitation from a UML 2.0 business process specification. In <i>Advances in Conceptual Modeling--Foundations and Applications</i> (pp. 106–115). Springer.



68	Rubinstein, I. S. (2011). REGULATING PRIVACY BY DESIGN. <i>Berkeley Technology Law Journal</i> , 26(3), 1409–1456. Retrieved from <a href="http://ra.ocls.ca/ra/login.aspx?url=http://search.ebscohost.com/login.aspx?direct=true&amp;db=bth&amp;AN=74237061&amp;site=eds-live">http://ra.ocls.ca/ra/login.aspx?url=http://search.ebscohost.com/login.aspx?direct=true&amp;db=bth&amp;AN=74237061&amp;site=eds-live</a>
69	Sabo, J., Willet, M., & F Brown, P. (2012). <i>Privacy Management Reference Model Version 1.0</i> (p. 23). Retrieved from <a href="https://www.oasis-open.org/committees/download.php/45085/PMRM-v1.0-wd01-2012-02-07-clean.pdf">https://www.oasis-open.org/committees/download.php/45085/PMRM-v1.0-wd01-2012-02-07-clean.pdf</a>
70	Saleh, K. A. (2009). <i>Software Engineering</i> (pp. 74–75). J. Ross Publishing, Inc.
71	Salmenkaita, J.-P., & Sorvari, A. (2006). Method and business process to maintain privacy in distributed recommendation systems. Google Patents.
72	Sarma, S. E., Weis, S. A., & Engels, D. W. (2003). RFID systems and security and privacy implications. In <i>Cryptographic Hardware and Embedded Systems-CHES 2002</i> (pp. 454–469). Springer.
73	Schaar, P. (2010). Privacy by design. <i>Identity in the Information Society</i> , 3(2), 267–274.
74	Shin, D., Shin, D., Ahn, G.-J., Ahn, G.-J., Cho, S., Cho, S., ... Jin, S. (2003). On Modeling System-Centric Information for Role Engineering. In <i>Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies</i> (pp. 169–178). doi: <a href="http://doi.acm.org/10.1145/775412.775434">http://doi.acm.org/10.1145/775412.775434</a>
75	Shokri, R., Freudiger, J., & Hubaux, J.-P. (2010). <i>A unified framework for location privacy</i> .
76	Sindre, G., & Opdahl, A. L. (2005). Eliciting security requirements with misuse cases. <i>Requirements Engineering</i> , 10(1), 34–44.
77	Singh, S., & Bawa, S. (2007). A privacy, trust and policy based authorization framework for services in distributed environments. <i>International Journal of Computer Science</i> , 2(2), 85–92.
78	Spiekermann, S., & Cranor, L. F. (2009). <i>Engineering Privacy</i> . <i>IEEE Transactions on Software Engineering</i> (Vol. 35, pp. 67–82). doi:10.1109/TSE.2008.88
79	Steane, P. (2004). Fundamentals of a literature review. In <i>Surviving Your Thesis</i> (pp. 124–137). doi:10.4324/9780203299975
80	Sutcliffe, A., Fickas, S., & Sohlberg, M. M. (2006). PC-RE: a method for personal and contextual requirements engineering with some experience. <i>Requirements Engineering</i> , 11(3), 157–173.
81	Toro, A. D., Jiménez, B. B., Cortés, A. R., & Bonilla, M. T. (1999). A Requirements Elicitation Approach Based in Templates and Patterns. In <i>WER</i> (pp. 17–29).
82	Van Lamsweerde, A. (2004). Elaborating security requirements by construction of intentional anti-models. In <i>Proceedings of the 26th International Conference on Software</i>

	<i>Engineering</i> (pp. 148–157).
83	Van Lamsweerde, A. (2004). Goal-oriented requirements engineering: a roundtrip from research to practice [engineering read engineering]. In <i>Requirements Engineering Conference, 2004. Proceedings. 12th IEEE International</i> (pp. 4–7).
84	Van Lamsweerde, A., Brohez, S., De Landtsheer, R., Janssens, D., & others. (2003). From system goals to intruder anti-goals: attack generation and resolution for security requirements engineering. <i>Proc. of RHAS, 3</i> , 49–56.
85	Verdon, D., & McGraw, G. (2004). Risk analysis in software design. <i>Security &amp; Privacy, IEEE, 2(4)</i> , 79–84.
86	Xiao, X., & Tao, Y. (2006). Personalized privacy preservation. In <i>Proceedings of the 2006 ACM SIGMOD international conference on Management of data</i> (pp. 229–240).
87	Yang, H.-L., & Tang, J.-H. (2003). A three-stage model of requirements elicitation for Web-based information systems. <i>Industrial Management &amp; Data Systems, 103(6)</i> , 398–409.
88	Young, J. D., & Antón, A. I. (2010). A method for identifying software requirements based on policy commitments. In <i>Requirements Engineering Conference (RE), 2010 18th IEEE International</i> (pp. 47–56).
89	Yu, E. (2002). Designing for privacy and other competing requirements. <i>2nd Symposium on Requirements Engineering</i> . Retrieved from <a href="http://ftp.cs.toronto.edu/pub/cysneiro/privacy\n10.pdf">http://ftp.cs.toronto.edu/pub/cysneiro/privacy\n10.pdf</a>
90	Zuccato, A. (2004). Holistic security requirement engineering for electronic commerce. <i>Computers &amp; Security, 23(1)</i> , 63–76.

### 9.3 REFERENCIAS 2ª ITERACIÓN

1	Adolphus, M. (n.d.-a). How to conduct a systematic or evidence-based literature review. Retrieved February 07, 2015, from <a href="http://www.emeraldgroupublishing.com/authors/guides/write/evidence_based.htm">http://www.emeraldgroupublishing.com/authors/guides/write/evidence_based.htm</a>
2	Adolphus, M. (n.d.-b). How to... carry out a literature review for a dissertation or research paper. Retrieved January 23, 2015, from <a href="http://www.emeraldgroupublishing.com/research/guides/methods/literature2.htm">http://www.emeraldgroupublishing.com/research/guides/methods/literature2.htm</a>
3	Agarwal, A., & Gupta, D. (2008). Security Requirements Elicitation Using View Points for Online System. In <i>Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on</i> (pp. 1238–1243).
4	Agrawal, S., & Haritsa, J. R. (2005). A framework for high-accuracy privacy-preserving mining. In <i>Data Engineering, 2005. ICDE 2005. Proceedings. 21st International Conference on</i> (pp. 193–204).
5	Anton, A. I., & Earp, J. B. (2004). A requirements taxonomy for reducing web site privacy vulnerabilities. <i>Requirements Engineering, 9</i> (3), 169–185.
6	Antón, A. I., Earp, J. B., & Carter, R. A. (2003). Precluding incongruous behavior by aligning software requirements with security and privacy policies. <i>Information and Software Technology, 45</i> (14), 967–977.
7	Antón, A. I., Earp, J. B., Potts, C., & Alspaugh, T. A. (2001). The role of policy and stakeholder privacy values in requirements engineering. In <i>Requirements Engineering, 2001. Proceedings. Fifth IEEE International Symposium on</i> (pp. 138–145).
8	Antón, A. I., Earp, J. B., & Reese, A. (2002). Analyzing website privacy requirements using a privacy goal taxonomy. In <i>Requirements Engineering, 2002. Proceedings. IEEE Joint International Conference on</i> (pp. 23–31).
9	Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. In <i>Security and Privacy, 2006 IEEE Symposium on</i> (p. 15–pp).
10	Beckers, K. (2012). Comparing privacy requirements engineering approaches. In <i>Proceedings - 2012 7th International Conference on Availability, Reliability and Security, ARES 2012</i> (pp. 574–581).
11	Breaux, T. D., Vail, M. W., & Anton, A. I. (2006). Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. In <i>Requirements Engineering, 14th IEEE International Conference</i> (pp. 49–58).
12	Castro, J., Kolp, M., & Mylopoulos, J. (2002). Towards requirements-driven information systems engineering: the Tropos project. <i>Information Systems, 27</i> (6), 365–389.
13	Cavoukian, A., & others. (2009). Privacy by design: The 7 foundational principles. <i>Information and Privacy Commissioner of Ontario, Canada</i> .

14	Compagna, L., El Khoury, P., Krausová, A., Massacci, F., & Zannone, N. (2009). How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. <i>Artificial Intelligence and Law</i> , 17(1), 1–30.
15	Cysneiros, L. M., & do Prado Leite, J. C. (2004). Nonfunctional requirements: From elicitation to conceptual models. <i>Software Engineering, IEEE Transactions on</i> , 30(5), 328–350.
16	Da Rocha, S. V., Abdelouahab, Z., & Freire, E. (2005). Requirement Elicitation Based on Goals with Security and Privacy Policies in Electronic Commerce. In <i>WER</i> (pp. 63–74).
17	Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. Le, Tirtea, R., & Schiffner, S. (2015). Privacy and Data Protection by Design - from policy to engineering, 79. <i>Cryptography and Security</i> . Retrieved from <a href="http://arxiv.org/abs/1501.03726">http://arxiv.org/abs/1501.03726</a>
18	Davies, N., & Langheinrich, M. (2013). Privacy by design. <i>IEEE Pervasive Computing</i> . Institute of Electrical and Electronics Engineers Inc.
19	Deng, M., Petkovic, M., Nalin, M., & Baroni, I. (2011). A Home Healthcare System in the Cloud--Addressing Security and Privacy Challenges. In <i>Cloud Computing (CLOUD), 2011 IEEE International Conference on</i> (pp. 549–556).
20	Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. <i>Requirements Engineering</i> , 16, 3–32. doi:10.1007/s00766-010-0115-7
21	Duncan, G. (2007). Engineering. Privacy by design. <i>Science (New York, N.Y.)</i> , 317(5842), 1178–1179.
22	Elahi, G., Yu, E., & Zannone, N. (2010). A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities. <i>Requirements Engineering</i> , 15(1), 41–62.
23	EPPI. (2007). EPPI-Centre Methods form Conducting systematic review. Retrieved from <a href="https://eppi.ioe.ac.uk/cms/LinkClick.aspx?fileticket=hQBu8y4uVwl=&amp;tabid=88">https://eppi.ioe.ac.uk/cms/LinkClick.aspx?fileticket=hQBu8y4uVwl=&amp;tabid=88</a>
24	Fiegen, A. M. (2010). Systematic review of research methods: the case of business instruction. <i>Reference Services Review</i> . doi:10.1108/00907321011070883
25	Giorgini, P., Massacci, F., Mylopoulos, J., & Zannone, N. (2004). Requirements engineering meets trust management. In <i>Trust Management</i> (pp. 176–190). Springer.
26	Giorgini, P., Massacci, F., Mylopoulos, J., & Zannone, N. (2005). Modeling security requirements through ownership, permission and delegation. In <i>Requirements Engineering, 2005. Proceedings. 13th IEEE International Conference on</i> (pp. 167–176).
27	Gritzalis, S., Kavakli, E., Kalloniatis, C., Loucopoulos, P., & Gritzalis, S. (2006). Incorporating privacy requirements into the system design process: The PriS conceptual framework.

	<i>Internet Research</i> , 16(2), 140–158.
28	He, Q., Antón, A. I., & others. (2003). A framework for modeling privacy requirements in role engineering. <i>Proc. of REFSQ</i> , 3, 137–146.
29	Hoepman, J. (2012). Privacy design strategies. <i>arXiv Preprint arXiv:1210.6621</i> , 12. Retrieved from <a href="http://arxiv.org/abs/1210.6621">http://arxiv.org/abs/1210.6621</a>
30	Iachello, G., & Abowd, G. D. (2008). From privacy methods to a privacy toolbox. <i>ACM Transactions on Computer-Human Interaction</i> . doi:10.1145/1375761.1375763
31	Islam, S., Mouratidis, H., & Wagner, S. (2010). Towards a framework to elicit and manage security and privacy requirements from laws and regulations. In <i>Requirements Engineering: Foundation for Software Quality</i> (pp. 255–261). Springer.
32	Jensen, C., Tullio, J., Potts, C., & Mynatt, E. D. (2005). <i>STRAP: A Structured Analysis Framework for Privacy. Technology</i> . Retrieved from <a href="http://smartech.gatech.edu/handle/1853/4450">http://smartech.gatech.edu/handle/1853/4450</a>
33	Juels, A., & Pappu, R. (2003). Squealing Euros: Privacy protection in RFID-enabled banknotes. In <i>Financial cryptography</i> (pp. 103–121).
34	Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2007). Using privacy process patterns for incorporating privacy requirements into the system design process. In <i>Proceedings - Second International Conference on Availability, Reliability and Security, ARES 2007</i> (pp. 1009–1016). doi:10.1109/ARES.2007.156
35	Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2008). Addressing privacy requirements in system design: The PriS method. <i>Requirements Engineering</i> , 13(3), 241–255. doi:10.1007/s00766-008-0067-3
36	Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2009). Methods for designing privacy aware information systems: A review. In <i>PCI 2009 - 13th Panhellenic Conference on Informatics</i> (pp. 185–194). doi:10.1109/PCI.2009.45
37	Kotz, D., Avancha, S., & Baxi, A. (2009). A privacy framework for mobile health and home-care systems. ... <i>Privacy in Medical and Home-Care Systems</i> , 12. doi:978-1-60558-790
38	Kung, A., Freytag, J. C., & Kargl, F. (2011). Privacy-by-design in ITS applications. In <i>2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2011 - Digital Proceedings</i> . doi:10.1109/WoWMoM.2011.5986166
39	Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. In <i>Ubicomp 2001: Ubiquitous Computing</i> (pp. 273–291).
40	Lapouchnian, A. (2005). Goal-oriented requirements engineering: An overview of the current research. <i>University of Toronto</i> .
41	Le Métayer, D. (2009). A formal privacy management framework. In <i>Formal Aspects in</i>

	<i>Security and Trust</i> (pp. 162–176). Springer.
42	Liu, L., Yu, E., & Mylopoulos, J. (2003). Security and privacy requirements analysis within a social setting. In <i>Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International</i> (pp. 151–161).
43	Mayer, N., Rifaut, A., Dubois, E., & others. (2005). Towards a risk-based security requirements engineering framework. In <i>Workshop on Requirements Engineering for Software Quality. In Proc. of REFSQ</i> (Vol. 5).
44	Mellado, D., Blanco, C., Sánchez, L. E., & Fernández-Medina, E. (2010). A systematic review of security requirements engineering. <i>Computer Standards &amp; Interfaces</i> , 32(4), 153–165.
45	Miyazaki, S., Mead, N., & Zhan, J. (2008). Computer-aided privacy requirements elicitation technique. In <i>Proceedings of the 3rd IEEE Asia-Pacific Services Computing Conference, APSCC 2008</i> (pp. 367–372). doi:10.1109/APSCC.2008.263
46	Pearson, S. (2009). Taking account of privacy when designing cloud computing services. In <i>Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing</i> (pp. 44–52).
47	Rajagopalan, S. R., Sankar, L., Mohajer, S., & Poor, H. V. (2011). Smart meter privacy: A utility-privacy framework. In <i>Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on</i> (pp. 190–195).
48	Rodríguez, A., Fernández-Medina, E., & Piattini, M. (2007). M-BPsec: a method for security requirement elicitation from a UML 2.0 business process specification. In <i>Advances in Conceptual Modeling--Foundations and Applications</i> (pp. 106–115). Springer.
49	Rubinstein, I. S. (2011). REGULATING PRIVACY BY DESIGN. <i>Berkeley Technology Law Journal</i> , 26(3), 1409–1456. Retrieved from <a href="http://ra.ocls.ca/ra/login.aspx?url=http://search.ebscohost.com/login.aspx?direct=true&amp;db=bth&amp;AN=74237061&amp;site=eds-live">http://ra.ocls.ca/ra/login.aspx?url=http://search.ebscohost.com/login.aspx?direct=true&amp;db=bth&amp;AN=74237061&amp;site=eds-live</a>
50	Sabo, J., Willet, M., & F Brown, P. (2012). <i>Privacy Management Reference Model Version 1.0</i> (p. 23). Retrieved from <a href="https://www.oasis-open.org/committees/download.php/45085/PMRM-v1.0-wd01-2012-02-07-clean.pdf">https://www.oasis-open.org/committees/download.php/45085/PMRM-v1.0-wd01-2012-02-07-clean.pdf</a>
51	Saleh, K. A. (2009). <i>Software Engineering</i> (pp. 74–75). J. Ross Publishing, Inc.
52	Schaar, P. (2010). Privacy by design. <i>Identity in the Information Society</i> , 3(2), 267–274.
53	Shokri, R., Freudiger, J., & Hubaux, J.-P. (2010). <i>A unified framework for location privacy</i> .
54	Sindre, G., & Opdahl, A. L. (2005). Eliciting security requirements with misuse cases. <i>Requirements Engineering</i> , 10(1), 34–44.

55	Singh, S., & Bawa, S. (2007). A privacy, trust and policy based authorization framework for services in distributed environments. <i>International Journal of Computer Science</i> , 2(2), 85–92.
56	Spiekermann, S., & Cranor, L. F. (2009). <i>Engineering Privacy</i> . <i>IEEE Transactions on Software Engineering</i> (Vol. 35, pp. 67–82). doi:10.1109/TSE.2008.88
57	Steane, P. (2004). Fundamentals of a literature review. In <i>Surviving Your Thesis</i> (pp. 124–137). doi:10.4324/9780203299975
58	Toro, A. D., Jiménez, B. B., Cortés, A. R., & Bonilla, M. T. (1999). A Requirements Elicitation Approach Based in Templates and Patterns. In <i>WER</i> (pp. 17–29).
59	Van Lamsweerde, A. (2004). Elaborating security requirements by construction of intentional anti-models. In <i>Proceedings of the 26th International Conference on Software Engineering</i> (pp. 148–157).
60	Yu, E. (2002). Designing for privacy and other competing requirements. <i>2nd Symposium on Requirements Engineering</i> . Retrieved from <a href="http://ftp.cs.toronto.edu/pub/cysneiro/privacy\n10.pdf">http://ftp.cs.toronto.edu/pub/cysneiro/privacy\n10.pdf</a>

## 9.4 REFERENCIAS 3ª ITERACIÓN

1	Adolphus, M. (n.d.-a). How to conduct a systematic or evidence-based literature review. Retrieved February 07, 2015, from <a href="http://www.emeraldgrouppublishing.com/authors/guides/write/evidence_based.htm">http://www.emeraldgrouppublishing.com/authors/guides/write/evidence_based.htm</a>
2	Adolphus, M. (n.d.-b). How to... carry out a literature review for a dissertation or research paper. Retrieved January 23, 2015, from <a href="http://www.emeraldgrouppublishing.com/research/guides/methods/literature2.htm">http://www.emeraldgrouppublishing.com/research/guides/methods/literature2.htm</a>
3	Agrawal, S., & Haritsa, J. R. (2005). A framework for high-accuracy privacy-preserving mining. In <i>Data Engineering, 2005. ICDE 2005. Proceedings. 21st International Conference on</i> (pp. 193–204).
4	Anton, A. I., & Earp, J. B. (2004). A requirements taxonomy for reducing web site privacy vulnerabilities. <i>Requirements Engineering</i> , 9(3), 169–185.
5	Antón, A. I., Earp, J. B., & Carter, R. A. (2003). Precluding incongruous behavior by aligning software requirements with security and privacy policies. <i>Information and Software Technology</i> , 45(14), 967–977.
6	Antón, A. I., Earp, J. B., Potts, C., & Alspaugh, T. A. (2001). The role of policy and stakeholder privacy values in requirements engineering. In <i>Requirements Engineering, 2001. Proceedings. Fifth IEEE International Symposium on</i> (pp. 138–145).
7	Antón, A. I., Earp, J. B., & Reese, A. (2002). Analyzing website privacy requirements using a privacy goal taxonomy. In <i>Requirements Engineering, 2002. Proceedings. IEEE Joint International Conference on</i> (pp. 23–31).
8	Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. In <i>Security and Privacy, 2006 IEEE Symposium on</i> (p. 15–pp).
9	Beckers, K. (2012). Comparing privacy requirements engineering approaches. In <i>Proceedings - 2012 7th International Conference on Availability, Reliability and Security, ARES 2012</i> (pp. 574–581).
10	Cavoukian, A., & others. (2009). Privacy by design: The 7 foundational principles. <i>Information and Privacy Commissioner of Ontario, Canada</i> .
11	Compagna, L., El Khoury, P., Krausová, A., Massacci, F., & Zannone, N. (2009). How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. <i>Artificial Intelligence and Law</i> , 17(1), 1–30.
12	Cysneiros, L. M., & do Prado Leite, J. C. (2004). Nonfunctional requirements:



	From elicitation to conceptual models. <i>Software Engineering, IEEE Transactions on</i> , 30(5), 328–350.
13	Da Rocha, S. V., Abdelouahab, Z., & Freire, E. (2005). Requirement Elicitation Based on Goals with Security and Privacy Policies in Electronic Commerce. In <i>WER</i> (pp. 63–74).
14	Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. Le, Tirtea, R., & Schiffner, S. (2015). Privacy and Data Protection by Design - from policy to engineering, 79. <i>Cryptography and Security</i> . Retrieved from <a href="http://arxiv.org/abs/1501.03726">http://arxiv.org/abs/1501.03726</a>
15	Davies, N., & Langheinrich, M. (2013). Privacy by design. <i>IEEE Pervasive Computing</i> . Institute of Electrical and Electronics Engineers Inc.
16	Deng, M., Petkovic, M., Nalin, M., & Baroni, I. (2011). A Home Healthcare System in the Cloud--Addressing Security and Privacy Challenges. In <i>Cloud Computing (CLOUD), 2011 IEEE International Conference on</i> (pp. 549–556).
17	Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. <i>Requirements Engineering</i> , 16, 3–32. doi:10.1007/s00766-010-0115-7
18	Duncan, G. (2007). Engineering. Privacy by design. <i>Science (New York, N.Y.)</i> , 317(5842), 1178–1179.
19	EPPI. (2007). EPPI-Centre Methods form Conducting systematic review. Retrieved from <a href="https://eppi.ioe.ac.uk/cms/LinkClick.aspx?fileticket=hQBu8y4uVwI=&amp;tabid=88">https://eppi.ioe.ac.uk/cms/LinkClick.aspx?fileticket=hQBu8y4uVwI=&amp;tabid=88</a>
20	Fabian, B., Gürses, S., Heisel, M., Santen, T., & Schmidt, H. (2010). A comparison of security requirements engineering methods. <i>Requirements Engineering</i> , 15, 7–40. doi:10.1007/s00766-009-0092-x
21	Fiegen, A. M. (2010). Systematic review of research methods: the case of business instruction. <i>Reference Services Review</i> . doi:10.1108/00907321011070883
22	Gritzalis, S., Kavakli, E., Kalloniatis, C., Loucopoulos, P., & Gritzalis, S. (2006). Incorporating privacy requirements into the system design process: The PriS conceptual framework. <i>Internet Research</i> , 16(2), 140–158.
23	He, Q., Antón, A. I., & others. (2003). A framework for modeling privacy requirements in role engineering. <i>Proc. of REFSQ</i> , 3, 137–146.
24	Hoepman, J. (2012). Privacy design strategies. <i>arXiv Preprint arXiv:1210.6621</i> ,

	12. Retrieved from <a href="http://arxiv.org/abs/1210.6621">http://arxiv.org/abs/1210.6621</a>
25	Iachello, G., & Abowd, G. D. (2008). From privacy methods to a privacy toolbox. <i>ACM Transactions on Computer-Human Interaction</i> . doi:10.1145/1375761.1375763
26	Islam, S., Mouratidis, H., & Wagner, S. (2010). Towards a framework to elicit and manage security and privacy requirements from laws and regulations. In <i>Requirements Engineering: Foundation for Software Quality</i> (pp. 255–261). Springer.
27	Jensen, C., Tullio, J., Potts, C., & Mynatt, E. D. (2005). <i>STRAP: A Structured Analysis Framework for Privacy. Technology</i> . Retrieved from <a href="http://smartech.gatech.edu/handle/1853/4450">http://smartech.gatech.edu/handle/1853/4450</a>
28	Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2007). Using privacy process patterns for incorporating privacy requirements into the system design process. In <i>Proceedings - Second International Conference on Availability, Reliability and Security, ARES 2007</i> (pp. 1009–1016). doi:10.1109/ARES.2007.156
29	Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2008). Addressing privacy requirements in system design: The PriS method. <i>Requirements Engineering</i> , 13(3), 241–255. doi:10.1007/s00766-008-0067-3
30	Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2009). Methods for designing privacy aware information systems: A review. In <i>PCI 2009 - 13th Panhellenic Conference on Informatics</i> (pp. 185–194). doi:10.1109/PCI.2009.45
31	Kotz, D., Avancha, S., & Baxi, A. (2009). A privacy framework for mobile health and home-care systems. ... <i>Privacy in Medical and Home-Care Systems</i> , 12. doi:978-1-60558-790
32	Kung, A., Freytag, J. C., & Kargl, F. (2011). Privacy-by-design in ITS applications. In <i>2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2011 - Digital Proceedings</i> . doi:10.1109/WoWMoM.2011.5986166
33	Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. In <i>UbiComp 2001: Ubiquitous Computing</i> (pp. 273–291).
34	Lapouchnian, A. (2005). Goal-oriented requirements engineering: An overview of the current research. <i>University of Toronto</i> .
35	Le Métayer, D. (2009). A formal privacy management framework. In <i>Formal Aspects in Security and Trust</i> (pp. 162–176). Springer.
36	Liu, L., Yu, E., & Mylopoulos, J. (2003). Security and privacy requirements analysis within a social setting. In <i>Requirements Engineering Conference</i> ,

	2003. <i>Proceedings. 11th IEEE International</i> (pp. 151–161).
37	Miyazaki, S., Mead, N., & Zhan, J. (2008). Computer-aided privacy requirements elicitation technique. In <i>Proceedings of the 3rd IEEE Asia-Pacific Services Computing Conference, APSCC 2008</i> (pp. 367–372). doi:10.1109/APSCC.2008.263
38	Pearson, S. (2009). Taking account of privacy when designing cloud computing services. In <i>Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing</i> (pp. 44–52).
39	Rajagopalan, S. R., Sankar, L., Mohajer, S., & Poor, H. V. (2011). Smart meter privacy: A utility-privacy framework. In <i>Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on</i> (pp. 190–195).
40	Rubinstein, I. S. (2011). REGULATING PRIVACY BY DESIGN. <i>Berkeley Technology Law Journal</i> , 26(3), 1409–1456. Retrieved from <a href="http://ra.ocls.ca/ra/login.aspx?url=http://search.ebscohost.com/login.aspx?direct=true&amp;db=bth&amp;AN=74237061&amp;site=eds-live">http://ra.ocls.ca/ra/login.aspx?url=http://search.ebscohost.com/login.aspx?direct=true&amp;db=bth&amp;AN=74237061&amp;site=eds-live</a>
41	Sabo, J., Willet, M., & F Brown, P. (2012). <i>Privacy Management Reference Model Version 1.0</i> (p. 23). Retrieved from <a href="https://www.oasis-open.org/committees/download.php/45085/PMRM-v1_0-wd01-2012-02-07-clean.pdf">https://www.oasis-open.org/committees/download.php/45085/PMRM-v1_0-wd01-2012-02-07-clean.pdf</a>
42	Saleh, K. A. (2009). <i>Software Engineering</i> (pp. 74–75). J. Ross Publishing, Inc.
43	Schaar, P. (2010). Privacy by design. <i>Identity in the Information Society</i> , 3(2), 267–274.
44	Shokri, R., Freudiger, J., & Hubaux, J.-P. (2010). <i>A unified framework for location privacy</i> .
45	Singh, S., & Bawa, S. (2007). A privacy, trust and policy based authorization framework for services in distributed environments. <i>International Journal of Computer Science</i> , 2(2), 85–92.
46	Spiekermann, S., & Cranor, L. F. (2009). <i>Engineering Privacy</i> . <i>IEEE Transactions on Software Engineering</i> (Vol. 35, pp. 67–82). doi:10.1109/TSE.2008.88
47	Steane, P. (2004). Fundamentals of a literature review. In <i>Surviving Your Thesis</i> (pp. 124–137). doi:10.4324/9780203299975
48	Toro, A. D., Jiménez, B. B., Cortés, A. R., & Bonilla, M. T. (1999). A Requirements Elicitation Approach Based in Templates and Patterns. In <i>WER</i> (pp. 17–29).

49	Yu, E. (2002). Designing for privacy and other competing requirements. <i>2nd Symposium on Requirements Engineering</i> . Retrieved from <a href="http://ftp.cs.toronto.edu/pub/cysneiro/privacy/n10.pdf">http://ftp.cs.toronto.edu/pub/cysneiro/privacy/n10.pdf</a>
----	--