Elementos Reusables para Experimentar con Metodologías Basadas en Estrategias y Patrones de Privacidad

Caiza, Julio C.[1,*]; **López, Gabriel**[1]; **Guamán, Danny S.**[1]

[1]*Escuela Politécnica Nacional, Departamento de Electrónica, Telecomunicaciones y Redes de Información, Quito, Ecuador*

Resumen: En línea con el avance global, la región latinoamericana ha establecido legislaciones que buscan establecer orden en un contexto donde la explotación de los datos personales y la protección de la privacidad de las personas son de gran relevancia. Uno de los mecanismos establecidos para alcanzar tal orden es la *Protección de Datos desde el Diseño* de los sistemas. Para materializarlo, los investigadores en el dominio han enfocado muchos esfuerzos en los patrones de privacidad, en metodologías basadas en ellos y en las estrategias de diseño. Sin embargo, el estado del arte señala que hace falta evidencia empírica para validar su aplicación y utilidad. Asimismo, señala la complejidad para llevar a cabo experimentos que provean dicha evidencia. El objetivo de este trabajo es contribuir a la obtención de evidencia empírica y realizar un análisis de las metodologías que hacen uso de patrones de privacidad y de estrategias de diseño para definir un conjunto de elementos que puedan ser reusados al realizar experimentos. Para ello, hemos revisado la literatura, siguiendo un conjunto de pasos sistematizados y un proceso de bola de nieve, en busca de metodologías basadas en patrones y estrategias de diseño. A partir de los resultados se observa que las estrategias de diseño de Hoepman son las más aceptadas y que hay tres enfoques de metodologías que hacen uso de ellas. En estos enfoques, se identifican elementos que podrían ser reusables al plantear experimentos: estrategias, subestrategias, patrones de privacidad, PETs, relaciones y sistemas de patrones.

Palabras clave: privacidad, protección de datos, metodologías, diseño, estrategias, patrones.

Reusable Elements for Experimenting with Methodologies Based on Strategies and Privacy Patterns

Abstract: In line with global trends, Latin America has established legislation to provide order in a context where personal data exploitation and the protection of people's privacy are relevant. *Data Protection by Design* is one of the mechanisms for achieving such an order. To materialize it, researchers in the domain have focused their efforts on privacy patterns, methodologies based on them, and design strategies. However, state of the art shows that there is a lack of empirical evidence about their application and utility. Likewise, it also highlights the complexity of carrying out experiments to provide such evidence. This study aims to contribute to providing such evidence and make an analysis of methodologies based on privacy patterns and design strategies to propose a set of reusable elements to be used in experiments. We have reviewed the literature, following systematized steps and implementing the snowballing technique to find methodologies based on privacy patterns and design strategies. The results show that the design strategies by Hoepman are the most accepted, and there are three approaches of methodologies making use of them. In these three approaches, we have identified elements that could be reused when planning experiments: strategies, sub-strategies, privacy patterns, PETs, relationships, and pattern systems.

Keywords: privacy, data protection, methodologies, design, strategies, patterns.

1. INTRODUCCIÓN

La *Privacidad* y la *Protección de Datos* han ido ganando protagonismo a medida que la región latinoamericana ha ido estableciendo legislaciones en esta materia. En el caso ecuatoriano, el 26 de mayo de 2021 se publicó la **Ley Orgánica de Protección de Datos Personales** (Asamblea Nacional de la República del Ecuador, 2021). Esta ley busca establecer un orden para, por un lado, permitir la explotación adecuada de los datos, a la vez que busca salvaguardar los datos personales, y, por lo tanto, la privacidad de las personas.

Esta ley, fundamentada en el *Reglamento General de Protección de Datos Europeo* (European Parliament &

*julio.caiza@epn.edu.ec
Recibido: 10/05/2022
Aceptado: 22/02/2023
Publicado en línea: 01/05/2023
10.33333/rp.vol51n2.10

Council of the European Union, 2016), establece la *Protección de datos desde el diseño* como uno de los mecanismos para cumplir con su objetivo. Este concepto está alineado con el de la *Privacidad desde el diseño* (Cavoukian, 2009), que busca proteger la privacidad de las personas desde las etapas tempranas del proceso de ingeniería de los sistemas.

La literatura muestra que la cantidad de contribuciones para realizar el proceso de ingeniería con consideraciones de privacidad ha ido en aumento (Gürses & Del Alamo, 2016); más aún aquellas dentro de la actividad de diseño de los sistemas respetuosos de la privacidad (Caiza et al., 2019; Lenhard et al., 2017; Morales-Trujillo et al., 2019). En estos estudios ha quedado de manifiesto que los patrones de privacidad son un área que ha captado mucha atención por parte de los investigadores. Por su naturaleza, los patrones, que son soluciones reusables a problemas que se repiten en contextos determinados por varias fuerzas, se ajustan a un contexto donde se requieren elementos que sistematicen la inclusión de cuestiones de privacidad en el proceso de desarrollo brindando un soporte adecuado a ingenieros no expertos en privacidad.

En el ámbito de investigación en patrones, los autores en Caiza et al. (2019) señalan la importancia que iban adquiriendo elementos como las estrategias (enfoques para materializar principios) y las metodologías, aunque de manera independiente. En ese mismo trabajo se señala la carencia de estudios empíricos que evalúen la aplicación de los patrones o sus beneficios, dejando a estos como asunciones extrapoladas de otros dominios como el de la orientación a objetos (Gamma et al., 1995), donde han tenido un notable éxito.

Específicamente, preguntas como ¿están los patrones de privacidad listos para ser usados?, ¿son fáciles de aplicar? y ¿proveen beneficios? habían quedado planteadas y su respuesta era necesaria de cara a avanzar en la investigación en patrones de privacidad y dar pruebas de su utilidad. En Caiza et al. (2021), se llevó a cabo un estudio empírico exploratorio, sin que aún se hayan obtenido resultados concluyentes. En este estudio, se señalan las limitaciones y oportunidades de experimentación en el área, haciendo énfasis en la dificultad y complejidad del proceso de experimentación.

En este contexto, en el presente artículo presentamos un conjunto de elementos que se pueden reusar al experimentar con metodologías que hacen uso de estrategias de diseño y patrones. Esto incluye aquellos elementos que forman parte de una metodología y aquellos que forman parte de la instrumentación para llevar a cabo un experimento.

Con este objetivo, se ha revisado el estado del arte siguiendo un proceso sistematizado guiado por los pasos dados en Petersen et al. (2015). Este proceso se ha organizado para contestar las siguientes preguntas de investigación:

RQ1. ¿Qué metodologías de diseño respetuosas con la privacidad que hacen uso de patrones y estrategias han sido reportadas en el estado del arte?
RQ2. ¿Qué elementos forman parte de las metodologías encontradas?
RQ3. ¿Qué instrumentos para experimentar con esas metodologías son requeridos?

2. TRABAJO RELACIONADO

Aunque se han llevado a cabo algunos estudios de literatura que buscan y estudian el desarrollo de los patrones de privacidad (Lenhard et al., 2017; Caiza et al., 2019 y Al-Slais, 2020), aún no se ha realizado un análisis de los patrones de privacidad trabajando conjuntamente con estrategias de diseño y dentro de métodos. Menos aún, con un objetivo hacia determinar elementos que ayuden a obtener evidencia experimental, que es aún carente en el dominio.

El trabajo reportado en Lenhard et al. (2017) estudia aquellos artículos primarios que proponen patrones de privacidad, y los categoriza, por ejemplo, según la etapa en el proceso de desarrollo en la que podrían servir. Asimismo, los categoriza según el nivel de madurez de las propuestas, y concluye que hace falta más trabajo empírico, sin realizar un análisis en profundidad respecto al ámbito de la experimentación o como lograrlo.

El estudio reportado en Caiza et al. (2019) toma un enfoque más amplio que el anterior y se orienta a determinar todos los posibles elementos, incluyendo los patrones de privacidad, que se usen en el proceso de diseño respetuoso con la privacidad. Dentro de sus resultados, resaltan que elementos como las estrategias, los patrones y los modelos de referencia son los más estudiados en el ámbito. Específicamente, identifican que los patrones de privacidad son los elementos más reportados y mencionan que solo la propuesta de más patrones no garantiza su implementación o adopción. Aunque señalan la falta de evidencia empírica y dejan planteadas preguntas referentes a la efectividad, a los beneficios y a su adopción; no señalan cómo avanzar hacia obtener evidencia.

Al-Slais (2020) adopta un enfoque más amplio y estudia la literatura para categorizar metodologías para la ingeniería de privacidad. Las categoriza por aquellas basadas en la evaluación de impacto a la privacidad, en aquellas basadas en modelos y aquellas orientas a la ingeniería de requisitos de privacidad. Además, identifica a los patrones de privacidad como elementos usados dentro de ellas y llama por el desarrollo de más patrones para la amplia variedad de aplicaciones de software que pueden existir. Sin embargo, no se aborda la necesidad de la evidencia empírica de cara a probar su aplicación.

En este escenario, donde aún varios esfuerzos se van centrando en el desarrollo de nuevos patrones de privacidad, sigue pendiente el conseguir evidencia empírica respecto a su proceso y facilidad de aplicación, además de probar sus beneficios. Uno de los tipos de estudio más relevantes para tal fin es la experimentación. Precisamente, el presente trabajo analiza y aspira a brindar un conjunto de elementos reusables para llevar a cabo experimentos con metodologías que hacen uso de estrategias de diseño y patrones de privacidad.

3. MÉTODO

La estrategia utilizada para la búsqueda de información se basa en un proceso sistematizado que utiliza los pasos de estudios sistemáticos de literatura (Petersen et al., 2015) y en la búsqueda de referencias a través de una bola de nieve hacia atrás — *backward snowballing* (Wohlin 2014). La base de datos utilizada en el proceso fue Scopus, reconocida como la mayor base de datos de trabajo por pares (Elsevier, 2020) y que ofrece buenos resultados respecto a la búsqueda de estudios primarios en el dominio de la computación (Cavacini, 2015).

Tabla 1. Cadenas de búsqueda

	Cadenas de búsqueda	Fecha
1	TITLE-ABS-KEY (("privacy" OR "data protection") AND ("engineering" OR "design") AND ("methodology" OR "method" OR "process" OR "procedure" OR "approach") AND ("strategy" AND "pattern"))	3/24/2021
2	TITLE-ABS-KEY (("privacy engineering" OR "privacy design" OR "privacy by design") AND ("methodology" OR "method" OR "process" OR "procedure" OR "approach") AND ("review" OR "mapping" OR "survey" OR "state of the art")) AND TITLE ("review" OR "mapping" OR "survey" OR "state of the art")	3/24/2021

Tabla 2. Criterios de inclusión y exclusión

Inclusión/exclusión automática	
Tipo de documento	Artículo de revista, artículo de conferencia, libro y capítulo de libro.
Idioma	Inglés.
Área	Informática e ingeniería.
Inclusión/exclusión manual	
Inclusión general	Área de privacidad y protección de datos.
Inclusión de estudios primarios	Reporta una metodología de diseño de privacidad basada en estrategias y patrones.
Inclusión de estudios secundarios	Reporta metodologías sobre el diseño de la privacidad.

Tabla 3. Procedimiento de inclusión y exclusión

Paso	Descripción
1	**Primera Iteración**: leer el título de cada artículo resultado de la *cadena 1* y marcarlo: - *Poco claro* => Si no hay un argumento claro para la exclusión. - *Inclusión* => Si cumple con todos los criterios de inclusión. - *Exclusión* => Si hay un criterio de inclusión que no se cumple.
2	**Segunda iteración**: leer el título y el resumen de los trabajos incluidos y no claros para finalmente incluirlos o excluirlos.
3a	Reunir un conjunto *cap1* de artículos primarios.
3b	Reunir un conjunto *cas1* de artículos secundarios.
4	Examinar el conjunto *cas1* de artículos secundarios y obtener artículos primarios de interés.
5	Leer el título y el resumen de los trabajos anteriores recogidos en el paso 4. Inclúyalos o exclúyalos.
6	Reunir un conjunto *cap2* de artículos primarios incluidos en el paso 5.
7	Reunir el conjunto final de artículos que unen *cap1* y *cap2*.

Una vez definido las preguntas de investigación, se procedió a estructurar dos cadenas de búsqueda (Tabla 1), una para identificación de estudios primarios y otra para estudios secundarios. Sobre los resultados obtenidos al ejecutar las cadenas (136 para la cadena 1 y 82 para la cadena 2), se aplicaron criterios de inclusión y exclusión considerando el objetivo del estudio (Tabla 2). Estos criterios se dividieron en aquellos que podían ser aplicados de manera automática mediante las funcionalidades de Scopus y aquellos que se aplican de manera manual al leer la información de los artículos. Además, se definió el proceso que debían seguir los dos miembros del equipo de investigación asignados a esta etapa (Tabla 3).

Luego de un proceso de 2 iteraciones de inclusión y exclusión, se obtuvieron 7 artículos primarios relevantes para el contexto del estudio y 3 secundarios. Sobre los artículos secundarios, se aplicó la técnica de bola de nieve hacia atrás, se adicionaron 3

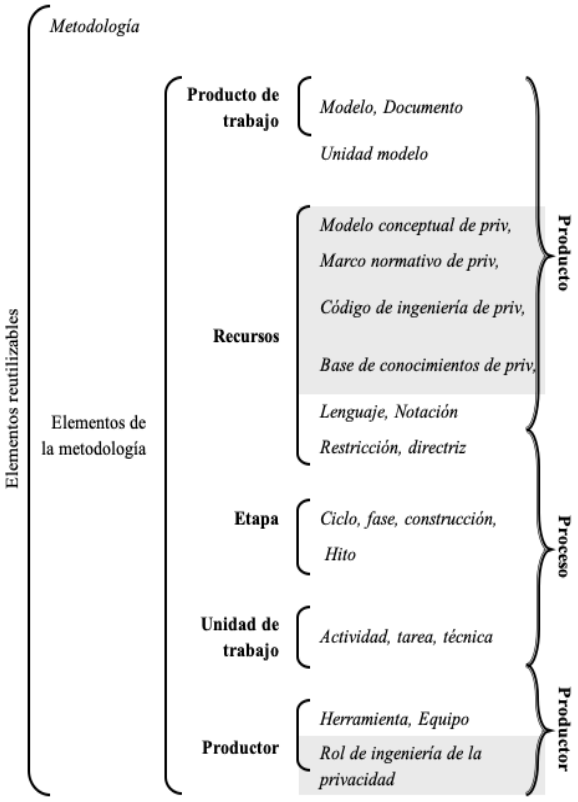

Figura 1. Elementos de metodologías según (International Organization for Standardization, 2014)

artículos primarios. De los 10 artículos primarios, se escogieron aquellos que utilizaban un enfoque común hacia las estrategias y patrones de privacidad, aquel propuesto en Hoepman (2014); se obtuvieron 8 artículos para la etapa de extracción y análisis. Vale la pena destacar que este enfoque, además de ser acogido por varios investigadores en el área de la ingeniería de privacidad, también ha sido considerado y adoptado por entidades europeas (Danezis et al., 2014), por la Agencia Española de Protección de Datos (Spanish Data Protection Authority, 2019) e incluso en el reciente estándar sobre Ingeniería de Privacidad para los Procesos del Ciclo de Vida de los Sistemas (International Organization for Standardization, 2019).

Para la etapa de extracción de información, se han utilizado diferentes categorizaciones obtenidas de normativas o de propuestas ampliamente aceptadas por los investigadores. Para extraer los elementos de las metodologías estudiadas. Hemos usado los tipos de elementos propuestos en el *Metamodelo de ingeniería de software para desarrollar metodologías de desarrollo definido en el estándar ISO/IEC 24744*

(International Organization for Standardization, 2014) (Figura 1). Asimismo, se ha procedido a refinar los elementos del tipo *Base de conocimiento de privacidad* mientras se los identificaba en el proceso de lectura.

Para establecer los tipos de elementos requeridos para preparar la instrumentación de un experimento, hemos tomado aquellos mencionados para el ámbito de la ingeniería de software (Wohlin et al., 2012) (Tabla 4). Debido a que estos elementos aparecen cuando las propuestas alcanzan un nivel de madurez de evidencia empírica, lo hemos determinado a través de la clasificación propuesta en Wieringa et al. (2006): *artículos de experiencia*, *artículos de opinión*, *artículos filosóficos*,

Tabla 4. Elementos de instrumentación en un experimento (Wohlin et al., 2012)

Página	Superior
Objetos de estudio	Se refieren a aquellos elementos que serán usados para evaluar lo que se está estudiando. Por ejemplo, los documentos con especificaciones de requerimientos o documentos código, o problemas a proponer.
Guías de experimentación	Son las instrucciones que guían a los participantes a través del experimento. Por ejemplo, las descripciones del proceso o procesos a seguir o un listado de tareas.
Instrumentos de medición	Aquellos elementos relacionados a la medición y recolección de los datos en un experimento. Por ejemplo, formularios manuales o entrevistas.
Herramientas de soporte	Son aquellas herramientas que van a servir como soporte en alguna de las etapas del proceso de experimentación.

Tabla 5. Artículos primarios analizados

Año	Cita	Título
2014	(Hoepman, 2014)	Privacy design strategies
2016	(Colesky et al., 2016)	A Critical Analysis of Privacy Design Strategies
2017	(Berendt & Preibusch, 2017)	Toward accountable discrimination-aware data mining: The importance of keeping the human in the loop and under the looking glass.
2018	(Colesky et al., 2018)	A system of privacy patterns for user control
2018	(Colesky & Caiza, 2019)	A system of privacy patterns for informing users: Creating a pattern system
2019	(Baldassarre et al., 2019)	Privacy Oriented Software Development
2020	(Baldassarre et al., 2020)	Integrating security and privacy in software development
2019	(Ahmadian et al., 2019)	Privacy-enhanced system design modeling based on privacy features

propuestas de solución, *investigación de validación* e *investigación de evaluación*. Las dos últimas categorías se asocian a estudios que muestran evidencia empírica a nivel controlado (e.g., en laboratorios) o a nivel de la práctica en un ambiente de producción, respectivamente.

4. RESULTADOS

La Tabla 5 muestra los 8 artículos que se basan en un enfoque común: aquel propuesto por Hoepman (Hoepman, 2014), los mismos que han sido finalmente analizados.

4.1 RQ1. ¿Qué metodologías de diseño respetuosas con la privacidad que hacen uso de patrones y estrategias han sido reportadas en el estado del arte?

Considerando los artículos estudiados, se puede notar que el enfoque de Hoepman, inicialmente planteado en Hoepman (2014) se ha ido extendiendo en términos de elementos en el modelo (e.g., aparecimiento de tácticas) (Colesky et al., 2016) o en términos a nuevas instancias de los elementos (e.g., nuevas estrategias) (Berendt & Preibusch, 2017).

Se puede notar tres procesos o métodos basados en las estrategias y patrones. El primero (Colesky et al., 2018; Colesky & Caiza, 2019) se alinea con la evolución de los conjuntos de patrones de diseño (Buschmann et al., 1996). Es decir, los conjuntos de patrones se agrupan en catálogos, luego llegan a ser sistemas, para finalmente, evolucionar a lenguajes de patrones. En este enfoque, se espera que a medida que los conjuntos de patrones evolucionen, estos lleguen a estar fuertemente interrelacionados, a definir guías claras de aplicación, e incluso a permitir construir sistemas, estructuras fundamentales o módulos completos en dominios muy específicos. En este enfoque, se tendría un contexto en el que se presentan requisitos de privacidad (planteados como objetivos o como amenazas (Notario et al., 2015)), sobre el cual habría que identificar las estrategias a aplicar y, dentro de estas, las tácticas. Al llegar al conjunto de patrones apropiado para esa táctica, se deberá identificar al menos un patrón que podría ser útil; luego, bajo las relaciones entre ellos, se podría identificar el conjunto de patrones más apropiado para el problema planteado.

En el planteamiento propuesto por Baldassarre et al., (2019, 2020) se contempla un método para todo el ciclo de desarrollo de software. Aquí, las estrategias de diseño y los patrones de privacidad se incluyen dentro de un producto de trabajo (de una etapa de evaluación) conocido como *reporte de privacidad* que es usado en la etapa de diseño. Esto se logra a través del análisis de un contexto, en el que se llega a determinar un conjunto de *vulnerabilidades OWASP* que se mapean con los *principios de PbD* (Privacy by Design – Privacidad desde el diseño) a los que afectan. Las *estrategias* son definidas a través de una tabla de mapeo a partir de los *principios de PbD* que ayudarían a alcanzar. A continuación, se definen los *patrones de privacidad*, a través de una tabla de mapeo entre las *estrategias* y los *patrones de privacidad*. El *reporte de privacidad* se usa como insumo de un proceso de diseño que toma la arquitectura objetivo y da lugar a una versión respetuosa con la privacidad. El proceso continúa hacia la codificación y luego hacia la verificación y validación.

Finalmente, en Ahmadian et al. (2019) se propone un método para modelar sistemas que mejoran la privacidad basado en elementos llamados *características de privacidad* (privacy features) que incluyen *estrategias* y *subestrategias* de diseño, los *patrones de privacidad* y las *PETS* (Privacy enhancing technology – tecnologías para el fortalecimiento de la privacidad). En este proceso, se determina un conjunto de *características de privacidad* que luego se integra en el modelo inicial de un sistema para producir una versión respetuosa con la privacidad. Antes de seleccionar las características de privacidad, se define, en función del contexto, un conjunto de *riesgos a la privacidad* y de *controles*

de privacidad según al NIST (National Institute of Standards and Technology - Instituto Nacional de Estándares y Tecnología). Los controles posteriormente son mapeados a las *estrategias* de diseño. Es fundamental resaltar en este enfoque la integración e interrelación jerárquica de las *estrategias de diseño*, las *sub-estrategias* de diseño, los *patrones* y las *PETS*.

Incluso, dentro del proceso de selección de las *características de privacidad* también se incluye una estimación de costos de las mismas. Esto se consigue a través de la representación de las *estrategias*, *subestrategias*, *patrones* y *PETS* usando diagramas de actividades. Eventualmente, todo este esquema serviría de guía para encontrar las soluciones más específicas a un problema y podría ayudar a automatizar dicho proceso.

Tabla 6. Elementos de diseño en las metodologías

(Hoepman, 2014) (Colesky et al., 2018; Colesky & Caiza, 2019)	(Baldassarre et al., 2019, 2020)	(Ahmadian et al., 2019)
Entrada: N/A	**Entrada:** Vulnerabilidades OWASP (Open Web Application Security Projec, 2022)	**Entrada:** - Riesgos para la privacidad. - Controles de privacidad del NIST (National Institute of Standards and Technology, 2020).
Recursos para diseño: - Principios de privacidad - Estrategias - Tácticas - Patrones de privacidad - Relaciones entre patrones - Sistemas de patrones - PETS	**Recursos para diseño:** - Principios de PbD - Estrategias - Patrones de privacidad - PETS - Tablas de asignación **Producto del trabajo:** - Informe sobre la privacidad	**Recursos para el diseño:** - Modelo de características - Modelo de costes - Configuración de características - Conjunto de RAM (modelos de aspecto reutilizables) - Perfil de mejora de la privacidad *El modelo de características contiene:* - Estrategias de diseño - Sub-estrategias de diseño - Patrones de diseño de privacidad -PETS - Relaciones entre esos elementos - Principios de privacidad (indirectos)
Resultado del diseño: Diseño del sistema (e.g., arquitectura)	**Resultado del diseño:** Arquitectura	**Resultado del diseño:** Modelo de sistema mejorado

* Se puede utilizar en el análisis y el diseño.

4.2 RQ2. ¿Qué elementos forman parte de las metodologías encontradas?

La Tabla 6 muestra el conjunto de elementos que se reportan dentro de las metodologías estudiadas, exclusivamente las que se orientan a la actividad de diseño de un sistema.

4.3 RQ3. ¿Qué instrumentos para experimentar con esas metodologías son requeridos?

Únicamente dos de los tres métodos han hecho esfuerzos por proveer evidencia empírica a través de casos de estudio: la propuesta en c y en Ahmadian et al. (2019). No obstante, se trata de estudios diferentes a un experimento, donde estos últimos se desarrollan en ambientes más controlados. En este sentido, únicamente considerando los artículos estudiados, no se puede responder directamente a la pregunta RQ3 debido a que no hay experimentos reportados.
Sin embargo, aprovechando el hecho de que un caso de estudio es un trabajo de gran valor a nivel empírico, hemos mapeado la información limitada que se ha reportado en los artículos a los elementos expresados en la Tabla 4, y lo describimos en los siguientes párrafos.

En la propuesta reportada en Baldassarre et al. (2019), el *objeto de estudio* es un sistema heredado que procesa datos personales y las *guías de experimentación* son aquellas establecidas en esta metodología. Como elementos relacionados a los instrumentos de medición se puede señalar como criterios de evaluación a las *vulnerabilidades* y al *número de vulnerabilidades* que ayudan en la toma de decisiones de diseño para implementar las soluciones. No se identifica algún elemento relacionado a *herramientas software de soporte*.

En la propuesta reportada en Ahmadian et al. (2019), el *objeto de estudio* incluye modelos de sistema UML (Unified Modeling Language – Lenguaje de Modelado Unificado) (incluyen diagramas de clase, componentes, actividades y de estado). Las *guías de experimentación* corresponderían a las señaladas dentro de la metodología propuesta. Respecto a los elementos relacionados a los *instrumentos de medición*, se puede considerar el criterio de *número de riesgos mitigados*. Al igual que el caso anterior, no se identifica algún elemento relacionado a *herramientas software de soporte*.

5. ELEMENTOS REUSABLES PARA EL PROCESO DE EXPERIMENTACIÓN

Para determinar los elementos que podrían ser reusables en un proceso de experimentación con diferentes metodologías, hemos realizado un proceso de adaptación de aquellas estudiadas a las etapas genéricas de desarrollo: *desarrollo del concepto*, *análisis de requerimientos* y *diseño* (Figura 2, 3 y 4). Se ha denominado bancos al conjunto de elementos de un mismo tipo que se podrían re-utilizar. Un subgrupo de elementos de un banco es el que se usaría a lo largo de las acciones llevadas a cabo en el análisis y el diseño usando una metodología determinada.

Hemos encontrado posibles bancos de elementos reusables que son específicos y otros que son generalizables a los tres métodos analizados.

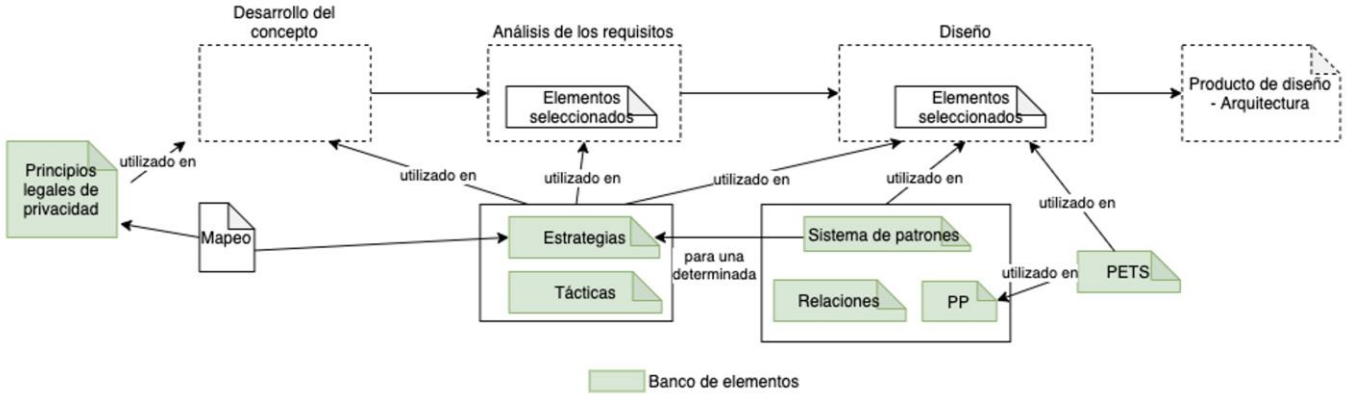

Figura 2. Interpretación de la propuesta de Colesky (Colesky et al., 2016) extendiendo a Hoepman (Hoepman, 2014)

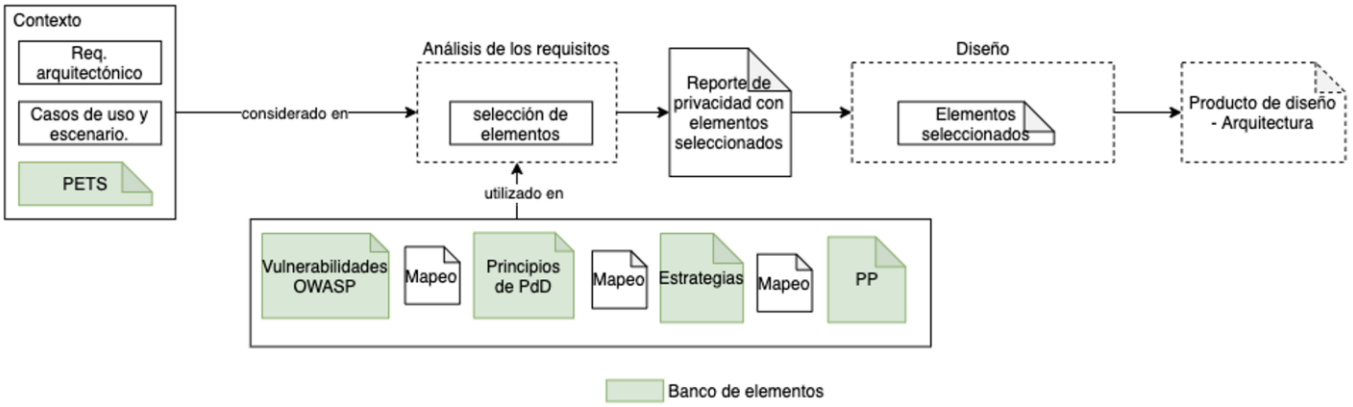

Figura 3. Interpretación de la propuesta de Baldassarre (Baldassarre et al., 2019, 2020)

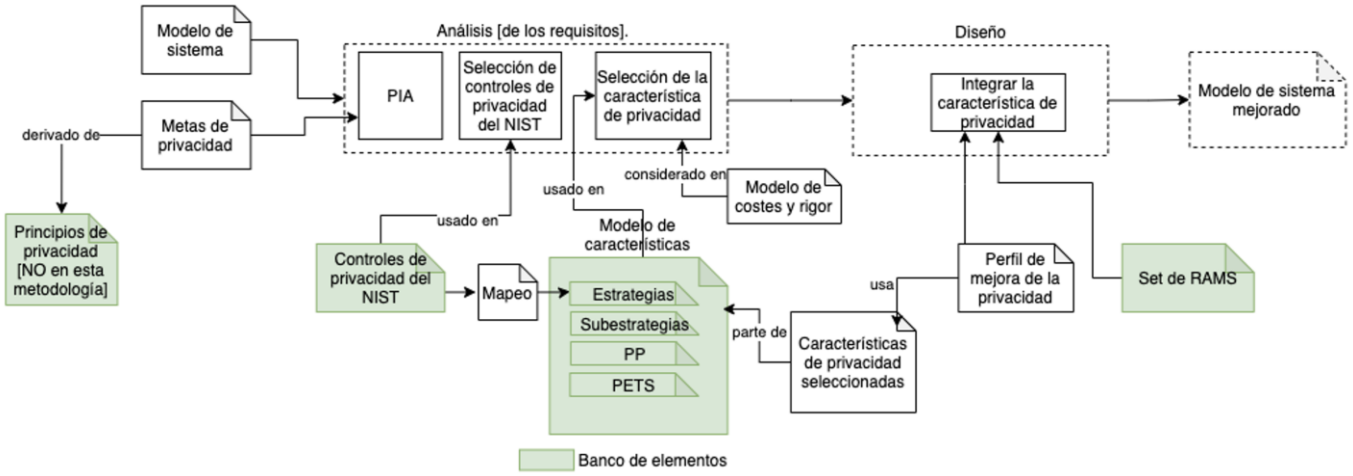

Figura 4. Interpretación de la propuesta de Ahmadian (Ahmadian et al., 2019)

- Aquellos elementos que son comunes a los tres métodos: *estrategias*, *patrones* y *PETs*. También se observa que se utilizan directa o indirectamente *principios* relacionados a la privacidad.
- Aquellos elementos comunes en al menos 2 métodos: *tácticas* o *sub-estrategias*.
- Otros elementos para el diseño: *sistemas de patrones*, *relaciones*, *controles de privacidad NIST* y *modelos de características de privacidad*. Otros para el análisis: *vulnerabilidades OWASP*.

El método reportado en Ahmadian et al. (2019) incluye elementos fuertemente enlazados dentro de sus *modelos de características de privacidad* que podrían servir para la automatización del proceso de selección. Este fuerte enlazamiento hace que este tipo de modelos no sean generalizables. Al contrario, los *sistemas de patrones*, las *relaciones* y los *controles de privacidad NIST* sí podrían serlo. Hay que considerar que las relaciones y sistemas van en línea con la evolución de los patrones de privacidad, que tiene como una de sus características principales el ser reusables. Respecto a los *controles de privacidad NIST*, se trataría de elementos ya estandarizados, y ahí radica su relevancia. Finalmente, aunque las vulnerabilidades OWASP parecen estar más cerca del análisis, podrían ser un elemento relevante que considerar

debido a la fuerte proximidad natural que existe entre las etapas de análisis y de diseño.

Respecto a los elementos de instrumentación experimentales, estos no han sido encontrados directamente debido a que ninguno de los trabajos estudiados ha reportado un experimento. Sin embargo, luego de revisar los casos de estudio reportados, se considera que hay elementos que podrían ser útiles para ser reusados en un proceso de experimentación. Estos elementos incluyen los *modelos*, *lenguajes de modelado* y *diagramas* que se usen para representar sistemas existentes a ser extendidos para que soporten criterios de privacidad. Este tipo de elementos ya ha sido ampliamente estudiado y hay muchos bien conocidos y aceptados por la ingeniería; por ejemplo, los usados en el modelado UML. En el ámbito de los instrumentos de medición, sería interesante el analizar los *criterios* y *métricas de evaluación* aplicables a los casos de diseño con criterios de privacidad. Es decir, que permitan identificar si un diseño cumple con requisitos o consideraciones de privacidad.

6. DISCUSIÓN

Los resultados muestran el surgimiento de propuestas que integran los patrones de privacidad y las estrategias en métodos completos (Baldassarre et al., 2019, 2020) (Ahmadian et al., 2019) que buscan guiar a los ingenieros a lo largo del proceso de desarrollo. Aunque las contribuciones encontradas son escasas (10 artículos de acuerdo con el contexto de este estudio y 8 que mantienen un esquema común), se puede empezar a realizar algunas estimaciones, mientras se esperan más propuestas.

Por ejemplo, se puede notar que además del enfoque de proponer cada vez más patrones y de evolucionarlos hacia lenguajes (Colesky et al., 2016, 2018; Colesky & Caiza, 2019), aquellos más recientes (Baldassarre et al., 2019, 2020) (Ahmadian et al., 2019) los consideran dentro del proceso de desarrollo, en particular en las etapas de análisis y diseño. Esto indica la atención y esfuerzo que los autores prestan hacia su aplicación al crear sistemas. Inclusive la propuesta de Ahmadian et al., (2019) brinda un mayor detalle hacia cómo lograr la integración de cuestiones de privacidad a lo largo del proceso de modelado.

En este sentido, merece la pena notar dos aspectos. Por una parte, el enfoque de evolución de los patrones y el de su aplicación dentro de métodos pueden avanzar de manera simultánea; y no es necesario que los patrones terminen de evolucionar para comenzar a probar su aplicación. También, es importante recordar que los patrones, para alcanzar su nivel de sistema, deberían delinear su proceso de aplicación. Por otra parte, aunque se comience a hacer esfuerzo para materializar el proceso de aplicación de los patrones (paso muy relevante), aún es necesario determinar los efectos que provoca el uso de los mismos.

En tal sentido, llevar a cabo estudios empíricos donde se apliquen patrones de privacidad, dentro de un método o no, sigue siendo necesario. Los trabajos que reporten casos de estudio (Baldassarre et al., 2019) podrían responder afirmativamente a la pregunta ¿están los patrones listos para ser usados?, pero en el contexto de los patrones usados en dichos estudios. Por ende, aún se requiere contestar a otras preguntas como ¿son fáciles de aplicar? y ¿proveen beneficios? Consideramos que los experimentos o cuasiexperimentos pueden ser muy relevantes para ello, ya que nos permitirán evaluar los efectos (ventajas o desventajas) al alterar diferentes variables o dependiendo de los tratamientos aplicados.

Finalmente, la complejidad inherente a llevar a cabo este tipo de estudios puede frenar a los autores de realizar este tipo de estudios; lo cual hace que el objetivo de nuestro estudio cobre aún más relevancia: proveer de un conjunto de elementos que puedan ser reusados al hacer experimentos. Consideramos que aportamos en esta vía al identificar aquellos elementos comunes a los enfoques actuales aquí encontrados: principios, estrategias, patrones, PETS, sub-estrategias. Inclusive la forma de llegar a los elementos más apropiados a través de tablas de mapeo o esquemas jerárquicos de categorizaciones.

7. CONCLUSIONES

Se ha llevado a cabo una búsqueda en la literatura guiado por un conjunto de pasos sistematizados basados en la propuesta de Petersen et al. (2015) para encontrar aquellas metodologías que hacen uso de estrategias y patrones. De un conjunto de 136 artículos primarios y 82 secundarios, se han obtenido 10 artículos útiles para este estudio. La mayoría de ellos (8 de 10) se fundamentan en la propuesta de Hoepman (2014). Se pueden identificar tres enfoques derivados: el propuesto por Colesky et al. (2016, 2018) y Colesky & Caiza (2019), por Baldassarre et al. (2019, 2020), y por Ahmadian et al. (2019).

Luego de analizar estos enfoques, se han identificado elementos reusables que podrían ser usados para experimentar en esta área. Un primer grupo de elementos corresponden a las comunes a las metodologías estudiadas e incluyen *estrategias*, *patrones*, *PETs*, *tácticas* o *sub-estrategias*. Dentro de este mismo grupo se podrían considerar a elementos que aparecen de manera única pero que podrían ser útiles en la etapa de diseño: los *sistemas de patrones*, las *relaciones* (entre patrones o entre elementos de diferentes niveles de abstracción), los *controles de privacidad NIST* y las *vulnerabilidades OWASP*. Un segundo grupo de elementos corresponden a la instrumentación en los experimentos. El análisis menciona que elementos para el modelado como los lenguajes y diagramas serían útiles para expresar sistemas base que se van a extender con criterios de privacidad. Este tipo de elementos ha sido ampliamente estudiado en la literatura; por ejemplo, el lenguaje UML. Asimismo, se puede considerar las métricas o criterios que permitan determinar si un determinado diseño cumple con los requisitos de privacidad planteados.

AGRADECIMIENTOS

Extendemos el agradecimiento al Vicerrectorado de Investigación, Innovación y Vinculación de la Escuela Politécnica Nacional, ya que este trabajo ha sido desarrollado dentro del proyecto PII-DETRI-2021-03 “Soporte a la

experimentación en el diseño de sistemas respetuosos con la privacidad".

REFERENCIAS

Agencia Española de Protección de Datos. (2019). *A Guide to Privacy by Design*. https://www.aepd.es/es/documento/guia-privacidad-desde-diseno_en.pdf.

Ahmadian, A. S., Strüber, D., & Jürjens, J. (2019). Privacy-enhanced system design modeling based on privacy features. *Proceedings of the ACM Symposium on Applied Computing*, *Part F1477*, 1492–1499. https://doi.org/10.1145/3297280.3297431

Al-Slais, Y. (2020). Privacy Engineering Methodologies: A survey. *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, 1–6. https://doi.org/10.1109/3ICT51146.2020.9311949

Asamblea Nacional de la República del Ecuador. (2021, Mayo). *Ley orgánica de protección de datos personales*. Asamblea Nacional de la República del Ecuador. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Baldassarre, M. T., Barletta, V. S., Caivano, D., & Scalera, M. (2019). Privacy Oriented Software Development. *Communications in Computer and Information Science*, *1010*, 18–32. https://doi.org/10.1007/978-3-030-29238-6_2

Baldassarre, M. T., Barletta, V. S., Caivano, D., & Scalera, M. (2020). Integrating security and privacy in software development. *Software Quality Journal*, 1–32. https://doi.org/10.1007/s11219-020-09501-6

Berendt, B., & Preibusch, S. (2017). Toward accountable discrimination-aware data mining: The importance of keeping the human in the loop—and under the looking glass. *Big Data*, *5*(2), 135–152. https://doi.org/10.1089/big.2016.0055

Buschmann, F., Meunier, R., Rohnert, H., Sommerlad, P., & Stal, M. (1996). *Pattern-Oriented Software Architecture: A System of Patterns* (Vol. 1). John wiley & sons.

Caiza, J. C., Alamo, J. M. D., Guamán, D. S., & Jaramillo-Alcázar, Á. (2021). An exploratory experiment on privacy patterns: Limitations and possibilities. *Proceedings of the ACM Symposium on Applied Computing*, 1209–1216. https://doi.org/10.1145/3412841.3441995

Caiza, J. C., Martin, Y.-S., Guaman, D. S., Del Alamo, J. M., & Yelmo, J. C. (2019). Reusable Elements for the Systematic Design of Privacy-Friendly Information Systems: A Mapping Study. *IEEE Access*, *7*, 66512–66535. https://doi.org/10.1109/ACCESS.2019.2918003

Cavacini, A. (2015). What is the best database for computer science journal articles? *Scientometrics*, *102*(3), 2059–2071. https://doi.org/10.1007/s11192-014-1506-1

Cavoukian, A. (2009, Agosto). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Colesky, M., & Caiza, J. C. (2019). A System of Privacy Patterns for Informing Users: Creating a Pattern System. *Proceedings of the 23rd European Conference on Pattern Languages of Programs - EuroPLoP '18*, 1–11. https://doi.org/10.1145/3282308.3282325

Colesky, M., Caiza, J. C., Del Álamo, J., Hoepman, J.-H., & Martín, Y.-S. (2018). A system of privacy patterns for user control. *33rd Annual ACM Symposium on Applied Computing*, 1150–1156. https://doi.org/10.1145/3167132.3167257

Colesky, M., Hoepman, J.-H., & Hillen, C. (2016). A critical analysis of privacy design strategies. *2016 IEEE Security and Privacy Workshops (SPW)*, 33–40. https://doi.org/10.1109/SPW.2016.23

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. Le, Tirtea, R., & Schiffner, S. (2014). *Privacy and Data Protection by Design - from policy to engineering*. European Union Agency for Cybersecurity. https://doi.org/10.2824/38623

Elsevier Research Intelligence. (2020). *Scopus content coverage guide*. Elsevier. https://www.elsevier.com/ data/assets/pdf file/0007/69451/Scopus_ContentCoverage_Guide_WEB.pdf

European Parliament, & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da*. http://eur-lex.europa.eu/eli/reg/2016/679/oj

Gamma, E., Helm, R., Johnson, R., & Vlissides, J. (1995). *Design Patterns : Elements of Reusable Object-Oriented Software*. Addison-Wesley.

Gürses, S., & Del Alamo, J. M. (2016). Privacy engineering: shaping an emerging field of research and practice. *IEEE Security and Privacy*, *14*(2), 40–46. https://doi.org/10.1109/MSP.2016.37

Hoepman, J.-H. (2014). Privacy design strategies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, & T. Sans (Eds.), *ICT Systems Security and Privacy Protection. SEC 2014. IFIP Advances in Information and Communication Technology* (Vol. 428, pp. 446–459). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-55415-5_38

International Organization for Standardization. (2014). *Software engineering – Metamodel for development methodologies* (ISO Standard No. 24744:2014). https://www.iso.org/standard/62644.html

International Organization for Standardization. (2019). *Information technology — Security techniques — Privacy engineering for system life cycle processes* (ISO Standard No. 27550:2019). https://www.iso.org/standard/72024.html

Lenhard, J., Fritsch, L., & Herold, S. (2017). A literature study on privacy patterns research. *Proceedings - 43rd Euromicro Conference on Software Engineering and Advanced Applications, SEAA 2017*, 194–201. https://doi.org/10.1109/SEAA.2017.28

Morales-Trujillo, M. E., García-Mireles, G. A., Matla-Cruz, E. O., & Piattini, M. (2019). A Systematic Mapping Study of Privacy by Design in Software Engineering. *CLEI*

electronic journal, *22*(1). https://ruidera.uclm.es/xmlui/handle/10578/22819

National Institute of Standards and Technology. (2020, Septiembre). *Security and Privacy Controls for Information Systems and Organizations.* https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

Notario, N., Crespo, A., Martin, Y. S., Del Alamo, J. M., Metayer, D. Le, Antignac, T., Kung, A., Kroener, I., & Wright, D. (2015). PRIPARE: Integrating privacy best practices into a privacy engineering methodology. *2015 IEEE Security and Privacy Workshops*, 151–158. https://doi.org/10.1109/SPW.2015.22

Open Web Application Security Project. (2022). *OWASP Top Ten*. https://owasp.org/www-project-top-ten/.

Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, *64*, 1–18. https://doi.org/10.1016/j.infsof.2015.03.007

Wieringa, R., Maiden, N., Mead, N., & Rolland, C. (2006). Requirements engineering paper classification and evaluation criteria: A proposal and a discussion. *Requirements Engineering*, *11*(1), 102–107. https://doi.org/10.1007/s00766-005-0021-6

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). Experimentation in Software Engineering. In *Experimentation in Software Engineering*. https://doi.org/10.1007/978-3-642-29044-2

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*. New York: ACM Press. 1-10. http://dx.doi.org/10.1145/2601248.2601268.

BIOGRAFÍA

Julio C. Caiza, Ingeniero en Electrónica y Redes de Información por la Escuela Politécnica Nacional, Ecuador, y Doctor en Ingeniería de Sistemas Telemáticos por la Universidad Politécnica de Madrid, España. Actualmente es profesor titular agregado en la Escuela Politécnica Nacional. Sus principales temas de interés son el diseño de sistemas respetuosos con la privacidad y la realización de estudios de literatura siguiendo procesos ordenados y sistemáticos.

Gabriel López, Ingeniero en Electrónica y Redes de la Información, por la Escuela Politécnica Nacional, Ecuador, Máster en Seguridad de Sistemas por Sheffield Hallam University, Reino Unido, y Magister en Gestión de las Comunicaciones y Tecnologías de la Información, Escuela Politécnica Nacional. Actualmente se desempeña como docente investigador de la Escuela Politécnica Nacional en Quito.

Danny S. Guamán, Ingeniero en Electrónica y Redes por la Escuela Politécnica Nacional, Ecuador, y Doctor en Ingeniería de Sistemas Telemáticos por la Universidad Politécnica de Madrid, España. Actualmente, es profesor en la Escuela Politécnica Nacional. Su principal trabajo de investigación actual se centra en el análisis de la divulgación de datos y la evaluación del cumplimiento de requisitos de protección de datos en los sistemas de información.