La ingeniería de requerimientos en el cumplimiento de la normativa de protección de datos personales

Ma. Carolina Sacoto[0000-0002-8799-8947] y Juan Pablo Carvallo[0000-0001-6678-4774]
CEDIA, Cuenca 010150, Ecuador
carolina.sacoto@cedia.org.ec
jpcarvallo@cedia.org.ec

Resumen. Este artículo examina el desafío del cumplimiento normativo en la protección de datos personales, enfocándose en su intersección con la ingeniería de requerimientos. Se introduce un enfoque que subraya la importancia de la "protección de datos desde el diseño" y propone un método sistemático para traducir las obligaciones legales en requerimientos no funcionales concretos, implementados a través de controles específicos. Este proceso resulta de gran valor para los ingenieros de software, ya que les facilita una comprensión más profunda de las obligaciones legales y les permite implementar las medidas adecuadas para su cumplimiento. Mediante esta metodología, se busca integrar controles eficaces desde las primeras fases del diseño de software, con el objetivo de minimizar los riesgos económicos y reputacionales para la organización y de proteger eficazmente los derechos de los titulares de los datos personales**.**

Keywords: RGPD, privacidad desde el diseño, protección de datos desde el diseño, ingeniería de requerimientos

1 Planteamiento General

Esta investigación adopta una metodología cualitativa y teórico-exploratoria, apoyándose principalmente en la revisión bibliográfica y el análisis hermenéutico. Estos métodos facilitarán la interpretación de textos legales en un área del derecho que requiere atención multidisciplinaria para ser aplicada de manera efectiva y preventiva.

La lectura de este documento presupone que el lector posee, al menos, un conocimiento básico sobre las regulaciones en protección de datos personales. En este contexto, es importante destacar que los términos “protección de datos desde el diseño” y “privacidad desde el diseño” serán tratados como conceptos equivalentes a lo largo de este texto. Este enfoque asegurará una comprensión coherente de cómo deben integrarse estas prácticas en todas las etapas de un proceso que involucre datos personales, para el este caso puntual, en la etapa de ingeniería de requerimientos de software.

2 Introducción

El cumplimiento de la normativa de protección de datos personales en la ingeniería de requerimientos no solo es una exigencia legal, sino que también constituye una base

Proceedings of the 27th Workshop on Requirements Engineering (WER24), August 07-09, 2024, Buenos Aires, Argentina.
DOI: 10.29327/1407529.27-32

esencial para construir la confianza de los usuarios en los productos tecnológicos. En este contexto, la ingeniería de requerimientos, como disciplina encargada de identificar, analizar, documentar y mantener un conjunto de requisitos de software, juega un papel fundamental en asegurar que la protección de datos personales se integre con un enfoque preventivo, desde las fases iniciales del desarrollo de cualquier proyecto tecnológico [1].

En el ámbito legal, la violación al principio de protección de datos personales desde el diseño ha sido, en varias ocasiones, un factor determinante para imponer sanciones a empresas por sus desarrollos tecnológicos. A continuación, se presentan algunos ejemplos importantes: Facebook and Cambridge Analytics (2018) [2] [3]; Uber (2018) [4], con una multa impuesta por la Comisión de Protección de Datos de los Países Bajos; Amazon (2021) [5] [6] [7], con una sanción impuesta por la Agencia de Protección de Datos de Luxemburgo por 746 millones de euros; Meta (2023) [8] con la multa más grande impuesta en la Unión Europea por 1.299 millones por la Comisión de Protección de Datos (DPC) de Irlanda.

En este contexto, la disponibilidad de procesos y recursos que faciliten la traducción de obligaciones legales en requerimientos técnicos y acciones concretas se convierte en una necesidad imperante. Este trabajo presenta una ruta para generar un proceso como el descrito sobre la base de la normativa europea en protección de datos personales.

3 Antedecentes y trabajo relacionado

3.1 Privacidad desde el diseño

La privacidad por diseño es un concepto que surgió en la década de 1990 de la mano de la Dra. Ann Cavoukian, Comisionada de Privacidad de Ontario, Canadá. La idea principal detrás de este enfoque era abordar las preocupaciones de privacidad desde el diseño mismo de los sistemas y las prácticas empresariales, en lugar de intentar corregir problemas de privacidad después de que ya se hayan producido. Este concepto se popularizó en el año 2010 con la publicación de un informe titulado "Privacy by Design: The 7 Foundational Principles"[1] [9] y se ha robustecido con el aparecimiento del requisito legal de protección de datos personales desde el diseño en el Reglamento General de Protección de Datos de la Unión Europea[2] que entró en vigor en mayo de 2018 [10][11].

A medida que las regulaciones en protección de datos personales se han adoptado con una intensidad considerable en diferentes jurisdicciones, varios autores han puesto interés en la integración de los principios de protección de datos en las etapas iniciales

[1] 1) Proactividad, no Reactividad; Prevención, no Corrección 2) Privacidad como Configuración Predeterminada 3) Privacidad Insertada en el Diseño 4) Funcionalidad Completa: Ganancia de Privacidad, no una Suma Cero. 5)Seguridad Extrema de Extremo a Extremo 6) Visibilidad y Transparencia. 7)Respeto por la Privacidad del Usuario

[2] La obligatoriedad de la protección de datos por diseño se encuentra establecida en el artículo 25 del RGPD. Esto implica que las medidas necesarias para la protección de datos personales deben ser consideradas desde el diseño inicial del sistema, producto o servicio.

del proceso de desarrollo de software [12] [13] [14]. Sin embargo, al día de hoy, abordar el cumplimiento de la norma sigue siendo un reto para la ingeniería de requerimientos. Un estudio publicado el 27 de enero de 2023, realizó una revisión sistemática de la literatura, partiendo de 6046 artículos primarios, publicados hasta mayo de 2022. Dicha investigación concluyó que existe "una falta de modelos, procesos y herramientas para respaldar la privacidad por diseño a lo largo del ciclo de vida del desarrollo del software y que se ha vuelto más relevante considerando los requisitos del Reglamento General de Protección de Datos (RGPD)" [15].

3.2 La notación *i**

El marco conceptual y la notación *i** [16] fueron formulados para representar, modelar y razonar acerca de los sistemas sociotécnicos, incluidas las interacciones que se pretenden describir en este artículo. Su lenguaje de modelado está constituido por un conjunto de constructos gráficos que pueden utilizarse en dos modelos: el modelo de Dependencia Estratégica (SD), que permite representar a los actores organizacionales y sus dependencias, y el modelo de Racionalidad Estratégica (SR), que representa la lógica interna del actor. Sus constructos están formalizados en [17], y se explican brevemente a continuación. En los modelos SD, los actores se representan como círculos y actúan como entidades con autonomía. Pueden estar interrelacionados a través de enlaces y pueden exhibir dependencias. Las dependencias ocurren entre actores, donde un actor, llamado "Dependiente", depende de otro actor, llamado "Proveedor" para lograr una intención interna. Estas dependencias se caracterizan por elementos intencionales conocidos como "dependencia". Existen cuatro tipos de elementos intencionales: objetivos (óvalos), recursos (rectángulos), tareas (hexágonos) y cualidades (óvalos reducidos). Los objetivos representan requerimientos funcionales, mientras que las cualidades a menudo representan requisitos no funcionales. Los recursos representan elementos físicos o lógicos necesarios para alcanzar un objetivo, mientras que las tareas representan maneras específicas de lograr los objetivos.

4 De la ley a la práctica

En este apartado se explica el proceso utilizado para, transformar las obligaciones legales en requisitos técnicos. El proceso incluye seis pasos que parten de, la obligación general de la protección de datos personales desde el diseño, tomando en cuenta los principios de la norma y los derechos de los titulares de datos personales (paso 1), los objetivos de privacidad como categorías de requerimientos no funcionales (paso 2), las estrategias de privacidad (paso 3), para establecer controles específicos (paso 4), que pueden ser implementados de diferentes formas (paso 5) [9]. De manera transversal, con la información obtenida es estos pasos, se trabaja en la formalización de la especificación de requerimientos, utilizando la nomenclatura *i**(paso 6).

4.1 Paso 1. Identificación de requerimientos legales, su alcance e interrelación

Para abordar este proceso es necesario determinar el alcance de la normativa de Protección de datos Personales aplicable al contexto especifico en el que debe operar el sistema de información. En el caso específico del Ecuador se ha considerado el RGPD y esta revisión a permitido identificar requerimientos normativos, entre los que se cuenta: la obligación de la protección de datos personales desde el diseño y por defecto como un aspecto transversal y de alcance global (art. 25), los principios contenidos en el artículo 5 y subsiguientes, y de manera más específica la garantía para el ejercicio de los derechos de los titulares de los datos personales contenidos en el capítulo tercero.

El resultado de este paso es el listado de obligaciones contenidas en la norma. Para ello, se debe tener en cuenta la interrelación existente entre el enfoque de privacidad del diseño con sus máximas, los principios normativos de la protección de datos y los derechos de los titulares de dicha información personal. Se notará que los principios revelan un enfoque coherente y complementario sirviendo de base para los derechos otorgados a los titulares de los datos personales. Por ejemplo: el principio de visibilidad y transparencia[3] se corresponde directamente con el principio de licitud, lealtad y transparencia[4], y a su vez, soportan los derechos del titular a estar informado y de acceso y portabilidad de datos.

4.2 Paso 2. Establecer categorías de requerimientos no funcionales

Entendidas cuáles son las obligaciones legales que han de cumplirse, se propone partir considerando como categorías de requerimientos no funcionales a ser analizados, aquellas tradicionalmente asociadas a la seguridad de la información: 1) confidencialidad, 2) integridad y 3) disponibilidad, sumadas a las consideradas fundamentales desde el enfoque de privacidad: 4) desvinculación, 5) transparencia y 6) control [18][19]. Estas categorías establecen un amplio contexto que permite razonar sobre los riesgos asociados a los sistemas que tratan datos personales, incluidos aquellos derivados de las obligaciones legales identificadas en el paso 1.

4.3 Paso 3. Establecer estrategias de diseño de la privacidad

En el estado del arte descrito en [20] se han identificado ocho estrategias de diseño de la privacidad, de entre las cuales se ha de escoger las más apropiadas para satisfacer los requerimientos asociados a la aplicación de la normativa. Para cada requerimiento puede existir más de una estrategia posible. Estas estrategias se dividen en dos categorías principales: orientadas a los datos (minimizar, separar, abstraer, ocultar) y orientadas a los procesos (informar, controlar, cumplir y demostrar).

---

[3] Principio de privacidad desde el diseño.
[4] Principio normativo del RGPD.

4.4 Paso 4. Identificación de controles y patrones de diseño

Para concretar las estrategias descritas en el párrafo precedente, se han de identificar los controles adecuados de acuerdo con el contexto específico. Los controles pueden ser legales, técnicos u organizativos. Un control puede soportar a más de una estrategia de privacidad y generalmente, resuelve más de un problema que puede presentarse en diferentes etapas o procesamiento de datos de un sistema. Aquí, son útiles los patrones de diseño de la privacidad que ayudan a estandarizar las soluciones [9], proporcionando un enfoque sistemático y replicable para abordar las cuestiones de privacidad. Cada patrón debe abordar un problema específico de privacidad y debe ofrecer una solución probada que puede ser adaptada y aplicada en diferentes contextos.

4.5 Paso 5. Aplicación de Tecnologías de Mejora de la Privacidad

Una vez que se han identificado y definido los controles adecuados para implementar las estrategias de privacidad, el siguiente paso es llevar estos controles a la práctica. Esto se puede realizar mediante Tecnologías de Mejora de la Privacidad (PETs). Estas tecnologías están diseñadas para proteger la información personal de manera efectiva, minimizando los riesgos asociados con el procesamiento de datos y procurando el cumplimiento de las normativas de privacidad.

Existen diferentes tipos de PETs como, por ejemplo: de cifrado, de anonimización y pseudonimización, de control de acceso (basado en roles o con autentificación multifactor), técnicas de minimización para recolección de datos (selectivas o de eliminación automática), herramientas de transparencia y control para el usuario (ej. paneles de privacidad) y notificaciones en tiempo real, entre otras. El uso de una u otra tecnología, dependerá del caso en concreto y, aunque su integración presente desafíos, los beneficios en términos de seguridad de datos y confianza del usuario hacen que estas tecnologías sean una inversión valiosa en la protección de la privacidad.

4.6 Paso 6. modelización en notación *i**

Una vez identificados los PETs apropiads, la notación *i** es utilizada para modelar y visualizar las relaciones y dependencias entre los actores involucrados en el sistema sociotécnico. Para ello se debe proceder con:

1) Identificación de actores: Determinar los actores clave para el sistema, tales como el responsable de tratamiento, el encargado de tratamiento y el titular de los datos.
2) Definición de dependencias entre actores: Especificación de elementos intencionales en diagramas de Dependencia Estratégica SD (objetivos, recursos, tareas y cualidades).
3) Construcción de modelo de Racional Estratégico: Construir un modelo SR para para detallar cómo los actores logran sus objetivos y gestionan sus dependencias internas.
4) Validación y optimización: Revisar y ajustar los modelos para asegurar los pasos previos estén correctamente representados y que los controles técnicos

sean efectivos, esto puede implicar la iteración y refinamiento de los modelos para abordar cualquier problema identificado.

4.7 Ejemplo de Aplicación Practica

De manea ilustrativa se presenta el siguiente ejemplo genérico para para una empresa teórica E-Commerce XYZ.

Paso 1: Identificación de requerimientos legales, su alcance e interrelación

- **Norma aplicable**: RGPD
- **Contexto:** Tienda en línea llamada "E-Commerce XYZ" que procesa datos personales de sus clientes para gestionar las ventas, envíos y comunicaciones de marketing.
- **Obligación legal**: Cumplimiento del principio de transparencia.

Paso 2. Establecer categorías de requerimientos no funcionales

- **Categorías:** Confidencialidad**,** Transparencia.
- **Requerimientos:** Datos personales procesados de manera transparente en la compra de un producto. Datos personales encriptados.

Paso 3: Establecer estrategias de diseño de la privacidad

- **Estrategia de diseño de la privacidad seleccionada:** Ocultar, Informar

Paso 4. Identificación de controles y patrones de diseño

- **Política de Privacidad Clara y Accesible**
- **Controles:**
  1. Redactar una política de privacidad detallada que describa prácticas de recolección, utilización, almacenamiento y protección de datos personales.
  2. Notificar oportunamente sobre cambios en políticas de privacidad.
  3. Registrar aceptaciones explicitas de clientes sobre cambios en políticas de privacidad.
  4. Encriptar información personal de clientes.
  5. Transferir la información utilizando protocolos de transmisión seguros.

Paso 5: Aplicación de Tecnologías de Mejora de la Privacidad

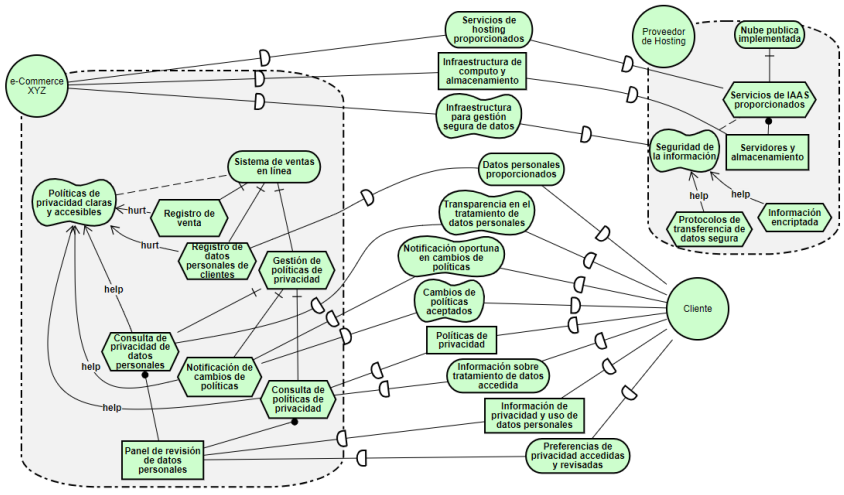
Table 1. PETs recomendadas (ejemplo)

Patrón de Diseño	Descripción	PETs Recomendadas
Atributos Basados en credenciales	Garantiza confidencialidad de datos mediante autenticación (usualmente de 3 vías) para acceder a la información almacenada y encriptada.	1) Encriptación de datos. 2) Uso de protocolos seguros para transmisión de datos. 3) Autenticación de 3 vías.
Declaración de Privacidad Transparente	garantiza que la política esté escrita en un lenguaje comprensible, sin terminología técnica compleja, y sea fácilmente	1) Consultas a políticas de privacidad y uso de datos personales. 2) Notificaciones oportunas en cambios de políticas

	accesible desde todas las páginas del sitio web.	3) Aceptación expresa por parte de clientes

Paso 6: modelización en notación i*
Identificación de Actores: E-Commerce XYZ (responsable del tratamiento de los datos), Proveedor de servicios de hosting (encargado del tratamiento de los datos), Clientes (titular de los datos).
Las dependencias y demás elementos intencionales identificados y validados y optimizados para el caso de ejemplo se presentan en el diagrama SR incluido en la figura 1.

Fig. 1. Modelización en notación i*



5 Conclusiones y trabajo futuro

En este documento, se ha abordado el desafío de facilitar el cumplimiento de las regulaciones de protección de datos desde la ingeniería de requerimientos desarrollando un enfoque basado en la integración práctica de la privacidad desde el diseño. El documento resultante, proporciona una ruta para llevar los requisitos legales a su aplicación técnica. Asimismo, procura reducir la brecha de conocimiento sobre las regulaciones en la materia y promueve la implementación preventiva de medidas de protección de datos desde las etapas iniciales del desarrollo de software.

Se debe señalar que, la ruta propuesta no aborda cuestiones específicas relacionadas con la necesidad de realizar un análisis de riesgo o una evaluación de impacto cuando el tratamiento de los datos suponga un riesgo importante para el titular de los datos personales; tampoco se abarcan aspectos requeridos por nuevas normativas relacionadas con el uso de inteligencia artificial. Finalmente, una mayor validación de la propuesta aquí presentada será considerada como trabajo futuro.

Referencias

1. Netto, D., Peixoto, M., Silva, C.: Privacy and Security in Requirements Engineering: Results from a Systematic Literature Mapping. Workshop en Ingeniería de Requerimientos WER (2019)
2. Isaak, J., Mina H.: User data privacy: Facebook, Cambridge Analytica, and privacy protection. Computer 51 (8), 56-59 (2018)
3. Kozlowska, I.: Facebook and data privacy in the age of Cambridge Analytica. The Henry M. Jackson School of International Studies (2018): 1.
4. Kennedy, C.: Uber's Ongoing Data Privacy Woes. Computer Law Review International 20 (1), 15-18 (2019)
5. Lintvedt, M.: Putting a price on data protection infringement. International Data Privacy Law 12(1), 1-15 (2022).
6. Daigle, B., Mahnaz K.: The Changing Tides of Data Protection Regulation and Enforcement in Europe. Office of Industries, US International Trade Commission (2022)
7. Saemann, M, et al.: Investigating GDPR Fines in the Light of Data Flows. Proceedings on Privacy Enhancing Technologies 4, 314-331 (2022)
8. EFE Homepage, https://efe.com/ciencia-y-tecnologia/2023-05-22/irlanda-multa-meta-facebook-privacidad-usuarios/, accedido 17/05/2024
9. AEPD.: Guía de privacidad desde el diseño (2019), https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf , accedido el 15/05/2024
10. Tamburri, D.: Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. Information Systems 91(2020), 101469, (2020)
11. Breaux, T., Rao, A.: Formal analysis of privacy requirements specifications for multi-tier applications. 21st IEEE International Requirements Engineering Conference (RE), Rio de Janeiro, Brazil, 14-23 (2013)
12. Sartoli, S., Ghanavati S., Siami Namin, A.: Towards Variability-Aware Legal-GRL Framework for Modeling Compliance Requirements. IEEE 7th International Workshop on Evolving Security&Privacy Requirements Engineering (ESPRE), Zurich, Switzerland, 7-12, (2020)
13. Ghanavati, S., Rifaut, A., Dubois, E., Amyot, D.: Goal-oriented compliance with multiple regulations. IEEE 22nd International Requirements Engineering Conference (RE), Karlskrona, Sweden, 73-82 (2014)
14. A. Siena, A. Perini, A. Susi and J. Mylopoulos, "Towards a framework for law-compliant software requirements," 2009 31st International Conference on Software Engineering - Companion Volume, Vancouver, BC, Canada, 2009, pp. 251-254, doi: 10.1109/ICSE-COMPANION.2009.5070994.
15. Andrade, V., Deda R., Reinehr, S., Obladen De Almendra Freitas, C., Malucelli, A.: Privacy by Design and Software Engineering: a Systematic Literature Review. Proceedings of the XXI Brazilian Symposium on Software Quality (SBQS '22). Association for Computing Machinery, New York, NY, USA, Article 18, 1–10 (2023)
16. u, E.: Modelling Strategic Relationships for Process Reengineering. Ph.D. Thesis, University of Toronto, Department of Computer Science, Canada (1995)
17. Dalpiaz, F., Franch, X., Horkoff, J.: iStar 2.0 Language Guide. CoRR abs/1605.07767 (2016)
18. Zwingelberg, H., Hansen, M.: Privacy Protection Goals and Their Implications for eID Systems. 7th PrimeLife International Summer (PRIMELIFE), 245-260, Trento, Italy (2011)
19. Hansen, M. Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals.7th PrimeLife International Summer (PRIMELIFE), 14-31, Trento, Italy (2011)
20. Hoepman, J.: Privacy Design Strategies (The Little Blue Book) (2019)